Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Managers Unit 1 Week 1 Unit name: Introduction Webinar	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Gabriel Vladut • Valentin Istratie
Learning Activity Goals	1. About Erasmus+ InCyT project 2. Objectives 3. Results and products 4. How to protect yourself against cyber attacks 5. Training and mentoring 6. Social engineering 7. Social Network (Social Media)
Skills to be Gained	• TS3 Network Security • TS4 Penetration (exploitable vulnerabilities) testing • SS3 Cognitive and behaviour analysis
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • To learn about Erasmus+ InCyT project / objectives / Results and products • How to protect yourself against cyber attacks • Training and mentoring • Social engineering / Social Network (Social Media)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
InCyT is an Erasmus + project that aim to create a Framework, a methodology for training, which provides a mechanism for VET and companies to describe the competences and skills, necessary in cyber security for professionals and not professionals in order to avoid cyber-attacks, as well digital gaps and other ones. NIST's National Initiative for Cyber security Education (NICE) underlines that it should be done a crucial step toward remedying shortage of "people with the knowledge, skills, and abilities to perform the tasks required for cyber security work." Such a workforce will include "technical and nontechnical roles that are staffed with knowledgeable and experienced people." The project will like to implement some solutions in this context. It has as objective first the development a Framework, which provides a mechanism for VET and companies to describe the digital gaps and other ones necessary in cyber security for professionals and not professionals in order to avoid cyber-attacks and help them to improve this situation. Taking into consideration of advantages of interdisciplinary training and mentoring programs particularly in the field of cyber security the project will develop, and test digital interdisciplinary training programs supported by e-mentoring for SMEs and adapt it for VET. Collaboration and communication between educators, researchers and people who use information technologies are necessary. One problem is that companies, particularly SMEs with less resource need help to appreciate the competences and skills gaps of their employees, methods to evaluate the existing situation as well as using training possibilities to reskill their employees. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace. All these documents are on the digital interactive project platform. The learners can test their answers on self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forum and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the meetings. They will be supported to develop e-portfolio important for reflection and evaluation of the training.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Content of the Learning Material

Competence Framework

There will be 3 transnational meetings in our project. It was planned in the 3rd, 13th and 20th month of the project. Some additional project meetings will be held as we think that 3 meetings will not be enough to run a 24-month project. These meetings are online and held regularly every month. The project senior management team will organize these projects.

The projects will be led by the project coordinator, the WP leader. There will be 7 multiplier events in our project. Each partner institution will organize these activities to popularize the project idea in its own country and to share the developed products. Each partner institution will run the Interdisciplinary Training for SME employees and teachers in Cyber Securityactivity in its own country.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

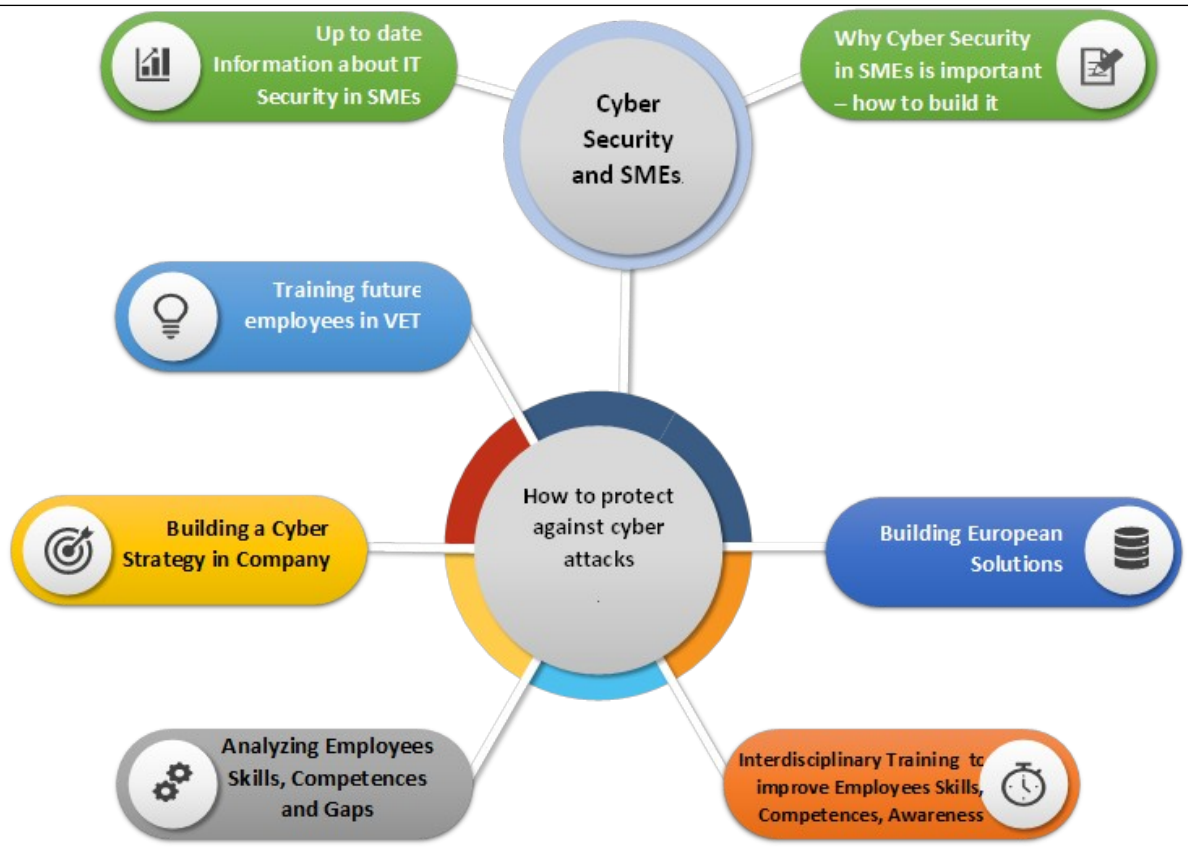


Figure 1: Activities supported by the InCyT project

Objectives

The InCyT project will like to implement some solutions:

- The development of a Framework, which provides a mechanism for VET and companies to describe the competences and skills, necessary in cyber security for professionals and not professionals in order to avoid cyber-attacks, as well digital gaps and other ones.
- Taking into consideration of advantages of interdisciplinary training and mentoring programs particularly in the field of cyber security the project will develop, and test digital interdisciplinary training programs supported and a collaborative e-Learning platform for SMEs
- Adapt it for VET.
- Develop a European transferability model
- Taking into consideration of advantages of interdisciplinary training and mentoring programs particularly in the field of cyber security the project will develop, and test digital interdisciplinary training programs supported by e-mentoring for SMEs and adapt it for

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

VET.

Outcomes of the project will be:

- Methodological Framework for Implementation
- Existing and followed training (courses)
- Opportunities for improvements of these by using interdisciplinarity and mentoring.
- Learning and mentoring methodology

Products:

1. Framework

2. A digital Interdisciplinary cyber security training material for SMEs supported by mentoring and an adapted methodology for a VET special course.

3. A digital platform to support the training

4. Report how interdisciplinary skills provide advantages for SME and VAT.

5. European transferability model for the tested interdisciplinary training and mentoring

Partners from: Germany (coordinator), Turkey, Poland, Italy, Austria, Denmark, Romania.

Activities

- Methodological Framework for Cyber Security - Leading Organisations: IAT, Germany, Italy
- A Digital Interdisciplinary Cyber Security Training Material - Leading Organisation: St. Pölten University of Applied Sciences, Austria
- ICT Platform for Cyber Security - Leading Organisation: IPA, Romania
- Methodological Model for Cyber Security - Leading Organisation: Politechnik University, Poland
- Transferability Model - Leading Organisation: European Training Center Copenhagen, Denmark
- Multiplier Events - Leading Organisation: Turkey

How to protect yourself against cyber attacks

The digital economy is primarily based on data. In the era of Industry 4.0, cyber-physical systems and the Internet of Things, more and more products and processes are digitized. Cybersecurity,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

meaning the protection of this data and associated information processing systems, is more relevant today than at any time in economic history.

Business processes can be significantly disrupted, slowed down or even completely blocked, for example if data records are incorrect, incomplete or not available at all, data synchronization between systems is disrupted, IT systems work incorrectly or fail completely.

SMEs in particular are targets for criminal activity related to these issues. Unlike big corporations, their resources are limited - and hackers know it! SMEs are the backbone of the economy in Europe, meaning over 99% of companies in Germany are SMEs.

More than half of the workforce is employed by SMEs. It is therefore necessary to help SMEs avoid cyber attacks.

The Cyber Security Education Initiative points out that a critical step should be taken to address the lack of "individuals with the knowledge, skills, and abilities to perform the tasks required for cybersecurity work."

Such a group includes "technical and non-technical functions that are filled by employees with knowledge and experience."

However, it is difficult to create a workforce with the necessary interdisciplinary skills and to solve the problem of communication between educators, researchers and people who use information technologies.

Cooperation and communication between these groups is necessary.

One problem is that companies, especially SMEs with fewer resources, need help to assess the skills and gaps of their employees, using digital methods to improve the existing situation and organizing training opportunities to reskill their employees.

Training and mentoring

Entrepreneurs, including future ones, need complex ways of thinking and the ability to understand and integrate knowledge from different sectors, which requires interdisciplinary learning.

Complex engineering problems require creating an interdisciplinary situation in an almost natural

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

way.

In an interdisciplinary approach, learners should integrate information from different disciplines and fields.

They develop an interdisciplinary understanding, learn to integrate areas of expertise and discipline-specific ways of thinking.

This increases cognitive skills and critical thinking more than through single disciplinary means.

Social engineering

- it means manipulating human beings, (often using psychological methods), to gain access to data, documents and information of interest to the attacker.
- is one of the main threats to information security today and is an effective form of cybercrime.
- could have dangerous repercussions, for example, data breaches, more than any other type of attack.
- the attacks have a financial purpose and thus organizations have lost considerable amounts of money.
- it is particularly dangerous because it relies more on human error than on vulnerabilities in software and operating systems.

The companies:

- they could suffer lost productivity, a drop in employee morale, and difficulties in recovery.
- they have reputational damage because customers are not convinced that the organization can protect itself.
- often need to trigger an old incident response.
- should provide security software to help prevent future attacks.
- they would often have to retrain employees to be ready for attacks.

Social Engineering Training (cyber awareness)

- of employees and managers for whom it is important to recognize social engineering attacks because the risk of becoming a victim is high.
- could be included in community, individual and citizen security awareness programs and protect individuals and their organization.
- is particularly lacking in SMEs that have fewer resources, so they should be helped to take

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

cyber awareness training seriously and provide opportunities for employees to take it.

The Social Engineering Attack Lifecycle

Attacker:

- first investigate the targeted victim to gather the necessary basic information, such as entry points and weak security protocols, that are required for the attack.
- then try, gain the victim's trust and provide incentives for actions that are not usually security practices, such as becoming sensitive information or granting access to critical resources.

The Figure 2 explains the life cycle of an attack.

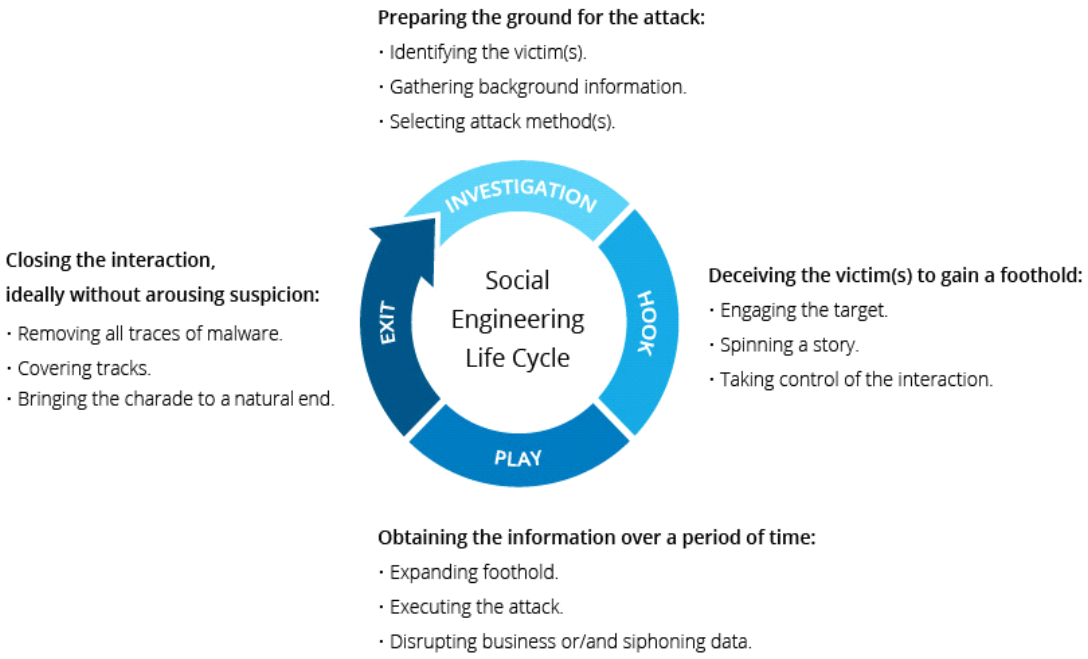


Figure 2: Life cycle of an attack

Social network

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- has become very popular in recent years, providing users with a platform to communicate with their family, friends and colleagues.
- and Social Networking refers to the use of Internet-based social networking sites to connect and communicate with friends, family, colleagues, clients or customers.
- they have their servers in data centers co-located with the main network access points of the Internet.

Social Media Roles (Figure 3) shows some areas where social media plays a role:

- Entertainment
- building business opportunities
- to make a career
- improving social skills
- developing relationships with other individuals

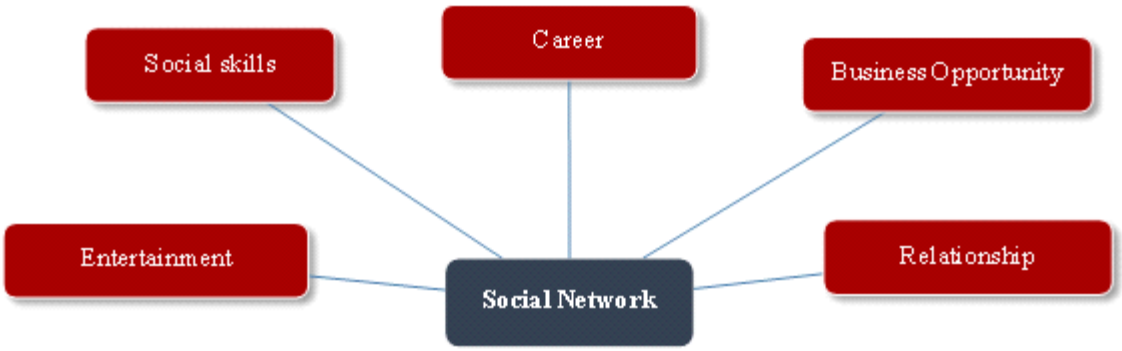


Figure 3: Roles in the Social Network

Social network:

- is a foundation for marketers looking for customers to increase brand recognition, foster brand loyalty, improve conversion rates, provide access and engagement with new, recent and old customers.
- make it possible, by sharing blog posts, images, videos or comments on social networks, for more people to visit the company's website and become customers.
- it makes it difficult to keep up with changes and also affects a company's marketing success rate.

The most popular social networking (social media) sites in the United States and Europe are:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- Facebook
- Instagram
- Twitter
- YouTube
- WhatsApp
- LinkedIn that helps connect professionals with coworkers, business contacts, and employers.

Social networking is based on developing and maintaining personal and business relationships using technology and social networking sites (Social Media) that allow people and businesses to connect with each other, developing relationships, sharing information, ideas and messages.

Family members could stay connected through personal social networks like Facebook, share photos and send other messages about their lives.

People can also connect with others (strangers) who share the same interests.

There are also disadvantages to social media, including the spread of misinformation and the high cost of using and maintaining social media profiles.

The functionality of social platforms can be classified into:

Network functions serve to foster social relationships between users within virtual platforms and provide functionality for building and maintaining the social network graph.

Data functions are responsible for managing user-provided content and communication between users, helping to improve (extend) user interaction and make the platform more attractive

Access control features aim to implement user-defined privacy measures and restrict unauthorized access to user-provided data and information.

Advantages and disadvantages of social networks

Benefits

- Social media allows businesses to:
- To connect with new and existing customers.
- to be able to create, promote and increase brand awareness.
- to rely on reviews and comments made by their clientele important to increase brand sales

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

and higher search engine rankings.

- to be able to establish a new brand. to demonstrate a high level of service to its customers.
- to be able to improve products and relations with consumers.

Disadvantage

- they can contribute to the spread of misinformation.
- can have a negative impact on companies because criticism of a brand has spread very quickly on social media.
- requires work hours and costs each week to build and maintain a company profile.

Security and privacy in social networks

- Information shared in social networks and media spreads very quickly, which makes it attractive for attackers to gain it.
- Security and privacy issues related to user-shared information when a user uploads personal content such as photos, videos, and audio should be respected because the attacker can maliciously use the shared information for illegitimate purposes.
- Lack of user awareness about security and privacy has the potential to lead to various cyber attacks through social media.

Threats can be divided into three categories:

- Conventional threats include threats that users have encountered since the beginning of the social network.
- Modern threats are attacks that use advanced techniques to compromise user accounts.
- Targeted attacks are attacks targeting a specific user, which can be committed by any user for various personal vendettas.

Solutions for social network operators

- Authentication procedures such as CAPTCHA, multi-factor authentication, and photo identification of friends have been proposed.
- Security and privacy setting to allow the customer to enter personal information from unwanted access by outsiders or applications.

User reports of any form of abuse or policy violations by any user on their network. that is, when Facebook receives a user report, it is reviewed and removed according to Facebook's community

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

standards.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. Witch are yours expectations concerning InCyT project
2. How to protect yourself against cyber attacks
3. What is a social engineering
4. Social Network (Social Media)

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- How to protect yourself against cyber attacks
- What is a social engineering
- Social Network (Social Media)

Attachments

PowerPoint presentation
Video movies

References:

- InCyT – Interdisciplinary Cyber Training
- Cyber Incident Recovery
- Minimize Cyber Attacks - Cyber Resiliency Strategy
- How to Prevent Cyberattacks: Top Ways to Protect Yourself
- Social Media Security: How Safe is Your Information?
- Internal Controls Over Information Systems
- Social Media Adoption Brings New Risks
- Social Media Security – 5 Security Tips

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- 19 Social Media Security Best Practices

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Employees **Unit 1 Week 1** **Unit name: Introduction Webinar**	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Gabriel Vladut • Valentin Istratie
Learning Activity Goals	1. Introduction about Erasmus+ InCyT project 2. Objectives 3. Results and products 4. How to protect yourself against cyber attacks 5. Training and mentoring 6. Social engineering 7. Social Network (Social Media)
Skills to be Gained	• TS3 Network Security • TS4 Penetration (exploitable vulnerabilities) testing • SS3 Cognitive and behaviour analysis
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • To learn about Erasmus+ InCyT project / objectives / Results and products • How to protect yourself against cyber attacks • Training and mentoring • Social engineering / Social Network (Social Media)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
InCyT is an Erasmus + project that aim to create a Framework, a methodology for training, which provides a mechanism for VET and companies to describe the competences and skills, necessary in cyber security for professionals and not professionals in order to avoid cyber-attacks, as well digital gaps and other ones. NIST's National Initiative for Cyber security Education (NICE) underlines that it should be done a crucial step toward remedying shortage of "people with the knowledge, skills, and abilities to perform the tasks required for cyber security work." Such a workforce will include "technical and nontechnical roles that are staffed with knowledgeable and experienced people." The project will like to implement some solutions in this context. It has as objective first the development a Framework, which provides a mechanism for VET and companies to describe the digital gaps and other ones necessary in cyber security for professionals and not professionals in order to avoid cyber-attacks and help them to improve this situation. Taking into consideration of advantages of interdisciplinary training and mentoring programs particularly in the field of cyber security the project will develop, and test digital interdisciplinary training programs supported by e-mentoring for SMEs and adapt it for VET. Collaboration and communication between educators, researchers and people who use information technologies are necessary. One problem is that companies, particularly SMEs with less resource need help to appreciate the competences and skills gaps of their employees, methods to evaluate the existing situation as well as using training possibilities to reskill their employees. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace. All these documents are on the digital interactive project platform. The learners can test their answers on self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forum and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the meetings. They will be supported to develop e-portfolio important for reflection and evaluation of the training.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Content of the Learning Material

Competence Framework

There will be 3 transnational meetings in our project. It was planned in the 3rd, 13th and 20th month of the project. Some additional project meetings will be held as we think that 3 meetings will not be enough to run a 24-month project. These meetings are online and held regularly every month. The project senior management team will organize these projects.

The projects will be led by the project coordinator, the WP leader. There will be 7 multiplier events in our project. Each partner institution will organize these activities to popularize the project idea in its own country and to share the developed products. Each partner institution will run the Interdisciplinary Training for SME employees and teachers in Cyber Securityactivity in its own country.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

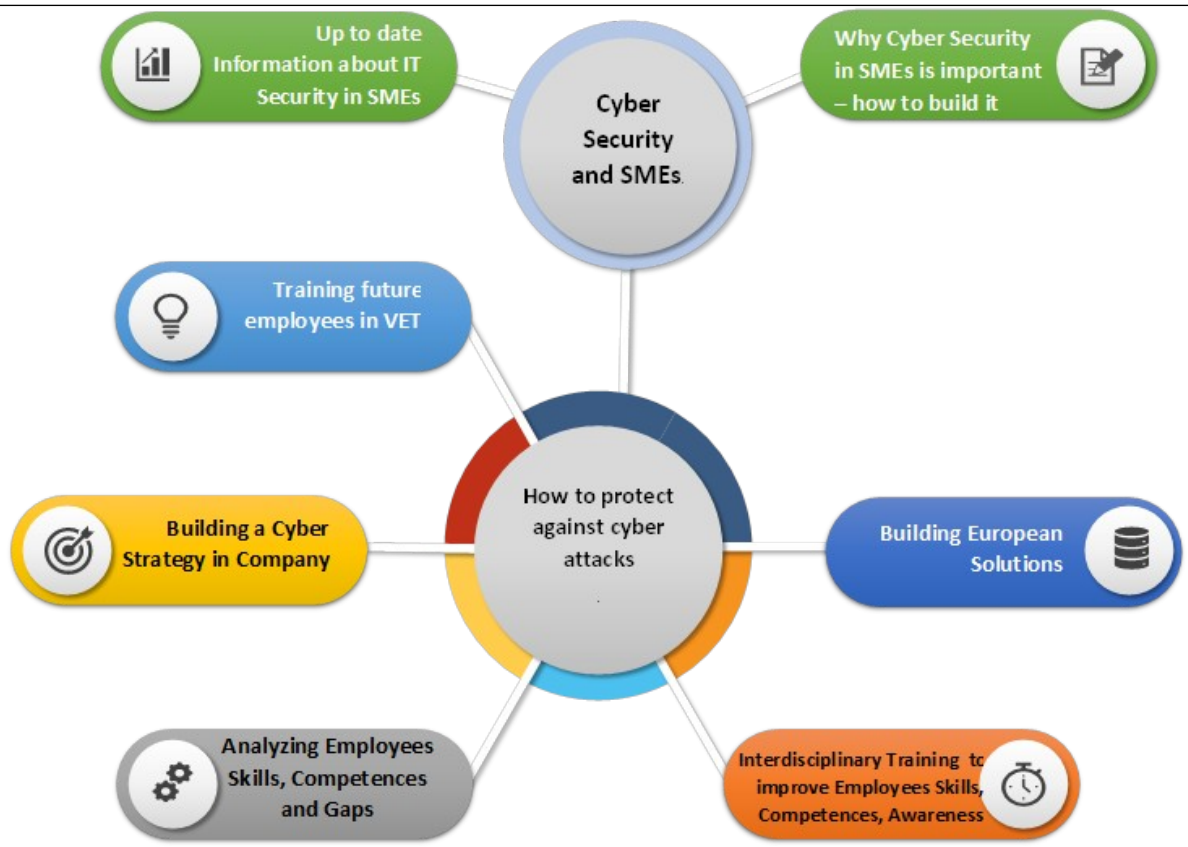


Figure 1: Activities supported by the InCyT project

Objectives

The InCyT project will like to implement some solutions:

- The development of a Framework, which provides a mechanism for VET and companies to describe the competences and skills, necessary in cyber security for professionals and not professionals in order to avoid cyber-attacks, as well digital gaps and other ones.
- Taking into consideration of advantages of interdisciplinary training and mentoring programs particularly in the field of cyber security the project will develop, and test digital interdisciplinary training programs supported and a collaborative e-Learning platform for SMEs
- Adapt it for VET.
- Develop a European transferability model
- Taking into consideration of advantages of interdisciplinary training and mentoring programs particularly in the field of cyber security the project will develop, and test digital interdisciplinary training programs supported by e-mentoring for SMEs and adapt it for

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

VET.

Outcomes of the project will be:

- Methodological Framework for Implementation
- Existing and followed training (courses)
- Opportunities for improvements of these by using interdisciplinarity and mentoring.
- Learning and mentoring methodology

Products:

1. Framework

2. A digital Interdisciplinary cyber security training material for SMEs supported by mentoring and an adapted methodology for a VET special course.

3. A digital platform to support the training

4. Report how interdisciplinary skills provide advantages for SME and VAT.

5. European transferability model for the tested interdisciplinary training and mentoring

Partners from: Germany (coordinator), Turkey, Poland, Italy, Austria, Denmark, Romania.

Activities

- Methodological Framework for Cyber Security - Leading Organisations: IAT, Germany, Italy
- A Digital Interdisciplinary Cyber Security Training Material - Leading Organisation: St. Pölten University of Applied Sciences, Austria
- ICT Platform for Cyber Security - Leading Organisation: IPA, Romania
- Methodological Model for Cyber Security - Leading Organisation: Politechnik University, Poland
- Transferability Model - Leading Organisation: European Training Center Copenhagen, Denmark
- Multiplier Events - Leading Organisation: Turkey

How to protect yourself against cyber attacks

The digital economy is primarily based on data. In the era of Industry 4.0, cyber-physical systems and the Internet of Things, more and more products and processes are digitized. Cybersecurity,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

meaning the protection of this data and associated information processing systems, is more relevant today than at any time in economic history.

Business processes can be significantly disrupted, slowed down or even completely blocked, for example if data records are incorrect, incomplete or not available at all, data synchronization between systems is disrupted, IT systems work incorrectly or fail completely.

SMEs in particular are targets for criminal activity related to these issues. Unlike big corporations, their resources are limited - and hackers know it! SMEs are the backbone of the economy in Europe, meaning over 99% of companies in Germany are SMEs.

More than half of the workforce is employed by SMEs. It is therefore necessary to help SMEs avoid cyber attacks.

The Cyber Security Education Initiative points out that a critical step should be taken to address the lack of "individuals with the knowledge, skills, and abilities to perform the tasks required for cybersecurity work."

Such a group includes "technical and non-technical functions that are filled by employees with knowledge and experience."

However, it is difficult to create a workforce with the necessary interdisciplinary skills and to solve the problem of communication between educators, researchers and people who use information technologies.

Cooperation and communication between these groups is necessary.

One problem is that companies, especially SMEs with fewer resources, need help to assess the skills and gaps of their employees, using digital methods to improve the existing situation and organizing training opportunities to reskill their employees.

Training and mentoring

Entrepreneurs, including future ones, need complex ways of thinking and the ability to understand and integrate knowledge from different sectors, which requires interdisciplinary learning.

Complex engineering problems require creating an interdisciplinary situation in an almost natural

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

way.

In an interdisciplinary approach, learners should integrate information from different disciplines and fields.

They develop an interdisciplinary understanding, learn to integrate areas of expertise and discipline-specific ways of thinking.

This increases cognitive skills and critical thinking more than through single disciplinary means.

Social engineering

- it means manipulating human beings, (often using psychological methods), to gain access to data, documents and information of interest to the attacker.
- is one of the main threats to information security today and is an effective form of cybercrime.
- could have dangerous repercussions, for example, data breaches, more than any other type of attack.
- the attacks have a financial purpose and thus organizations have lost considerable amounts of money.
- it is particularly dangerous because it relies more on human error than on vulnerabilities in software and operating systems.

The companies:

- they could suffer lost productivity, a drop in employee morale, and difficulties in recovery.
- they have reputational damage because customers are not convinced that the organization can protect itself.
- often need to trigger an old incident response.
- should provide security software to help prevent future attacks.
- they would often have to retrain employees to be ready for attacks.

Social Engineering Training (cyber awareness)

- of employees and managers for whom it is important to recognize social engineering attacks because the risk of becoming a victim is high.
- could be included in community, individual and citizen security awareness programs and protect individuals and their organization.
- is particularly lacking in SMEs that have fewer resources, so they should be helped to take

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

cyber awareness training seriously and provide opportunities for employees to take it.

The Social Engineering Attack Lifecycle

Attacker:

- first investigate the targeted victim to gather the necessary basic information, such as entry points and weak security protocols, that are required for the attack.
- then try, gain the victim's trust and provide incentives for actions that are not usually security practices, such as becoming sensitive information or granting access to critical resources.

The Figure 2 explains the life cycle of an attack.

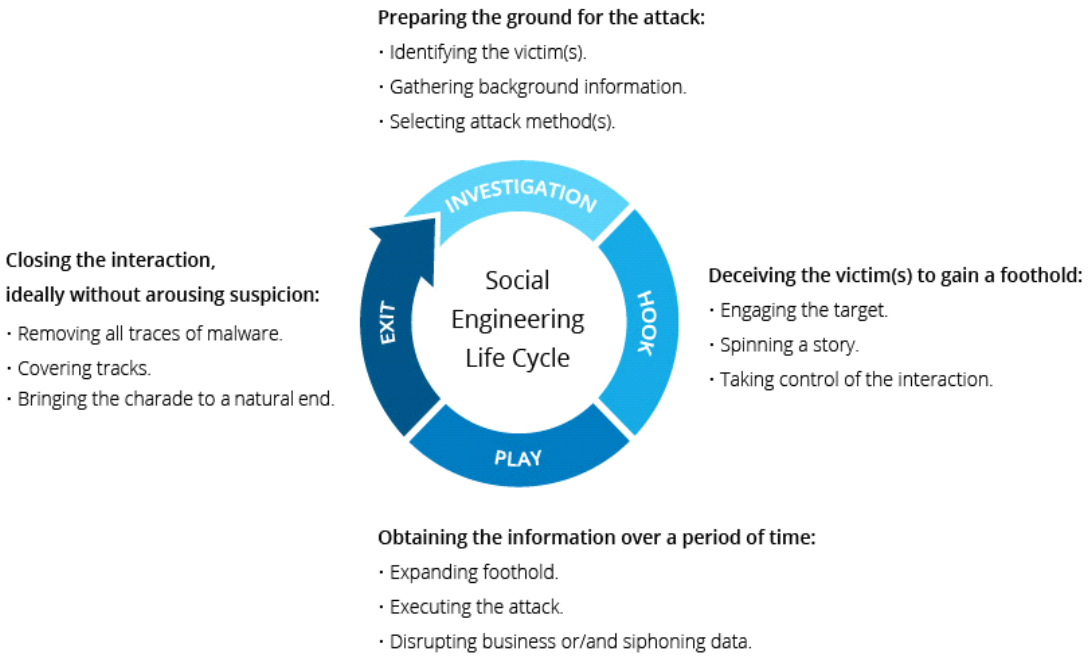


Figure 2: Life cycle of an attack

Social network

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- has become very popular in recent years, providing users with a platform to communicate with their family, friends and colleagues.
- and Social Networking refers to the use of Internet-based social networking sites to connect and communicate with friends, family, colleagues, clients or customers.
- they have their servers in data centers co-located with the main network access points of the Internet.

Social Media Roles (Figure 3) shows some areas where social media plays a role:

- Entertainment
- building business opportunities
- to make a career
- improving social skills
- developing relationships with other individuals

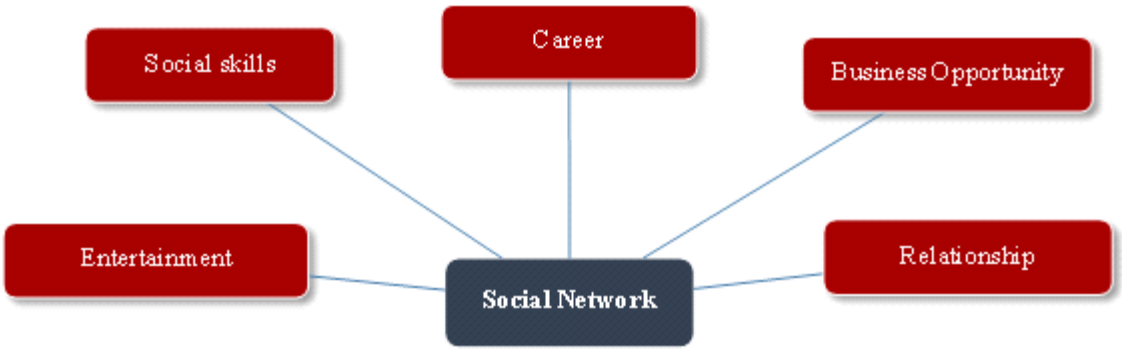


Figure 3: Roles in the Social Network

Social network:

- is a foundation for marketers looking for customers to increase brand recognition, foster brand loyalty, improve conversion rates, provide access and engagement with new, recent and old customers.
- make it possible, by sharing blog posts, images, videos or comments on social networks, for more people to visit the company's website and become customers.
- it makes it difficult to keep up with changes and also affects a company's marketing success rate.

The most popular social networking (social media) sites in the United States and Europe are:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- Facebook
- Instagram
- Twitter
- YouTube
- WhatsApp
- LinkedIn that helps connect professionals with coworkers, business contacts, and employers.

Social networking is based on developing and maintaining personal and business relationships using technology and social networking sites (Social Media) that allow people and businesses to connect with each other, developing relationships, sharing information, ideas and messages.

Family members could stay connected through personal social networks like Facebook, share photos and send other messages about their lives.

People can also connect with others (strangers) who share the same interests.

There are also disadvantages to social media, including the spread of misinformation and the high cost of using and maintaining social media profiles.

The functionality of social platforms can be classified into:

Network functions serve to foster social relationships between users within virtual platforms and provide functionality for building and maintaining the social network graph.

Data functions are responsible for managing user-provided content and communication between users, helping to improve (extend) user interaction and make the platform more attractive

Access control features aim to implement user-defined privacy measures and restrict unauthorized access to user-provided data and information.

Advantages and disadvantages of social networks

Benefits

- Social media allows businesses to:
- To connect with new and existing customers.
- to be able to create, promote and increase brand awareness.
- to rely on reviews and comments made by their clientele important to increase brand sales

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

and higher search engine rankings.

- to be able to establish a new brand. to demonstrate a high level of service to its customers.
- to be able to improve products and relations with consumers.

Disadvantage

- they can contribute to the spread of misinformation.
- can have a negative impact on companies because criticism of a brand has spread very quickly on social media.
- requires work hours and costs each week to build and maintain a company profile.

Security and privacy in social networks

- Information shared in social networks and media spreads very quickly, which makes it attractive for attackers to gain it.
- Security and privacy issues related to user-shared information when a user uploads personal content such as photos, videos, and audio should be respected because the attacker can maliciously use the shared information for illegitimate purposes.
- Lack of user awareness about security and privacy has the potential to lead to various cyber attacks through social media.

Threats can be divided into three categories:

- Conventional threats include threats that users have encountered since the beginning of the social network.
- Modern threats are attacks that use advanced techniques to compromise user accounts.
- Targeted attacks are attacks targeting a specific user, which can be committed by any user for various personal vendettas.

Solutions for social network operators

- Authentication procedures such as CAPTCHA, multi-factor authentication, and photo identification of friends have been proposed.
- Security and privacy setting to allow the customer to enter personal information from unwanted access by outsiders or applications.

User reports of any form of abuse or policy violations by any user on their network. that is, when Facebook receives a user report, it is reviewed and removed according to Facebook's community

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

standards.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. Witch are yours expectations concerning InCyT project
2. How to protect yourself against cyber attacks
3. What is a social engineering
4. Social Network (Social Media)

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- How to protect yourself against cyber attacks
- What is a social engineering
- Social Network (Social Media)

Attachments

PowerPoint presentation
Video movies

References:

- InCyT – Interdisciplinary Cyber Training
- Cyber Incident Recovery
- Minimize Cyber Attacks - Cyber Resiliency Strategy
- How to Prevent Cyberattacks: Top Ways to Protect Yourself
- Social Media Security: How Safe is Your Information?
- Internal Controls Over Information Systems
- Social Media Adoption Brings New Risks
- Social Media Security – 5 Security Tips

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- 19 Social Media Security Best Practices

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Employees Unit 1 Week 2 Unit name: Introduction into Information Security, internal control systems	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Gabriel Vladut • Valentin Istratie
Learning Activity Goals	1. Introduction about Erasmus+ InCyT project 2. Cyber-security 3. Concepts, definitions and terms 4. Internal Control Standard 5. Elaboration of cyber security controls
Skills to be Gained	• TS3 Network Security • TS4 Penetration (exploitable vulnerabilities) testing • SS3 Cognitive and behaviour analysis
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?***
	• Gain Cyber-security awareness and learn what is a Cyber-security attacks • Learn methods to prevent data breaches used by attackers to access sensitive data and exploit organizational vulnerabilities • Learn how to proceed in case of a Cyber-security attack

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
Information Security, internal control systems are important and verry often threat to cyber – security The protection of information and information systems against unauthorized access or modification of information, whether in storage, processing, or transit, and against denial of service to authorized users. Information security includes those measures necessary to detect, document, and counter such threats. Information security is composed of computer security and communications security. Also called INFOSEC. See also communications security; computer security; information security; information system. Internal controls are used by management, IT security, financial, accounting, and operational teams to achieve the following goals: 1. Ensure the reliability and accuracy of financial information – Internal controls ensure that accurate, up to date and complete information is reflected in accounting systems and financial reports. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace. All these documents are on the digital interactive project platform. The learners can test their answers on self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forum and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the meetings. They will be supported to develop e-portfolio important for reflection and evaluation of the training.

Content of the Learning Material

Cyber attacks and the competence framework

A competency framework is regularly used by companies to understand their skill-based requirements, required competencies, employee skills, and gaps.

When a competency framework is developed taking into account the company's profile and employee interests, it can improve performance and provide clarity for each individual role requirement and develop talent in the workplace. In recent years, due to many cyber attacks,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

cyber security frameworks are mainly adopted by large organizations (businesses, NGOs and other entities) or by state actors.

A successful cyber attack can cause major damage to a company's business. It can affect its bottom line as well as the company's business status and consumer confidence. The impact of a security breach can be divided into three categories: financial, reputational and legal.

Cyber attacks

Cyber-attacks often result in substantial financial loss resulting from the theft of corporate information, financial information (eg bank details or payment card details), money, transaction disruptions (eg inability to transact online), loss of business or of the contract. Businesses that have suffered a cyber breach will generally spend money associated with repairing affected systems, networks and devices.

Cyber attacks can damage a company's reputation and the trust customers have in the company. This could lead to lost customers, lost sales and reduced profits. The effect of reputational damage can even affect the company's suppliers or affect relationships with partners, investors and other third parties involved in the company's business.

So data protection and privacy laws require the security management of all personal data held by the company (of its own staff or customers). If this data is accidentally or deliberately compromised and the company does not implement adequate security measures, it may face regulatory penalties.

Risks in the company

It is important to manage your risks accordingly. After an attack occurs, an effective cyber security tool or incident response plan, i.e. using a cyber consultant, can help to:

- reduce the impact of the attack
- report the incident to the appropriate authority
- clean up the affected systems
- get your company business up and running in the shortest possible time.

It is necessary to invest in training and educating users in the field of cyber security in order to avoid attacks and continuously develop awareness for a cyber strategy in one's organization.

Cyber Security Framework

A cybersecurity framework is a set of best practices and documented processes that are used to

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

develop IT security policies within an organization. But unlike traditional policy strictly related to the legal domain, a cybersecurity framework should also include documented examples of problems to be avoided by those policies and of the appropriate processes and ways to implement the security policies described in the framework.

It is both a guide for employees and users as well as a compelling compendium of security best practices that can be consulted by authorized external parties (such as authorities). A cybersecurity competency framework can also help better assess the competencies needed to avoid attacks, gaps, and remediation measures.

Cyber security

Despite increased awareness and bold efforts, the highly significant and growing shortage of cybersecurity professionals in the European Union and the knowledge and skills of employees to avoid cyber-attacks worldwide is known, and these shortages continue to present major problems for the public and private sector.

The 2019 CYBERSECURITY WORKFORCE 2019 Strategies for Building and Growing Strong Cyber Security Teams (ISC) study estimates that there are 2.8 million cybersecurity professionals globally, while the gap is actually 4.07 million.

The study notes that the current gap in Europe is 291,000, and this number has doubled from previous years. Many countries with highly developed expertise prefer to create their own set of regulations and documents, but many countries and small and medium-sized companies (SMEs) need help in this context.

Social engineering

- it means manipulating human beings, (often using psychological methods), to gain access to data, documents and information of interest to the attacker.
- is one of the main threats to information security today and is an effective form of cybercrime.
- could have dangerous repercussions, for example, data breaches, more than any other type of attack.
- the attacks have a financial purpose and thus organizations have lost considerable amounts of money.
- it is particularly dangerous because it relies more on human error than on vulnerabilities in software and operating systems.

The companies:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

- they could suffer lost productivity, a drop in employee morale, and difficulties in recovery.
- they have reputational damage because customers are not convinced that the organization can protect itself.
- often need to trigger an old incident response.
- should provide security software to help prevent future attacks.
- they would often have to retrain employees to be ready for attacks.

Social engineering; Training (cyber awareness)

- of employees and managers for whom it is important to recognize social engineering attacks because the risk of becoming a victim is high.
- could be included in community, individual and citizen security awareness programs and protect individuals and their organization.
- is particularly lacking in SMEs that have fewer resources, so they should be helped to take cyber awareness training seriously and provide opportunities for employees to take it.

Training and mentoring

Entrepreneurs, including future ones, need complex ways of thinking and the ability to understand and integrate knowledge from different sectors, which requires interdisciplinary learning. Complex engineering problems require creating an interdisciplinary situation in an almost natural way.

In an interdisciplinary approach, learners should integrate information from different disciplines and fields. They develop an interdisciplinary understanding, learn to integrate areas of expertise and discipline-specific ways of thinking.

This increases cognitive skills and critical thinking more than through single disciplinary means.

Entrepreneurial skills and mentoring

Assessing learners' performance in developing entrepreneurial skills can take a holistic view, including a look at the learning environment and learning outcomes, and facilitate interactive, effective and active learning.

Mentoring is an experienced method to support more individual learning and to gain personal and career skills for new professions. There is research on the outcomes of mentoring in general, but there is little research on mentoring.

Mentoring offers a number of benefits for employees who train in companies. Interdisciplinary

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

team mentoring has gained importance in recent years, reflecting the need for a change in the orientation of mentoring as various entrepreneurial developments and fields are increasingly multidisciplinary.

Interdisciplinary mentoring and networks of mentors can produce synergy in groups, generate innovative ideas and complex solutions to challenges, and create opportunities for collaboration and work.

Concepts, definitions and terms

The term "**cyberspace**" was coined in 1982 by William Gibson. The term entered everyday life in the 1990s with the advent of the World Wide Web

cyber infrastructures - information and communications technology infrastructures, consisting of IT systems, related applications, networks and electronic communications services;

cyber space - the virtual environment, generated by cyber infrastructures, including the informational content processed, stored or transmitted, as well as the actions carried out by users in it;

cyber security - the state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, of public or private resources and services, in cyber space.

Proactive and reactive measures may include security policies, concepts, standards and guidelines, risk management, training and awareness activities, implementation of technical solutions to protect cyber infrastructures, identity management, consequence management;

cyber defense - actions carried out in cyber space for the purpose of protecting, monitoring, analyzing, detecting, countering aggressions and ensuring a timely response against threats to cyber infrastructure specific to national defense;

operations in computer networks - the complex process of planning, coordinating, synchronizing, harmonizing and carrying out actions in cyberspace for the protection, control and use of computer networks in order to obtain informational superiority, simultaneously with the neutralization of the adversary's capabilities;

cyber threat - circumstance or event that constitutes a potential danger to cyber security;

cyber attack - hostile action carried out in cyber space likely to affect cyber security;

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

cyber incident - event occurring in cyber space, the consequences of which affect cyber security;

cyber terrorism - premeditated activities carried out in cyberspace by politically, ideologically or religiously motivated individuals, groups or organizations that can cause material destruction or victims, likely to cause panic or terror;

cyber espionage - actions carried out in cyber space, with the aim of obtaining unauthorized confidential information in the interest of a state or non-state entity;

computer crime - all the acts provided for by the criminal law or other special laws that present a social danger and are committed with guilt, through or on cyber infrastructures;

vulnerability in cyber space - weakness in the design and implementation of cyber infrastructures or related security measures that can be exploited by a threat;

security risk in cyber space - the probability that a threat will materialize, exploiting a specific vulnerability specific to cyber infrastructures;

risk management - a complex, continuous and flexible process of identifying, evaluating and countering cyber security risks, based on the use of complex techniques and tools, to prevent losses of any kind;

identity management - methods of validating the identity of people when they access certain cyber infrastructures;

The components of internal control

According to the INTOSAI GOV 9100 Standard "Guidelines for Internal Control Standards". In 2001, at the Congress of the International Organization of Supreme Audit Institutions (INCOSAI), it was decided to update the INTOSAI Guidelines for internal control standards in the public sector, originally issued in 1992, by introducing into the document all aspects of recent developments in the field internal control and to integrate a series of elements of the COSO model (Internal Control – Integrated Framework).

By integrating it into the Guidelines - an activity carried out by the operative group of the Internal Control Standards Committee of INTOSAI - an attempt was made to obtain a unified understanding of how the new internal control system works, by the representatives of the Supreme Audit Institutions.

The "INTOSAI Guidelines for Internal Control Standards in the Public Sector" are part of the INTOSAI GOV category (good governance guidance) and are considered extremely useful both for

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

public sector managers who have to implement the internal control system and external public auditors, who must know this system and evaluate it.

Internal control standards

According to the INTOSAI GOV 9100 Guidelines), internal control consists of five interdependent components (identical to those of the COSO model):

- Control Environment
- Risk evaluation
- Control activities
- Information and communication
- Monitoring

Internal control is designed to provide reasonable assurance regarding the achievement of the institution's overall objectives. Objectives clearly established by the heads of the entity and the appropriate planning of the budget are a mandatory condition for an effective internal control.

Control environment

The control environment encompasses the general attitude, awareness and actions taken by management and those charged with governance regarding the internal control system and its importance within the entity. The control environment sets the tone of the organization, influencing the control consciousness at the staff level.

It represents the basis of all other components of internal control, ensuring a discipline within the organization that must be respected and a structure of the entity, so that the internal control system can be effectively applied. The internal control environment is an effective tool in preventing corruption and fraud.

The elements that define the control environment are:

- personal and professional integrity, the ethical values established by management for all staff, including a permanent supportive attitude towards internal control;
- a continuing management concern for staff competence;
- "the tone given from above" (the philosophy and activity style of management);
- the organizational structure of the entity;
- HR policy and practices.

Types of Cyber Security Controls

Cybersecurity controls are mechanisms used to prevent, detect and mitigate cyber threats and

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

attacks. Mechanisms range from physical controls such as security guards and surveillance cameras to technical controls including firewalls and multi-factor authentication.

A one-sided approach to cyber security is simply outdated and ineffective. And because it is impossible to prevent all attacks in today's threat landscape, organizations should evaluate their assets based on their importance to the business and establish controls accordingly.

Adding to the challenge is that employees are unlikely to follow compliance rules if stringent controls are implemented across all company assets. The severity of a control should directly reflect the asset and threat landscape.

The consequences of a hacker exposing thousands of personal customer data through a cloud database, for example, can be far greater than if an employee's laptop is compromised.

Cyber security controls

"There are many different ways to apply controls based on the nature of what you're trying to protect," said Joseph MacMillan, author of Infosec Strategies and Best Practices and cybersecurity global black belt at Microsoft.

"What is the nature of the threat you are trying to protect against?

Is it a malicious actor?

Or is it a devastating attack?"

Securing information assets

It refers to the implementation of appropriate information security controls for assets. We want to ensure that we focus on strong and effective ideologies to understand to select the appropriate controls, which means that the asset is considered "safe enough" based on its criticality and classification. There are different classes that divide the types of controls:

- Administrative/managerial controls are the firm's policies and procedures. They're not as "cool" as a new software control, but they exist to provide structure and guidance to individuals and other members of the organization, ensuring that no one gets fined or causes a breach.
- Physical controls that limit access to systems in a physical way.
- Technical / logical controls are those that limit access based on hardware or software, such as encryption, fingerprint readers, authentication or trusted platform modules (TPM).

They do not limit access to physical systems as physical controls do, but rather access to data or

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

content. Operational controls are those that involve people carrying out processes on a day-to-day basis. Examples might include awareness training, asset classification, and log file review.

Types of controls

Preventive controls exist to prevent an action and include firewalls, fences, and access permissions.

Detective commands are only triggered during or after an event, such as video surveillance or intrusion detection systems. Deterrents discourage threats from trying to exploit a vulnerability, such as a "Watchdog" or dogs sign. Corrective controls are capable of taking action from one state to another. The fail open and fail closed commands are addressed here.

Recovery commands get something back from a loss, such as recovering a hard drive. Compensating controls are those that attempt to compensate for deficiencies in other controls, such as regularly reviewing access logs. This example is also a detective control, but compensation controls can be of different types.

Order of controls

It discourages actors from trying to access something they shouldn't be. Deny/Prevent Access through a preventive control such as access permissions or authentication.

Detect risk by making sure to record detection, such as with endpoint protection software. Delay the process from repeating the risk again, such as with a "too many attempts" feature for entering a password.

Correct the situation by responding to the compromise, such as with an incident response plan. Recover from a compromised state, such as a backup generator that restores availability to a server.

In addition, in the field of continuous improvement, we should monitor the value of each asset for any changes. The reason is that we may need to rethink our controls for protecting those assets if they become more or less valuable over time or during certain major events in your organization.

Controls and recovery

When we look at controls we should also think about recovery, we want to be able to recover from any adverse situations or changes in assets and their value. Just as examples, we are talking about backups, redundancy, restoration processes and the like.

A concept to remember, especially in the era of cloud, SaaS, PaaS, IaaS, third-party solutions and

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

all other forms of "someone else's computer" is to ensure that Service Level Agreements (SLAs) are clearly defined and have maximum allowable downtime agreements, as well as penalties for non-compliance with these agreements. This is an example of compensatory control.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. Witch are the risks in the company for cyber attacks?
2. Call some types of cyber security controls
3. Witch are internal control standards
4. How to Control and recover informations

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- Risks in the company for cyber attacks
- Internal control standards and rouls
- Control environment

Attachments

PowerPoint presentation
Video movies

References:

- Cyber Attacks on Companies: Are You at Risk?
- The rising strategic risks of cyberattacks
- 10 Common Cyber Security Risks For Businesses
- Internal Controls and Data Security: How to Develop Controls That Meet Your IT Security Needs
- Internal Controls Over Information Systems

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Module

Information Security for Employees Unit 2 Week 3 Unit name: Introduction to Cryptography	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	Claudio Fornaro
Learning Activity Goals	1. Cryptography 2. Cryptoanalysis 3. One time pad algorithm 4. Symmetric algorithms 5. Asymmetric algorithms 6. Hash functions 7. Signatures & public key infrastructures 8. Cryptographic Tokens 9. Challenge-response mechanism
Skills to be Gained	• Basic knowledge about cryptography algorithms and infrastructures Technical Skill 2 - TS2
Duration of Learning activity	1 week
Learning requirements	***What is needed?*** • No previous specific knowledge is required

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Cryptography pertains to methodologies for hiding information from disclosure, both during a communication and for archival purposes. Its objectives are achieved with the design and implementation of protocols that prevent an unauthorized third party from retrieving the information. In a secure communication, the adversary third party cannot access the information transmitted, in the case of archiving the third party cannot trace the content of what has been archived.

In Cryptography, the third party is always a malicious entity that aims to retrieve information that it must not have access to, whether for privacy, trade secret or national security purposes. The data confidentiality and integrity, the authentication of the parties involved and the non-repudiation of what the data source has transmitted or stored are the fundamental principles of modern cryptography.

After an introductory part, where the fundamental concepts are described, we present a progression of basic cryptographic techniques, starting from the *One Time Pad Algorithm* and then building up for considering the two cryptographic families of algorithms: Symmetric Algorithms and Asymmetric (or Public Key) Algorithms with a comparison of them. The role of the Hash Functions is also discussed to introduce Digital Signatures. A description of the key concept of Public Key Infrastructures is presented in depth with some details on the standard mechanisms and formats. To conclude, some information about Cryptographic Tokens and the Challenge-Response Mechanism is provided.

Content of the Learning Material

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Introduction

Cryptography is the mechanism by which the content of a message is hidden from other entities. In other words encryption deals with encrypting messages, i.e. taking a plaintext, using an algorithm and generally a key, making the content of the message unintelligible.

Cryptanalysis studies how to decrypt the message without knowing the key. In an attack, cryptanalysis consists in trying to trace the content of the message without having the key. Cryptographers and cryptanalysts are actually the same people: who writes the cryptographic algorithms also analyzes them to find their weaknesses or validate their robustness. As always, when dealing with security, the idea of being able to deal with protection issues without knowing how attack techniques work is not very effective.

Information in messages is generally redundant, in a formal sense, messages generally use a much higher number of bits than that really necessary to carry the information. **The redundancy of information facilitates cryptanalysis**: redundancy in the information means that the messages can show a structure that makes it easier to trace the content of the message, as not all messages are equally likely. If we think of a text represented with normal ASCII characters in byte we know that the combinations of bits that can represent meaningful messages are relatively few compared to all possible combinations. The true messages that can be represented with a certain number of bytes are very few. This makes it possible to identify valid messages by discarding those that do not carry true information. All this vastly helps the activity of the cryptanalyst, so the purpose of the encryption algorithm is also to hide this redundancy to better hiding the information.

Example: Encoding *a sequence* of the four colors BLUE, GREEN, RED and YELLOW.

These can be coded:

- with 2 bits (00, 01, 10, 11)
- as 4 different uppercase letters
- encrypting the color names

In the first case, the minimum number of entities (bits) is used, by substituting each color name with the corresponding 2 bits will conceal the original sequence, but not the order as there is a correspondence between COLOR and the 2 bits. In the second case, as each letter uses 8 bits in the ASCII code, 6 bits are redundant for every color → 75% redundancy and we achieve the same grade of hiding as the 2 bits. We still cannot associate colors and values.

Consider the following very simple cipher, the so-called *Caesar cipher*, which does nothing but

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

scroll the letters in the alphabet by a certain number of positions. For example, if we slide them by 3, all the 'A's become 'D's, all the 'B's become 'E's, and so on. This is a very simple cipher; actually attributed to Julius Caesar, but if the color names are encrypted with this method, the repeating pattern of their encoded letters are easily identified (the ASCII code for R followed by the ASCII code of E followed by the ASCII code of D are easy to recognize as an entity). So the sequence can be identified, and if the words are also known in this case just counting the number of letters is enough to identify the original words.

This simple example allows us to understand that cryptanalysis is not an analysis that is independent of the content of the message: a completely randomized message would be much more difficult to identify and analyze than a message that has a recognizable structure.

Some types of cryptographic attacks and algorithms rely on knowing part of the text. In some cases, knowing part of the text makes it possible to trace the key and then access the rest of the text. This is very significant when it comes to network communications, because in network communications the protocols at different levels usually have a certain amount of information that is in any case recognizable, e.g. in an IP packet we know that the header contains the sender address and the recipient address.

An encryption algorithm hides also redundant information, so applying a compression algorithm to an encrypted message does not bring much advantage, because it would reduce compression rate. If we want to use compression and encryption, we must first use compression and then encryption.

The One Time Pad Algorithm

The One Time Pad (OTP) is an algorithm, so to speak, "perfect". It is a very simple encryption algorithm, very simple to implement and has a characteristic that makes it particularly interesting: it is proven that without knowing the key it is impossible to go back to the original text. Now we look at it and then we discuss why, as we have such a good algorithm, we have to find others.

The EXCLUSIVE OR $\oplus$ (XOR) is a logical function where the result is True when the two operands are different, it operates on logical values but translated to binary digits, usually True=1 and False=0, its *truth table* is:

$0 \oplus 0 = 0$

$0 \oplus 1 = 1$

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

$1 \oplus 0 = 1$

$1 \oplus 1 = 0$

From this table it is clear that if $X \oplus Y \rightarrow Z$, then $Z \oplus Y \rightarrow X$ and $Z \oplus X \rightarrow Y$. The EXCLUSIVE OR is a very simple function and also easy to implement as an electronic circuit.

The OTP mechanism is used to transfer a message from two parties. In the scientific literature it is common practice to identify the actors with personal names, they are usually called Alice (A) and Bob (B). So we will describe how Alice can securely transmit an *n*-bytes message (*PlainText*) to Bob.

The One Time Pad algorithm requires a setup phase:

- A random sequence of exactly *n* bytes is generated, this is the *One Time Pad* (OTP) or simply the *Key*;
- The OTP is securely shared between the two parts in some way (given in advance, sent in an already secured channel, etc.).

When both parties possess the key, they can use it to transmit messages. In case Alice wants to send a message to Bob:

- Alice calculates a *bit by bit* EXCLUSIVE OR of the *PlainText* with the *Key*, producing a *CypherText*:
  Encryption: PlainText $\oplus$ Key $\rightarrow$ CypherText
- The resulting *CypherText* is transmitted by Alice to Bob over a possibly insecure channel
- Bob calculates the *bit by bit* EXCLUSIVE OR of the *CypherText* and the *Key*, so recovering the original *PlainText*:
  Decryption: CypherText $\oplus$ Key $\rightarrow$ PlainText

Example

Let us suppose both Alice and Bob have already agreed upon a random OTP (*Key*).

Alice wants to send "HELLO" to Bob (in ASCII Code, spaces are here introduced for ease of reading):

	H	**E**	**L**	**L**	**O**
PlainText:	01001000	01000101	01001100	01001100	01001111
	$\oplus$				

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Key:	10101001	01110010	10110010	10000110	11000110
			=		
CypherText:	11100001	00110111	11111110	11001010	10001001

Bob receives the *CypherText* and applies the *Key*:

CypherText:	11100001	00110111	11111110	11001010	10001001
			⊕		
Key:	10101001	01110010	10110010	10000110	11000110
			=		
PlainText:	01001000	01000101	01001100	01001100	01001111
	H	**E**	**L**	**L**	**O**

The *PlainText* has been recovered.

As the *Key* is a random sequence, there is no way to say if a certain bit of the sequence is '0' or '1', as they are equally probable. Without the *Key*, given a *CypherText* bit, we have no chance of trying to guess what the original bit might be. This is true for single bits, for the whole message, for any fragment of our message.

In case a part of the *Key* is known, it is possible to recover the corresponding part in the *PlainText*, but without the rest of the *Key* there is no lack of information on the other bits of the *PlainText*. Therefore, the cryptanalysis mentioned before is not effective. In this case, to discover the remaining part of the original message, the remaining part of the *Key* is needed. All the information conveyed by the *Key* is needed in order to recover all the information of the text.

One Time Pad Problems

The strength of the OTP mechanism relies on the length of the *Key* being exactly equal to the length of the text and on using it just one time. The main drawback is that the transmission of the OTP has the same problems as the message.

In some cases this problem is easily solved, for example a diplomatic briefcase with a ribbon containing a very long key could be provided to an embassy and subsequently the messages that will be exchanged with that embassy can be encrypted by consuming the bits of the key gradually.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

These are very peculiar uses, but quite effective. It is clear that if we consider network communication, the real uses of the One Time Pad are very limited. There is a need for something more flexible, something that allows the exchange of a key that can be used for a very long time.

Let us consider each of the problems.

Offline transmission in advance

This is a general problem with keys: keys have to be agreed in some way by the parties. This need to agree on keys is the most important problem of using cryptography. The problem with cryptography is not so much algorithms and cryptanalysis, as well as key management: that is being sure that all and only the right subjects have access to the keys, then exchange them in advance, and be sure that the keys exchanged are the correct ones.

One time use

The One Time Pad is used only once, as the name suggests, this is an important aspect and limitation. If we tried to use the same key on two messages, we would weaken the security of the method.

Generating random numbers in a deterministic system is very difficult

General purposes computers use *pseudorandom* number generation where each number is computed from the previous one with some computation, this produces a sequence of numbers that repeat after a very long period. These are not true random numbers as a computer is a deterministic machine. In cryptography, however, this feature is deleterious. If it is possible to derive the next random number from a previous one, the protections offered by cryptographic algorithms or protocols become much less secure. Writing code that implements cryptographic algorithms is not trivial: there is a great deal of detail to watch out for, all the flaws that have been identified over the years by code developers that only the code developers in this specific area have learned to manage. This means that it is always a bad idea to develop and/or implement in-house cryptographic algorithms instead of using well-tested, widely used, extensively validated libraries.

Algorithms other than OTP

The other algorithms use fixed length keys. If we use an n bit key, we have 2^n different keys, if the value of n is big enough and you just apply a brute force attack (that is trying all the possible keys), it would require so many years to find the right one so that "probably" the content of the message is no more of interest. For example, with one of the fastest supercomputers available, checking a 256 bit key would require 3.67×10^{55} years. Clearly, using keys of sufficient length has some

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

additional computational cost even for those who legitimately encrypt and decrypt, but the impact is limited.

There are Symmetric and Asymmetric algorithms.

Symmetric Algorithms

The most typical and old family of cryptographic algorithms, the ones we typically think of when we think about encrypting messages, are the ***symmetric algorithms***, called after the symmetry of the encryption and decryption operations. These algorithms use a single key that must be known to both the sender and the recipient; it is used to encrypt a message and then to decrypt it.

A simple symmetric schema could be the same as the OTP, as OTP is a symmetric algorithm, with the big difference that the *Key* has a fixed length (e.g. 256 bits) and it is repeated in some way, possibly after some complex change each time:

Encryption: *encryption_function*(PlainText, Key) → CypherText

Decryption: *decryption_function*(CypherText, Key) → PlainText

More in general, even if we use the same *Key* the function used to decrypt is not necessarily the same used to encrypt. For example, if we consider Caesar's cipher, it is clear that the function that deciphers the message slides the alphabet to the left and not to the right, but decryption uses the same key: number 3.

Some important symmetric key algorithms

DES (Data Encryption Standard)

This historical algorithm, now outdated, uses a 56-bit key that in the late 1970s (when the algorithm was developed) was absolutely adequate for many uses, because a brute force attack on a 56-bit key to get the message with the computing resources available at the time and in the contexts in which that algorithm was used, was impractical. 40 years later the DES algorithm would not last even a few minutes of a home computer. This is a very important aspect: the length of the key is chosen based on the *actual* available computing capabilities. A key that is considered robust enough now may no longer be that strong in 20 years. In general we tend to abound with the length of the key in order to ensure that there is some margin, both because computing capabilities increase, but also because cryptanalysis as a discipline is making progress

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

and may be able to find weaknesses in the algorithm. This is quite an interesting aspect. Contrary to what one might think, normally a cryptographic algorithm does not fail suddenly, i.e. the day a flaw is discovered in an algorithm it instantly turns from secure to completely insecure and anyone can find the plaintext in a moment. What happens is that researchers analyze the algorithm and maybe found small weaknesses that can ease attacking it in certain cases. Then someone possibly founds some algorithm optimization to solve the problem. As time passes the algorithm is gradually weakened due to unsolvable problems, until it is no longer adequate for certain uses or at all. There is a progressive erosion of the defenses of cryptographic algorithms, and this progressive weakening is a more difficult problem to manage, because obviously we cannot know what progress there will be in the future from the point of view of cryptanalysis.

AES (Advanced Encryption Standard, also known by its original name Rijndael)

AES was chosen based not only on robustness, but also on the efficiency of implementation in typical architectures. No secret algorithm was sought because a secret algorithm is not considered more robust than a non-secret one: on the contrary, the algorithm was intended to be analyzed by as many valuable cryptanalysts as possible to ensure that it was intrinsically robust. An algorithm that is safe but too slow, too expensive in terms of computing resources, would be not usable. This constraint was set to be as the most difficult for competitors to overcome, compared to that of robustness.

Asymmetric (or Public Key) Algorithms

Asymmetric algorithms do not use just one key, but two: one key is used to encrypt and the other to decrypt. Therefore, in the exchange of messages, sender and receiver do not use the same key. These keys are generated and managed in pairs: what a key (any of the pair) encrypts can be decrypted only by the other key of the pair.

The reason to use asymmetric algorithms derive from the problems symmetric cryptography has:

1. Confidential communications between 2 entities requires that a unique key be shared between them only, if the entities are n then $n \cdot (n-1)/2$ different keys are required to allow for confidential communication between each pair of the parties
2. Both sender and recipient know their shared key, so *non-repudiation* (repudiation is denying of being the author of a certain message) is not possible

The first problem is not about the number of keys that each subjects has to manage, the problem is *exchanging* them. Each subject must agree on a key with each of the other n-1 subjects, which is actually a complex operation; this makes symmetric cryptography impractical for many uses.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The second problem, the *non-repudiation*, lies in the fact that we often want to make sure that a certain message was actually sent by a certain subject. It is clear that if a subject receives a message from some other subject and the two subjects are the only ones that know the key used to encrypt it, each subject is sure that the other subject is the author of the message. Vice versa, since they only know the key, each subject knows that only the other subject can read the message. The problem appears when there is a need to prove this to a third party, for some kind of litigation, as this mechanism does not work: each party is able to create a message, encrypt it, and then say that the other party is the author. The *non-repudiation* problem is not solvable by using symmetric cryptography.

The asymmetric schema is similar to the symmetric one, but the keys used are the two that are generated in pair:

Encryption: *encryption_function*(*PlainText*, ***Key1***) → *CypherText*

Decryption: *decryption_function*(*CypherText*, ***Key2***) → *PlainText*

The names ***Key1*** and ***Key2*** have been used instead of *EncryptionKey* and *DecryptionKey* because the two keys are mathematically interchangeable. The subject that generates the keys generally keeps one private/secret (called the *private key*) and makes the other public (called the *public key*), hence the name of the algorithm class that is also called the *public key algorithm*. More on the term *public* will be discussed later.

The function used to encrypt is not necessarily the same as the one used to decrypt. The important thing is that together they represent the cryptographic algorithm, one part relies on one key and the other part relies on the other key.

The two keys have such mathematical properties that discovering one key from the other is quite complex and requires an enormous amount of time. In particular, even knowing the public key, the *PlainText* and the *CypherText*, reconstructing the private key would require an unreasonable amount of time.

Asymmetric Algorithm Uses

Suppose (details will be given later) that the *public key* is publicly available and its owner is the sole to know the corresponding private key. Being the public key available to anyone, anyone can use it to encrypt a message, but only the owner of the corresponding private key will be able to decrypt the message, this provides **confidentiality** of the message transmission.

So we have moved from a situation where one subject needed *n* different keys to confidentially communicate with *n* other subjects to a situation where just one key (the receiver's public key) is

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

needed for everyone to send a confidential message to a subject.

In order to allow *n* subjects to communicate to each other, each subject must have a pair of keys, so the total number of keys is 2·*n*. The interesting point is not so much that the keys have decreased in number; but that being public keys these can be communicated in a much more simple way. If someone else gets to know those public keys, it is not a problem at all. Therefore, these keys can be really published, made available to everyone and everyone can use them without weakening the protection of the messages.

If the subject is the only owner of a private (secret) key, whose public counterpart is publicly available, anyone can verify (decrypt) messages encrypted with the private key of the subject. Then if it is possible to use the public key of a subject to decrypt a message, it means that only the subject that has the corresponding private key could have encrypted the message, this provides for the **non-repudiation** of the message.

A problem is still to be solved: ensuring that a public key is really associated to the legitimate subject. Here a *super partes* certification method must be provided, this is provided by a *Public Key Infrastucture* (PKI), discussed later.

As a side note, asymmetric algorithms can also be used as a *challenge-response algorithm*. In order for subject A to *authenticate* (prove that a subject is genuinely who claims to be) subject B, A sends (in the clear) a random number to B; then B encrypts it with its private key and sends it back to A. If A is able to decrypt the message with the public key of B, A is sure that the other party is B, as it is the only one that can encrypt something the public key of B can decrypt.

Advantages and Disadvantages

The total number of keys is significantly decreased, which decreases the complexity of guaranteeing the correct management of all the keys (and only the owner knows the secret key). Since public keys are made publicly available, there is no need for specific agreements between different subjects. This use of public keys is, for example, very important in e-commerce, because e-commerce cannot require that there is an a priori agreement of the seller with customers.

To obtain this link between the two keys and, at the same time, guarantee that one cannot be computed from the other, and that what is encrypted with one is decrypted with the other, make asymmetric algorithms much more complex in terms of mathematical problems than symmetric algorithms. These mathematical problems essentially require slower algorithms than symmetric algorithms and the use of longer keys, at least with the currently used algorithms. Therefore, if on one hand there is a greater flexibility, on the other they are more onerous in terms of computing

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

resources.

Prominent algorithm: RSA *(from the initials of Ronald* ***R****ivest, Adi* ***S****hamir, and Leonard* ***A****dleman)*
This algorithm is based on the complexity of prime factorization: it is easy to multiply two primes and obtain the result, but it is complex/intractable to find the two primes from the result. Prime factorization is a difficult problem. We also know that it is not easy to find very high prime numbers, as there is no rule that allows finding out prime numbers other than to try to factor them and discover if they are prime. This means that working on very large numbers, finding out which are the two prime numbers from which a given number is derived is a problem that requires significant computing resources. On the other hand, legitimate operations can be done with limited computing resources.

Prominent algorithm: Elliptic Cryptography *(ECC - Elliptic Curve Cryptography)*

The "difficult problem" in this case is the computation of the discrete logarithm (in a finite field). A "finite field" means that integers values are in a limited set (very rough definition).

The ECC problem is more complex than prime factorization, so you get the same security with shorter keys. ECC algorithms are faster than RSA.

Comparison of Symmetric and Asymmetric Algorithms
Asymmetric algorithms exploit mathematical problems other than those of symmetric cryptography. This means that the lengths of the keys are not comparable to those of symmetric cryptography. The problem with symmetric encryption is just that the key is long enough to prevent trying all possible numbers that could match a key, so with a 128-bit key there are 2^{128} (that is $3.4 \cdot 10^{38}$) possible keys. Today's symmetrical algorithms typically use 128-, 256- and sometimes
512-bit keys.

If we consider RSA, for example, which exploits prime numbers, it is clear that not all keys are possible, because they are related to the presence of prime numbers. Not all numbers are prime, so not all numbers are possible keys. Very simplifying, to have the same algorithm robustness (therefore the same difficulty from the computational point of view) of a 128-bit symmetric algorithm, the RSA algorithm needs a key of the order of 1024 bits. Today's asymmetrical algorithms typically use 1024, 2048 and 4096 bit keys.

Hash Functions

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Hash functions calculate a short fixed length summary of a text of arbitrary length; this summary is called a *digest*. A hash function must be simple and fast to calculate.

Security properties

Hash functions are "one- way functions" in the sense that it is very complex and slow from the digest to recover a *possible* text that generates it, but this text is hardly useful. This is a consequence of the fact that the original text digest is (and should be) larger than the digest, so virtually infinite sequences of bytes can result in a specific digest. Even if a text is found to have the given digest, it is extremely improbable it is the original text or even makes sense. Building two meaningful messages with the same digest or building a meaningful messages out of a given digest is extremely difficult, any modification of a message, even a single bit, will give a completely different digest (about 50% of its bits are different).

Integrity check

Given a message M, its digest D is computed by means of a hash function H: D = H(M)

A secure transmission of digest D enables to ensure that message M is correct: the receiver of message M calculates the digest on it and compares it with the one (D) received; if they are the identical, the message has not been modified. It is essential that the digest is transmitted in a secure way, otherwise there is no protection at all.

This mechanism is also used as a verification of a downloaded software instead of other less powerful (but faster) algorithms known as CRCs (Cyclic Redundancy Checks), common in network protocols.

Some Important Hash Algorithms

The following are two of the most known hash algorithms.

MD5 (Message Digest #5, 1991)

MD5 requires a low computational power (compared to the majority of the other hash algorithms) and produces a 128-bit hash. Over time it has been gradually weakened to be completely unreliable for security purposes (at present it is possible to find two distinct messages with the same MD5 hash – which is called a *collision* – in seconds), anyway it is still useful in non-cryptographic applications, for example to discover transmission errors instead of the more common (and weak, but faster) CRC-32.

SHA-3 (Secure Hash Algorithm #3, 2015)

SHA are actually a family of secure hash algorithms, SHA-3 is the last version and the result of a competition among cryptographers. The algorithm can be tuned balancing security with speed; it

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

produces hash values of 224, 256, 334 and 512 bits. It is 2-3 times slower than MD5 but no weakness have been found so far.

Signatures (Digital Signatures)

Digital signatures, called electronic signature in the legislation of some countries, take a message, calculate a hash, and encrypt it (just the hash) with the secret key of an asymmetric algorithm. This hash signed with the secret key is called a *signature*. A digital signature then does not encrypt the original message, just allow to guarantee that the corresponding text has not been modified, because otherwise the digest would change. It also guarantees that the origin can be verified (*non repudiation*), as it was actually encrypted with the private key of an asymmetric algorithm. This means that anyone can verify that the text is intact and has actually been generated by a certain subject.

Similar to digital signatures are **Message Authentication Codes** (MACs). They also aim to ensure the integrity and authenticity of a message. The digest is computed hashing the text to be protected and a *symmetric algorithm* key (there is no assurance of non-repudiation, so it is suitable only when this characteristic is not needed). One of the most known algorithm is HMAC: Keyed-hash MAC.

Public Key Infrastructures

The confidentiality, integrity and authenticity requirements of asymmetric encryption and digital signature operations require establishing a relationship of trust between the parties involved. As often the parties had no contact before, a trusted (by them) third party must provide the needed guarantees, in other words this third party must assure the authenticity of the owner of a public key.

A *Certificate Authority* (CA) is a part of a hierarchical trust model that guarantees for the user's identity. It must be recognized as “trusted” by all entities involved in the communication.

In order to assure about the authenticity of a subject, a CA signs a *digital certificate* that links the subject to its public key (it is conceptually similar to an Identity document of a person). The signature applied by the CA is a digital signature, so it is computed by using CA’s private key. Of course, the digital certificate must be validated by using CA’s public key.

A *Public Key Infrastructure* (PKI) is a hierarchical structure of CAs, where every CA has its public key signed by the previous level CA (which uses its private key for this purpose), the process goes up to the *Root Certificate Authority* that self-sign a certificate holding its public key by using its

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

private key.

A hierarchical model allows building hierarchies of any depth. For example, within a Country we could have the municipal, …, regional certification authorities, up to a national root CA.

The root CA certificate must be made public in many locations and ways in order to make it impossible to substitute it with a forged one. As an example, the Operating Systems themselves are shipped with a set of root and trusted intermediate CAs. Figure 1 shows an excerpt of the Root Certificates list from a MS Windows 10 operating system.

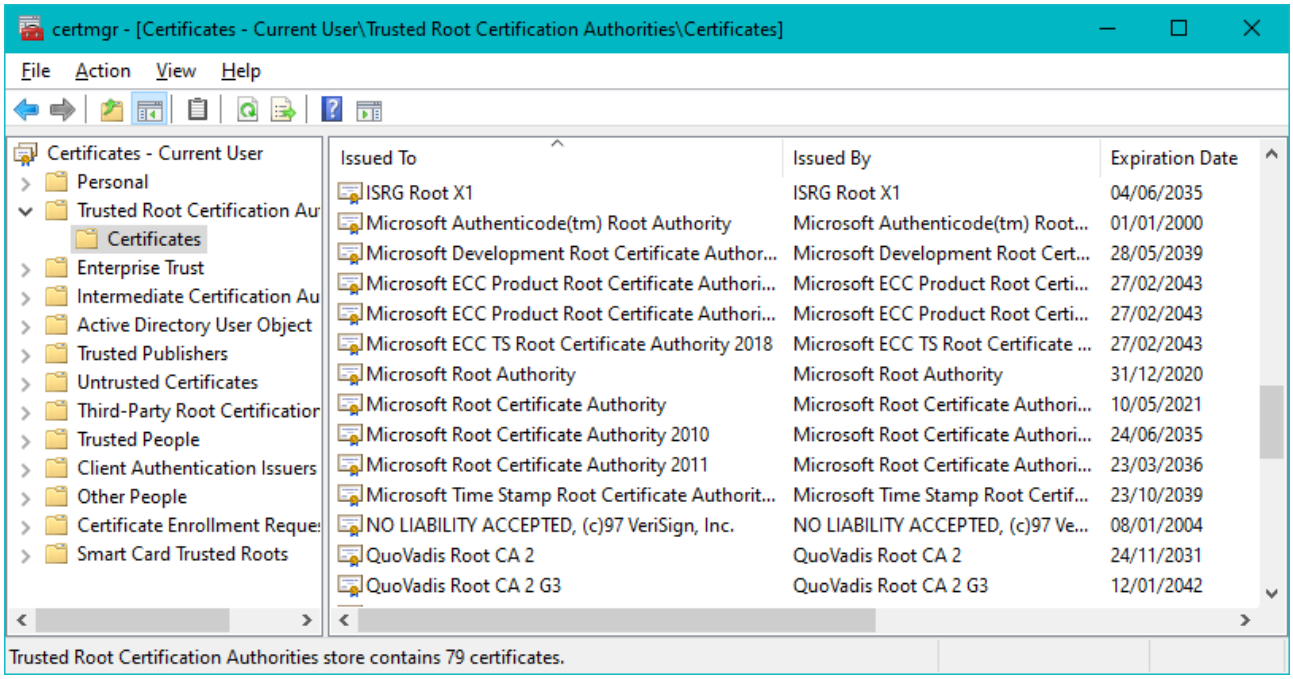


Figure 1. Windows 10 Certificate Manager

Components of a PKI

The main actor is the **Certification Authority (CA)**, it manages the cryptographic keys and certificates of the PKI. It is the component that holds the real keys and that then performs the cryptographic operations. Obviously, in this sense it is also the most critical element of the certification authority.

The **Registration Authority (RA)** manages certificate requests and provides issued certificates. It deals with the distribution of cryptographic tokens and software (it is the front-end of the CA). It is like a counter, for example, to which a citizen can go to request a digital certificate and from which it can be obtained. It can be a physical counter or a website, the type is associated to different levels of security. In addition an RA generally can also assist the user in generating the

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

key pair and managing these certificates securely, for example by providing ad hoc software or hardware tools that support the applicant in generating signatures, encrypting documents, verifying signatures, and decrypting information.

A **Certificate Server** is directory where user certificates are published and in some way made searchable. The directory follows the X.500 standard and is queried by using the LDAP protocol.

The Digital Certificate

The digital certificate structure and format is described by the ITU-T X.509 standard (it is a standard of the International Telecommunication Union numbered X.509).

An X.509 digital certificate must contain at least the following fields:

DN (distinguish name) user: Gaius Julius Caesar

CN (common name): Julius Caesar

O (organization): Government

OU (organization unity): Senate

C (country): Roman Empire

This is the classic pattern of a certificate that meets the X.500 standard, of which X.509 is a member of the family. A certificate can have other attributes (e.g. email). There may be an IP address or a URL that corresponds to an X.500 Directory path (e.g. LDAP – Lightweight Directory Access Protocol):

IT / Roman Empire / Government / Julius Caesar / Gaius Julius Caesar /

An X.509 digital certificate must also contain at least the following fields:

DN Issuer: name of the Authority in X.500 format (the certification authority also has its own distinguished name, which appears in the certificate. Obviously the format with which it is represented is the same as the distinguished name of the subject to which the certificate applies.

Serial Number: serial number of the certificate held by the Authority (each certificate is uniquely identified by the serial number assigned to it by the authority. On the other hand, the pair (*serial number* & *issuer distinguish name*) uniquely identifies a certificate throughout the plethora of certificates that can be issued worldwide as a unique pair).

NotBefore: activation date

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

NotAfter: expiration date

These are two information strictly related to each other. A certificate therefore has a date of beginning of life and an expiration date, beyond which it is no longer valid. The reason derives from the desire to protect the keys from excessive use.

Public Key: the public key of the certified subject (the certificate contains personal data and the public key)

Public Key Algorithm: the algorithm the public key is suitable for

Signature Algorithm: the algorithm used by the Authority to sign the Certificate

Signature: the signature affixed to the Certificate by the Certificate Authority (therefore the element that guarantees the authenticity of the certificate itself)

KeyUsage: the purposes the key can be used for

Generation and Revocation of Certificates

The RFC 2314 standard (from PKCS # 10) defines the format of the *certificateRequest* message and contains the public key and data of the applicant (both given to an RA). The request message requires the so-called *proof of possession* of the private key: the certificateRequest message must be signed with the private key of the applicant. The authority, by verifying this signature substantially verifies that the applicant actually possesses this key (otherwise the applicant would not have been able to produce this signature).

On the date corresponding to the "notAfter" attribute, the Certificate is considered "expired". The expiration is a mechanism that also serves to ensure that the same asymmetric keys associated with the digital certificate cannot be used for an excessive period of time, which could expose them to a series of cryptoanalytic attacks.

The expiration can refer to:

- **the certificate** (the association subject-key)
- **the associated keys**, in relation to the use for which they are intended (a key can be used for certain goals only and not for others)

An expired certificate cannot be used by its owner, since it has expired its use is in practice prohibited. In reality, nothing prevents the holder of the certificate from using it for other purposes but all those who communicate with him will somehow detect that this certificate has expired and will not accept it. The certificate is of course available to verify and decrypt messages issued before expiration. In some cases, it is possible to “renew” a certificate, which is usually not

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

automatic.

Sometimes a certificate can be made invalid prior to expiration through *revocation* (this happens before the "notAfter" attribute value. The reason could be, for example, the key associated with the certificate has been compromised, the subject is no longer associated to the company or changed unit, the CA that issued the certificate (or one of its higher level CAs) has been compromised or other reasons. A revoked certificate cannot be used anymore, except when it is just kept "on hold". This is a particular form of revocation in which the certificate is temporarily inserted in the CRL because of specific reasons (such as "possible key compromise", "request of revocation by a person other than the owner", "temporary non-use of the certificate" e.g. for vacation)", etc. and its validity could be restored later. In case of "reactivation" from suspension, a new entry in the CRL is inserted with a with a special reason code: *removeFromCRL*, as no entry can ever be deleted from the CRL.

To inform the PKI users that a certificate has lost validity, its serial number is listed in a *Certificate Revocation List* (CRL). This list is issued periodically by the issuer Certification Authority and propagated (actively or passively) to all the users, so that all the subjects who have such a certificate can no longer use it. The CRL complies with ITU-T X.509 standard - rfc3280 - rfc4325 which means that its format is standardized. It is signed periodically by the CA and includes a field called the "nextUpdate" which contains the date and time in which the new Certificate Revocation List will be available. If this date belongs to the past it means that our CRL is "expired", if the date belongs to the future we know when we will have to update our list of revoked certificates. Each revoked certificate includes the reason of revocation. The CRL is provided as a service via the LDAP protocol.

As CRLs can become quite large, especially if the certification authority has hundreds of thousands or even millions of users, it can be partitioned and the CA just provides pieces of the Certificate Revocation List, for example referring to a certain period of time. Therefore, when it is necessary to verify a certificate, the citizen downloads the only piece of CRL of interest. Instead of downloading a CRL or a part of it, a service implementing the *Online Certificate Status Protocol* (OCSP - RFC 2560) can be used to find if a certain certificate number is in the CRL. The responses are signed by the CA in order to be trusted

The Chain of Trust

To verify a certificate, a subject must verify all the chain of the intermediate CAs starting from a trusted one, possibly the root CA. First the certificate to check is verified against the issuer CA, then the CA certificate is verified against its parent CA, and so on up to an intermediate trusted (by the user) CA or the root CA itself.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

KeyUsage

Actually, keys can be used for different purposes and a certificate specify the allowed uses, among them we have:

- **nonRepudiation**: the key can be used for producing a signature with legal value which can then be opposed to third parties as a handwritten signature
- **dataEncipherment:** the key can be used to encrypt data
- **keyAgreement:** the key can be used to securely exchange keys

TimeStamping

A PKI can also be used to time stamping a document according to the Time Stamp Protocol (RFC 3161) to prove its existence in a point in the past. A CA will sign the document and includes a temporal mark. The signature also ensure that the document has not been altered after affixing the timestamp. A Time Stamp can extend the validity of an electronic signature beyond the lifetime of the digital certificate associated with the keys used, for example by requesting the affixing of a new time stamp on the contract every year that passes. The affixing will be done every year using cryptographic techniques with a strength adequate for the period in which the signature itself is applied.

Standard Mechanisms and Formats

The following are the two standard mechanism and formats commonly used.

PKCS #7 - Public key cryptography standard #7

PKCS #7 describes the format of messages/files signed, encrypted (with symmetric and asymmetric encryption) and verifiable by MAC (digested data)

S/MIME - Secure Multipurpose Mail Extension

Secure Multipurpose Mail Extension (RFC 3851 - SMIMEv3) is an extension of the MIME standard (RFC 2045, 2046 and 2047 as an extension of RFC 822) and describes the encryption of mail messages. PKCS #7 entities are substantially translated into new MIME entities and therefore describe new containers in which we can find portions of signed or encrypted e-mail messages or signed or encrypted attachments.

Exchange and Storage Formats

The **PKCS #12 (Personal Information Exchange Syntax Standard #12)** defines a format for the exchange and secure storage (on file) of cryptographic keys and digital certificates (trusted certificate chain). Storage is safe because it is based on encryption of both the keys and the

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

certificates, and of the entire chain of certificates a subject chooses to trust. It is the format used by browsers, e-mail clients and operating systems when a user exports a signature and encryption key and a certificate, for example for a backup copy or to copy it to another device.

A PKCS #12 encrypts the data with a symmetrical algorithm whose key is derived from a password provided by the user. It guarantees the integrity of the content through HMAC, or through a digital signature.

The benefits of using PKCS #12 are:

- there are **no implementation costs** as it is a format available in many libraries for many devices (from computers to cellphones)
- they are **already supported by most operating systems** and software, this means that it is immediately available
- it **uses "strong" symmetric algorithms** (the encryption that is applied is a strong, very resistant encryption, so they are keys that resist for example brute force attacks
- it is **portable on different devices**, it is possible to move a file to other devices or copy it to all the devices we use to have the keys always available

There are also some disadvantages:

- **it can be deleted, copied, transmitted**, this is an important problem because it can be stolen, erased, copied to take it away or just made unavailable
- **the private key must be used directly by the signing/decryption software**, this means that the software uses decrypts this file and accesses the key directly, so there is a moment when the key is in the clear on the system, unprotected, although maybe it is just the volatile memory which is the least easily accessible area; however it is available in clear text on the system in some way and this is a very strong limitation of this format
- **it possible to perform a brute force attacks**, for example, in the event that someone steals the PKCS #12 file, they can try all possible passwords in a separate computer system

Cryptographic Tokens

Cryptographic tokens are hardware devices that natively implement encryption algorithms. They do not allow direct access to cryptographic material from outside, they are the only enabled to access and use the key. Moreover, these commands can generally be executed only after the user, and the system on behalf of the user, authenticate to the token, for example by entering a PIN. Tokens can have a small Operating System through which the user requests key generation, encryption and data signature operations. The secure destruction of the token often means not only the cancellation, but also the inability to access the memory areas where the key was

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

written, so to avoid any form of attack that we could not conceive today. The operating system and token hardware can be certified according to specific security standards.

The Challenge-Response Mechanism

A challenge/response mechanism allows two parties to authenticate without exposing useful information on the communication channel. The idea is that one party A "challenges" the other party B to operate on a random number (called *nonce* because it is a number used just one time) with its own key, for example with a One-Way function H. Then B returns H(nonce) to A. If B returns what A expects, A is sure about the identity of B. In the simplest case, B encrypts the nonce with a secret key known to A. A, which has the same key, in turn applies the function to the nonce using the same key, and verifies that the number given to it by B matches the one it calculated.

This is an authentication based on a password that has not been sent over the channel, so it is not possible to trace the key. What makes the mechanism effective is the fact that the random number is different for each session. Since the information read on the channel is different for each session, it is not useful for subsequent authentication. An advantage is that no synchronization is needed (differently from the One-Time-Password mechanism, where it is important to know the starting point of the Pad to use). As it is uneasy to be used by humans, it is typically used in machine-to-machine authentication. A challenge-response mechanism is found in the network authentication mechanisms of ADSL routers to the provider authentication server.

Questions:

In separate file.

Attachments:

Powerpoint in a separate file.

References:

Every topic has its own page on Wikipedia, sometimes already too thorough for the purposes of this course; books are too specialized and are useful only after a very deep training on the specific subject.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Managers Unit-2 Week-3 Unit name: Information security management -1	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other** Streaming Webinar, Text, Self-assessment Exercises, Exercises with answers on discuss forums and be discussed with trainer/mentor
Learning Responsible	• Fatma Gökdemir • Ali Gökdemir
Learning Activity Goals	1. Information security 2. Information security policies 3. Information security roles
Skills to be Gained	• IS 1 • IS 3 • MS 3
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Intermediate computer skills

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
Information security is of great importance in ensuring the continuity of every organization and ensures the protection of the organization's critical information and other information assets in various environments, especially electronic ones. Not only large companies, holdings, but also SMEs, government agencies, any non-profit organization, school or people alone are constantly experiencing information security problems and risks, albeit at different levels. In investments to meet these risks, the most expensive and most complex solution is not always the safest solution. Each person or organization needs to choose and implement the most appropriate and correct solution. It should not be forgotten that while a simple and low-cost security solution may be insufficient for some institutions, the same solution may be sufficient and effective for another institution. However, information security is not a work to be started and finished. Information security management is a life cycle that must be constantly managed and audited as long as institutions and information exist. In this module, the concept of information security, its importance and what should be done for information security will be explained. The subject was supported by a practical example

Content of the Learning Material

1. Information Security

Information security is to prevent unauthorized or unauthorized access, use, modification, disclosure, destruction, replacement and damage to information. It consists of three basic elements called Confidentiality, Integrity and Accessibility (Figure 1). If any of these three basic security elements is damaged, a security vulnerability occurs.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

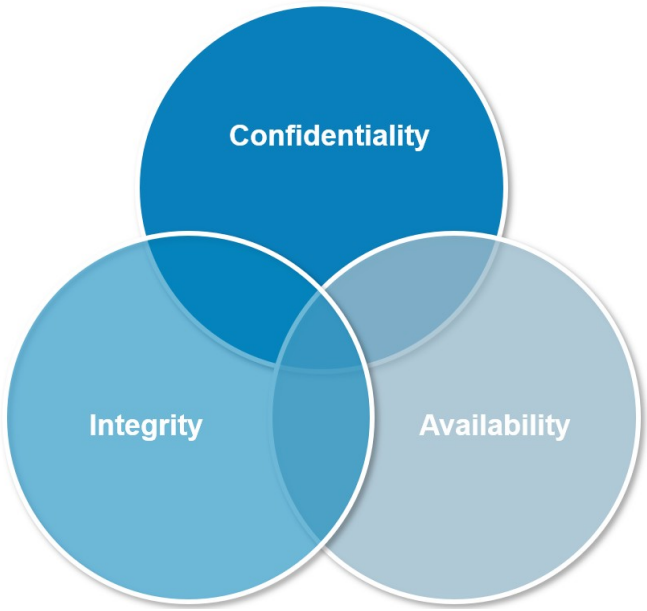


Figure 1. Information security elements

- Confidentiality: It is the protection of information against unauthorized access and unauthorized access.
- Integrity: Information is not changed by unauthorized persons.
- Accessibility: Information is accessible and usable when needed by authorized persons.

1.1. What is an information security policy?

Security threats are constantly evolving, and compliance requirements are becoming increasingly complex. Organizations must create a comprehensive information security policy to cover both challenges. An information security policy (ISP) is a set of rules, policies and procedures designed to ensure all end users and networks within an organization meet minimum IT security and data protection security requirements. An information security policy makes it possible to coordinate and enforce a security program and communicate security measures to third parties and external auditors.

1.2. What is the Purpose of an Information Security Policy?

An information security policy aims to enact protections and limit the distribution of data to only those with authorized access. Organizations create ISPs to:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Establish a general approach to information security
- Document security measures and user access control policies
- Detect and minimize the impact of compromised information assets such as misuse of data, networks, mobile devices, computers and applications
- Protect the reputation of the organization
- Comply with legal and regulatory requirements like ENISA, NIST, GDPR, HIPAA and FERPA
- Protect their customer's data, such as credit card numbers
- Provide effective mechanisms to respond to complaints and queries related to real or perceived cyber security risks such as phishing, malware and ransomware
- Limit access to key information technology assets to those who have an acceptable use

1.3. Why is an Information Security Policy is Important?

Creating an effective information security policy and that meets all compliance requirements is a critical step in preventing security incidents like data leaks and data breaches.

ISPs are important for new and established organizations. Increasing digitalization means every employee is generating data and a portion of that data must be protected from unauthorized access. Depending on your industry, it may even be protected by laws and regulations.

Sensitive data, personally identifiable information (PII), and intellectual property must be protected to a higher standard than other data.

Whether you like it or not, information security (InfoSec) is important at every level of your organization. And outside of your organization.

Information security policies can have the following benefits for an organization:

- **Facilitates data integrity, availability, and confidentiality —** ffective information security policies standardize rules and processes that protect against vectors threatening data integrity, availability, and confidentiality.
- **Protects sensitive data — I**nformation security policies prioritize the protection of intellectual property and sensitive data such as personally identifiable information (PII).
- **Minimizes the risk of security incidents — A**n information security policy helps

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

organizations define procedures for identifying and mitigating vulnerabilities and risks. It also details quick responses to minimize damage during a security incident.

- **Executes security programs across the organization —** Information security policies provide the framework for operationalizing procedures.
- **Provides a clear security statement to third parties** — Information security policies summarize the organization's security posture and explain how the organization protects IT resources and assets. They facilitate quick response to third-party requests for information by customers, partners, and auditors.
- **Helps comply with regulatory requirements** — Creating an information security policy can help organizations identify security gaps related to regulatory requirements and address them.

1.4. What Should be in an Information Security Policy?

An information security policy can be tough to build from scratch; it needs to be robust and secure your organization from all ends. It should cover all software, hardware, physical parameters, human resources, information, and access control. It also needs to be flexible and have room for revision and updating, and, most importantly, it needs to be practical and enforceable. Wishful thinking won't help you when you're developing an information security policy. You need to work with the major stakeholders to develop a policy that works for your company and the employees who will be responsible for carrying out the policy.

1. ***Acceptable Use Policy***

This policy outlines the acceptable use of computer equipment and the internet at your organization. Improper use of the internet or computers opens your company up to risks like virus attacks, compromised network systems, and services, and legal issues, so it's important to have in writing what is and isn't acceptable use.

An acceptable use policy should outline what employees are responsible for in regard to protecting the company's equipment, like locking their computers when they're away from their desk or safeguarding tablets or other electronic devices that might contain sensitive information. It should also outline what the company's rights are and what activities are not prohibited on the company's equipment and network.

2. ***Clean Desk Policy***

A clean desk policy focuses on the protection of physical assets and information. Ideally, this policy will ensure that all sensitive and confidential materials are locked away or otherwise secured when not in use or an employee leaves their desk. This policy should establish the

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

minimum requirements for maintaining a clean desk, such as where sensitive information about employees, intellectual property, customers, and vendors can be stored and accessed. It should also cover things like what kinds of materials need to be shredded or thrown away, whether passwords need to be used to retrieve documents from a printer, and what information or property has to be secured with a physical lock. In addition to being a common and important part of any information security policy, a clean desk policy is ISO 27001/17799 compliant and will help your business pass a certification audit.

3. ***Data Breach Response Policy***

This is also known as an incident response plan. The purpose of a data breach response policy is to establish the goals and vision for how your organization will respond to a data breach. This plan will help to mitigate the risks of being a victim of a cyber-attack because it will detail how your organization plans to protect data assets throughout the incident response process.

This policy should define who it applies to and when it comes into effect, including the definition of a breach, staff roles and responsibilities, standards and metrics, reporting, remediation, and feedback mechanisms.

4. ***Disaster Recovery Plan Policy***

This policy is different from a data breach response plan because it is a general contingency plan for what to do in the event of a disaster or any event that causes an extended delay of service. This policy should describe the process to recover systems, applications, and data during or after any type of disaster that causes a major outage. This disaster recovery plan should be updated on an annual basis.

The contingency plan should cover these elements:

- Emergency outreach plan. Explicitly list who needs to be contacted, when do they need to be contacted, and how will you contact them?
- Succession plan. Describe the flow of responsibility when normal staff is unavailable to perform their duties.
- Data classification plan. Detail all the data stored on all systems, its criticality, and its confidentiality.
- Criticality of service list. List all the services provided and their order of importance.
- Data backup and restoration plan. Detail which data is backed up, where, and how often. Also explain how the data can be recovered.
- Equipment replacement plan. Describe which infrastructure services are necessary to resume providing services to customers.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- Public communications. Document who will own the external PR function and provide guidelines on what information can and should be shared.
- It's important that the management team set aside time to test the disaster recovery plan. During these tests, also known as tabletop exercises, the goal is to identify issues that may not be obvious in the planning phase that could cause the plan to fail. This way, the team can adjust the plan before there is a disaster takes place.

5. *Email Policy*

Email is a critical communication channel for businesses of all types, and the misuse of email can pose many threats to the security of your company, whether it's employees using email to distribute confidential information or inadvertently exposing your network to a virus. It's important for all employees, contractors, and agents operating on behalf of your company to understand appropriate email use and to have policies and procedures laid out for archiving, flagging, and reviewing emails when necessary.

This policy needs to outline the appropriate use of company email addresses and cover things such as what types of communications are prohibited, data security standards for attachments, rules regarding email retention, and whether the company is monitoring emails. This policy should also be clearly laid out for your employees so that they understand their responsibility in using their email addresses and the company's responsibility to ensure emails are being used properly. This email policy isn't about creating a "gotcha" policy to catch employees misusing their email, but to avoid a situation where employees are misusing an email because they don't understand what is and isn't allowed.

6. *End-User Encryption Key Protection Policy*

Certain documents and communications inside your company or distributed to your end users may need to be encrypted for security purposes. Have a policy in place for protecting those encryption keys so they aren't disclosed or fraudulently used.

This policy should outline all the requirements for protecting encryption keys and list out the specific operational and technical controls in place to keep them safe. This includes things like tamper-resistant hardware, backup procedures, and what to do in the event an encryption key is lost, stolen, or fraudulently used.

7. *Password Protection Policy*

Your employees likely have a myriad of passwords they must keep track of and use on a day-to-day basis, and your business should have clear, explicit standards for creating strong passwords

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

for their computers, email accounts, electronic devices, and any point of access they have to your data or network.

This policy also needs to outline what employees can and can't do with their passwords. It might seem obvious that they shouldn't put their passwords in an email or share them with colleagues, but you shouldn't assume that this is common knowledge for everyone. Give your employees all the information they need to create strong passwords and keep them safe to minimize the risk of data breaches.

Finally, this policy should outline what your developers and IT staff need to do to make sure that any applications or websites run by your company are following security precautions to keep user passwords safe.

Research conducted in the last decade around the world shows that the most preferred passwords of users are as follows:

- 123456
- password
- qwerty
- 111111
- 123123
- 987654321
- 123456789
- asdfgh

Despite annual warnings, this list has not changed much. For this, users are advised to follow a set of passwords setting rules. These rules are listed below:

- Setting complexity requirements, such as meeting the minimum character requirement
- Not choosing previously used passwords
- Changing passwords periodically and perhaps frequently
- The passwords used should not be chosen from common and weakly used passwords as in the list above

The National Institute of Standards and Technology (NIST) aimed to solve the problem of password policies to determine passwords and achieve certain standards. NIST sets out details about passwords and how they should be managed and stored. Accordingly, possible passwords should be checked against a list of commonly used and known values. Considerations for determining passwords are as follows:

- User-supplied passwords should consist of at least eight alphanumeric

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

characters.

- They should not be passwords obtained from previous breaches.
- There should be no dictionary words.
- There should be no dates between 1900-2020, such as birth dates.
- No repetitive or sequential characters (e.g. aaaaaaaa or 1234abcd)
- Words specific to the intended use, such as the name of the service, username and derivatives thereo should not be.

The above criteria should be taken into account when determining passwords and passwords with complex structures should be created.

Password complexity : Password complexity is defined as the number of passwords that are strong for a password we mean that it meets a set of rules. The key to password complexity The rules are as follows:

- The password cannot contain the account name or variations of the account name.
- The password must contain both uppercase letters (A-Z) and lowercase letters (a-z).
- Special characters **(~! @ # $% ^ & * _- + = `| \ () {} [] :;" '<>,.? /)** (These are the characters that usually appear with the ALT key. However, currency such as Euro symbols do not count as special characters).
- The minimum number of characters must be respected. This value varies from system to system, user to user. may change.

The minimum password length should be 8 characters, while the recommended character is is 12.

When passwords are created with at least 8 characters according to the rules listed above, this means at least 218,340,105,584,896 different possibilities for a single password. The probability of the generated password makes a brute force attack very difficult, but the password is still not impossible to crack. For a password that is close to impossible to crack, it is necessary to increase the number of password characters. The higher the minimum number of characters, the longer it takes to crack the password.

In addition to the benefits of password complexity, it also brings some challenges. One of the main ones is forgetting the password. It is difficult to remember a password that is longer and contains special characters. Especially when all the passwords are different, it is difficult to remember and not confuse them with others. Therefore, a certain logic should be followed when creating passwords.

For example;

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

- I am the 2nd child in a family with 3 children!

You can write a sentence like this based on your own real life. When you take the first characters and special characters of the sentence, you get a password like **Iat2ciafw3c!**

- I Became A Member of This Website (about education) on July 19.

You can customize a sentence like "I became a member of this website (about education) on July 19th according to the area of interest of the website and the date of membership, so that you do not forget it. When you get their first character and special characters
You will get a password like **IBAMoTW(ae)oJ19.**

8. Security Response Plan Policy

A security response plan lays out what each team or business unit needs to do in the event of some kind of security incident, such as a data breach. According to the SANS Institute, it should define, "a product description, contact information, escalation paths, expected service level agreements (SLA), severity and impact classification, and mitigation/remediation timelines."

The key to a security response plan policy is that it helps all the different teams integrate their efforts so that whatever security incident is happening can be mitigated as quickly as possible. While each department might have its own response plans, the security response plan policy details how they will coordinate with each other to make sure the response to a security incident is quick and thorough.

1.5. Information Security Policy Examples

In order to create a successful cyber security plan, 5 main issues need to be considered.

a. ***Identify:*** The organization should have an understanding of the cybersecurity risks it faces so it can prioritize its efforts.

b. ***Protect***: This is about putting appropriate safeguards in place to protect data assets and limit or contain the impact of a potential cybersecurity event. This includes educating and empowering staff members within the organization to be aware of risks, establishing procedures that focus on protecting network security and assets, and potentially utilizing cyber liability insurance to protect a company financially in the event a cybercriminal is able to bypass the protections that are in place.

c. ***Detect***: Outline the activities that assist in discovering the occurrence of a cyber

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

attack and enable timely response to the event. In order to quickly and efficiently diagnose a cyber attack, companies should implement data classification, asset management, and risk management protocols that alert them when data appears to be compromised.

d. ***Respond***: Document the appropriate actions that should be taken following the detection of cybersecurity threats. A company's response should include proper and thorough communication with staff, shareholders, partners, and customers as well as with law enforcement and legal counsel as needed.

e. ***Recover***: Determine how an organization can recover and restore any capabilities or services that were impaired due to a cyber attack.

Almost every security standard must include a requirement for some type of incident response plan because even the most robust information security plans and compliance programs can still fall victim to a data breach.

1.6. Exercises of Information Security Policy

1. Lock your session: Strengthen your online accounts by activating the strongest authentication tools available, such as biometrics (a person's measurable biological traces), security keys, or a unique one-time code generated by an application tool on your mobile device. Your usernames and passwords may not be sufficient to protect accounts such as e-mail, banking and social media.

Exercises-1:

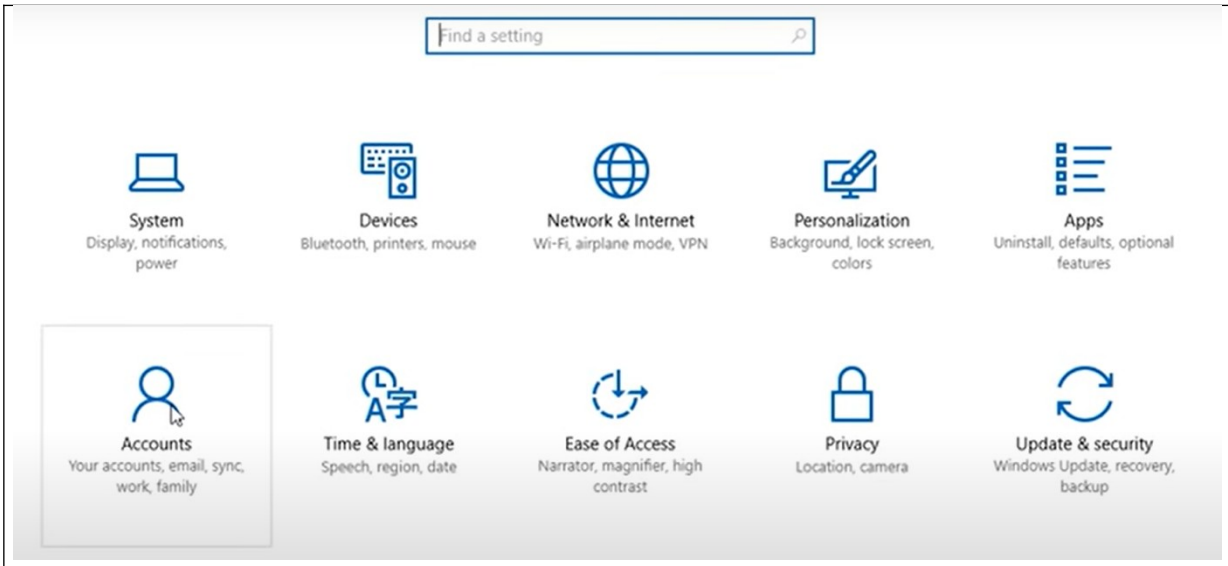
To have the computer lock automatically when you get up from the computer.

Step-1: Click the Windows Settings button.

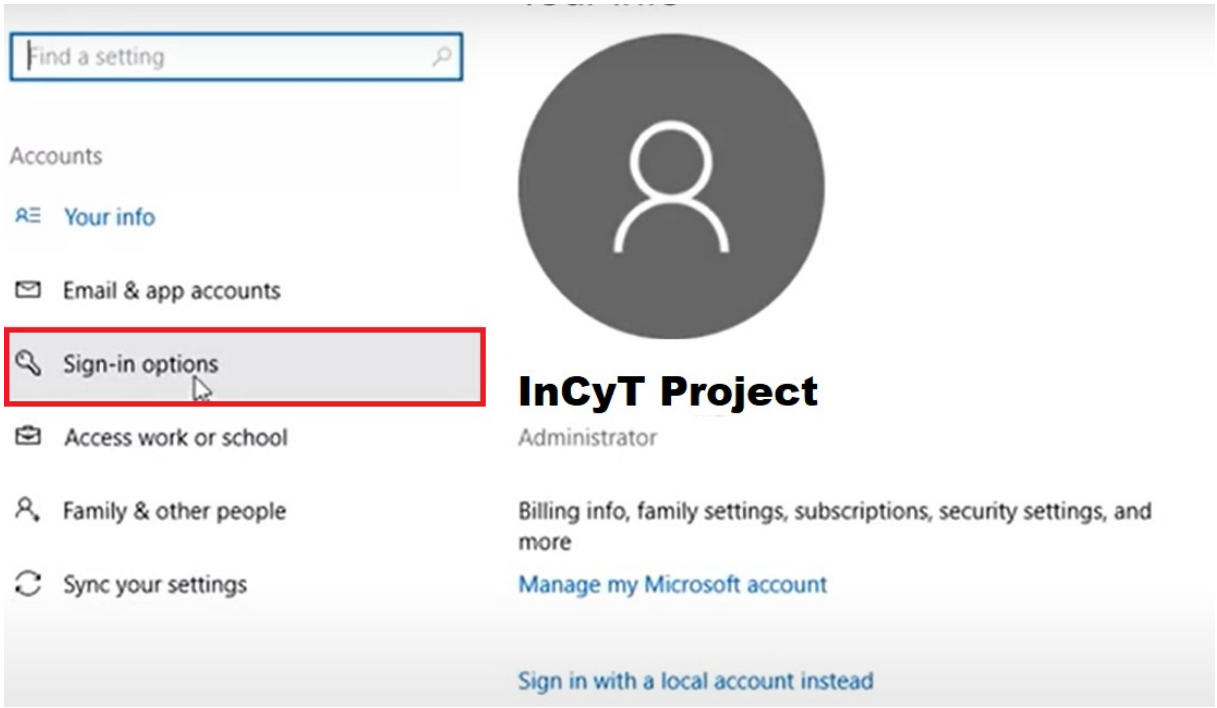
Step-2: Click the Accounts tab.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



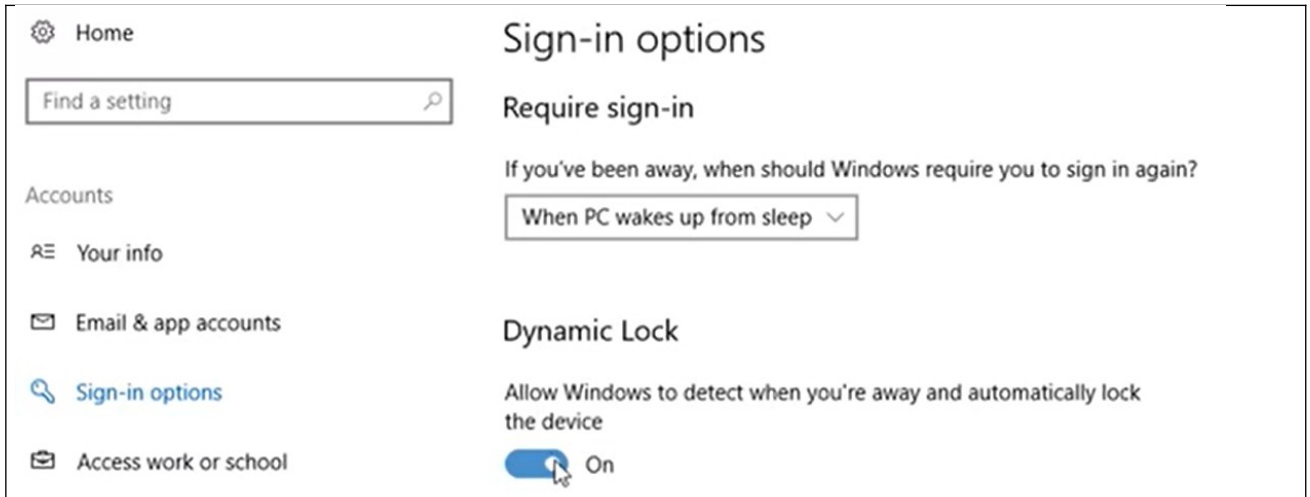
Step-3: Click on Sign-in section.



Step-4: Enable to the Dynamic Lock speficication.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



2- Create a strong password: Password has an important place in information security. Weak passwords can be solved in a short time with password cracking programs. For this reason, it is necessary to take the utmost care by considering the following rules when creating and using passwords on all devices and accounts. The password is generally used in many places in computer systems. We use a password when creating an e-mail account, setting a password on the computer log in, and prohibiting access to files. However, passwords should not be weak or guessable. Passwords should be created according to the following criteria:

a. Passwords must be at ***least 8 characters*** long and contain at least one uppercase letter, one lowercase letter, one number, and one special character (.-+=_,!@$#* %<>[]{}).
b. The password field ***should not be*** left blank or default; ***123456, 01062022, qwerty, password etc.*** it should not be determined in such a way that it is predictable and easily broken like words that can be found in any dictionary.
c. Passwords should **not contain personal information** (your child's name, date of birth, or institution name).
d. ***Different passwords*** should be created for different systems and accounts.
e. Passwords should be ***changed*** frequently (at least every 6 months).
f. Passwords should ***not be written*** in places that can be noticed by other people (such as leaving them next to the computer by writing on paper) and should not be stored in clear text without encryption on a computer or in any digital medium.
g. No staff or student should ***share*** their password (e-mail password, e-signature password, PC password, etc.) with another person. Users should know that all legal responsibility that may arise in case of sharing will belong to him.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

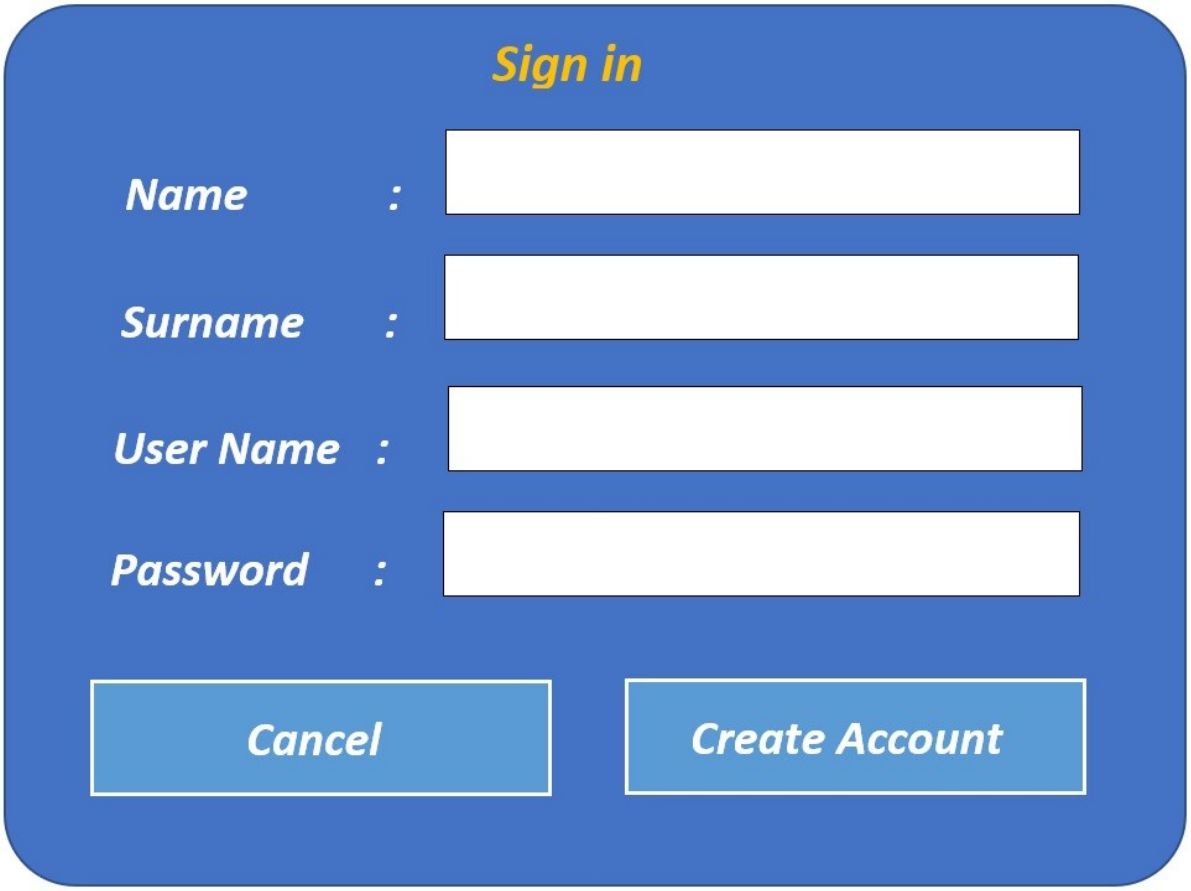
h. Unique account, unique password: Having a separate password for each account helps thwart cybercriminals. At the very least, separate your work and personal accounts and make sure your critical accounts have the strongest passwords.
i. Remember and keep it safe: Strong passwords are difficult to create and remember. Set your passwords in a way that is meaningful and memorable only to you, or keep them in a safe place and format. Alternatively, you can use a service such as a password manager to keep track of your passwords.

Exercises-2:

Password security when creating an email account through your corporate email service provider or a public email service provider's application or website

Step-1: Open the website or application.

Step-2: Enter your personal information to create an account.



Step-3: When creating a password, use uppercase, lowercase, digit, symbol combinations

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

together.

Some coding can be done to make the password easy to remember by the user. For example, you can write a sentence suitable for the subject and use the first characters, numbers, and special characters of the sentence you wrote.

This cybersecurity project is supported by Erasmus+ 2021

Step-4: We set our password; TcpisbE+2021

Step-5: Make sure that the password consists of at least 8 characters. 12 characters are preferred. It can be said that the password we use is suitable because it has 12 characters.

3- Access to secure sites (Safe Browser): When you go online to shop or read news, you are using a browser. Browsers are one of the primary ways to interact with the Internet. As a result, browsers are primary targets for cyber attackers. Always use the latest version of your browser and keep your security shield strong against browser attacks. Updated browsers have the latest security patches and are much harder for cyber attackers to exploit. Not sure if you have the latest browser update? Contact the Technical Support Team or the Information Security Team to verify. Stay safe online by not connecting to websites when you receive a warning from your browser. Modern browsers can recognize certain malicious websites that are designed to harm. If your browser notifies you that the website you are about to visit is dangerous, close that web page and try to find the information you are looking for on a safer website. Before sending sensitive information online, for example when sending your credit card information for online shopping, make sure your browser is using HTTPS, which is a sign of encryption. Encryption mixes the information transmitted between your computer and the destination so that only the authorized website can read it. For a secure connection, look for encryption marks such as the website address that starts with HTTPS and a padlock icon in the status bar.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

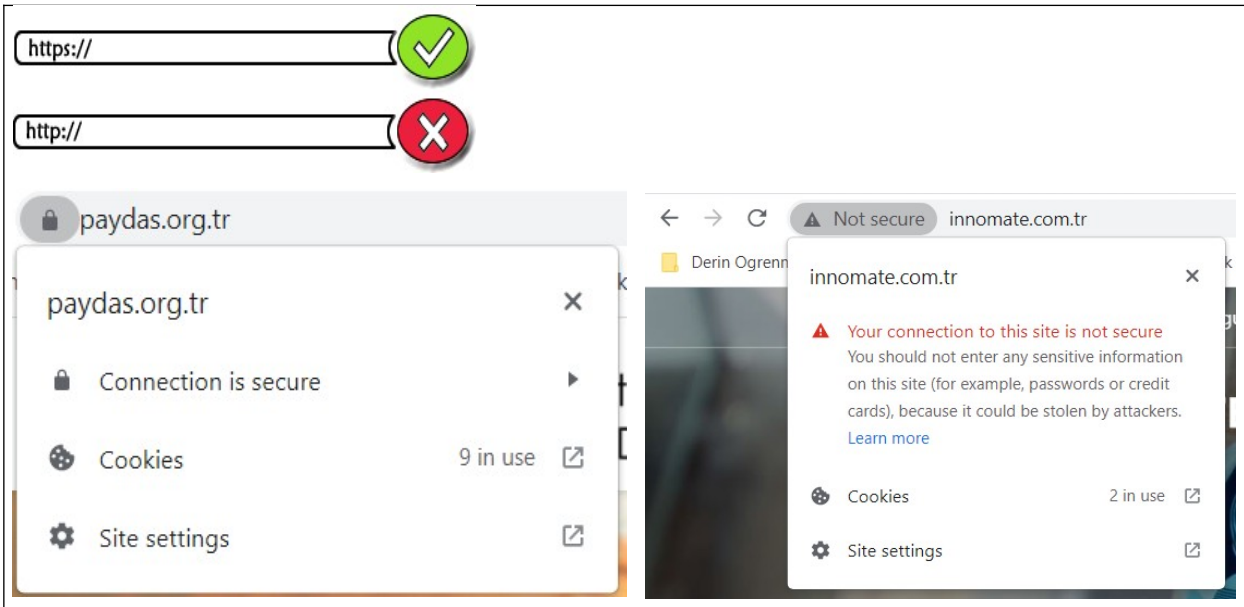


Figure 2. Secure and Not secureweb sites

Add-ons; are small pieces of software added to browsers that are used for additional features such as playing games, watching movies, or editing text. Every add-on installed in your browser potentially adds additional security vulnerabilities. If you absolutely need them and only with prior approval, install the add-ons in your browser. Once installed, always use the latest version of the plugin, just like in your browser. Finally, after you've finished visiting a website, make sure you're logged out. This removes sensitive login and password information before closing the browser. Remember, your safe browsing behavior and security shield are strengthened.

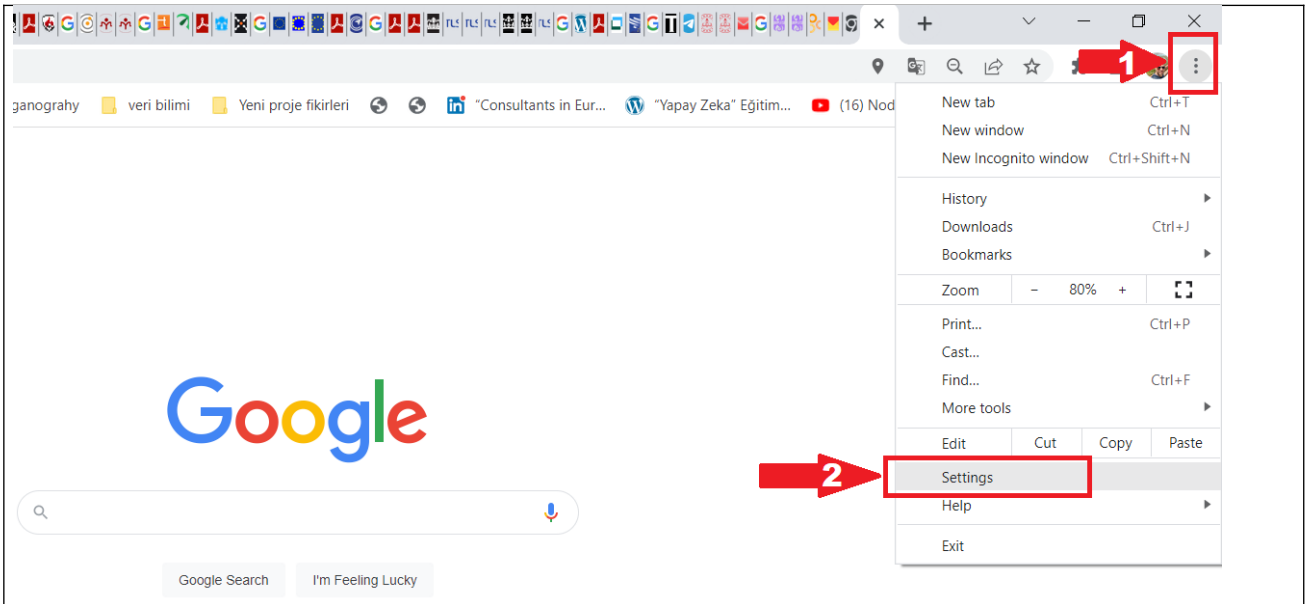
Exercises-3:

Follow the steps below to edit plug-ins in the web browser.

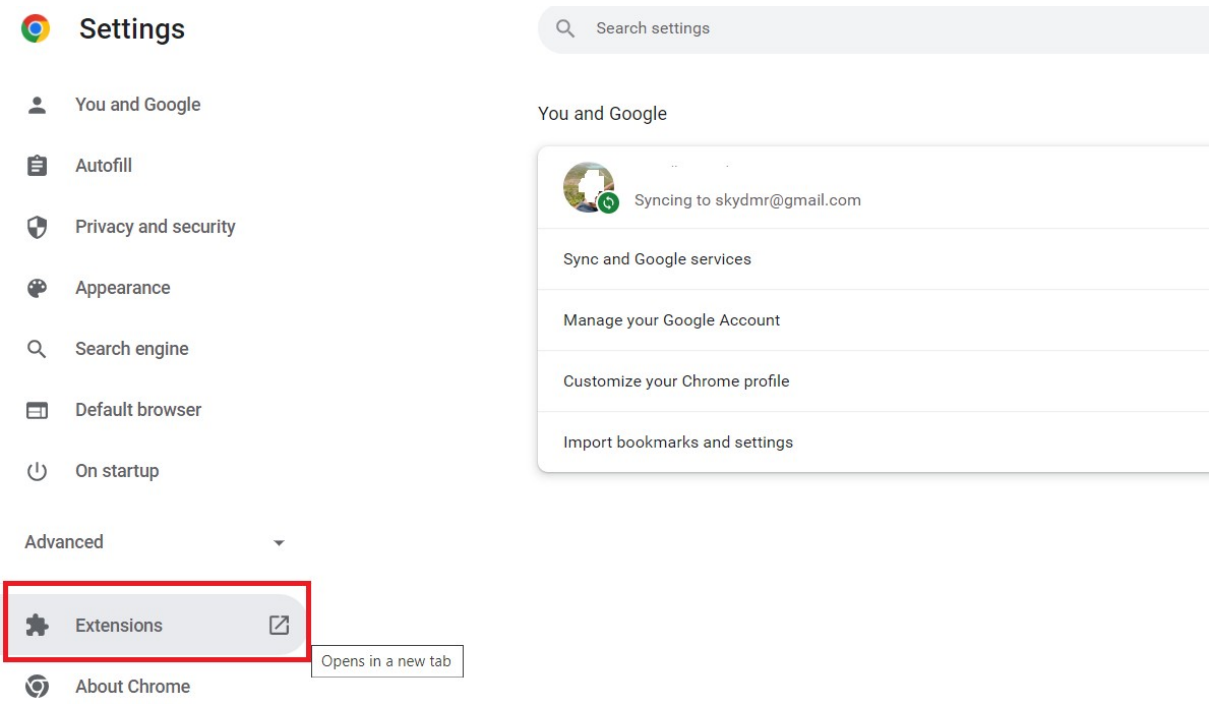
Step-1: Open your web browser and click the “Costume and Control…” button in the upper left corner (1). Click on the “Settings” tab from the drop-down menu (2).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



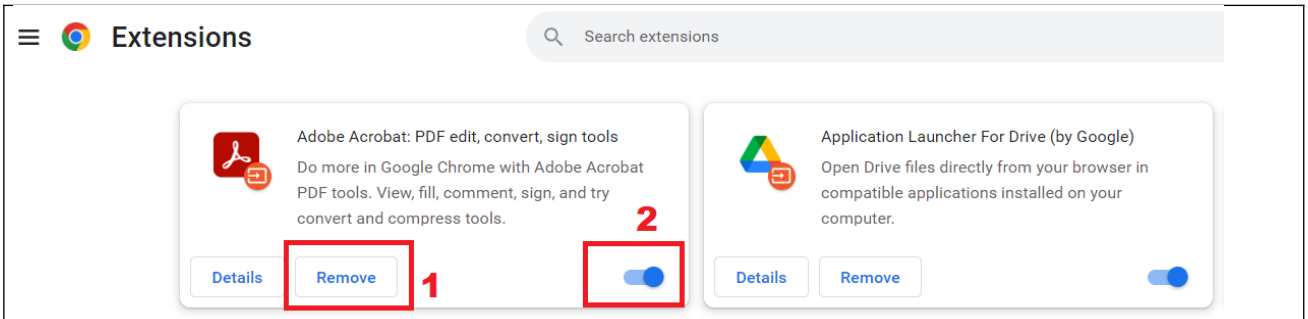
Step-2: Click the "Extensions" button in the window that comes up.



Step-3: You can see the add-ons installed on your browser on this screen. If you want to delete the add-on, you can delete it (1) by pressing the “Remove” button. If you want the plugin to remain inactive, you can deactivate it from the "On-Off" button (2).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



4. Email, Messaging, and Phishing: Have an email in your inbox or a message on your phone. "There is a problem with your account and your account should be updated immediately. All you must do is click a link." When you get a message with content, stop, and think before you click! "Phishing" is a social engineering attack that uses emails or messaging as bait, like using bait for fishing. Cyber attackers send thousands of emails in hopes that someone will take the bait. Emails prompt you to take an action, such as clicking a link, opening an attachment, or filling out a form. Cyber attackers aren't sure exactly who will receive these emails but performing one of these seemingly harmless actions could get you hooked. A more sophisticated form of phishing called "Spear phishing" targets specific individuals. For example, when everyone in our organization receives a generic phishing email regarding an undelivered package; like five people in our purchasing unit being targeted with a fake invoice request. How do we know if an email or message is a phishing attack?

Some signs to look for:

- Messages beginning with "Dear Customer" or other general greeting entries.
- Messages that require immediate action or create a sense of urgency, such as threatening to close your account.
- Messages that claim to be from an official organization but have grammatical or spelling mistakes or use a personal email address such as @gmail.com, @yahoo.com, or @hotmail.com.
- Any message that asks for highly sensitive information, such as your credit card number or password. Be suspicious of such messages. If someone you know, such

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

as a coworker, sends you a message that requires urgent action, reach out through different channels to verify that it is really him who sent you, for example by phone call Try to confirm if the message is his.

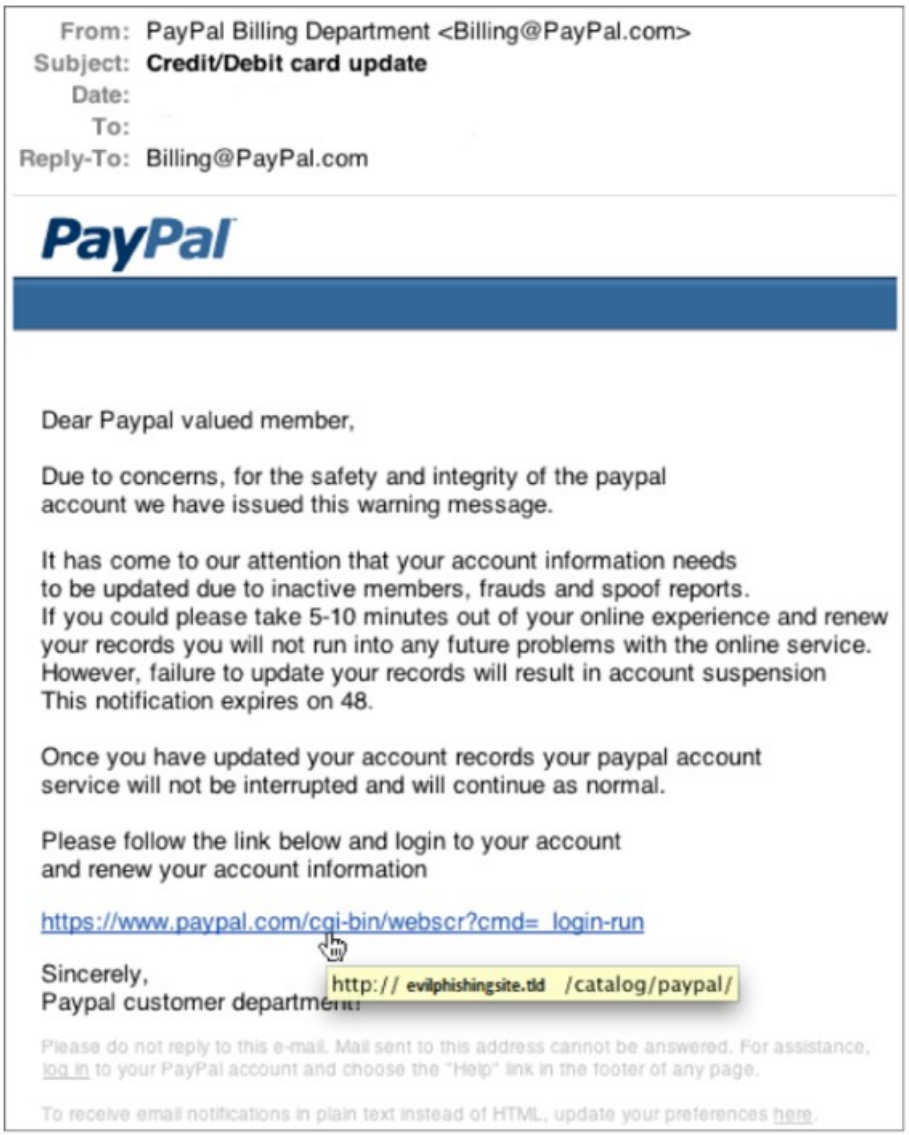
Remember, it's very easy for a cyber attacker to create an email that looks like it came from a friend or colleague. To be safe, you should always take these precautions when using email or messaging. Hover your mouse over a link before clicking it. This will display the true destination of the link so you can confirm that you've been redirected to a legitimate website. Even better is to type the website address directly into your browser. For example, if you receive an email from your bank asking you to update the account details, ignore the emailed link. Simply type your bank's website address in your browser and log in as usual. When messages have attachments, only open attachments that you expect. Because antivirus solutions may not detect all versions of malware, you are the best defense we have against infected attachments. When using e-mail or messaging, be careful not to accidentally reveal important information. Email features like autocomplete make it easy to unintentionally send email to the wrong person. For example, when you want to send an e-mail to someone working in your unit, you may accidentally send an e-mail to a friend with a similar name working in another unit. Remember that once an email is sent it is out of your control.

Samples of the Phishing

Sample-1: In this example, the email looks like it was sent from PayPal.com, but is sent through a fake server. If we look only at the web address to which it is directed, without clicking on the given link, we can detect that it is an e-mail harvested by an attacker who wants to obtain credentials.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

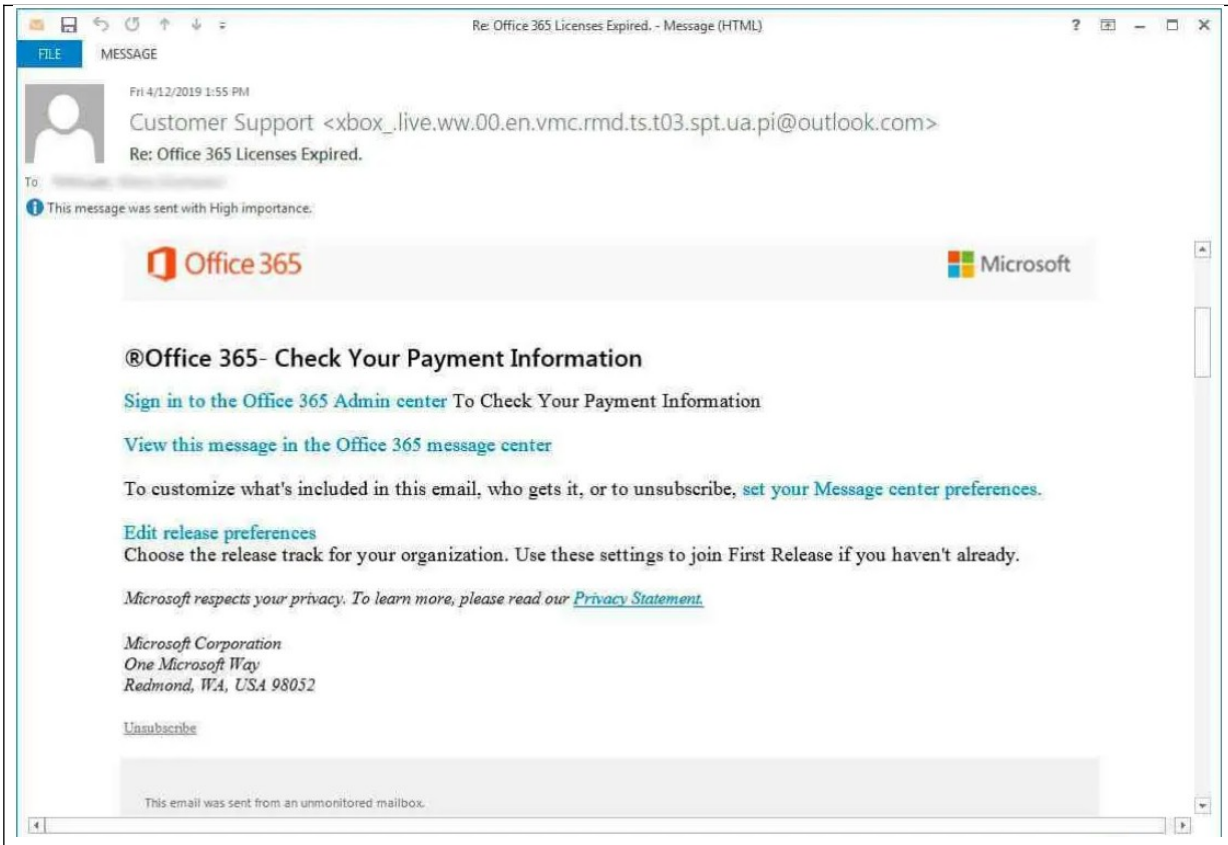
Co-funded by the Erasmus+ Programme of the European Union



Sample-2: In this example, an incoming email is an example indicating that an organization's Office 365 licenses have expired. The mail then keeps telling the user to login to Office 365 Admin Center to check their payment information.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union



However, when the sender e-mail address is carefully examined, it should be noted that such an address will not exist. In short, it is obvious that this email was not sent by Office365.

5. Social networks

Social networking sites help us share information and communicate with others. Unfortunately, these sites also make it easier for cyber attackers to track you down and learn what you're doing. Protect yourself by protecting each account with a strong, unique password. Better still, use a different password for each account and use two-factor authentication if available. Many social networking sites also support third-party apps. Only install apps you need from trusted sources and only. Check any app's rating, comments, and permissions before installing it. If you no longer need an app, uninstall it or disable its access to your social networking profile.

Just like email and messaging, cyber attackers can try to scam you on social networking sites. He can send messages pretending to be your friend. If you receive a strange or suspicious message from a friend, contact them via email or phone, not by replying to the message. Finally, to

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

protect our Institution, do not post any confidential information about our Institution on any website. If you have any questions about what you can post or share about the job, please ask your supervisor.

After enabling two-factor authentication (verification), a security code will be sent to your phone or authentication app every time you log into your account from a new device or browser. You have to enter this code and you will be allowed to login. If a cybercriminal tries to log into your account, they cannot do so if they do not have access to your mobile phone. You will also be able to notice an attempt to log into your account as you will receive a notification with a code. Never share this code with others! An attacker will try to take it. If you received the code but did not try to log in, delete the code message and change your password as soon as possible.

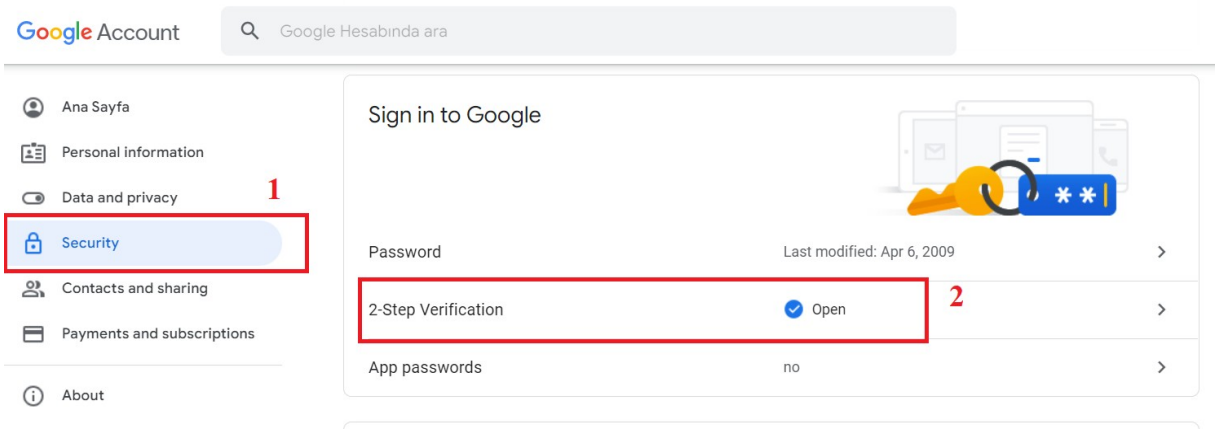
Exercises-4:

Perform two-factor authentication- verification to access the email account you created. The first of these processes is the password you use to access the account. The other can be a verification code (SMS) to be sent to your phone or a confirmation link to be sent to another email address.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

The screenshot below shows how to activate the two-factor authentication feature of the Gmail account.
Complete the process and try to access your email account again.

Step-1: Open your Google Account.
Step-2: Click to the “Settings” section.
Step-3: Select the "Security" tab from the menu on the left side of the page that opens (1). Then activate the "2-Step Verification" feature in the middle of the page.



1.7. Best practices for successful information security policies

1. **Information and data classification:** Can make or break your security program. Poor information and data classification may leave your systems open to attacks. Additionally, lack of inefficient management of resources might incur overhead expenses. A clear classification policy helps organizations take control of the distribution of their security assets.
2. **IT operations and administration:** Should work together to meet compliance and security requirements. Lack of cooperation between departments may lead to configuration errors. Teams that work together can coordinate risk assessment and identification through all departments to reduce risks.
3. **Security incident response plan:** Helps initiate appropriate remediation actions during security incidents. A security incident strategy provides a guideline, which includes initial threat response, priorities identification, and appropriate fixes.
4. **SaaS and cloud policy** — provides the organization with clear cloud and SaaS adoption guidelines, which can provide the foundation for a unified cloud ecosystem. This policy

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

can help mitigate ineffective complications and poor use of cloud resources.

5. **Acceptable use policies (AUPs):** Helps prevent data breaches that occur through misuse of company resources. Transparent AUPs help keep all personnel in line with the proper use of company technology resources.
6. **Identity access and management (IAM) policy:** Outlines how IT administrators authorize systems and applications to the right employees and how employees create passwords to comply with security standards. A simple password policy can reduce identity and access risks.
7. **Data security policy:** Outlines the technical requirements and acceptable minimum standards for data security to comply with relevant laws and regulations
8. **Privacy regulations**: G overnment-enforced regulations such as the General Data Protection Regulation (GDPR) protect the privacy of end users. Organizations that don't protect the privacy of their users risk losing their authority and may be fined.
9. **Personal and mobile devices policy:** Outlines if employees are allowed to use personal devices to access company infrastructure and how to reduce the risk of exposure from employee-owned assets. Nowadays, most organizations have moved to the cloud. Companies that encourage employees to access company software assets from any location, risk introducing vulnerabilities through personal devices such as laptops and smartphones. Creating a policy for proper security of personal devices can help prevent exposure to threats via employee-owned assets.
10. **Remote access policy**: Outlines acceptable methods of remotely connecting to internal networks
11. **Email/communication policy**: Outlines how employees can use the business's chosen electronic communication channel such as email, slack or social media
12. **Disaster recovery policy**: Outlines the organization's cybersecurity and IT teams input into an overall business continuity plan
13. **Business continuity plan (BCP):** Coordinates efforts across the organization and is used in the event of a disaster to restore the business to a working order
14. **Incident response (IR) policy**: An organized approach to how the organization will manage and remediate an incident
15. **Change management policy**: Refers to the formal process for making changes to IT, software development and security

Questions:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

1- Which is not one of the information security elements?

A) Confidentiality

B) Integrity

C) Vulnerability

D) Accessibility

2- Which of the following is not one of the institutions that determine information security policy?

A) ENISA

B) IPA

C) GDPR

D) NIST

3- Which of the following advantages does not directly have information security policies for an organization?

A) Protecting sensitive data

B) Minimizing the risk of security incidents

C) Providing a clear statement of security to third parties

D) Reducing the working hours of employees

4- Which of the following is not included in information security

A) Hardware Policy

B) Email Policy

C) Disaster Recovery Plan Policy

D) Password Protection Policy

5- Which of the following would be an example of a well-defined password?

A) 20220829

B) InCyT#2021!

C) Erasmus+

D) 123456!

6- Which of the following is not one of the measures to be taken for information security?

A) Prefer https web pages

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

B) Using a strong password

C) Visiting links of unknown origin

D) Watching at the computer screen for a maximum of 8 hours a day

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- ***Why is an Information Security Policy is Important?***

- ***Explain the password Protection Policy***

Attachments *(PowerPoint presentation, handouts, prints, links, video…):*

References:

http://bid.ankara.edu.tr/2018/10/02/siber-guvenlik-farkindaligi/
https://purplesec.us/resources/cyber-security-policy-templates/#Email
http://ix-one.com/domainhostingFAQ/article/MS_27805.html
https://www.siberguvenlik.web.tr/index.php/2019/07/22/kimlik-avcilari-sahte-yonetici-uyarilari-ile-office-365-yoneticilerini-hedefliyor/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Module

Information Security for Employees **Unit 2 Week 4** **Unit name: Malware and Most Common Attacks**	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	Claudio Fornaro
Learning Activity Goals	1. Introduction to the various types of malware 2. Knowledge of the most common types of attacks
Skills to be Gained	• Basic knowledge about what is malware and the most common attacks to computer systems Soft Skill 2 - SS2
Duration of Learning activity	1 week
Learning requirements	***What is needed?*** • No previous specific knowledge is required

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

When it comes to malware, the name already implies something malicious. This term generally refers to software designed intentionally to cause damage of various kinds, in particular (but not limited to): blocking of services and communications, interception of transmissions, theft of private information (personal, corporate or government) and of personal identities, unauthorized access to information or systems, deprivation of users of access to information.
After an introductory part, the fundamental concepts of malware are outlined, along with the description of the main types, the risks that they entail and how these can be mitigated.
The second part of the module intends to offer an overview of the most common attacks that a system can suffer, this list being by no means complete as new types of attacks are discovered every day. These attacks are attempts to gain access to a computer system or disrupt its services. The description starts from the most common and easiest attacks (Phishing) to more complex ones: Password Attacks, Buffer Overflow, SQL Injection, Cross-site Scripting (XSS), Cross-Site Request Forgery (CSRF), File Related Attacks, Denial of Service (DoS) and Distributed Denial of Service (DDoS), Man in The Middle (MITM), ARP Spoofing or ARP Poisoning, DNS Spoofing, Drive-by Attacks,
Credential Reuse, Web Session Hijacking, TCP Session Hijacking, IP Spoofing, Zero-day Exploits, and the consequences of Leak of Code.

Content of the Learning Material

In computer science, "hacker" and "cracker" are two terms that are used to indicate people with a great knowledge of computer systems. The main difference between the two lies in the attitude with which they act. A **hacker** (the term was born in the second half of the 1900s at the MIT) acts by exploring systems in order to better understand how they work and trying to discover new flaws in order to solve them and therefore increase the security of a system. Some actions can only be demonstrative or for ethical reasons, but never for profit. A **cracker**, on the other hand, uses his abilities illegally trying to break into systems to profit by stealing data or in a destructive way.

Hackers are constantly trying to acquire new knowledge of computer systems in order to better understand them, or improve their functions, performance and security. Some of them also engage in demonstrative and ethical actions, but never for profit. Hacker actions are performed almost always without any permission, so the Law punishes them (with great differences among the countries), for this reason hackers usually hide behind nicknames. Sometimes, wise security or

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

IT companies instead of prosecuting hackers, often hire them to take advantage of their high skills and creativity (possibly after paying part of their debt to Justice). They are then employed to test applications, security systems and programs both in production and already on the market in order to block attacks, and to prevent problems that could arise in the future from system bugs.

Real hackers have a reputation as experts, and are highly respected in their community. Competitions are organized with the aim of "piercing" a system or program in the shortest possible time. These competitions are called *hackathons* and are often sponsored by the giants of the computer industry.

The term "cracker" is attributed to Richard Stallman (a well-known figure of the free software movement, creator of the GNU project and member of the hacker community since the 1970s). He wanted to avoid the abuse of the term "hacker", differentiating who acted without any willing to harm and who, on the contrary, acts in order to have profit or just give damage. A cracker is a cyber-criminal who tries to attack computer systems in an unauthorized and illegal way, with malice, trying to take fraudulent advantage of them by exploiting vulnerabilities not yet known and resolved. Crackers are often involved in industrial espionage, data theft, and blocking of networks and websites, vandalism, etc.

The terms hacker and cracker have subtle bounds that divide them. For example, an intrusion can be considered an illegal act for some people and not for others, and the Law reflects these opinions; but this document is not about ethic or legislative aspects. Instead, we must consider that today, unfortunately, the two terms are considered synonymous.
In this document, we will *unhappily* use the more common and misused term hacker for both categories, being sure that the wise reader will be quite able to distinguish between a *hacker* and a *cracker*.

“Hackers” can be roughly classified into several categories, the most widely used are the following.

Black hat hackers use their knowledge for malicious or criminal purposes, being careful not to be traced.

White hat hackers test systems in order to identify possible vulnerabilities and eliminate them to prevent unwanted access. They often are security experts payed for this purpose.

Gray hat hackers are similar to white hats, but they often conduct research on system vulnerabilities without authorization and once these vulnerabilities are discovered they use them to force vendors to fix the problem, usually for free. Some vendors reward them with money,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

others prosecute them.

Suicide hackers are usually less competent than black/white hats, but they act for ideological reasons and have no interest in hiding their identity.

State-sponsored hackers are paid by a Government to launch cyber attacks against another Country; they have access to large resources as provided by the State as well as protection from prosecution for the offenses committed. They act to subtract confidential information, plans or projects, or to create generalized disorders and damage the population, the Army, the Government management, hospitals, plants for the production of energy, water and power supply, etc. These actions are considered real war actions.

Script kiddies do not have or have not yet acquired great skills, they usually make use of scripts and tools created by other hackers. All hackers before they acquire great skills are script kiddies.

Cyber terrorists are individuals or groups with hostile intentions that generally aim to create chaos in a Country; they are similar to state-sponsored hackers but do not have (yet) a Government to support them, or the support is not evident.

Malware

Malware is the acronym of "**mal**icious soft**ware**", a generic term that identifies any malicious program harmful to a system. Malware is the software hackers create to pursue their goals: making money, stole data, disrupt activities, etc.

One of the most common malware is the so called a **Trojan horse**[1] (or simply **Trojan**), a program that seems useful software and often act as such, but carries a hidden function that is executed to do along with the normal activated when the application is started. These are often shareware programs or cracked programs that are distribute modified in order to carry the Trojan horse. In other cases, it is just malware with a misleading name that makes it seem a useful software. Trojans are often spread by emails or by downloading programs through the Web and usually do not spread by themselves to other computers. Malicious code examples are *keyloggers* (programs that steals passwords and send them to the hacker), *backdoors* (programs that work as a terminal server and allows the remote hacker to access the computer in some ways bypassing the normal authentication procedures), *cryptominers* (programs that mines cryptocurrency), *bots* (short for robots, used for example for a distributed denial of service attack).

Rootkits are software installed by malware that try to hide the presence of a malware itself from detection; they achieve this by modifying the operating systems.

[1] The term is derived from the Ancient Greek story of the Trojan horse used to invade the city of Troy by stealth

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

The malware that infect other software can be a virus or a worm. These get their name from the way they spread rather than from any specific types of behavior. A computer **Virus** is software similar to Trojan horse but can produce copies of itself by infecting (introducing itself into) other software, including the operating system files. The virus is spread to other systems when infected software is copied and run on these systems.

Similar to a virus is a **Worm**, this is a stand-alone software that operates on a computer and infects other computers through the network, but without infecting files.

A **Ransomware** is a type of malware that restricts access to the device it infects, requiring a ransom to be paid to remove the restriction. The main types of ransomware are 1) *Screen-locking ransomware* that blocks screens with an intimidating accusation of illegal behavior and asking the victims to pay a fee; 2) *Encryption-based ransomware*, where the malicious software some type of files (pictures, documents) or all files on an infected machine. When the full encryption is done, a pop-up usually informs the user that (all) files have been encrypted and that a fee must be payed to recover them, usually in cryptocurrency. Examples of encryption-based ransomware are CryptoLocker and WannaCry. A variant known as a **Wiper** looks like a ransomware but just destroys the data, even if a payment is often required.

Greyware are a different category of malware: these programs can worsen the performance of computers and may cause security risks, behave in an annoying or undesirable manner, but usually are less dangerous (which is a relative opinion) than the previous categories of malware. Spyware (e.g. keyloggers, programs that record all the keys pressed on the keyboard), adware (advertisements windows on the screen or in the browser, fraudulent dialers, etc.), Potentially Unwanted Programs (PUPs, applications that the user installed just because of a mistake in a windows of agreement during another program installation) are typical form of greyware. They can be stand-alone programs or plugins for other programs, for example browsers. They sometime limits themselves to change the settings of other programs, for example in order to bring the user to a specific ad website or show an ad page each time the browser is started or occasionally.

Antiviruses

As antivirus engines enhance their power to detect malware, a combination of various techniques are used to try to avoid detection and analysis. More recent malware is able to adopt sophisticated countermeasures such as:

- analyzing and detecting by fingerprinting the environment to adopt specific hiding methods;
- trying to obfuscate themselves in order to confuse antivirus detection based on malware

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

signature;
- adopting a timing-based evasion in order to fool detection of anomalous behavior, the malware is normally quiescent and activates itself in very specific periods (for example during the boot process) or following certain actions taken by the user.

A very hard to discover technique for evasion is *Fileless malware* or *Advanced Volatile Threats*. This kind of malware runs in memory and does not require a file to operate. It uses existing system tools to perform its activity. The absence of any file on the file system makes them quite difficult to detect and analyze, except, partially, for those monitoring tools that check the resource usage and behavior of the system. The increase of this type of attacks is very high.

Risks

Vulnerable software can be exploited to gain privileges or bypass defenses, until the problem has been patched; this is the main reason that software should be up-to-date, in particular the Operating System. Firewalls and Intrusion Detection Systems monitor traffic patterns on the LAN.

The rule of the least privilege says that users and programs should have no more privileges than they require, otherwise malware can take advantage of this.

Mitigation

Antivirus software block and possibly remove some types of malware, they can provide real-time protection against the installation of malware software on a computer and a full scan of files and configuration (e.g. Windows registry) looking for potential threats.

Personal firewalls analyze any network connection and can spot unusual activity.

Sandboxing is running an application isolated from the rest of the system, some application can run a specific application while in more complex systems a virtual machine could be more appropriate.

Website vulnerability scans is performed by some antivirus software against a list of well-known dangerous sites and prevent the connection to them.

Network Segregation dividing a network in parts and enable only that traffic between them that is known to be legitimate, this prevents malicious software to spread across the network. Modern Software Defined Networking techniques are able to implement realize this segregation.

“Air gap” isolation or “parallel network” brings Network Segregation to the limit by completely

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

isolate a portion of a network and provide enhanced controls over the entry and exit of software and data from the outside world. Even this solution is not the definitive one, as software and data must enter the isolated system, for example for patching. A well-known example of breaching an isolated network is the famous **Stuxnet** malware that was introduced to the target environment via USB drives "casually" forgotten nearby, picked up by the plant staff and inserted into the plant computers to see the contents. Stuxnet has three modules: a worm that controls the attack; a link file that automatically executes the worm when inserted in a Windows computer; and a rootkit component responsible for hiding all malicious files and processes, to prevent detection. Other ways of crossing air gaps analyze electromagnetic, thermal and acoustic emissions.

Most Common Types of Attacks

This part describes some of the most common attacks to a computer system. It is not and cannot be complete as the variety of attacks is extremely huge, each one has many variants and many attacks and variants are created and discovered (and solved) every day. This means that the aim of this part is not to provide a complete classification, but to give an idea of the high level of knowledge required to both perpetrate and counter attacks.

Phishing

Phishing attacks are very common and easy to perform. They consist of sending e-mails that appear to come from a reliable sender, such as a colleague or a bank, with the aim of tricking the victim into doing a certain type of operation.

The attacker tries to persuade the victim to open an attachment or provides a link that leads to a page very similar to the original one, for example a bank home page, but created by the attacker, then to ask the victim to enter their credentials. To optimize this type of attack there are a whole series of techniques that are part of the so-called social engineering, since, in this case, the vulnerability of the computer system is to be identified in the user himself, who is deceived and unintentionally provides his credentials.

To defend against these attacks, a careful inspection of the link is needed (it is near impossible to distinguish between lowercase L 'l', an uppercase I 'I', and the digit one '1', or to notice the difference between .it and .lt in a URL). Moreover, one should be aware that serious companies never put links in their email that bring to a login page.

Password Attacks

To get passwords from a victim a hacker can try social engineering, as seen in the previous

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

paragraph, or launch a password attack. Passwords are usually stored as hashes, and hashes are very hard to invert. There are essentially two cases: the encrypted password is available or is unknown and this type of attack can be performed in different ways:

- **Brute force attack:** in this case the program will try all the possible combinations of characters out of a set;
- **Attack with dictionary:** the program will test a sequence of commonly used passwords (dictionary);
- **Attack with rainbow files:** a rainbow table is a precomputed table listing the output of hash functions of password. Use of a key derivation that employs a salt makes this attack infeasible.

System managers should test the password files of the users of their systems on a regular basis with programs capable of performing password attacks, both by brute force and by dictionary.

To protect against these attacks, a system should check the quality of the password before allowing the user to set it, requiring the use of a minimum number of characters (e.g. 10) from different sets (upper and lower case letters, digits, punctuation characters). If the password entered is incorrect for some subsequent attempts, it is appropriate to adopt an account lockout or delay policy on the next attempt, thus preventing the attacker from quickly trying many combinations.

Buffer Overflow

Buffer overflow (or overrun) occurs when you send more bytes to a buffer than it can hold, these bytes overflow the buffer intended to hold them and change other bytes or, depending on the Operating System and file type, even inject executable machine code. While modern Operating Systems may prevent running an executable file with mixed data and code, this is not true for the simpler Operating Systems often found in embedded systems, where in many cases there is no Operating System at all.

SQL Injection

A very common attack is SQL Injection. The SQL language is used in relational databases; hence, these types of attacks are aimed at information theft. In essence, due to the interpreted nature of the SQL query, malicious SQL code is sent to a web page that is know to use an SQL query to gather the data to present to the user. The malicious SQL code modifies (sometimes just adding other syntactic parts) the predefined SQL query that results is a modified query that exposes other data than those the original query was written for.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

While preventing this type of attacks is not complex (for example preventing the access to other tables of the database besides the ones needed to perform the original query), SQL injection is still one of the most common attacks.

Cross-site Scripting (XSS)

In a cross-site scripting (XSS) malicious executable scripts is injected into the code of a trusted web application (plugin) or website page, with the result that it is downloaded by other people (viewers). When the server sends back the compromised web page, the user's web browser considers it been delivered from a trusted source, and then the injected code is not identified as being malicious. The active content is usually a script (programming code that is executed by the browser) that can allow an attacker to get access to sensitive page content, session cookies, or other information the browser keeps on behalf of the user. With XSS attacks, it is possible to steal sensitive data of all users who access infected sites. For example, stealing the SESSIONID of a website session (which is located in the user browser cookies that in turn are used to avoid that each connection to the same website require authentication beyond the first one), could allow an impostor to bypass the login phase and illicitly operate on behalf of the user.

Cross-Site Request Forgery (CSRF)

A CSRF is an involuntary http request (wanted by the attacker) to a website performed by a user already authenticated to that website; the website at this point will execute the request without further verification, allowing the attacker to carry out his attack. This type of attack allows modifying user data or performing unwanted transactions, such as unwanted purchases, if it were for example an e-commerce site. The attacker must have very good knowledge of the site in question to carry out a CSRF attack.

An example of a CSRF attack is performed by changing an URL. For example the source code of the web page is analyzed by the malware to find the "Change password" link and verify that the http GET method is used, then a new link with a new password (chosen by the attacker) can be formed and sent to the victim, for example via an email attachment. If the link is clicked and it happens that the victim is already authenticated to the website, a hidden start of password changing procedure is activated, effectively giving the account to the hacker. Good password changing methods ask to insert the old password too (and the GET method is not used). Moreover, the use of a CAPTCHA method (a test to verify whether the user is a human or a computer) is quite effective.

File Related Attacks

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

There are many types of attacks on files. The most known vulnerabilities are:

- **Insecure Direct Object References:** occurs when an application requests a resource from a server calling it by its name, but allowing the user to modify the latter, in order to request another resource.
- **Local File Inclusion (LFI):** exploits the vulnerability of the GET and POST functions of the PHP language to insert malicious files into the code.
- **Path Traversal:** allows a malicious user to access directories with limited access and execute commands. Often, they are used following an LFI to get deep into the system and obtain the necessary privileges.

To protect against these types of attacks, it is important to prevent file uploads to servers, disable remote code execution, restrict PHP access to the file system, and update software periodically.

Denial of Service (DoS) and Distributed Denial of Service (DDoS)

Maybe the most know network attacks, DoS attacks basically consist in sending many packets to block the possibility to receive other packets, thus preventing access to the machine for regular users, blocking the services offered.

The difference between a DoS and a DDoS attack lies in the fact that in the first case a single host is used to carry out the attack, while in the second the attack is carried out with many hosts (called zombies) at the same time. These hosts have been previously infected by a malware and at the command of the attacker start the connection to the victim machine.

Among the DoS attacks, we can remember:

- **Syn-Flood**: consists of sending a large amount of connection requests. The machine that receives a request (a SYN packet) from a client will respond to the client by sending a message, allocating some resources for this connection, and waiting for the acknowledge packet (that will never arrive). Therefore, the connection request remains active until a timeout occurs. If all the possible connections have been started, the service provided by the machine will no longer be available. The timeout occurs within seconds but the huge rate of requests keeps the machine clogged.
- **Smurf**: this attack is a combination of IP spoofing and ICMP requests. IP spoofing refers to the sending of an IP packet in which the sender's IP is forged. By continuously sending *ICMP echo requests* (the message sent by the ping command, used to verify if a machine is reachable) to broadcast IP addresses after having substituted the sender IP address with victim's IP address, the victim machine will receive a response for every request from any host active on the network, thus blocking the connection (flood). To prevent these attacks from occurring, it is possible to disable in the routers the forwarding of broadcast IP addresses.
- **Ping of death**: consists in sending a fragmented packet with a total IP size greater than the

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

maximum allowable to a victim machine, once the machine reassembles the packet it can incur buffer overflows.

It is common for a DDoS attacks to use a **Botnet** that is thousands or millions of computers infected with malware, which at the command of the attacker, execute a Syn-Flood attack in unison on a victim server.

Man in The Middle (MITM)

With MITM we mean a whole typology of attacks that aim to intercept, analyze and retransmit a communication between two parties who believe they are communicating directly to each other.

This type of attack is usually carried out using IP spoofing: network sniffers eavesdrop a connection and new packets created by changing the IP address of the sender and recipient so that the sender sends data to the attacker who in turn it will re-send them to the recipient and vice-versa.

There are many ways to defend against these types of attack; the one most effective and used today is adopting *end-to-end encryption*, where the end subjects perform the encryption/decryption and all the intermediate systems can only see encrypted data.

ARP Spoofing or ARP Poisoning

The Address Resolution Protocol (ARP) enables network communications to reach a specific device on the local network. It is used to map IP addresses to Media Access Control (MAC) addresses (used to identify the hosts on a LAN). A host must use the ARP protocol to know the MAC address of the router/gateway in order to connect to the Internet. Each host maintain an *ARP cache* to map already requested and known IP/MAC pair. If the host does not know the MAC address for a certain local IP address, it sends out a broadcast ARP request packet, asking all the other hosts on the local network who has the IP address. The host with that IP address will answer, thus providing its MAC address.

An ARP spoofing/poisoning attack can be classified as a local network MITM attack. The attacker must have access to the local network and scans it to determine the IP addresses of the router and another host. The attacker sends forged ARP responses that make the router and the host to believe that the attacker's MAC address is the one of the host and the router respectively. This fools both router and workstation to connect to the attacker's machine, instead of to each other. As the two devices update their ARP cache entries, host and router communicate with the attacker instead of directly with each other.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

DNS Spoofing

The Domain Name System (DNS) is the naming system used to convert Internet names (more properly FQDN - Fully Qualified Distinguished Names, e.g. www.server.net) to the corresponding IP address. The system is hierarchical and decentralized with some top-level servers. Each time a system attempts to reach a network resource, a connection is made to a DNS server in order to convert the name of the resource to an IP address. The resource records usually contains administrative information and other data used for example by mail servers.

A hacker will want to alter DNS records in order to send traffic to a fake or "spoofed" website instead of the legit one. The spoofed machine could then do MITM attacks, spoofing, etc. To prevent DNS spoofing, DNS servers must be kept up-to-date.

Drive-by Attacks

In a drive-by attack, malicious code is embedded into an insecure website. When the infected page is visited, the script is automatically executed on the victim computer and compromises it, there is no need to do anything on the site or enter any information. In this case, the use of an updated recent and decent antivirus and/or personal firewall is the only protection as they can detect from their database if a site is unsafe before a user visits it.

Credential Reuse

The need to have credentials for several services brings users to reuse some of their passwords. Once an attacker has a list of usernames and passwords of compromised websites or services (for example obtained from the Dark Web), it is possible that the same user could use the same user/passwords pair on other systems. This will greatly reduce the number of password to check with a dictionary attack. In order to contrast this type of attack, the same countermeasures adopted to counter password attacks are effective. When many complex passwords are needed, some people find password managers useful.

Web Session Hijacking

A Session Hijacking attack consists of the exploitation of session tokens, used by web browser as session control mechanisms. The web server needs to relate different connections from the same user, as for each web page a TCP connection is created for each element (text, images, etc.). The most used method is based on a token that the Web Server sends to the client browser after a successful client authentication. A session token is just an identifier, a long unique string, and can

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

be used to avoid the need to perform an authentication procedure for each connection. This attack is performed by stealing or predicting a valid session token to gain unauthorized access to the Web Server.

TCP Session Hijacking

TCP connections must guarantee to deliver packets in the right sequential order, in order to achieve this it uses acknowledgement packets and sequence numbers. These acknowledgement packets are just numbers that are incremented in some way after the 3-way initial handshake. The goal of the TCP session hijacker is to create a state where the client and server are unable to exchange data; enabling him/her to forge acceptable packets for both ends, which mimic the real packets. Thus, the attacker is able to gain control of the session. If the sequence can be predicted, an attacker can send forged packets that are recognized as valid from the victim host.

IP Spoofing

An IP spoofing is usually performed with a DoS attack: a huge number of connections blocks the legitimate server and, at the same time, a fake server sets its IP address with the number of the legitimate server. Therefore, the user is driven to the fake server that sends messages with an IP address indicating that the message is coming from a trusted host.

Blind Hijacking: In cases where source routing is disabled, the session hijacker can also use blind hijacking where he injects his malicious data into intercepted communications in the TCP session. It is called blind because he cannot see the response; though the hijacker can send the data or commands, he is basically guessing the responses of the client and server.

Zero-day Exploit

Strictly speaking, zero-day exploit is not a specific attack as cyber-criminals learn of a vulnerability that has just been discovered in certain software and operating systems and then target organizations who are using that software before a fix becomes available.

Leak of Code

The source code of applications can sometimes contain sensitive information and give valuable insights for a cyber-attack, in addition to the intrinsic economic value of the code itself.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Questions:

In separate file.

Attachments:

In separate file.

References:

Every topic has its own page on Wikipedia, sometimes already too thorough for the purposes of this course; books are too specialized and are useful only after a very deep training on the specific subject.

1. Malware, or malicious software
   URL: https://www.malwarebytes.com/malware
2. Cybersecurity for everyone.
   https://www.avast.com/c-malware
3. What are Cyber Security Threats?
   URL: https://www.imperva.com/learn/application-security/cyber-security-threats/
4. 21 Top Cybersecurity Threats and How Threat Intelligence Can Help
   URL: https://www.exabeam.com/information-security/cyber-security-threat/

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Managers Unit (Module) no and Week No: Unit-2 Week-4 Unit (Module) name: Information security management -2	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other** Streaming Webinar, Text, Self-assessment Exercises, Exercises with answers on discuss forums and be discussed with trainer/mentor
Learning Responsible	• Fatma Gökdemir • Ali Gökdemir
Learning Activity Goals	1. Threat and vulnerability assessment 2. Threat and vulnerability management 3. Types of vulnerability assessment 4. Cyber Continuity of Operations 5. Cyber Asset 6. Evaluation of cyber security policies effectiveness
Skills to be Gained	• IS 1 • IS 3 • MS 5
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Intermediate computer skills

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
The management of assets has an important place within the scope of ISO 27001 Information Security Management System. In fact, identifying and classifying Information Assets is one of the first steps of information security setup. Identifying and assigning value to assets in an organization is a fundamental step in the risk analysis process. An asset inventory is prepared in order to assign value to assets. An exploratory study covering all employees should be conducted prior to the asset inventory. With this study, the asset inventory of the department is explored and listed with possible risks and confidentiality degree. Asset inventory should be done one by one on the basis of the covered processes. While preparing the asset inventory; the asset group, the environment in which the specified asset is located, the classification code is determined, and the asset value (confidentiality, integrity, accessibility) is calculated. According to the calculation result, the priority status is determined, and action decisions are taken. After the asset inventory work is completed, a detailed inventory list is prepared for the detected software-hardware inventories. Conditions/controls regarding asset management in the ISO27001 standard are gathered under Annex A.8. In this module we will examine the terms for Liability of Assets defined in A.8.1.

Content of the Learning Material

1. Assess Management of Information Security

In the first stage of asset management, it would be useful to first reveal and list what assets we have. What an institution has or does not have should be known first. Then their ownership needs to be defined. No business or transaction should be left unattended. Then, the rules for the use of these assets should be determined.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

For the details of the subject, the ISO27002 standard should be examined. The expectations regarding Asset management in ISO27002 are included in the 8th article of the standard:

Asset management and liability for assets

Purpose: To identify the organization's assets and define appropriate protection responsibilities.

1. Asset inventory

Control: Assets related to information and information processing facilities should be identified and an inventory of these assets should be made and maintained.

Application guide: An organization should identify relevant assets in the information lifecycle and document their importance. The information lifecycle should include creation, processing, storage, transmission, deletion, and destruction. Documentation should be maintained in accordance with existing inventories or specifically.

Asset inventory; must be current, consistent, accurate and compatible with other inventories.

Asset ownership should be allocated for each identified asset (see Article 2) and its class should be determined.

Other information: Asset inventory helps to provide effective protection and may also be necessary for other purposes such as health and safety, insurance or financial (asset management) reasons.

The ISO/IEC 27005[11] standard provides examples of assets that may need to be considered by the organization when identifying assets. The process of compiling an asset inventory is an important prerequisite for risk management (see ISO/IEC 27000 and ISO/IEC 27005[11]).

2. Ownership of assets

Control: Owner assignments must be made for all assets held in inventory.

Application guide: Individuals and other entities with approved management responsibility for the asset lifecycle are eligible to be designated as asset owners.

A process is often used to ensure that asset ownership is determined in a timely manner. Ownership must be determined when assets are created or transferred to the organization. The asset owner should be responsible for the proper management of the asset throughout the asset

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

lifecycle.

Asset owner:

a) Ensure that asset inventory is recorded,

b) Ensure that assets are properly classified and protected,

c) Define and periodically review restrictions on access to significant assets and their classification, taking into account the applicable access control policy,

d) Ensure that appropriate action is taken in deleting or destroying assets.

Other information: It can be an individual or entity with approval for management responsibility to control an asset throughout its lifecycle. The identified owner has no ownership interest in the asset.

Routine tasks may be delegated; (for example, a custodian who looks after an asset on a daily basis) but the responsibility rests with the asset owner.

Identifying groups of assets within complex information systems can be useful in providing functions together. In this case, this service owner is responsible for the delivery of the service, including the operation of the assets.

3. Acceptable use of assets

Control: Rules regarding the acceptable use of information and assets related to information and information processing facilities should be determined, documented, and implemented.

Application guide: Employees and external users who use or have access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information and information processing facilities and resources. These users should be responsible for the use of all information processing resources and for any use that occurs under their own responsibility.

4. Return of assets

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Control: All employees and users of external parties must return all corporate assets in their possession upon termination of employment, contract, or agreement.

Application guide: The termination process should be formulated to include the return of ownership of all previously granted physical and electronic assets or escrows of the organization.

When an employee or outside user purchases or uses the organization's equipment, procedures are followed to ensure that all relevant information is transferred to the organization and securely deleted from the equipment.

Where an employee or external user has information that is important to ongoing operations, this information needs to be documented and transferred to the organization.

During the termination notice period, the organization; control the unauthorized copying of related information, such as intellectual property, by terminated employees and contractors.

2. Threat and vulnerability assessment and management

Almost every organization has sensitive and valuable assets that need to be protected. However, not every organization has a comprehensive and fully thought-out strategy for protecting these assets. In cybersecurity, vulnerability management strategies are the foundation of strong defense. Typically, vulnerability management strategies are designed to help an organization's systems, networks, applications, etc. It adopts a holistic and continuous approach to managing security vulnerabilities in These vulnerabilities are then identified, evaluated, and fixed as soon as possible.

Security threats and trends are constantly evolving, requiring effective, preventive efforts to manage threats and vulnerabilities that could compromise your data. To identify all potential targets for a breach or attack, its risk must first be mitigated by conducting an asset inventory. The targets must then be classified and continuously monitored for new potential vulnerabilities. A threat model that identifies the organization's most valuable assets at high risk should then be developed and tested. The primary purpose of the Threat and Vulnerability testing process (assessment) is to best understand the criticality of assets, the vulnerabilities to these assets, and reduce the necessary measures to effectively protect these assets.

2.1. What is vulnerability assessment?

Vulnerability assessment is the process of identifying, classifying, and prioritizing vulnerabilities in computer systems, applications, and network infrastructures.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Vulnerability assessments also provide an organization with the knowledge, awareness and risk background necessary to understand and respond to threats to its environment. A vulnerability assessment process aims to identify threats and the risks they pose. Often they involve the use of automated testing tools, such as network security scanners, whose results are listed in a vulnerability assessment report.

Organizations of any size, even individuals at increased risk of cyberattacks, can benefit from some form of vulnerability assessment, but large organizations and other types of organizations exposed to ongoing attacks will benefit most from vulnerability analysis.

Because vulnerabilities can allow hackers to gain access to IT systems and applications, it is critical for organizations to identify and fix vulnerabilities before they are exploited. A comprehensive vulnerability assessment combined with a management program can help companies improve the security of their systems.

2.2. The importance of vulnerability assessments

To better illuminate the importance of vulnerability assessment, let's consider it through the eyes of a physical property owner. If you own a valuable building, you probably take a number of measures to protect it: You maintain it, insure it, and make sure the doors, windows, are locked, and alarms are activated. All of these steps can be termed as managing the risk to the property and its contents.

Now what if you could hire someone to test and report on your alarms and external defenses? Cybersecurity vulnerabilities are approached in a similar way. Vulnerability management is an overarching and ongoing strategy, while vulnerability assessments are a specific tool used in this broader management strategy.

A vulnerability assessment provides an organization with detailed information about any security weaknesses in its environment. It also provides direction on how to assess the risks associated with these weaknesses. This process provides the organization with a better understanding of its assets, security flaws and overall risk, reducing the likelihood of a cybercriminal breaching its systems and catching the business off guard.

2.3. Types of vulnerability assessment

Vulnerability assessments discover different system or network vulnerabilities. This means that

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

the assessment process includes using a variety of tools, scanners and methodologies to identify vulnerabilities, threats and risks.

Some of the different types of vulnerability assessment scans include (Figure 1):

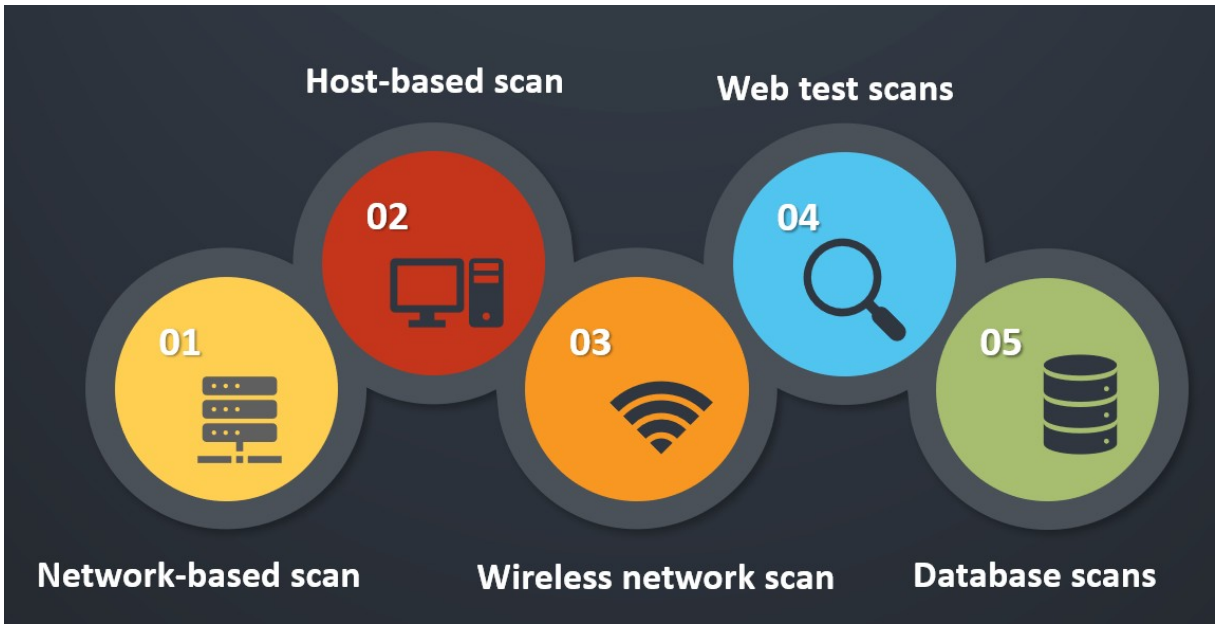


Figure 1. Types of vulnerability assessment

- **Network-based scans** are used to identify potential network security attacks. This type of scan can also detect vulnerable systems on wired or wireless networks.
- **Host-based scans** are used to find and identify vulnerabilities in servers, workstations, or other network hosts. This type of scan usually examines ports and services, which can also be seen in network-based scans. However, it offers greater visibility into the configuration settings and patch history of scanned systems, including legacy systems.
- **Wireless network scans** of an organization's Wi-Fi networks often focus on attack points in the wireless network infrastructure. In addition to identifying rogue access points, wireless network scanning can also verify that a company's network is securely configured.
- **Web scan test** sites to detect known software vulnerabilities and misconfigurations in application, network or web applications.
- **Database scans** can identify weak spots in a database to prevent malicious attacks.SQL

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

injection attacks.

2.4. Vulnerability assessments and penetration tests

A vulnerability assessment often includes a penetration testing component to identify vulnerabilities in an organization's personnel, procedures, or processes. Vulnerability assessments share many of the same characteristics as penetration tests because both allow organizations to rigorously examine their defenses. These vulnerabilities may not normally be detected by network or system scans. The process is sometimes referred to as vulnerability assessment/penetration testing or **VAPT**.

However, penetration testing is not sufficient as a complete vulnerability assessment and is actually a separate process. A vulnerability assessment aims to uncover vulnerabilities in a network and suggest appropriate mitigation or remediation to mitigate or eliminate risks.

A vulnerability assessment uses automated network security scanning tools. The results are listed in the vulnerability assessment report, which focuses on providing organizations with a list of vulnerabilities that need fixing. However, it does this without evaluating specific attack targets or scenarios.

Organizations should regularly perform vulnerability testing to ensure the security of their networks, especially when changes are made. For example, testing should be done when services are added, new equipment is installed, or ports are opened.

In contrast, penetration testing involves identifying vulnerabilities in a network and attempts to use them to attack the system. Although sometimes performed in conjunction with vulnerability assessments, the primary purpose of penetration testing is to check whether a vulnerability actually exists. Additionally, penetration testing attempts to prove that exploiting a vulnerability can harm the application or the network.

While a vulnerability assessment is usually automated to cover a wide variety of unpatched vulnerabilities, penetration testing often combines automated and manual techniques, helping testers further investigate vulnerabilities and leverage them to gain network access in a controlled environment.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

2.5. Vulnerability Management and Risk Management

While vulnerability management is an ongoing process of managing vulnerabilities, risk management takes a broader view of anything that can pose a threat to an organization. A sound risk management strategy allows risks to be identified, analyzed and effectively mitigated. This approach helps organizations understand not only the vulnerabilities that exist, but the scale of damage that can occur if abused. A risk and vulnerability assessment conducted under the umbrella of risk management can provide a particularly broad perspective on the strength of an organizational security posture.

3. Cyber Continuity of Operations

Increasing resilience against threats of destructive malware requires insight into the current security posture, planning and coordinating key defensive actions, and aligning key defensive resources correctly.

Cyber incidents have likewise challenged basic continuity planning efforts. While many jurisdictions have equipment and strategies to identify, detect, and protect against cyberattacks, far fewer have worked through the hard realities of continuity of their operations through an actual attack. When cyberattacks do strike, many affected jurisdictions find that that their basic COOP plans don't hold up. While the plans are adequate for transitioning to an alternate work site, they have much less to offer when it comes to working without access to the systems and data staff need to perform their mission essential functions. Existing plans also lack the specificity needed to guide the response, and major stakeholders such as members of the IT staff are often not integrated into response structures. And plans are untested against an exercise or real-world incident.

Traditional COOP plans fall short for continuity during cyber incidents in several ways (Figure 2):

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

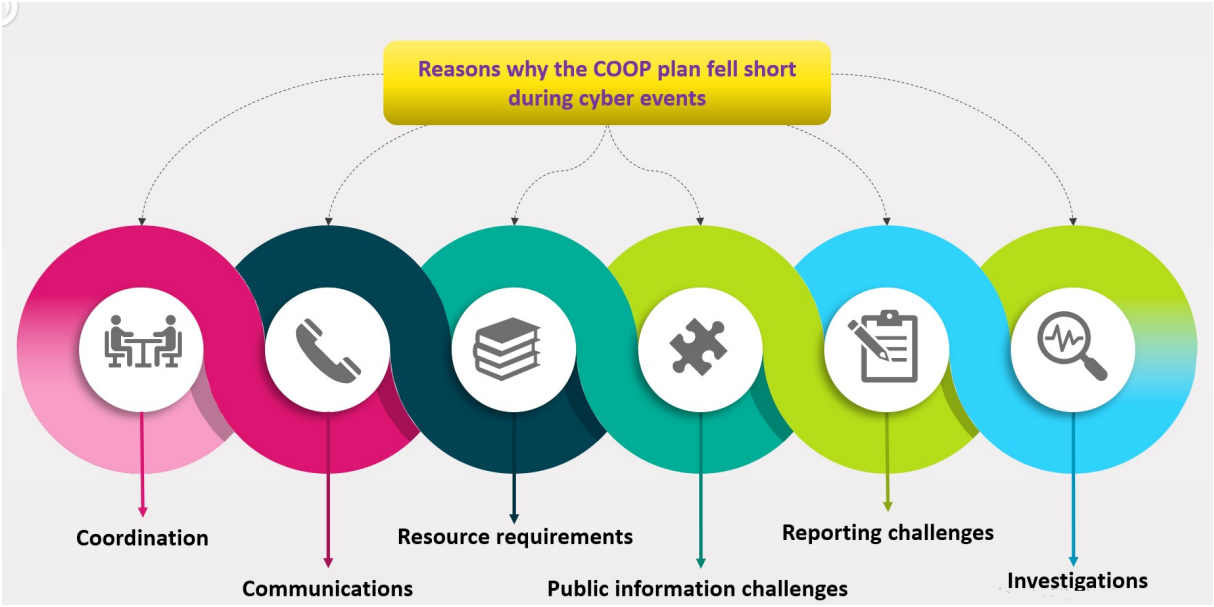


Figure 2. Reasons why COOP plans are insufficient for continuity during cyber events

Coordination: including who is involved in decision-making when it comes to ransomware, decisions to take systems offline, and decisions to activate the jurisdictional Emergency Operation Center. Additionally, most local governments do not have clear escalation levels for an attack, nor the associated action items for each level. Response leadership and staffing may also be unclear; the types of subject matter expertise needed to guide a community through a cyber incident are different from those needed for extreme weather.

Communications: including how local managers will rapidly provide information to staff when a cyberattack has severely compromised communications. This includes both immediate communications explaining what to do when the attack begins and ongoing communications, such as how salaries will be provided by payday. Both are critical to response, and yet both may have to be relayed without the benefit of typical emergency communications systems.

Resource requirements: Which may be very different from those for a more traditional response. For example, staff might require clean computers, clean servers, local printers, and even fax machines and paper. Importantly, staffing requirements may surge even more during recovery than in response, as departments and agencies struggle to replicate missing or suspect data.

Public information challenges: Including public information officers with little to no training or experience in cybersecurity, a lack of pre-scripted messages, and disagreement on when information about the attack should be made public. Providing information to the public is critical because citizens worry about their data and the trustworthiness of key democratic

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

systems such as voting and justice.

Reporting challenges: That can delay response, as outages aren't reported in a consistent manner, leaving IT departments without the necessary common operational picture to quickly identify an attack. In addition, the lines of reporting are often unclear, and few people outside of IT understand which systems are connected both within and external to the jurisdiction.

Investigations: Which is a black box for many localities. The involvement of one or more federal organizations and the limits investigations place on remediation efforts are not well understood or planned for. This makes continuity planning extremely difficult, because there is uncertainty about how and when remediation can even begin.

3.1. Priorities for Immediate Action with Coordinated Defense

- Develop a cyber 'Go Bag' with essential procedures and information.
    - o Assemble mobile cyber security toolkits that include procedures for establishing, implementing, maintaining, and enabling the continuance of cyber resilient TTPs within a COOP-designated facility
- Develop, test and validate playbooks, roles, responsibilities, and tools.
    - o Designate specific cyber roles, associated responsibilities, and the cyber tools that may be deployed to ensure implementation of cyber COOP.
    - o Define standard cyber COOP plays for individual or cyber team execution using cyber 'Go Bag' tools and elastic TTPs.
    - o Conduct different types of cyber exercises (e.g. mini-table top type exercises) using the cyber 'Go Bag' and playbook.
- Define collaboration processes and acquire tools for cyber defenders and incident responders.
    - o Ensure both mobile and stationary cyber COOP processes incorporate communication and coordination dovetailing to promote adequate management of cyber defenses, synergy among all response activities, and reduction of security coverage gaps during recovery activities.

While basic COOP plans have furthered local preparedness for many of the threats that jurisdictions face, they fall short during situations that create an environment very different than the norm. As IT departments around the country continue to make systems and data as secure as possible, it is up to emergency managers to stretch their imaginations and plan for cyberattacks that seriously impact critical systems and data.

3.2. Priorities for Immediate Action with Realignment

- Identify mission and business function dependencies on cyber resources.
    - o Determine the mission purposes of resources so that uses that increase risk without

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

any corresponding mission benefit can be identified and eliminated.

- ✓ Identify and remove or replace data feeds and connections for which risks outweigh benefits.

o Consider the interdependencies between and among mission and non-mission business functions and organizations that share critical roles in the delivery of NEF capabilities.

- ✓ Reallocate resources or reassign administrative and management responsibility based on risk to mission and business function.

• Identify non-mission and business function dependencies on or uses of cyber resources.

o Make use of mission flow analysis, mission dependency analysis, tabletop exercises, and Red Teaming to uncover undocumented mission dependencies.

o Review and correlate mission and business functions with dependency model mapping and impact analysis activities and results.

o Identify systems, applications and processes of non-mission critical functions and the resources that support them.

- ✓ Assess those functions against a fluid Cyber COOP implementation strategy to accommodate priority operations and better dependency utilization or elimination.

4. Cyber Asset, Change and Configuration Management

- ✓ **Asset:** Let's start with the definition of an asset. The dictionary definition of an asset is **a useful or valuable thing or person**. Similarly, assets of an IT service provider are its tools, applications, configuration items, and any other valuable items that help to deliver services to the customers or business. Assets are one part of service asset and configuration Management.

- ✓ **Configuration Item:** Configuration Item is abbreviated as CI and a configuration item is **any component that needs to be managed in order to deliver an IT Service.** Examples of configuration items are IT services, hardware, software, buildings, people and formal documentation. So briefly, any component or item that helps to deliver an IT service to the customer is classified as a Configuration Item. Information about each configuration item is recorded in a Configuration Record within the Configuration Management System and this information is

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

maintained through its lifecycle by Configuration Management.

- ✓ **Configuration Management Database:** Configuration Management database is abbreviated as CMDB. CMDB is a **database used to store configuration records throughout their lifecycle. CMDB** stores information about your CIs, each distinguished by a unique identifier, including identifying information like its serial number, MAC address or IP address; its current version; its location; and its vendor and supplier information.

- ✓ **Configuration Management System:** Configuration Management system is abbreviated as CMS and is **a set of tools and databases that are used to manage an IT Service Provider's Configuration Data.** Data about configuration items are stored in configuration records, and configuration records are included in the Configuration Management System Databases. The CMDBs of an IT Service provider to manage the configuration data is included in the service asset and configuration management process. The Configuration Management System also includes information about incidents, problems, known errors, changes and releases, employees, suppliers, locations, business units, customers, and users. In summary, all necessary information about configuration items and IT assets are included in the Configuration Management System. When needed, this information is acquired from the CMS and used respectively.

Configuration management, which is basically defined as the process of identifying, controlling, monitoring and auditing changes made, is a critical part of a strong security program. Change and configuration management within an organization has strong links to audit requirements in nearly all security frameworks and regulations.

Configuration management is based on the control and release of various product versions. Default configurations for operating systems and applications are generally geared towards ease of deployment and use, not cybersecurity best practices. Today, configuration management is an in-demand discipline with significant cybersecurity implications, especially as organizations move from out-of-the-box default configurations to more secure application and hardware configurations.

Today, configuration management means different things to different people. In some implementations, it refers to the way network devices are configured. In others, it's about the version of an app a team is running. Sometimes people in the industry confuse IT asset management with change and configuration management. While they are similar and equally important to the business, they are not the same. IT management solutions monitor, optimize and manage assets across the entire asset lifestyle. Meanwhile, CM collects, stores, manages, updates

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

and analyzes all configuration items.

While many organizations have immature CM programs, they are critical to the modern cybersecurity landscape and will only increase in importance as the threat landscape continues to evolve.

4.1. Configuration Management and Disaster Recovery

When it comes to modern disaster recovery, configuration management is essential. In the event of a cybersecurity disaster, (76% of organizations have experienced an IoT cybersecurity incident, after all) it can be impossible to recover to the most recent configuration if there is no documentation of said configuration.

The same goes for cybersecurity: it's impossible for teams to know if something is amiss if there's not a standardized way of configuring, changing, and documenting the digital environment.

4.2. Change Management

Change management runs parallel with configuration management, although the two things are *not* the same. People confuse them all the time.
While configuration management is the process of identifying and documenting hardware components and software and the associated settings, change management is an underlying function of the larger configuration management process. Change management relates to the associated processes and seeks to create stability within a system and prevent uncontrolled or random changes or to document change processes when you have turnover within the organization. In other words, it allows companies to plan for change, rather than just reacting to it.

4.2.1. The Change Management Process

Today, a well-structured change management process will include the following:

- Change request submittals
- Risk and impact assessments
- Approve/reject change functions
- Testing
- Scheduling/user notification/training functions
- Implementation
- Validation
- Documentation

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

One of the places change management thrives is in the event of emergency decisions, when changes must be made. Once the change has been implemented, it should be fed back into the change management process, where it will then benefit from the validation and documentation protocols that were already established.

4.3. Cybersecurity asset management

Cybersecurity asset management is the process of gathering asset data (devices, cloud instances, and users) to strengthen core security functions, including:

- **Detection and response:** Ensuring detection and response capabilities provide coverage across the enterprise
- **Vulnerability management:** Understanding which assets may be vulnerable to exploits, and ensuring all assets are being evaluated for vulnerabilities
- **Cloud security:** Ensuring that cloud instances are secure and configured to prevent overly permissive access rights, even when they're commissioned and decommissioned rapidly
- **Incident response:** Using enriched, correlated data on assets to expedite incident response investigations and remediation
- **Continuous control monitoring:** Identifying when security controls are missing and need to be applied

5. Evaluation of cyber security policies effectiveness

The development of an information system progresses through several distinct phases from analysing the problem through to the implementation of the system. Throughout this process each step is documented through a series of deliverables that range from a feasibility study, through to training manuals and system documentation. In the development of a security policy this self- documentation process generally does not occur.

Many policies developed currently attempt to fit everything into the security policy: the justification of importance and specific system instructions and descriptions. Certainly, the security policy itself is already long-winded enough, without having details on how the document was created, who was consulted in its production or how the policy formulation was achieved. Nor will there be any documentation of political problems that may have occurred during the implementation of the policy, or of how to train people about the policy. With the use of documentation techniques during the development of the policy, however, a security policy could become a principles document again. Other issues not dealing with the principles of

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

security policy would be documented elsewhere along with the justification for the policy.

The most important information that is often missing or just inadequate when we attempt to evaluate a security policy in an organization is the requirements documentation. Without a clear understanding of the requirements, evaluation of the quality of a security policy is almost impossible. An analysis of the risks/threats faced by the organization is only part of the requirements needed for the development of a security policy. The organization's objectives and other political issues that influence the development, implementation and acceptance of the security policy are just as important. The availability of extensive documentation including the outcomes of an extensive requirements analysis will allow the evaluation of the security policy to reach a greater depth, instead of just superficially evaluating the end product. For instance, rather than concentrating only on whether the policy has been implemented in a particular area, the evaluation can now also consider how that area was developed within the policy. Documentary evidence could be evaluated to determine if the policy adequately covers all issues identified within development without watering any of them down. However, security policies vary greatly depending on the context of the organization and one would expect that their development would also vary. Some commonalities between policies would exist, even as target areas digress. Unlike product evaluation however, many criteria in security policy evaluation will be of a subjective nature. This is because of the subjective nature of developing a policy and of the environment in which the policy is implemented.

5.1. Maintaining Effectiveness of IT Security Policies

Information technology, or IT, is arguably the technology of the century. It sure has transformed the world. With all the benefits of IT, however, a lot of security risks have also penetrated our lives. Organizations must design effective information security policies to ensure that their business operations remain safe from the malicious intruders and data to thieve. Ironically, an excellent way to maintain the effectiveness of security policies against the changing IT risk landscape is to use more IT.

Here are some of the ways in which IT can maintain the effectiveness of security policies:

- **Better risk assessment:** Security risk assessment is an essential first step in designing any information security policy. To address the threats arising from the rapidly evolving IT sector, IT is the only antidote. Since risks change constantly, IT is a must to keep the new threats in check. It allows you to easily discover new risks based on your previous compliance records, rank and classify the risk factors and assess the damages it can cause. Thus, it is important to learn from the new developments–good or bad–in IT. This

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

will improve your risk assessment as well as your preparedness in case a threat is imminent.

- **Better compliance**: IT helps you monitor how well the employees and the heads of your organization remain compliant with the regulatory authorities as well as your organization-specific security policies. Through a single software, you can keep an eye on access authorizations, insecure data sharing, unsafe web surfing, insufficient data encryption, and countless other factors that can gravely affect your security.
- **Constant up-gradation is a must**: Since the world of IT is changing with every breath we take, you must constantly be on the look-out for new changes that can break your system. Monitor the developments in the world of cyber-risks, cyber-crime, and cyber-security. Upgrade your information security policies and your security software frequently and regularly, because they can get out-of-date very quickly. This way, you can maintain the effectiveness of your security policies.
- **Quick mitigation**: If your organization does face an impending security threat that can lead to potential data loss or theft, you must have a mitigation or remediation plan at hand. IT helps you plan mitigation in a simple and efficient manner. With IT, you can assign and link risk mitigation steps to different potential risks when you design your security policies. This will make mitigation timely and more effective, thus maintaining the effectiveness of your security policies.
- **Improved accountability**: No information policy can remain effective if people are not held responsible and accountable for risks, compliance, and mitigation. IT makes it easier to ensure the accountability of remedial action. It can greatly improve the Visibility of Risks and Maturity assessment, compliance, and the remediation measures that your organization undertakes. This means that your employees will be more prompt and more accountable towards the steps listed in your information security policies.

5.2. Evaluation Security Risks

Risk Assessment, after determining which information assets will be protected, the risk assessment method is selected, and the risks are defined. According to the chosen risk assessment method, information assets are positioned on the risk map shown in the figure. After the assessment is made, the risk assessment map covers the processes of improving and controlling risks for threats with high impact and probability. Since the location of information assets in the risk map may change, the risk assessment map should be updated regularly, and necessary precautions should be taken.

Risk is defined as the combination of the probabilities of an event and its outcome. Risk

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

assessment, which is a step of risk management, is a process in which risks are defined and the effects and priorities of these identified risks are determined. Risk management is to determine an acceptable level of risk, to evaluate the current risk, to take the necessary steps to reduce this risk to an acceptable level, and to maintain this risk level. Information and other assets, threats to these assets, vulnerabilities in the existing system, and security system controls are the components that determine the current risk. Identifying information or assets that need to be protected; determining how valuable these assets are to the establishments; revealing which of the known and possible threats to these assets will be tried to be prevented; investigating how possible losses might occur; identifying the extent of possible threats to each asset; Examination of what can be done in the first place to reduce the extent and probability of losses that may occur in these assets and planning the steps to be taken to keep the forward-looking threats at a minimum level are certain phases of risk assessment. The cost of the security system to be established and implemented as a result of risk management is another important issue to be considered. The cost of the security system should be limited by the value of the information protected and the risk determined by examining possible threats. Along with the principle that there will be no 100% security, the ideal configuration of information security is realized through three processes. These processes are prevention, detection and response (response or reaction).

Prevention; It is the process that security systems focus on and work the most. Various measures are being developed to insulate the system against threats and attacks against computer systems, such as security measures used in daily life such as fencing a house's garden and using a steel door. Regarding personal computer security, having virus scanning programs installed, performing these programs and operating system service packs and error correction and updates at regular intervals, using a password-protected screen saver on the computer, leaving the system after being away from the computer for a long time, estimating the passwords used is difficult. determining, keeping these passwords confidential and changing them at regular intervals, being careful about disk sharing, paying attention to files downloaded from the Internet or sent by e-mail, protecting important documents with a password or keeping them encrypted, e-mail confidential or important information, sites without security certificates. Some of the measures that may seem simple, but save lives, such as not being sent via unsafe means, turning off internet access when not in use, taking regular backups of important information and documents. Prevention steps to be implemented in computer security in corporate environments are broader and more complex. Some of the things that are done about prevention in such systems where security experts work:

- Periodically reviewing the service packs and updates of the operating system and

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

software,
- Keeping user rights to a minimum, not running unused protocols, services, components and processes,
- Encryption techniques in data transmission, vulnerability scanners,
- Using Virtual Private Network,
- The use of Public Key Infrastructure and e-signature can be listed as the use of Biometric-based systems.

In fact, if the progress determined in the prevention process could be perfect, further processes would not be needed at all. All attacks would have been prevented at the worst. But no security product is perfect or complete. In addition, almost every day, various vulnerabilities are detected in transmission systems, Internet services, web technologies and security applications. From this point of view, using detection and matching processes increases.

Determination; Security is not just a matter of prevention. For example, the fact that a museum is well protected, that the museum is surrounded by fences, that the doors are closed and locked, does not necessitate the use of guards at night in that museum. In the same way, the use of methods to detect attack attempts on computer systems is also increased. Prevention is building a barrier that either makes attacks stronger (but not impossible) or discourages (but does not destroy) attackers. Prevention without detection and response may have only limited benefit. If only prevention were sufficient, most attacks would not even have been known. With detection, previously known or newly emerged attacks can be reported and given appropriate responses. The first and most basic step in detection is to monitor the entire state and movement of the system and to keep records of this information. In this way, data and evidence are also collected for post-attack analysis. Firewalls, intrusion detection systems, network traffic monitors, port scanners, honeypot usage, real-time protection virus and spyware tools, file checksum control programs and network Sniffer sensors are some of the most common methods used in the detection process.

AnswerBack; Just as a place equipped with guards, dogs, security cameras, sensors can attract the attention of thieves, computer systems with real-time detection systems are also attractive to hackers and attackers. Rapid response emerges as an essential element that complements the security system to repel these attacks. Response can be defined as the execution of actions that will respond immediately or as soon as possible to attack attempts that cannot be dealt with by the prevention process and determined by detection processes. Intrusion detection systems can make sense if there is someone or a system to respond to this detection. Otherwise, this situation does not go beyond the benefit of a car alarm that no one hears and cares about. In this respect, reciprocation is an important link that completes the security

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

process. Even if the attack is not completely prevented; It allows the system to return to its normal state, to identify the causes of the attack, to catch the attacker, when necessary, to identify security system vulnerabilities, and to reorganize the prevention, detection and response processes. Planning the actions to be taken when an attack is detected, in advance, will ensure that this process works effectively and will not waste time and money. Disaster recovery is at the forefront of the major worst-case plans undertaken for this phase.

Questions:

1. Which of the following is not one of the stages of asset management.

A) Making an inventory of assets

B) Determination of ownership of assets

C) Determination of the cost account

D) Determination of asset usage rules

2. What is the primary purpose of the Threat and Vulnerability testing process?

A) To best understand the security vulnerabilities of the assets and to take the necessary measures to protect these assets effectively.

B) Managing security vulnerabilities

C) Obtaining preliminary information about the asset inventory

D) Closing security vulnerabilities

3. Which of the following is not a type of vulnerability assessment?

A) Network-based scans

B) Host-based scans

C) Database scans

D) Server-based scans

4. Which of the following is not one of the Cybersecurity asset management process?

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

A) Vulnerability management

B) Cost management

C) Continuous control monitoring

D) Detection and intervention

5. Which of the following is not a way for IT to maintain the effectiveness of its security policies?

A) Risk assessment

B) Constant up-gradation

C) Quick mitigation

D) Security policies

6. Which of the following is not one of the three processes that constitute the ideal configuration of information security?

A) Preparation

B) Prevention

C) Determination

D) Answerback

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

- **What is vulnerability of IT systems**
- **Explain and give sample for Vulnerability Management and Risk Management**

Attachments *(PowerPoint presentation, handouts, prints, links, video…):*

References:

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

1. Evaluating IS Security Policy Development S.B. Maynard1 & A.B. Ruighaver2 Department of Information Systems University of Melbourne Australia
2. https://www.bizzsecure.com/how-it-can-maintain-the-effectiveness-of-security-policies/
3. https://blog.masterofproject.com/service-asset-and-configuration-management/
4. https://www.apptega.com/blog/change-configuration-management-cybersecurity
5. https://cam.scmagazine.com/it-service-management-vs-cybersecurity-asset-management/
6. http://www2.mitre.org/public/industry-perspective/documents/06-ar-cyber-coop-planning.pdf
7. https://icma.org/articles/pm-magazine/cyber-continuity-planning-go-big-or-go-home
8. https://www.kroll.com/en/services/security-risk-management/security-consulting/threat-vulnerability-assessments
9. https://www.xmcyber.com/blog/what-is-the-difference-between-vulnerability-assessment-and-vulnerability-management/
10. https://www.techtarget.com/searchsecurity/definition/vulnerability-assessment-vulnerability-analysis

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Employees Unit no: (3) Week 5 Unit (Module) name: (Security at business trips)	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Mirosław Mazurek • Paweł Dymora
Learning Activity Goals	1. Wireless networks 2. VPN 3. Email encryption
Skills to be Gained	• **TS3** • **SS2**
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Internet access • Internet Browser • MS Office365

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
The general outline of this module is to provide some theoretical and practical issues related to knowledge and practical skills security at business trips. You will have the possibility to protect your wireless network and use protected wireless networks with the idea of VPN. The module will also cover how to send emails securely using free PGP protocol for encrypted messages which no one can decipher without your permission.

Content of the Learning Material

1. Introduction to wireless networks. Theoretical basics: principle of operation, encryption protocols.

Earlier WEP and WPA protocols were used to secure wireless networks, but they were not resistant to hackers' attacks. The introduction of the WPA2 protocol allowed to ensure a sufficient level of security, but it does not provide full security anyway. There are many network topologies, wireless access protocols and network access acquisition techniques available, and both CPU (Central Processing Unit) and GPU (Graphics Processing Unit) computing architectures are used in network key acquisition [1,2].

WEP (Wired Equivalent Privacy) is one of the oldest IEEE 802.11 wireless encryption standards. It provides information protection based on the use of the RC4 algorithm. It has many known security vulnerabilities and has therefore been cracked multiple times. It is one of the oldest standards for securing WLAN networks (established in 1997). It does not require high computing power of the installed devices. It uses two user authentication methods: Open Authentication and Shared Key Authentication. In addition, it enables user verification based on physical MAC addresses using the ACL (Access Control List). There is a 64-bit WEP variant (based on a 40-bit key and 24-bit initialisation vector) and a 128-bit WEP variant (based on a 104-bit key). Some manufacturers have also introduced a 256-bit WEP standard [1,2].

WPA (Wi-Fi Protected Access) is another standard for encryption of IEEE 802.11 wireless networks. It was introduced to improve the level of security of WLAN networks, replacing known vulnerabilities in the WEP standard. It is based on the use of protocols: TKIP (Temporal Key Integrity Protocol) and EAP (Extensible Authentication Protocol), 802.1x standard and the MIC (Message Integrity Check) mechanism. The standard is based on the RC4 algorithm. It was

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

implemented as an interim solution between the WEP standard and the current most secure wireless encryption standard 802.11i. It provides work in two modes, which include: Enterprise (using a RADIUS server that manages the allocation of keys to users) and Personal (using a shared PSK key) [1,2].

WPA2 (Wi-Fi Protected Access 2) is currently the most powerful encryption standard for wireless networks (also known as 802.11i). It provides information protection based on the use of the AES (Advanced Encryption Standard). It was introduced to improve the level of security of WLAN networks, replacing known vulnerabilities in the WEP standard and the interim WPA standard. It implements the 802.1x protocol improving the control of user access to the network. It provides work in two modes, which include: Enterprise (using a RADIUS server that manages the allocation of keys to users) and Personal (using a shared PSK key) - often used in home solutions today [1,2].

The WEP algorithm is the least secure encryption standard for IEEE 802.11 wireless networks. It has been cracked many times by various methods due to the many currently known vulnerabilities in the security aspects of the algorithm. The main disadvantages of the standard include[3]:

- Lack of a defined key management system (often one network key is used by all nodes of a wireless network);
- Insufficient bit size of the network key (the first version of the WEP standard introduces 40-bit keys);
- Insufficient bit size of the IV initialization vector (the WEP standard introduces a 24-bit initialization vector, which turns out to be insufficient and, due to the relatively high probability of collisions with a small number of received packets, there is a possibility of a cryptographic attack to obtain the value of the WEP key);
- Weak ICV checksum based on CRC-32 linear function (there is a possibility of unnoticeable modification of the information sent in the network);
- Weak RC4 information encryption algorithm (there are too many dependencies between the network key and the result of information encryption);
- Insufficient user authentication system (there is a possibility of forging authentication messages).
- Based on the presented weaknesses of the WEP algorithm, many tools have been created to conduct attacks that test the security level of WLAN networks. The most popular attacks against WEP include:
- FMS attack - a statistical attack (developed by Fluhrer, Mantin and Shamir) on the RC4 algorithm used in the WEP encryption standard;
- KoreK attack - a statistical attack (developed by a person nicknamed KoreK) that uses several more (compared to the FMS attack) dependencies of the RC4 algorithm

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

encryption process;

- Chopchop attack - an interactive attack, carried out in the direction of gaining access to the network by gradually decrypting one of the received packets;
- PTW attack - is a statistical attack (developed by Pyshkin, Tews and Weinmann) on the RC4 algorithm, which, thanks to the successive dependencies of the data encryption process, significantly increases the probability of obtaining the key value with a relatively small number of received packets.

Another frequently used type of attack is the Dictionary attack. It is one of the brute-force methods of acquiring e.g. cryptographic key values in wireless computer networks. To obtain WPA/WPA2 key values, the method is based on one-way encryption and comparing entries in the dictionary with information in the captured 4-way handshake sequence. Dictionary attacks are carried out with the intention of reducing the time of obtaining key values compared to the brute-force method. The process of retrieving the key value continues until a positive result is obtained (i.e., when the entry in the dictionary turns out to be a valid key value) or until all entries in the dictionary are compared with the negative result. A negative result may indicate a high level of complexity of the key value and the need to use the brute-force method[3].

The success of this attack is the selection of an appropriate dictionary. Dictionary is a text file used in the case of dictionary attacks to obtain, for example, cryptographic key values. It contains a list of appropriately prepared items that may constitute the key value sought. The use of dictionaries in the case of force attacks allows to significantly reduce the set of examined values, which may result in speeding up the process of acquiring the cryptographic key value. The content of dictionaries is built, for example, on the basis of the presented items[3]:

- a list of words appearing in national and foreign dictionaries;
- combinations of words with uppercase and lowercase letters, words spelled backwards (i.e. palindromes);
- combinations of dictionary entries with cut out vowels or consonants;
- combinations of multiple repetitions of selected names, surnames, dictionary entries;
- combinations of words with numerical values, special characters, etc.;
- a list of passwords and logins most frequently used by users;
- a list of popular companies, organizations, technical terms, proper names, etc.;
- information leaks (i.e. logins, nicknames, passwords) from various internet portals;
- combinations of adjacent keyboard characters for selected patterns (Fig. 1).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

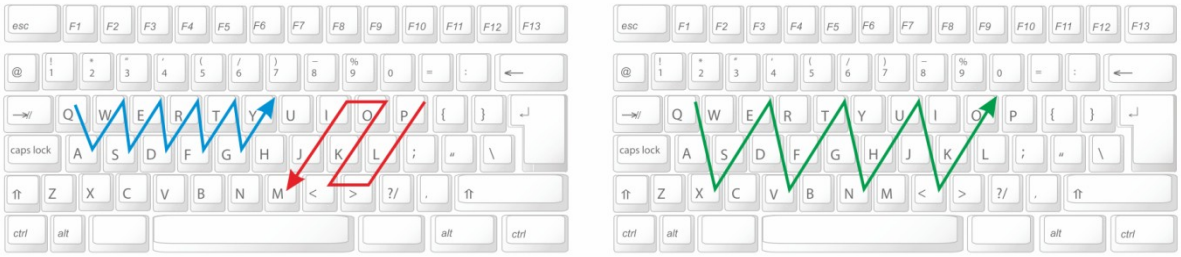


Fig. 1. Schema showing examples of network key creation patterns

The network key plays a key role in the study of network resilience. It is a sequence of characters used by network users in the authentication process. The authentication process is an important step in protecting access to shared services and network resources from unauthorized users. Network keys are often created and managed by network administrators and may constitute the weakest link in the security of a computer network. Key values that turn out to be relatively time-consuming or impossible to break using brute-force methods in realistic time should be generated, for example, based on the rules presented[3]:

- Each wireless network managed by the administrator should be secured using a different network key;
- Each network user should use an individual network key;
- Network keys should be built on a sufficient number of characters;
- The generation of keys should be based on the maximum available character space;
- Keys should not be generated using corporate and personal information;
- Keys generation should not be based on a list of items in publicly available dictionaries;
- Network keys should be built on the basis of random sequences of characters;
- Network keys should be updated periodically;
- Currently used key values should not be associated with key values that are no longer used.

2. Virtual VPN tunnels. Theoretical basis: types, architecture, principle of operation, encryption protocols. Installation of the Open VPN programme (configuration, addressing, parameter selection, key generation).

A Virtual Private Network is a tunnel through which private network traffic flows between the sender and recipient over a public network. VPN stands for 'Virtual Private Network'. A VPN network encrypts all activities on the internet, hides the IP address, protecting the identity of the network user. A VPN connection offers secure access to applications, websites and entertainment platforms from anywhere in the world. It is possible to optionally compress or encrypt transmitted data to provide better quality or a higher level of security, thus protecting privacy within the

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

network [4].

A secure tunnel is created by first authenticating the client with the VPN server. The server then applies an encryption protocol to all data that is sent and received. To ensure the security of each data packet, the VPN places it in an external packet, which is then encrypted by encapsulation. It ensures the security of the data during transmission and is a fundamental component of the VPN tunnel. After the data reaches the server, the external packets are removed in the decryption process [4].

VPNs can be divided into two main categories [5]:

- A remote access VPN that allows users to connect to a remote network, usually through special software.
- Site-to-site VPNs used by companies, especially large corporations. They allow users in selected locations to securely access other users' networks.

An example of a dedicated VPN development software is *RadminVPN*. In most cases it is not necessary to have a static IP address in your local network to set up a VPN tunnel. After downloading the appropriate software, it will create an appropriate network with a static address of your computer [6].

Radmin VPN allows you to connect to two computers on two different networks. A configuration example is shown below. For easier understanding of the operation of the VPN channel, Fig. 2 and 3 shows the initial configuration of computers between which a secure channel is to be created.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

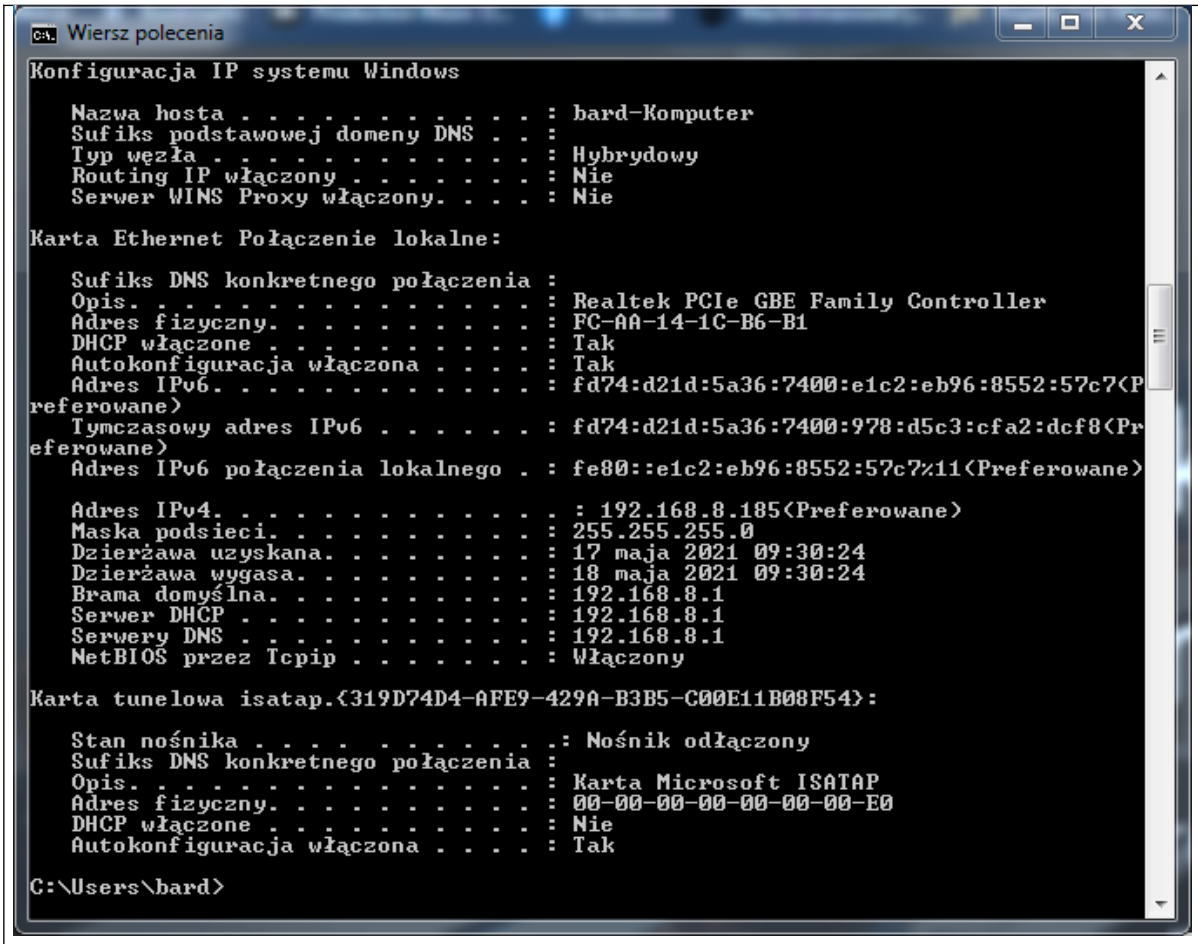


Fig. 2. Initial configuration of computers

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

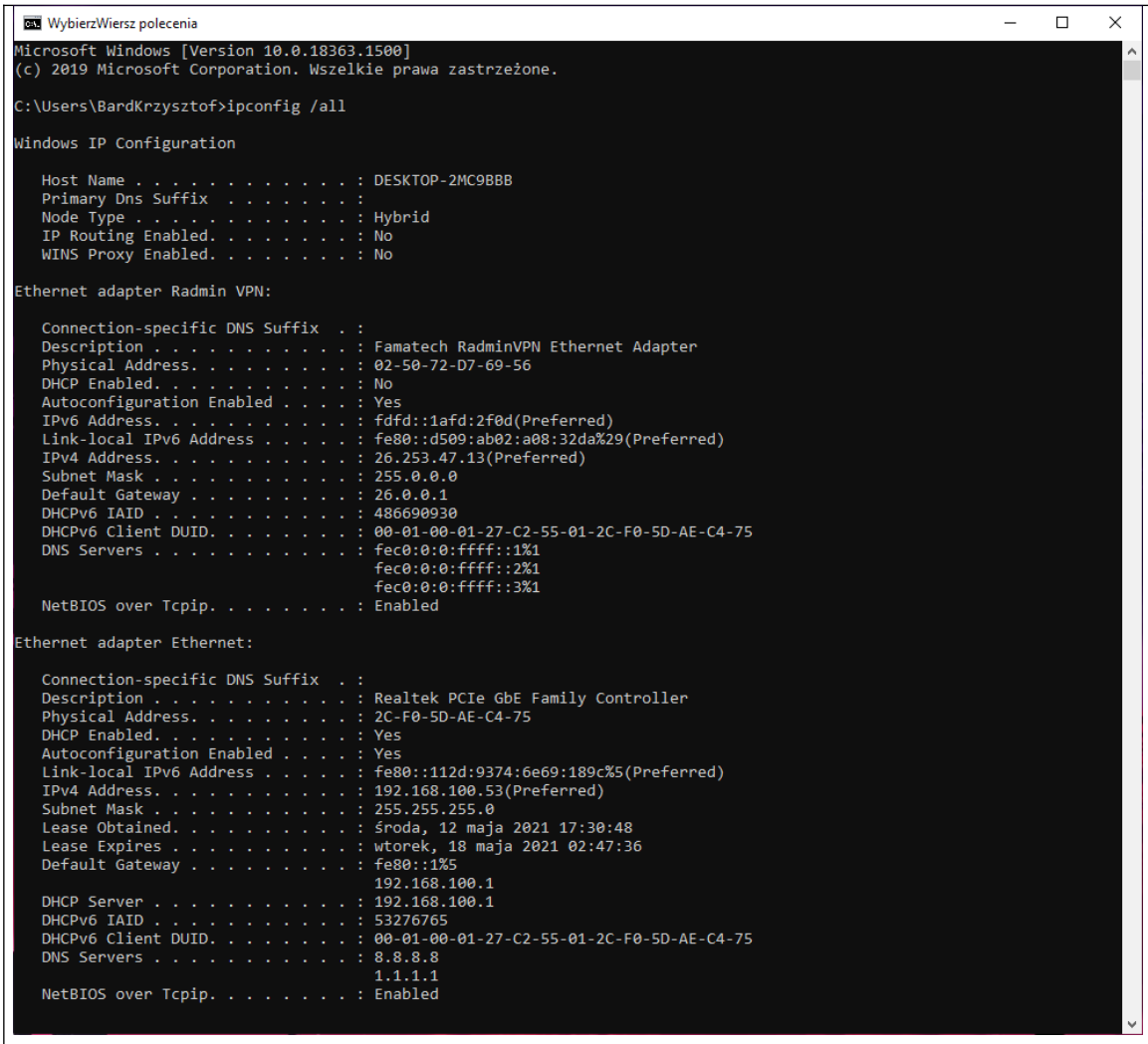


Fig. 3. Initial configuration of computers

As you can see, the gateway addresses are completely different, so computers do not have a physical or logical connection to each other. To create a channel, install RadminVPN on both computers. On one of them you need to start by creating your own network.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

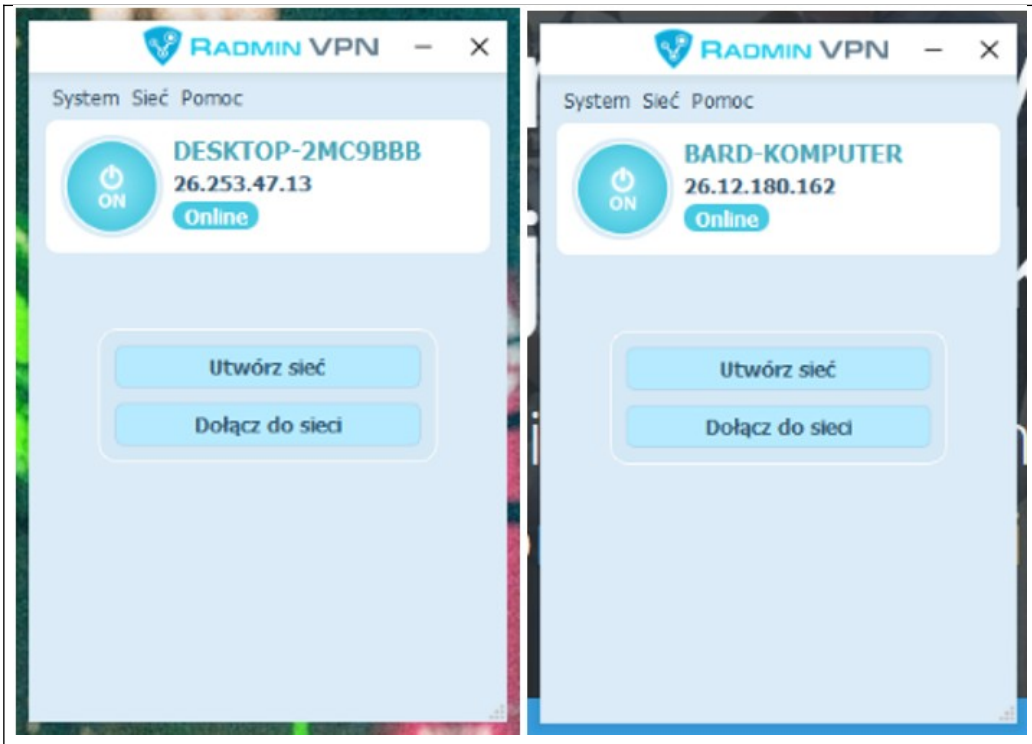


Fig. 4. View of application main screen (left image - configuration of computer 1, right image - computer 2).

To create a network, select **Create network** in the application window, provide a name and password for the network and confirm with the Create button. On the second computer, the network created in this way should be added by clicking the Join the network button, entering the name and password of the network just created.

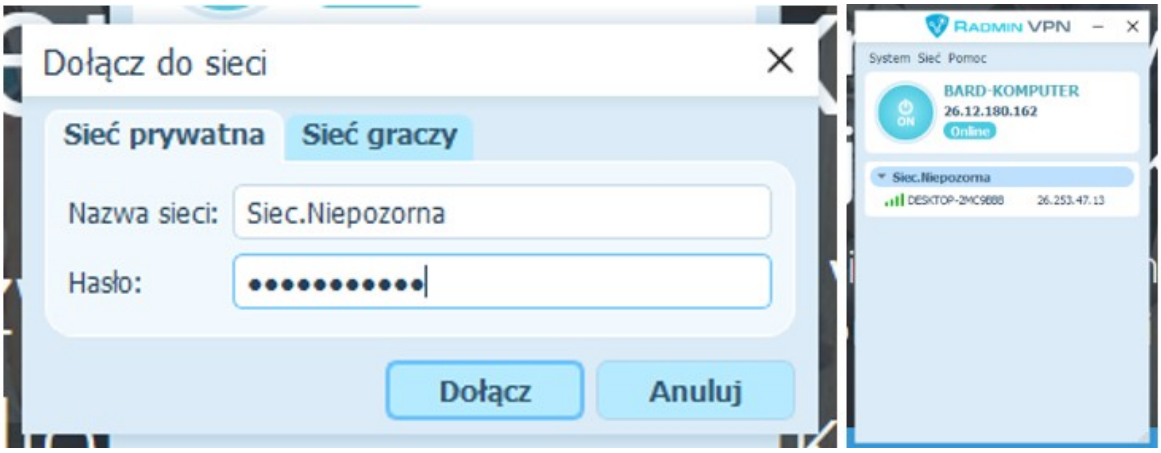


Fig. 5. a) View of the network connection window; b) connection status.

After successfully joining the network, both computers should be in a network connection view (as

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

shown in Figure 5b). In this case, you can see the name and address of the computer on the other side of the tunnel. It will be the same on the second computer. The connection attempt at this stage will fail as Radmin Server is required for system operation. Information about the installation will appear in the application and it must be done on both computers and restarted. After completing the entire installation process, computers will be able to communicate, but it will not be possible for one to take control over the other. In order to be able to control each other you have to configure the system remote desktop in Windows (Control Panel->System and on the right side choose Advanced System Settings).

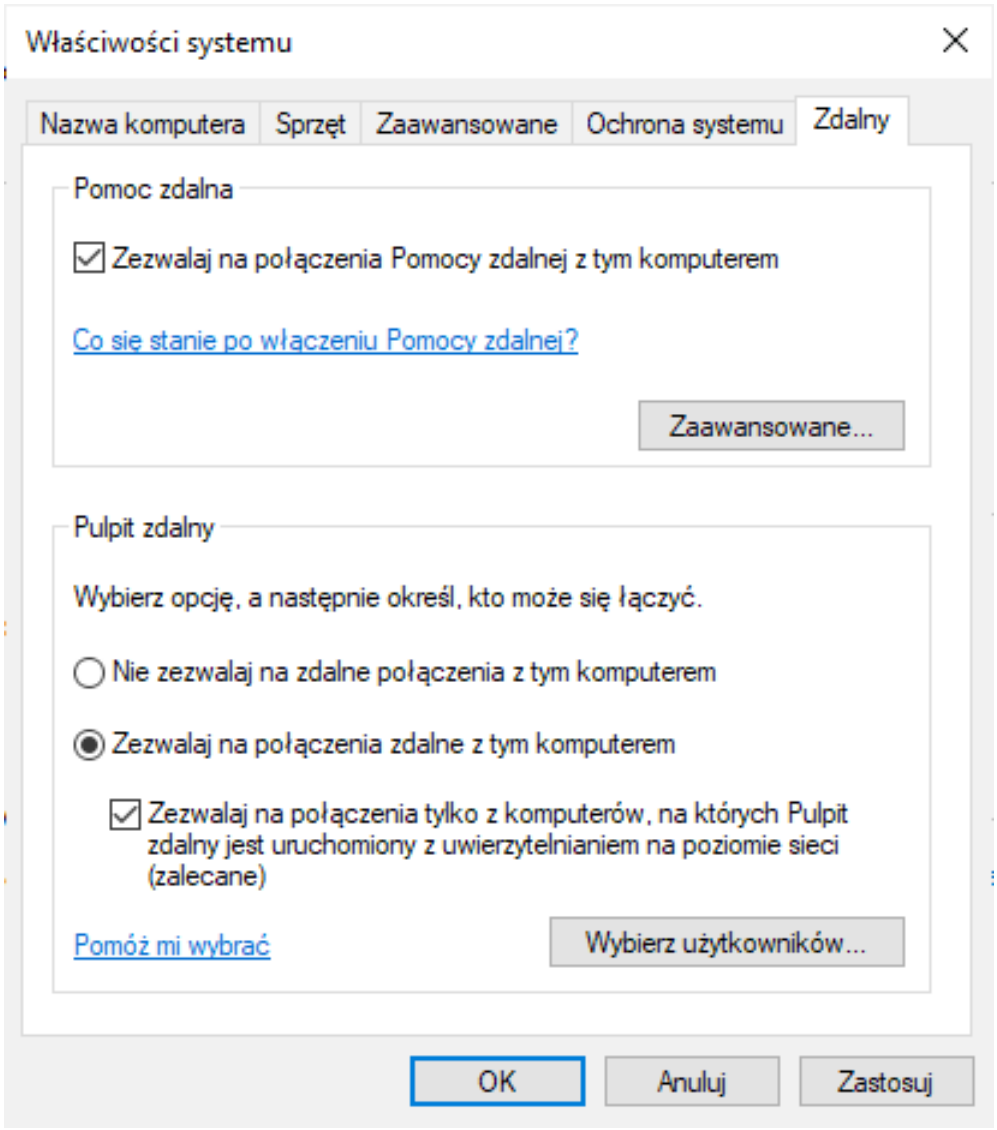


Fig. 6. Settings of Remote Desktop section

The System Properties window appears. Next select the Remote tab and the Remote Desktop

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

section by selecting Allow remote connections to this computer (Fig. 6). After approving the changes on both computers, create a user with given access rights. To do this, run RadminServer and from the fields on the right choose Permissions and then the Permissions option. In the permissions window, check Full access and create a user (you need to give him/her a name and a password). This completes the VPN channel configuration process. The created tunnel is bi-directional and can be easily used to control computers from both sides.

3. Email encryption. Theoretical basis: types of encryption (symmetric and asymmetric), security, protocols, keys. Installation and configuration of OpenPGP. Installation and configuration of an email client.

One of the most widely used communication channels is electronic mail (email), which is increasingly becoming a target for hacking attacks. Protecting this element is an important part of a cyber security solution package. Protecting email and encrypting attachments are two very important online security issues. Email encryption not only minimizes the risk of confidential data leaking, but prevents unauthorized interception. Email and its attachments are not secured by default with SSL and TLS protocols, and all messages are sent as plain text [8].

Encryption algorithms, like cryptography, fall into two categories:

- symmetric encryption algorithms;
- asymmetric encryption algorithms;

The main difference between the two encryption methods is the number of keys used. Symmetric encryption uses a single key, while asymmetric encryption uses two different but related keys. One of the keys is the private key and the other is the public key. Symmetric encryption algorithms use the same key to perform both encryption and decryption functions. The asymmetric encryption algorithm uses one key to encrypt data and another key to decrypt it. This means that if we want to send an encrypted message to someone, we encrypt it with the recipient's public key, and the recipient uses his/her private key to decrypt it.

Another criterion for dividing encryption is that of key length. The length of the key is directly related to the level of security provided by each of the cryptographic algorithms. The longer the key, the safer the data. In symmetric algorithms, the keys are randomly selected and their length is typically 128 or 256 bits, depending on the level of security required. In the case of asymmetric encryption, in order for encryption and decryption to take place, there must be a mathematical relationship between the public and private keys (in the form of some unique mathematical formula).

Due to its greater speed, symmetric encryption is widely used to protect information in many modern computer systems, such as the Advanced Encryption Standard (AES) used by the US

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

government to encrypt confidential and secret information. AES has replaced the earlier data encryption standard (DES).

Asymmetric encryption is used in systems where multiple users may require access to both encrypt and decrypt a message or data set. An example would be email encryption where the public key can be used to encrypt the message and the private key can be used to decrypt it.

One solution is the OpenPGP standard. Defines cryptographic email extensions - encryption and digital signatures. The standard was based on the existing PGP programme. Currently, there are many different implementations. The standard is defined in RFC 4880. Often, users use the Thunderbird email client in the process of sending emails. This client allows you to send and receive encrypted and digitally signed emails using the OpenPGP standard. This feature is commonly known as end-to-end (e2ee) encryption and makes communication more secure and less likely to be spied on by third parties. Thunderbird 78 has built-in support for two encryption standards, OpenPGP and S/MIME.

Previous versions of Thunderbird (v68 and earlier) had built-in S/MIME support, and you could add OpenPGP support using the Enigmail add-on and GnuPG software. The Enigmail add-on is no longer available for Thunderbird 78, except to help its former users migrate to OpenPGP in Thunderbird 78 or to get guidance on how to restore their 'Junior Mode' rules from Enigmail. You can upgrade your Thunderbird settings from an older version (e.g. 68.x) to version 78.x. Before using Thunderbird 78 for the first time, however, it is recommended that you back up your Thunderbird profile, as after the upgrade, the profile can no longer be used with Thunderbird 68.

Enigmail used GnuPG to store and manage all keys and trusted settings. You can migrate and Enigmail will read the old keys from GnuPG and import them. Thunderbird 78 uses different settings than Enigmail. With Enigmail, it was possible to enable OpenPGP for an email account, but let it automatically choose which key to use. Thunderbird 78 combines these settings. To enable OpenPGP for an email account, you must explicitly specify which key to use.

GPG4win software will be used for encryption. It is a set of advanced data encryption tools. It enables protection against unauthorised access not only of email, but also of files and folders. Working with Gpg4win is based on asymmetric encryption, i.e. on the basis of two keys - private and public. The first one is used to encrypt data, the second one should reach the recipients of the message who can access it. Keep the private key in a safe place.

The package includes such elements as the GnuPG encryption tool, Kleopatra certificate manager (Fig. 7), alternative GPA certificate manager, Claws Mail email client, as well as two plugins that allow integration with Microsoft Outlook (in versions 2003, 2007, 2010 and 2013) and Windows Explorer.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

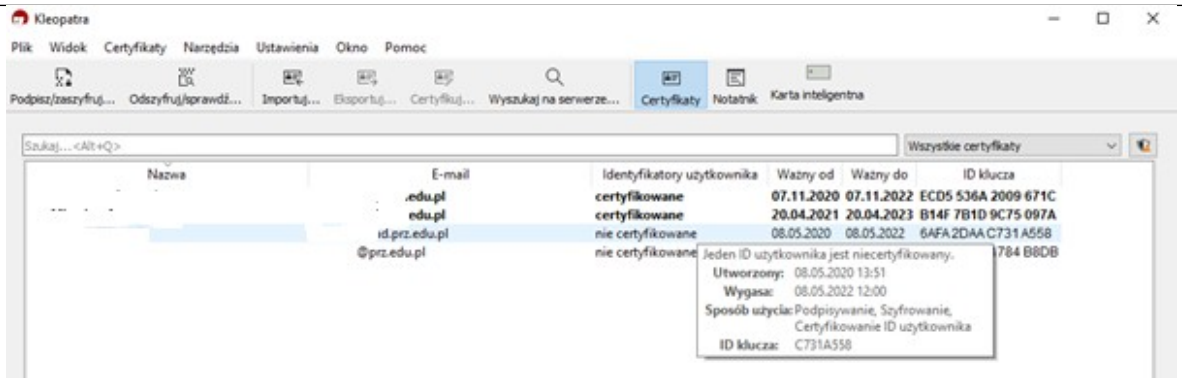


Fig. 7. Certificate manager - Kleopatra.

Gpg4win supports the OpenPGP and S/MIME (X.509) standards, creating certificates by default using 2048-bit keys. RSA is the standard encryption and signing algorithm. Additionally, the package also allows the generation and verification of SHA1, SHA256 and MD5 checksums.

Configuration of the message encryption environment.

After assigning email accounts to the GPG4WIN programme, a pair of keys should be generated. A pair of keys consists of a private key and a public key. The private key is assigned to a specific account. A person who wants to send an encrypted message to this account must have the recipient's public key.

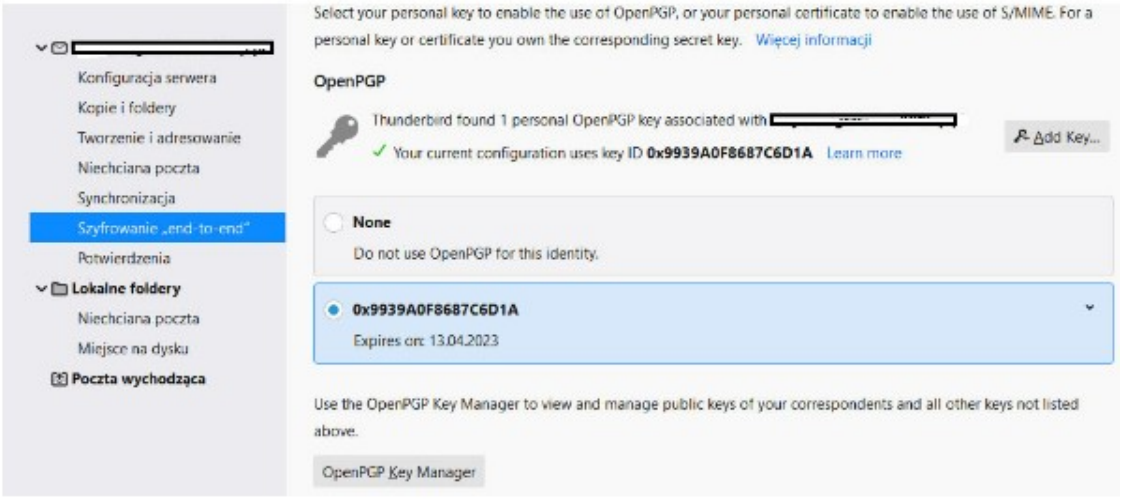


Fig. 8. Settings of Remote Desktop section

Once the accounts have been configured in Cleopatra, you can directly use Thunderbird to send and receive encrypted messages without using an external programme. Remember to send your public key when sending your first message to a new recipient (Fig. 8). An example of an

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

encrypted message is shown in Fig. 9.

```
-----BEGIN PGP MESSAGE-----

wcDMA0r5u59RHK/uAQv/cvK0XliobGKfmQ25IcGe4kxtcXan9oDhQ0HODeAQyLSfpPFYOitt4LpF
Kc2aae3ayqRN+0bhTESVFaxttCw76E5wszkM9cK8UdxYzrX9PuaujtzYj8kSx3m0skfXrdglYnM8
llIYNETSgTnFSZ4jHKQLVIHVw9ZMztoo/ibLVJY3TTd7aKn7+cYyepNasrPPzoxcSGjJ1pQCkJ6t
SGtm8HDBfekKbK6qTKefYdGrCDBS4sAsuszwaX5QtSn50LAE2FkXCiKzTh6DkdFxQQ7yk/rUTs93
MkRwRtjteDqO7KC1yNPBim+KVLVG20EibD1FrdFIsbaEaPIl3Y06LhmjBMrUOUaMhPJpYDM1Ki8u
gqGHOQmqISQU1y6/poyGDmOfSPOFchWaTB+9fjzpmEb32mK10D1JOM2llut5AtmZH8W11Kpy4cdC
XygSXMkJ4as+p9/MtICdESyFkDXamESbtI04Ay5Xj+YrBnQ+Wk0lHOeLfSFg+cj7fwUuasRvEIe0
wcDMA3pK1foZRRoWAQv/UVilR5h++k8Tq8uk/IeUchC3Si832Li8Ro++dGxy65Gomjlzg+oxbOoj
0u1kZGs5QbCywv5+vlo7CxpGSeMcBbjlT5jV/cKk1An9bdCjADXFLw4sEWCtqTR47OFqArvqi2gm
2iOW4g6Zcnd21cfGe5kmeyRKt8OmHL6LDaZXSnJCJkhNRwr3GKHh8gJeT00bn+72M9TbBKXxLe3T
bnGw2ypPIQJ55k2x+ZbgkjDnQQDogsHpB1ip7K5yYArf+rI4uPqbYQgSU3NYYAUsmOtI2yesouvV
gFic/0TE9xq0qhciE2bTWPxH5ikxCMwLQa33E8+hngsSDfoyoRdolSEwjhI8KHthzddXzPNSkdgn
Q4pdGU1jFaDivtLc7cNs3SFKoZBiZcQaHRTABVNDMQgRqgoG6F0Ditu03vXCh5aR8/zUVS6moGT8
2sh/VWvryEAHKLSUPZulgwaZlD5hxosUMuwzGibLzaCApbilNdzm4zaDz2KdGBwmvyGkC7oT4lvj
0sMwAbnd2f3Hz+AuXFajZ6uO8m6ibKMtJRM3EXggkNhue0rIU4KLchp9U9jLAt6GMQjPFKmgGqEj
U7/QPiVbJ8DjbmhYH90JwYH8hJCx1rq4AtXOxJgz8w0B+MOe6maKxDaDqS9gQj/n9N/Hvj8btZKz
turb54Y8MxZXXXoNxLAVZr1HHcbQoweHIx0EXanoMsxEwT3ugAiQetwBzXnR9DOzxTkzeOMK1ooS
6jnVTQy454q1+w6fNWAfBbpYY73Lt1NifD7mHoqe1G3oWhgzj/uUs67TJ1DjLfqzhxqw0TnfXyNM
+457fZCj+iYwdV8DhfDb4dyfYmDjA8LLP8Uw7gLtkFxD1dsaLf7/xQ5g98eKhz/4INI0xL+5Znno
x4SnkX++hy4z/nRKBNQcIupW7KuG1SOABTIhQWx3mtxyte0mxBRxiApfC5HfNzQM+vtmhJK8mlHK
Osc3kVw6kTodafSTi/qLghcOh2R7h8hL7qRc56ig7i4nPY5bnsPpfyyPYAuUDJQUz5z4tFrdEX/+
gw/gH3O8hTS17VSfgya0BUwJvMnlbS1+VZ7zomF405ne8hrFsT5j/dnjP7NgGS3CVMDLyEDtQA7k
Vbru0EN4JTsCu3T7rMnRrGtX1kfsTXBLayhcpbaMyHojMKw60p41o2gvTn5fw/+GJHGQdsZ3HJ+g
fr9EWKLQzQX6PSLsJ5OexLRkMtHXV4jBoSRyTzFTwprBkNNKZu2aRYa17BBFuVc5RTf8rSVWq7Eq
rKrXGOP+GgqGGTxoD8zfFtp0YJ+mP28L0DtuPnmG9IzxdbXO/JG6sT6hzPEA6MIlaW6Y++94Jpg2
XEKsGOdW9IHx9613FwjPtj6HKC8GtN5s8dgSAm3tw5KUWfchtKIOZYiynxuRnwIMN0UM0G2QFKYr
pU+50ba8rdui9D2YFzEcbw9a3meaWksO3Zvd8obQfwGFMX9DwV5VPEcmASHEUMULGBUO3KIUtaxU
Sdg9qmehxPMkkH3bB3x+G79WmV0ss0G9r+uVk/XhzxckqUI0w++q2PmWsXAIP2NsyX7W1BHyZ5J0
HhUwUllGtpl3gv/WwOxTyoEz2oeQucK5Eq91vEwaudCnip7STqK2WpboGvAQ54ZIZRFbm/4sOd/W
4kH6xyeYBTsIf3ft7LyvoB6Xq9lA1xOFe94CcAqty90FynvF26Da7QRsNQalhfhfB1bnaEQIgf+7
J9fpMYQEcC4tT8RW9vtozQurNpgZnZS9sjWjke6/j3XV7paxOW7OG8nc+1r09LQMMtVjvI5Zd1FV
JyAtr1EsoF/9MzFfofn6eCtU8VvXiS8+cIDjTqrb2EKS68Rpu9Z8LCgz
=MjYk
-----END PGP MESSAGE-----
```

Fig. 9. An example of an encrypted message.

Thunderbird automatically decrypts messages and attachments sent with them. Remember that you need to know the recipients' public keys before sending encrypted correspondence. Encryption with the GPG add-on protects not only the content, but also the attachments. Without knowing the recipient's key, we are unable to send an encrypted message. Additionally, Thunderbird allows you to synchronize several e-mail accounts.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. What is a VPN?
2. How you can use VPN solution?

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

3. Can you send someone your private key for PGP e-mail encryption?

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

1. Method of secure access to your data from remote access
2. Methods of securing your e-mail conversation

Attachments:

1. Presentation
2. Video movies

References:

1. Rana, Muhammad Ehsan & Abdulla, Mohamed & Arun, Kuruvikulam. (2021). Common Security Protocols for Wireless Networks: A Comparative Analysis. 10.2991/ahis.k.210913.080.
2. Habibi Lashkari, Arash & Sendón Varela, Juan & Samadi, Behrang. (2009). A survey on wireless security protocols (WEP, WPA and WPA2/802.11i). 10.1109/ICCSIT.2009.5234856.
3. Kumkar, Vishal & Tiwari, Akhil & Tiwari, Pawan & Gupta, Ashish & Shrawne, Seema. (2012). Vulnerabilities of Wireless Security protocols (WEP and WPA2). International Journal of Advanced Research in Computer Engineering & Technology. 1.
4. Costa, Luís & Fdida, Serge & M. B. Duarte, Otto Carlos. (2000). An Introduction to Virtual Private Networks: Towards D-VPNs.
5. https://www.vpnmentor.com/blog/different-types-of-vpns-and-when-to-use-them/
6. https://www.radmin-vpn.com
7. https://www.fortinet.com/resources/cyberglossary/pgp-encryption

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Employees Unit no: (3) Week 6 Unit (Module) name: (Privacy & Data Protection)	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Mirosław Mazurek • Paweł Dymora
Learning Activity Goals	1. Encryption of disks and partitions 2. How to use VeraCrypt Tool
Skills to be Gained	• **TS1** • **SS1** • **SS2**
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Internet access • Internet Browser • VeraCrypt program

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
The goal of this module is to gain knowledge and practical skills related to data protection and encryption of data on your private or corporate disk.

Content of the Learning Material

1. Encryption of disks and partitions. Theoretical basics: principle of operation, encryption algorithms. Installing the program (configuration, defining the disk, choosing parameters, generating keys).

The security of computer systems requires protection not only of resources such as the operating system itself, applications, but most of all data. Known security methods by preventing access to resources, such as a firewall, are not always effective. Therefore, multiple security methods should be combined with each other. The presented method of data encryption allows for the elimination of many threats resulting from an intruder's access to our computer.

One of the most widely used solutions is the free VeraCrypt data encryption software. It allows you to encrypt not only entire disks or partitions, but even portable USB disks and create virtual encrypted disks with a certain capacity. VeraCrypt enables encryption using the following algorithms: AES, Camellia, Kuznyechik, Serpent and Twofish; as well as multiple encryption with: AES-Twofish, AES-Twofish-Serpent, Serpent-AES, Serpent-Twofish-AES, Twofish-Serpent.

Depending on the configuration of the computer, the speed of encryption and decryption for each of these algorithms will vary, as shown in Figure 1.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

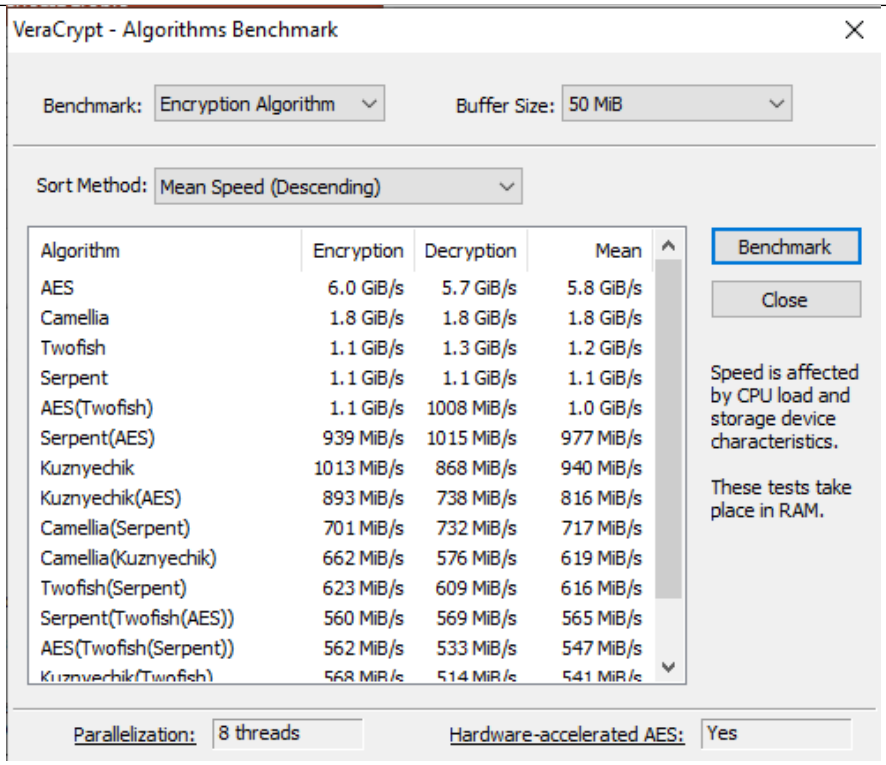


Fig. 1. Testing the speed of algorithms

The encryption process begins with the creation of the volume. You can encrypt an entire disk, partition or any volume (Fig. 2).

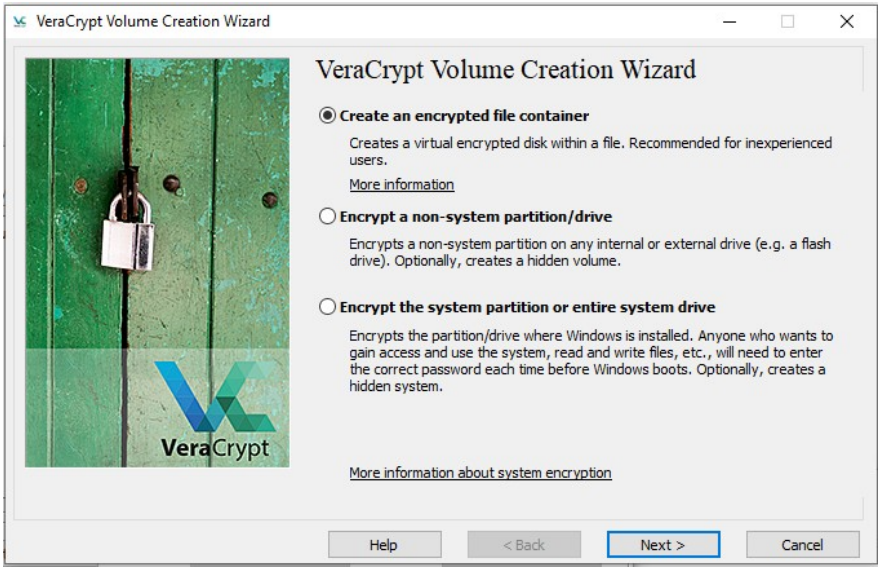


Fig. 2. Window of the VeraCrypt volume creation wizard

After selecting the location of the volume, you should give it a name. The VeraCrypt volume

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

is placed in a file that can be saved on a hard disk or a USB drive. The volume behaves like a normal file, i.e. we can copy it, rename it, etc. The next step is to select the appropriate encryption algorithm, e.g. AES, and to assign an access password in compliance with the relevant quality rules (appropriate length, upper and lower case letters, numbers, special characters). Then the volume is formatted. To increase its security, the wizard asks you to generate random mouse movements, which significantly improves the cryptographic quality of the generated keys (Fig. 3). After formatting, the volume is available for use. It only needs to be connected by entering the password (Fig. 4).

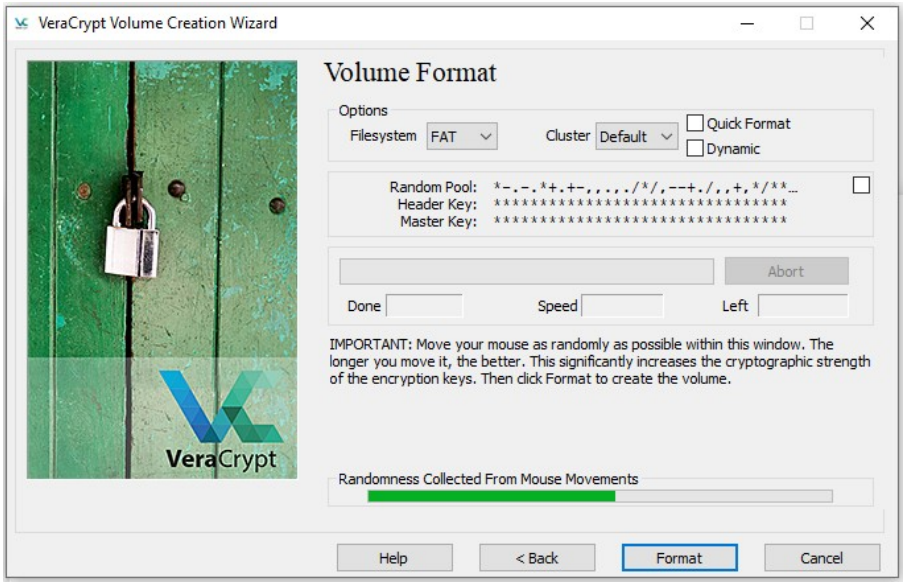


Fig. 3. The process of formatting VeraCrypt volumes

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

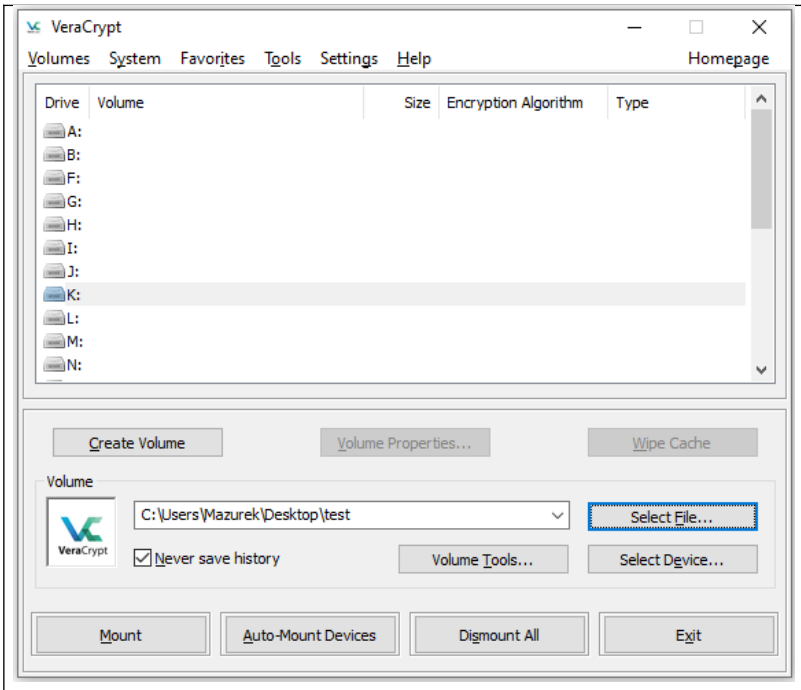


Fig. 4. VeraCrypt volumes connection window

In cases where we want a high level of protection, and we do not care about the encryption time, multiple encryption should be selected. Testing the performance during encryption for volumes of different capacities with different algorithms at the same time, one can notice that the stronger the encryption algorithm, the lower the speed of encrypting and decrypting the file. Not every algorithm responds to a change in volume size equally. Creating a volume is quick and easy, thanks to the clear instructions from the installer.

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions.

1. How you can protect your data on your computer hard drive?
2. What kind of computer programs you can used in order to protect your data?

Self-assessment questions. After answering the learner can see the results and compare them with these saved on the platform

1. What is the safest encryption method to secure your files?

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Attachments:

1. Presentation
2. Video

References:

1. https://www.veracrypt.fr/en/Home.html
2. https://github.com/veracrypt/VeraCrypt
3. https://veracrypt.eu/en/Beginner%27s%20Tutorial.html

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Employees Unit no: (4) Week 7 Unit (Module) name: (Social Engineering)	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other** Streaming Webinar, Text, Self-assessment Exercises, Exercises with answers on discussion forums and within the organized sessions with trainer/mentor, e-portfolios
Learning Responsible	• David Sommer • Ileana Hamburg
Learning Activity Goals	1. Social engineering attack techniques 2. Importance of Social Engineering Training 3. How to Protect from Phishing Attacks 4. Social engineering from an interdisciplinary view
Skills to be Gained	• **TS3 Network security** • **TS4 Penetration (exploitable vulnerabilites) testing** • **SS3 Cognitive and behaviour analysis**
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Internet access • Internet Browser • MS Office365

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
Social engineering is an important and verry often threat to information security. This module explains shortly the Lifecycle of social engineering, how an attack occurs and can be prevented. Particularly phishing is described, as one of the most popular social engineering attacks. Many companies use technical solutions to prevent attacks, but technological measures are not very effective if staff is not trained correspond. This is one of the aims of this unit. The learners could be informed about such aspects by reading the corresponding text, watching streaming webinars and solving exercises at own pace. All these documents are on the digital interactive project platform. The learners can test their answers on Self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forum and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the meetings. They will be supported to develop e-portfolio important for reflection and evaluation of the training

Content of the Learning Material

What is social engineering?

Social engineering can be defined as manipulating human beings, most often with the use of psychological methods, to gain access to data, documents, and information that the attacker should not have access to obtain. Various forms of social engineering can be found years ago but due to increased use of technology in main aspects of business and life, the threats grow and became a complex process difficult to stop. Social engineering is one of the leading threats to information security today and is an effective form of cybercrime. Potential repercussions of a successful social attack can be very dangerous for people and organizations. In 2019, for example, phishing, a form of social engineering crime, was responsible many data breaches, more than any other type of attack._

Many social engineering attacks have financial scops and sop organizations lost considerable money

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

amounts. In 2020, for example, U.S. losses $4.2 billion, according to the FBI (Abbate, 2020).

Companies could suffer business disruption — loss of productivity, a decline in employee morale and difficulties for organization to recover. This process can have consequences, often an incident response team is fired, security software to help prevent future attacks should be provided and employees must be requalified. Companies, in case of a social engineering attack could suffer also damage of reputation because customers are not convincing that the organization can protect itself.

Importance of Social Engineering Training

It is difficult to protect against social engineering because the tactics that attackers use are based on individuals' behaviour and if employees do not have corresponding training to recognize social engineering attacks, the risk of falling victim is great.

Social engineering training could be included in security awareness programs and gives employees the knowledge and tools they need to recognize these types of attacks and protect both themselves and their organization (Weßelmann, 2008).

Due to importance of social engineering training in minimizing threats, many organizations particularly SMEs which have less resources should be helped to take cyber awareness training including social engineering very seriously and offer their employees possibilities to follow it (Mimecast Contributing Writer, 2021).

By 2022, for example, it is planned that 60% of large organizations will consider security awareness (Gartner Magic Quadrant for SAT 2019).

Social Engineering Attack Lifecycle

Often social engineering attacks are done in more steps. The attacker first investigates the intended victim to gather necessary background information, such as points of entry and weak security protocols which are needed to the attack. Then, the attacker tries to gain victim's trust and provide stimuli for actions not usually security practices, such as become sensitive information or granting access to critical resources. Figure 1 explains the Lifecycle of an attack.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

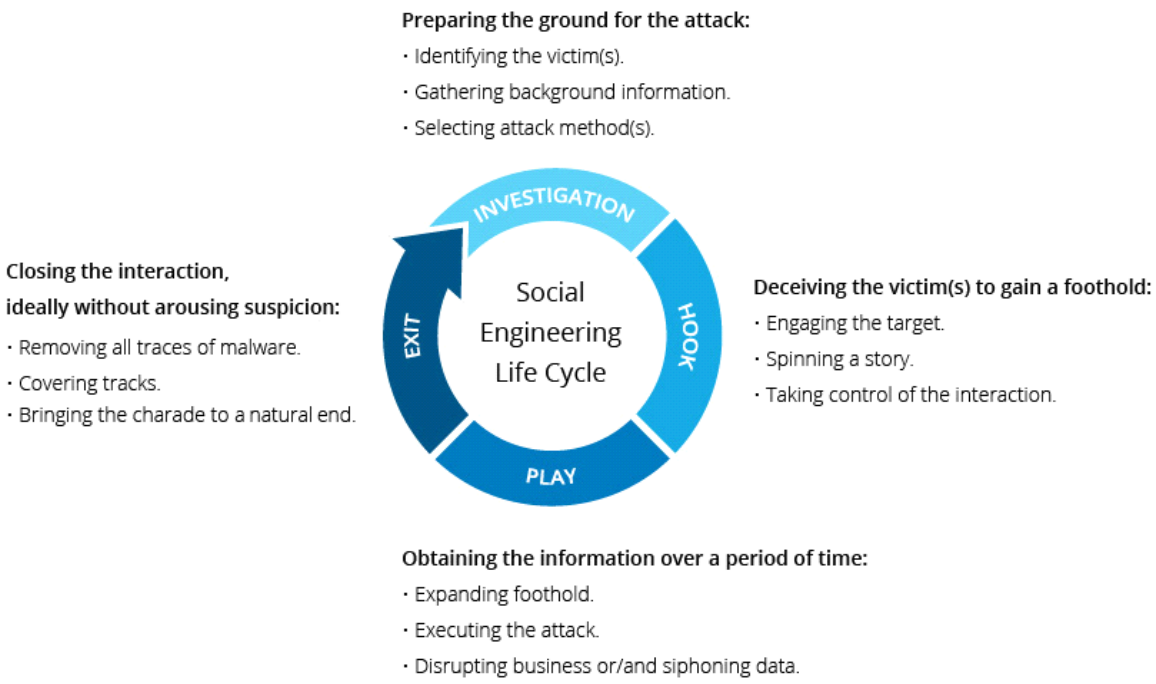


Figure 1: Attack Lifecycle (https://www.iacpcybercenter.org/resource-center/what-is-cyber-crime/cyber-attack-lifecycle/)

Social engineering is particularly dangerous because it is based more on human error, not on vulnerabilities in software and operating systems. It is more difficult to predict mistakes made by legitimate users, identify and stop these than a malware-based intrusion.

Social engineering attack techniques

Social engineering attacks have different forms and can be done anywhere where human interaction is involved. The most common forms of digital social engineering attacks are the followings:

Baiting

Baiting attacks try to achieve a victim's curiosity. They attract users into a trap stealing their personal information or infecting their systems with malware. The most often form of baiting uses physical media to disperse malware. For example, malware-infected flash drives, in conspicuous areas where it is sure that potential victims see them (e.g., bathrooms, elevators, the parking lot of a targeted company). The bait has an authentic look, such as a label presenting it as the company's payroll list. Victims pick up the bait and insert it into a work or home computer,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

resulting in an automatic malware installation on the system. Baiting attacks don't necessarily be done out in the physical world. Online forms of baiting consist of tempting ads that lead to malicious sites, which encourage users to download a malware-infected application.

Scareware

Victims become false alarms and fictitious threats. Users think their system is infected with malware and they must install software that has benefit only for the attacker or is malware itself. Scareware is considered as deception software, rogue scanner software and fraud ware. A common scareware example is the legitimate-looking popup banners in own browser while surfing the web with text such as, "Your computer may be infected with harmful spyware programs." It either offers to install the tool (often malware-infected) or direct the victim to a malicious site where own computer will be infected. Scareware is also distributed via spam email that makes offers users to buy worthless/harmful services.

Pretexting

Attacker obtains information through a series through lies. The scam (fraud) is often initiated by a perpetrator underlying to need sensitive information from a victim so as to perform a critical task. The attacker usually starts by establishing trust with their victim by impersonating co-workers, police, bank and tax officials, or other persons who have right-to-know authority. Attacker asks questions that are required to confirm the victim's identity, through which they gather important personal data. Many important information and records can be gathered using this fraud, i.e., social security numbers, personal addresses and phone numbers, phone records, staff vacation dates, bank records and even security information related to a physical plant.

Phishing

Is one of the most popular social engineering attack types; phishing scams (frauds) are emails and text message campaigns aimed to achieve curiosity or fear in victims and encourage them to give sensitive information, clicking on links to malicious websites, or opening attachments that contain malware. An example is an email sent to users of an online service that alerts them of a policy violation requiring immediate action, such as a required password change. It includes a link to a not legitimate website—nearly identical in appearance to its legitimate version— and the user enters their current credentials and new password. The information is sent to the attacker. Because identical, or near-identical, messages are sent to many users in phishing campaigns, detecting and blocking them are easier for mail servers having access to threat sharing platforms.

Spear phishing

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

This is a special form of the phishing attack because an attacker chooses specific individuals or enterprises. Attackers adapt their messages to characteristics, job positions, and contacts of their victims to make their attack less conspicuous. Spear phishing requires more effort from the perpetrator (person who commits the illegal act) and could take weeks and months to prepare it. It is much difficult to detect such attacks and they have better success rates. As an example, a spear phishing scenario involves an attacker who, as an (existing) organization's IT consultant, sends an email to one or more employees. It is signed exactly as the consultant normally does and recipients think it's an authentic message. The message requires victims to change their password and provides them with a link that redirects them to a malicious page where the attacker steals their credentials.

Detect Phishing

Scammers (people making fraudulent business) use email or text messages to trick persons to communicate their personal information. They try to steal passwords, account numbers, or social security numbers. If they get that information, they could gain access to email, bank, or other accounts. Scammers launch thousands of phishing attacks like every day — and they're often successful. Scammers often update their tactics, but there are some signs that help victims to recognize a phishing email or text message, like following:

- Phishing emails and text messages can look like they're from a company you know or trust. They look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.
- Phishing emails and text messages often tell a story to trick victims into clicking on a person link or opening an attachment. They may say they've noticed some suspicious activity or log-in attempts, claim there's a problem with the account or payment information, say that person must confirm some personal information, include a fake invoice, want the person to click on a link to make a payment, say the person is eligible to register for a government refund, etc.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Figure 2 shows a real-world example of a phishing.

The email looks like it's from a company the person know could and trust: Netflix. It even uses a Netflix logo and header.

The email says own account is on hold because of a billing problem.

The email has a generic greeting, "Hi Dear." If the person has an account at the business, it probably wouldn't use a such generic greeting.

The email invites the person to click on a link to update your payment details.

This email might look real, but it's not. The scammers who send emails like this one do not have anything to do with the companies they pretend to be. Phishing emails can have real consequences for people who give scammers their information. And they can damage the reputation of the companies they're spoofing.

Protect against phishing

Own email spam filters could keep many phishing emails out of own inbox. But scammers are

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

always trying to outsmart spam filters, so it is useful to add extra layers of protection.

Methods to protect:

- To protect own computer by using security software, software should be updated automatically to deal with security threats.
- To protect own mobile phone, software should update automatically.
- To protect own accounts, multi-factor authentication should be used.

The additional credentials to log in to own account can be grouped into:

- A passcode gets via an authentication app or a security key.
- A scan of own fingerprint, retina, or face.

Multi-factor authentication makes it harder for scammers to log in to other accounts if they do get corresponding username and password. It is important to protect own data by backups which aren't connected to own home network. Own computer files should be copied to an external hard drive or cloud storage. Also, data on own phone should be copied.

Act to a Suspect a Phishing Attack

- If an email or a text message comes that asks to click on a link or open an attachment, ask: Do I have an account with the company or know the person that contacted me?
- If the answer is "No," it could be a phishing scam. You have to review the tips in How to recognize phishing, look for signs of a phishing scam, report the message and then delete it.
- If the answer is "Yes," contact the company using a phone number or real website without put the information in the email because attachments and links can install harmful malware.

Responding to a Phishing Email

There are specific steps to take based on the information lost

- Run a scan.
- If a phishing email or text message is received, report it.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Social engineering from an interdisciplinary view

The networked today's world and the intensive use of the internet and technology are catalysts for social engineering attacks. System protections are helpful to mitigate some social engineering attacks, but it is not enough. The Federal Bureau of Investigation's internet crime underlined the increased use of social engineering and business email fraud schemes resulted in billions of dollars in losses over the past several years (Abbate, 2020). Again, methods of hackers, it is necessary to use an interdisciplinary approach to understand this phenomenon and all its complexities, especially in the context of how it affects businesses. Literature reviews highlight perspectives from different disciplines: information technology, psychology, business and ethics. Figure 3 illustrates this view (Washo, 2021).

Information technology discipline

Social engineering cannot be discussed unless in the context of the actual information systems and their use in the business. Technical defences can be used as a form of risk mitigation and control strategies are recommended to be used. Multi-factor authentication is a common and often effective way for organizations to confirm that the person accessing the systems should actually have that access. For example, a login process with a username and password would be one way for the user to be authenticated. An additional factor could be the use of a virtual private network (VPN) login to further validate the user.

Psychology discipline

Social engineering is connected with deception, so a psychological approach to understanding the concept is important to understand the thoughts and behaviours of both the attacker and victim. The use of psychological methods is important to social engineering because they are used to support the protections such as firewalls and systems used to identify intruders (Bullee, Montoya, Pieters, Junger, & Hartel, 2018). The entire information technology network at a particular company is only as strong as the individual user of a particular system. In fact, the behaviour and actions of employees are one of the leading causes of data breaches.

Business Perspective

Social engineering impact many types of businesses and have implications for the way that organizations are structured and managed. The topic can be considered from the business perspective to determine the factors that impact social engineering attacks. This viewpoint is beneficial if it is related to the following areas of business: training and development, documented policies, internal audit procedures, budgets, and organizational culture. A deficiency in any of

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

these areas can contribute to attacks.

Ethical Perspective

Ethics is important in the context of social engineering and the related research on the topic. The idea of manipulating another human being violates many ethical principles. In case of a social engineering occurrence, treatment of the victims can vary, but often, they are not sufficient treated allowing the attack to occur. Unfortunately, the qualities usually found in ideal employees such as trust, the willingness to please others such as managers, customers, co-workers, and visitors, and the readiness to obey authority, are usually the same characteristics that make an individual susceptible to social engineering (Mouton, Malan, Kimppa, & Venter, 2015).

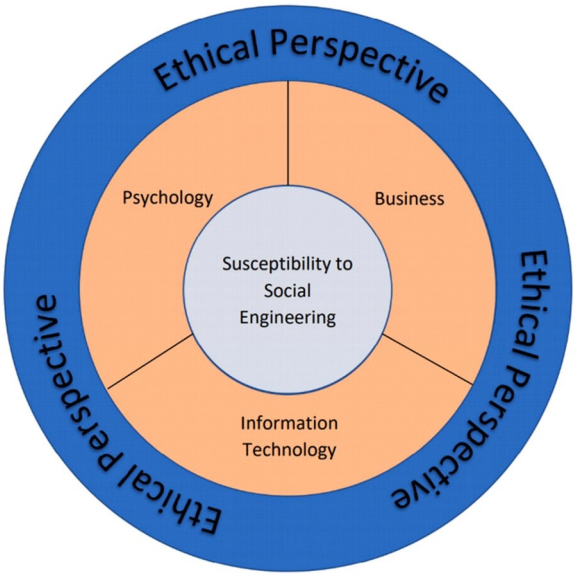


Figure 3: Social engineering from an interdisciplinary view (Washo, 2021)

The literature review from different disciplines explains the need for an integrated approach to study the complex subject of social engineering. Each discipline, provides information on how to understand and interpret the topic, protect against various types of attacks, and understand the impact of social engineering from both a human and organizational standpoint. However, each discipline's interpretation of the topic is only useful when viewed in the context of the other disciplines.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. How to recognize Phishing: i.e. Phishing emails and text messages often tell a story to determine victims to click on a link or open an attachment.
2. How to protect from Phishing Attacks
3. Please name some disciplines connected with Social Engineering and explain shortly these connections

Attachments:

1. Presentation
2. Video movies

References:

Abbate, P., (2020). Internet Crime Report 2020
URL: (https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf)

Bullee, J.W.H, Montoya, L., Pieter, W., Junger, M, Hartel, P. (2017). On the anatomy of social engineering attacks – A literature-based dissection of successcul attacks. *Journal of Investigative Psychology and Offender Profiling. 15. 20-45.*

Lee, T. (2020). Hire the Right Teachers for the Better Security Awarness. URL: https://www.gartner.com/smarterwithgartner/hire-the-right-teachers-for-better-security-awareness

Mimecast Contributing Writer (2021). Social Engineering Awarness Training for Emploeyees. URL: https://www.mimecast.com/blog/what-is-social-engineering/

Mouton, F., Malan, M., Kimppa, K., & Venter, H. (2015). Necessity for ethics in social engineering research. Computers & Security, 55, 114–127. https://doi.org/10.1016/j.HYPERLINK "https://doi.org/10.1016/j.cose.2015.09.001"cose.2015.09.001

Washo, A. (2021). An interdisciplinary view of social engineering: A call to action for research. URL: https://www.researchgate.net/publication/353448049_An_interdisciplinary_view_of_social_engineering_A_call_to_action_for_research

Weßelmann, B. (2008). Maßnahmen gegen Social Engineering: Training muss Awareness-Maßnahmen ergänzen. In: Datenschutz und Datensicherheit. DuD. 601–604.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Module

Information Security for Managers Unit (Module) 4, Week 7 and 8 Unit (Module) name: Cyber Risk and Resilience	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other**
Learning Responsible	• Simon Tjoa • Peter Kieseberg
Learning Activity Goals	1. The participants know foundations of risk and resilience management 2. The participants are able to perform business impact analysis and risk analysis 3. The participants can derive counter measures and security decisions from the results of analyses
Skills to be Gained	• IS 1, IS 3 • MS 1
Duration of Learning activity	2 weeks • Week 7 (2 hours) • Week 8 (2 hours)
Learning requirements	***What is needed?*** • Basic management skills • Basic IT skills • Basic security skills

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
Perfect security is not possible. Knowing this, it is vital to make informed decisions how to spend money for right security measures. Cyber risk and resilience management provides a vital set of tools and techniques to assess the current state of security of an organization and to plan controls to keep the information security risk at an acceptable level.

Content of the Learning Material

Without taking risks, making business is impossible. Therefore, risk management and the corresponding tools & techniques provide a systematic way to address risk. Questions such as how much security is enough or which counter measure should be implemented first are answered by risk management. Thus, risk management is an important activity to enable informed decisions. Important standards and best practices addressing this essential topic include ISO 27005, ISO 31000 or BSI 200-3.

Before taking a closer look into the risk management process, it is essential to define essential terms:

- **Vulnerability:** "Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source."[1]
- **Control:** "A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements."[2]
- **Threat:** "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via

[1] https://csrc.nist.gov/glossary/term/vulnerability
[2] https://csrc.nist.gov/glossary/term/security_control

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

unauthorized access, destruction, disclosure, modification of information, and/or denial of service."[3]

- Risk: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically is a function of: (i) the adverse impact, or magnitude of harm, that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."[4] "effect of uncertainty on objectives"[5]

From the definition of ISO 31000 ("effect of uncertainty"), we can derive that risks can have positive and negative impacts. Often if risks have positive impacts they are referred as opportunities.

The general risk management process starts with the scope, context and criteria. As not all risks for all activities can be analyzed it is important to prioritize and to decide which services, processes & organizational units should be included in the assessment. Having an adequate scope is crucial to ensure valid results on the one hand and reasonable effort on the other side. The context is the internal and external environment. The determination of risk criteria is important to ensure a and repeatable process, which leads to comparable results. The criteria should be defined in a way that different persons are able to assess risks in a common way.

Examples of criteria include impact criteria (e.g. low, medium, high) for various dimensions, such as financial, reputation or health.

In the following, an example of OCTAVE Allegro regarding reputation and customer impacts is presented:

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

[3] https://csrc.nist.gov/glossary/term/threat
[4] https://csrc.nist.gov/glossary/term/risk
[5] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Figure 1: Measurement Criteria for Reputation[6]

After the definition of risk criteria and the scope, the first step is to identify risks. Risk identification is crucial as only those risk can be assessed, which are identified. It therefore makes sense to compare identified threats with threat lists of ISO 27005, MEHARI or other best practices or standards.

There exist various techniques[7] to identify risks, such as brainstorming, Delphi technique, Failure Mode and Effects Analysis (FMEA) or Hazard and Operability studies (HAZOP).

In the next step risk analysis, a better understanding of the identified risks is gained. Therefore, occurrence probability/frequency and impact/consequences are determined. In order to determine consequences, it is important to define a systematic way how impacts are assessed. Often a qualitative measure (e.g., low, medium, high) is easier to use than quantitative measures.

Risks are often visualized in a so called risk matrix, which highlights the risk using the probability and impact as axes.

Probability	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Figure 2: Risk Matrix [Source Wikipedia][8]

In the next step, the risks are evaluated. This means that the results of the previous step are considered to decide, whether actions should be taken. Furthermore, a prioritization of risks takes place.

Next one of the four main strategies to address risks are determined:

- Risk acceptance: document and monitor risk if the risk is within the risk appetite of the

[6] https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf
[7] Cmp. https://www.iso.org/standard/72140.html
[8] https://en.wikipedia.org/wiki/Risk_matrix

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

organization

- Risk transfer: share risks (e.g., insurance, joint venture)
- Risk avoidance: remove the risk source (e.g., air gap)
- Risk mitigation: reduce the impact or occurrence probability (e.g., access control)

After the determination of measures, it is evaluated whether the residual risk is acceptable or further measures have to be taken.

As supporting activities beside the main risk assessment process, risk communication (i.e. communication with relevant stakeholder), risk monitoring, and risk reporting takes place.

As not all risks can be considered, in contrast to risk management, business continuity & resilience focuses on critical activities instead of individual risks. This way it is possible to prepare for unknown and low-probability/high-impact risks.

For ensuring an effective business continuity program, the support of top management is vital. An important artefact highlighting the importance of business continuity management, is the business continuity policy. In this document the management buy-in is formally expressed. Further, the document highlights the scope and aims of the business continuity activities, important roles and responsibilities (e.g, business continuity manager) as well as the operational framework used for performing the program. It should be stressed that the scope should not be too broad to ensure that the complexity of the analysis as well as the effort are not getting too high.

In order to understand the effects of services disruptions on the business and to have a good basis for planning recovery measures, business impact analyses are carried out. It is the central tool within the business continuity process and captures the relevance/significance of products/services. Apart from the criticality of products / services their dependencies are determined and assessed.

Important key figures, which are used when performing a business impact analysis include:

- **MAO (maximum acceptable outage):** "time it would take for adverse impacts [...], which can arise as a result of not providing a product/service or performing an activity […], to become unacceptable"[9]
- **RTO (recovery time objective):** "period of time following an incident […] within which a product and service […] or an activity […] is resumed, or resources […] are recovered"[10]
- **RPO (recovery point objective):** "point to which information […] used by an activity […] is

[9] MAO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[10] RTO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

restored to enable the activity to operate on resumption"[11]

In the first step, the most critical or essential products and services are identified. After the identification, it is assessed which damage would arise over time if a certain product or services is disrupted or interrupted.

The succeeding figure shows how the impact over time could be captured in a spreadsheet.

Assessment Period / Damage Category	1 Hour(s)	2 Hour(s)	4 Hour(s)	8 Hour(s)	24 Hour(s)	48 Hour(s)	96 Hour(s)	168 Hour(s)	240 Hour(s)	720 Hour(s)
Financial	0	0	0	0	0	0	2	3	4	4
Health & Safety	0	0	0	0	0	0	0	3	4	4
Legal, Regulatory & Contractual	0	0	0	0	1	1	1	2	2	2
Brand and Reputation	0	0	0	1	1	1	2	4	4	4
Environmental	0	0	0	0	0	0	0	0	0	0
Rational for the assessment (Description) Verbal Description of Implications										

Furthermore, the business impact analysis surveys from which processes, activities and resources relevant services are dependent. This way important key figures, such as the recovery time objective, recovery point objective and the maximum acceptable outage can be determined.

After knowing the criticality of processes, services and resources, business continuity strategies are elaborated. Strategies include amongst others diversification (e.g., activities at geographically separated places), replication (e.g., copying data to recover at other site) or subcontracting (e.g., using third party services).

Based on the strategies business continuity plans are written, which support organizations to react in an efficient manner following an incident. In order to be usable in high pressure situations it is vital that plans are written accordingly. This means that plans should only contain that information which is relevant while handling an incident. Furthermore, the information should be quick to grasp. Thus, clear and action-oriented checklists should be used.

Typical business continuity plans contain information about the purpose, scope, incident management structure, roles and responsibilities, plan activation, recovery arrangements, and

[11] RPO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

contact details.

In order to rehearse and check the adequacy of plans, different types of exercises are used. This can be either discussion-based exercises, such as desk checks or tabletop exercises or technical exercises, such as testing the restore of certain systems.

Questions:

See Word Documents

Attachments:

See Powerpoint and Video files

References:

- ISO 22301:2019, Security and resilience — Business continuity management systems — Requirements
- ISO 22313:2020, Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO/TS 22317:2021, Security and resilience — Business continuity management systems — Guidelines for business impact analysis
- ISO/TS 22331:2018, Security and resilience — Business continuity management systems — Guidelines for business continuity strategy
- ISO/TS 22332:2021, Security and resilience — Business continuity management systems — Guidelines for developing business continuity plans and procedures
- ISO 31000:2018, Risk management — Guidelines, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- IEC 31010:2019, Risk management — Risk assessment techniques

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

InCyT Training Modules

Information Security for Employees **Unit no: (4) Week 8** **Unit (Module) name: (Social Networking)**	
Learning Activities	❑ **Webinar** ❑ **Exercises** ❑ **Workshop** ❑ **Presentation** ❑ **Other** Streaming Webinar, Text, Self-assessment Exercises, Exercises with answers on discussion forums and within the organized sessions with trainer/mentor, e-portfolios
Learning Responsible	• David Sommer • Ileana Hamburg
Learning Activity Goals	1. Social networking roles 2. Functionality of social networking platforms 3. Security and privacy in social networks 4. Threats to online social networks and solutions to avoid them 5. Interdisciplinarity in social networks
Skills to be Gained	• **TS3 Network security** • **TS4 Penetration (exploitable vulnerabilites) testing** • **TS5 Intrusion detection** • **SS3 Cognitive and behaviour analysis**
Duration of Learning activity	2 weeks
Learning requirements	***What is needed?*** • Internet access • Internet Browser • MS Office365

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Brief information about the module

Description
Social networking helps people and organizations to connect with friends, are means of communication, help to launch a new business idea, sell products or services, and extend the reach of an own brand. Sure, there are also disadvantages of social networking like decreases face-to-face communication skills. Because organizations use intensively social media, attackers use trust and public nature of these platforms to attacks. Social networking security is important for business and private success so that training of employees like within this module can have a big contribution. The employees learn about such aspects by reading the corresponding text, watching streaming webinars, and solving exercises at own pace and reflecting about what they learn (e-portfolios). All the module documents are on the digital interactive project platform. The learners can test their answers on Self-assessment exercises. The answers on other exercises should be saved on the corresponding discussion forums and discuss with the mentor at the common organised meeting once a week. Learner can work cooperatively with other ones and mentor particularly during the weekly meetings.

Content of the Learning Material

Introduction

Also due to growing technology, (online) social networks became very popular over the past few years. One reason is their ability to provide a platform for users to communicate with their family, friends, and colleagues.

Social networking refers to the use of internet-based social media sites for connection and communication with friends, family, colleagues, customers, or clients.

Social media helps people to have better relationships with family, friends, clients and mobile devices supporting social media are gaining more and more interest compared to other ways of internet access.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Social networks have their servers in data centres co-located, when possible, with major Internets Network Access Points (NAPs) where big Internet service providers connect to each other and where they provide the direct access to the Internet's fast connections.

Social networking roles

Social networking can have a social role, a business one, or both, by using sites like Facebook, Twitter, LinkedIn, and Instagram. Figure 1 shows some fields in which social networks play a role (Milsova et al.): entertainment, building business opportunities, making a career, improving social skills, and developing relationships with other individuals.

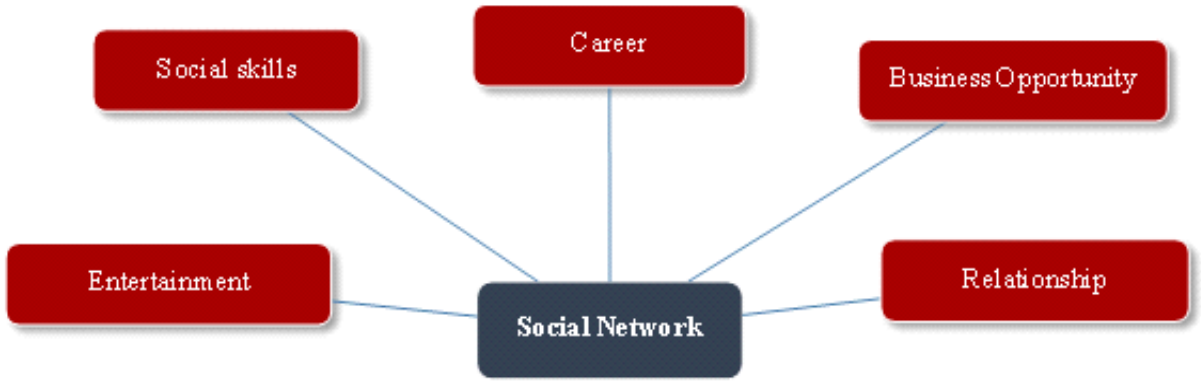


Figure 1: Social networks roles

Social networking is a base for marketers who seek customers. Marketers use social networking i.e. for increasing brand recognition and encouraging brand loyalty. Social media can help connect people and businesses and can help promote brand awareness. For example, a frequent Twitter user may learn about a company for the first time through a news feed and decide to buy a product or service. The company's chances of finding and retaining new customers increase through social networks. Marketers use social networking to improve conversion rates, provides access to and interaction with new, recent, and old customers. By sharing blog posts, images, videos, or comments on social media more people will visit the company's website and become customers. But there isn't a one approach to marketing strategies; every business is unique and has a different target demographic, history, and competitive marketplace. Because social networking companies want businesses to pay for their advertising, companies often restrict the number of reach businesses received through unpaid posts. For example, if a company has 500 followers, followers may not all receive the same post. The evolving nature of social networking makes it challenging to keep up with changes, and also influences a company's marketing success rate.

Facebook, Instagram, Facebook Messenger, and Twitter are the most popular social networking sites in the United States and also Europe. Others include Pinterest, Tumblr, Snapchat, TikTok, and YouTube, WhatsApp, Messenger by Google, and Tumblr. LinkedIn is another popular site, which helps connect professionals with co - workers, business contacts, and employers. Facebook remains the largest and most popular social network, with 2.91 billion people using the platform on a monthly basis, as of Dec. 31,

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

2021. Figure 2 shows number of users on platforms.

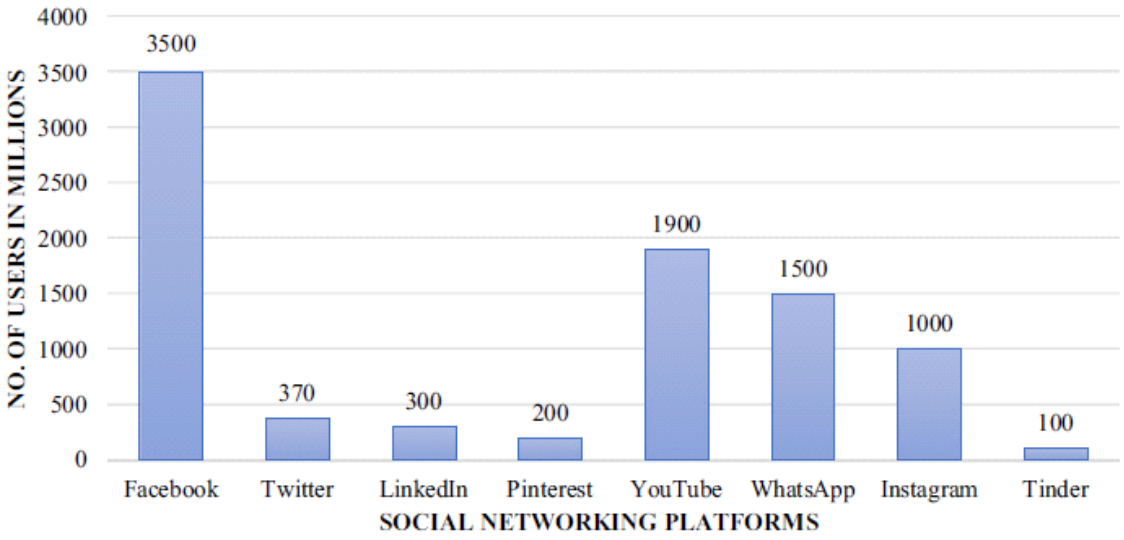


*Figure 2: Number of users on platforms (*https://w ww.dreamg row .com/t op)

Functionality of Social Networking

Social networking is based on the development and maintenance of personal and business relationships using technology by the use of social networking sites. These sites allow people and corporations to connect with one another so they can develop relationships and they can share information, ideas, and messages.

Family members who are far could remain connected through personal social networking sites like Facebook and share photos and send other messages from their lives. People can also connect with others (strangers) who share the same interests. Individuals can find each other through being members in groups, on lists, and the use of hashtags.

But there are also disadvantages related to social media, including the spread of misinformation and the high cost of using and maintaining social network profiles.

Each social network serves usually some specific use, but the functionality of these platforms is similar and can be classified into three main types:

- The networking functions serve to foster social relationships amongst users within the virtual platforms. In particular, they provide functionality for building and maintaining the social network graph.
- The data functions are responsible for the management of user-provided content and communications amongst the users. The variety contributes to the improvement (extended) of

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

users' interaction and makes the platform more attractive.

- The access control functions aim to implement the user-defined privacy measures and to restrict unauthorized access to the user-provided data and information. Figure 3 shows the functionality provided by a typical virtual social network platform and provides more details (Cutillo et al. 2010).

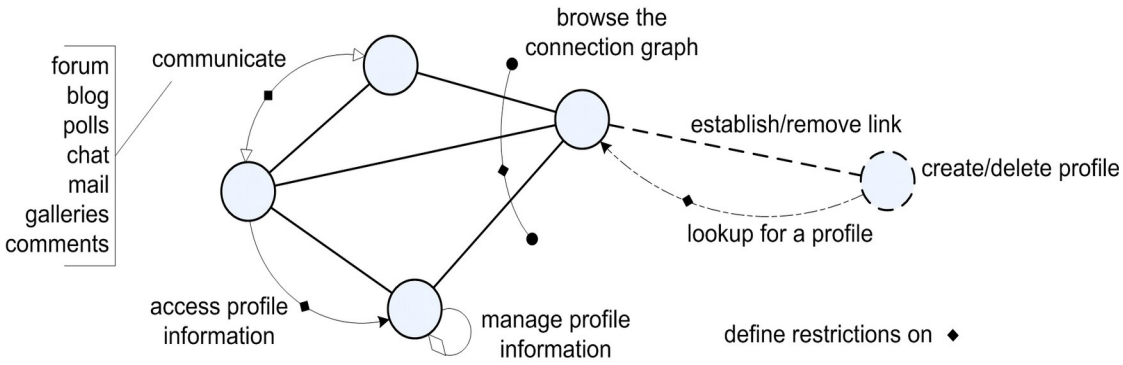


Figure 3: Main functionality of a typical social networking platform (https://hal.archives-ouvertes.fr/hal-00687145)

Social networking sites can be classified into 'social connections' 'multimedia sharing', 'professional' and 'discussion forums' (Figure 4 Jain et al., 2021)

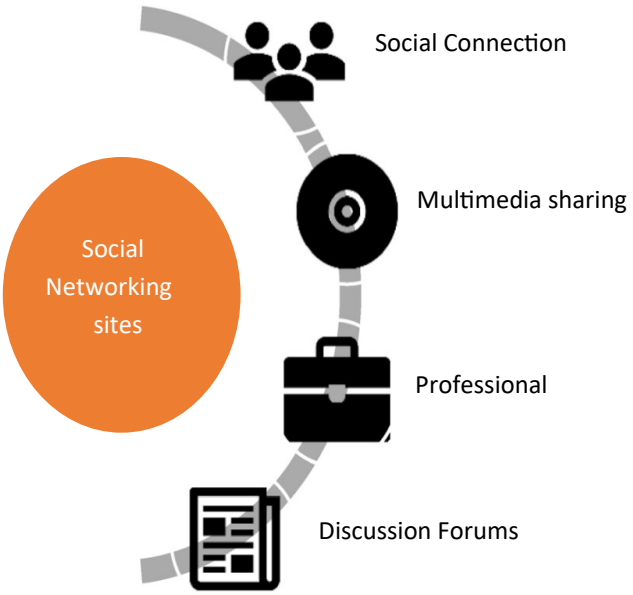


Figure 4: Social networking sites (Jain et al, 2021)

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Advantages and Disadvantages of Social Networking

Social networking has the ability to affect both individuals and corporations—both positively and negatively and so it's important to take into consideration advantages and disadvantages of using such social media sites.

Advantages

Social networking allows individuals to keep in contact with family and friends they would otherwise not possible due to distance or lost touch. People can also connect with other individuals who share the same interests and develop new relationships.

Social networking allows companies to connect with new and existing clients. Companies can also use social media to create, promote, and increase brand awareness. They also rely on reviews and comments made by their clientele important for brand. It can increase sales and a higher ranking in search engines.

Social networking can help to establish a new brand. A company may use social networking to demonstrate its customer high service level and improve products and relationships with consumers. For example, if a customer complains about a product or service on Twitter, the company apologize, and take action to improve the situation.

Disadvantages

Social networking can contribute to the spread of misinformation Sahoo and Gupta, 2020 found that misinformation is 70% more likely to be shared than right information on Twitter.

Networking on social media can have detrimental impact on companies. Criticism of a brand spread very quickly on social media. This has disadvantages for a company's public relations (PR) department.

Social networking itself is free, but building and maintaining a company profile need hours of work and costs each week. Businesses need many followers before a social media marketing campaign starts generating a positive return on investment (ROI). For example, submitting a post to 15 followers does not have the same effect as submitting the post to 15,000 followers.

Security and privacy in social networks

The information shared in social networks and media spreads very fast, which makes it attractive for attackers to gain it. There are security and privacy issues related to the user’s shared information when a user uploads personal content such as photos, videos, and audios. The attacker can maliciously use shared information for illegitimate purposes.

Some different security and privacy threats and existing solutions that can provide security to social network users are shortly presented.

Due to intensive use of technology, interactions have been extended through internet. Unfortunately, lack of awareness among users regarding security and privacy has the potential to lead to various cyber-attacks through social media The threats which users detected from the beginning of social networks can

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

be divided into three categories i.e., conventional threats, modern threats, and targeted threats (Fig. 5, Jain and Gupta, 2018). Conventional threats include threats that users have been experiencing from the beginning of the social network. Modern threats are attacks that use advanced techniques to compromise accounts of users and targeted attacks are attacks that are targeted on a particular user which can be committed by any user for varied personal vendettas.

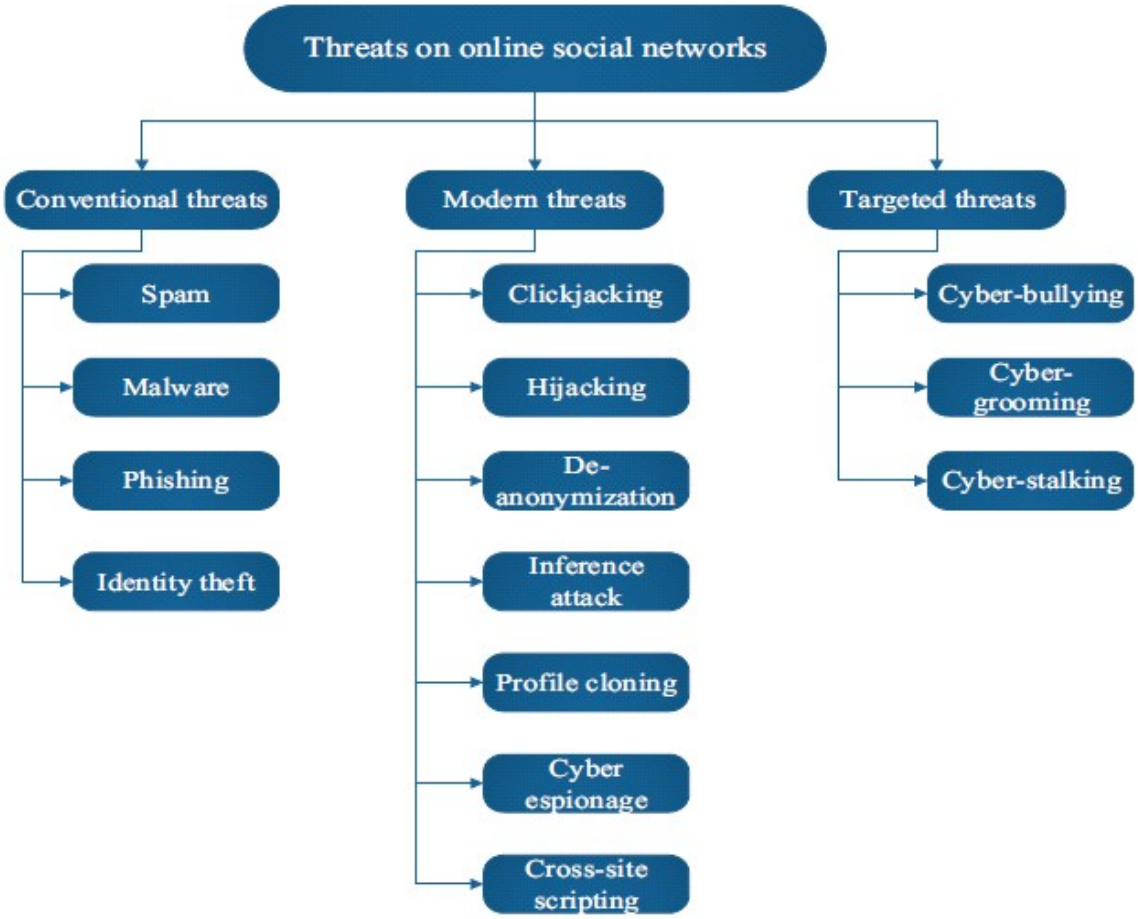
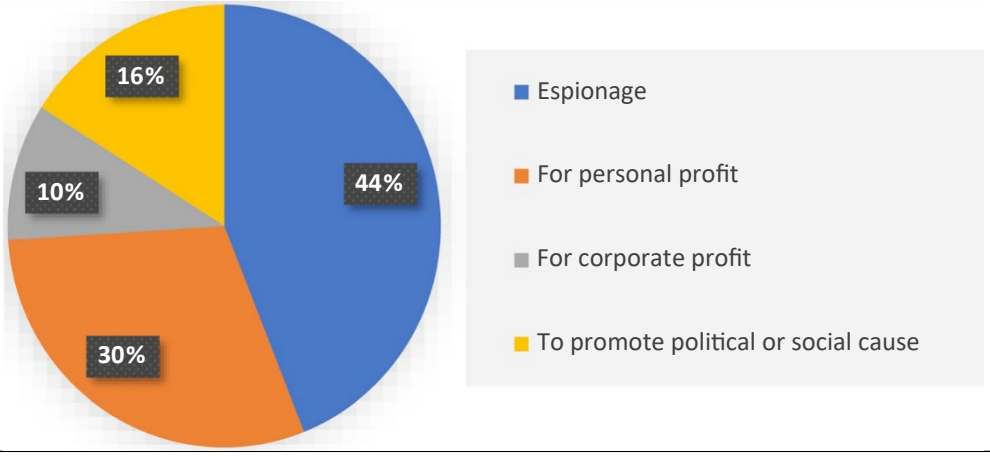


Figure 5: Classification of threats (Jain et al, 2018)



Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Figure 6: Most types of hacking in 2021 (Jain et al, 2021)

Solutions to threats

Researchers in academia and industries try to find solutions for the threats in social networks for different types of hacking like shown in Figure 6. Solutions and some approaches have been proposed and could be classified into two groups: social network operator solutions and academic solutions (Jain et al, 2021). Figure 7 shows the classification. A short description is presented below.

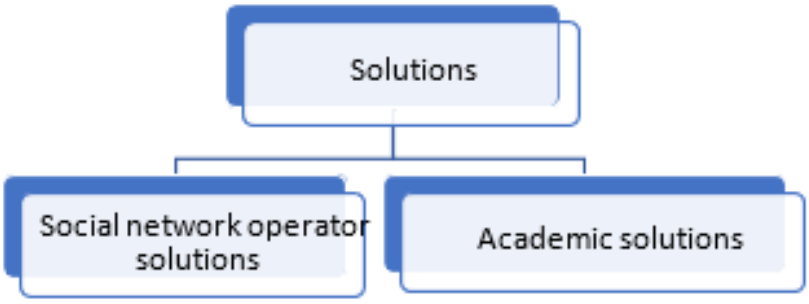


Figure 7: Classification of solutions to threats (Jain et al, 2021)

Social network operator solutions

Authentication mechanism

To make sure that only a legitimate user is logging or registering in a social network and not a social Bot, authentication procedures such as CAPTCHA, multi-factor authentication, and photos-of-friend identification have been proposed. For instance, social networks like Twitter and Facebook use two-factor authentication principles. This principle uses a login password and a verification code received through a mobile device. This helps to mitigate the risk of an account being compromised and prevents an attacker from hijacking a legitimate account and posting malicious content.

Security and privacy setting

Many social networking sites provide configurable security and privacy setting to empower the client to put personal information from undesirable access by outsiders or applications. For instance, the Facebook client can modify their security setting and select the audience (like friends, friends of friends, and everybody) in the network, who can see their details, pictures, posts, and other sensitive information.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Report users

Social networks protect people from attacks by providing the facility to report any form of abuse or policy violations by any user in their network. For instance, if a user sees something on Facebook that correspond to the individual's sentiments, but it doesn't violate the Facebook terms, then the user can utilize a report (links) to send a message to the one who posted it asking him to take it down or remove. When Facebook receives a user report, it is reviewed and removed according to the Facebook community standards.

Academic research-based solutions

Phishing detection

Phishing worried the privacy and security of many traditional web applications such as websites, social networking sites, emails, and blogs. Consequently, several anti-phishing techniques have been developed to detect phishing attacks. For instance, Aggarwal et al. proposed the PhishAri technique for real-time identification of phishing attacks occurring on Twitter. It utilized specific Twitter features like account age and number of followers to detect if the posted tweet is phishing or safe.

Cyberbullying detection

Cyberbullying is the use of electronic media such as emails, chats, phone conversations, and online social networks to oppress a person. Unlike traditional bullying, cyberbullying is a continuous process maintained through social media. Although detecting cyberbullying is more complex than detecting racist language and spam, some researchers have tried to detect it using more complex document representation and additional information about victims and bullies. Machine learning techniques can be applied to detect cyberbullying.

Clickjacking

An automated system can analyse web pages to protect the user against clickjacking attacks. It consists of a code that can detect overlapping clickable elements. And in addition to this solution, they also adopted the NoScript tool, which has an anti-clickjacking feature included in it.

Cyberstalking

Encryption techniques are available for devices on recent versions of Android and iOS. If a device is stolen, the thief cannot read the contents if encryption is enabled. Further, any attempts to read the information from internal or external memory is thwarted by the existence of a device password. There are various technologies which can be used against stalkers like smartphone fingerprint lock.

Spam detection

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

A framework called Spam Spotter can help against a spam attack on Facebook. It is based on the intelligent decision support system (IDSS). It gathers all relevant information from the user profile with the help of a decision process in IDSS and then analyses it by mapping user data to the classification of a user profile as a spammer or legitimate.

Malware

Cross Site Scripting Worms (XSS worms) are malicious programs that propagates through visitors of a website hopping to infect other visitors progressively.

The worm propagates slower when members mostly visit their friends rather than strangers. It can also be slowed down by the clustered nature of social networks.

Although academia developed such innovative solutions to address the security measures in connection with social network security, they lack real-world implementation and feasibility. Thus, there is an urgently need to continuously and iteratively review security issues in social networks taking into consideration technological developments.

Interdisciplinarity in social networks

The interdisciplinary field referring social networks is social network analysis (SNA) and include insights from other social science disciplines such as sociology, anthropology, psychology, communication, and others. SNA is part of an even larger interdisciplinary field in charge of studying all types of networks called network science which includes work in physics, computer science, data science, biology, engineering, mathematics, and other fields. The relationship between these fields is showed in Figure 8 (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html).

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

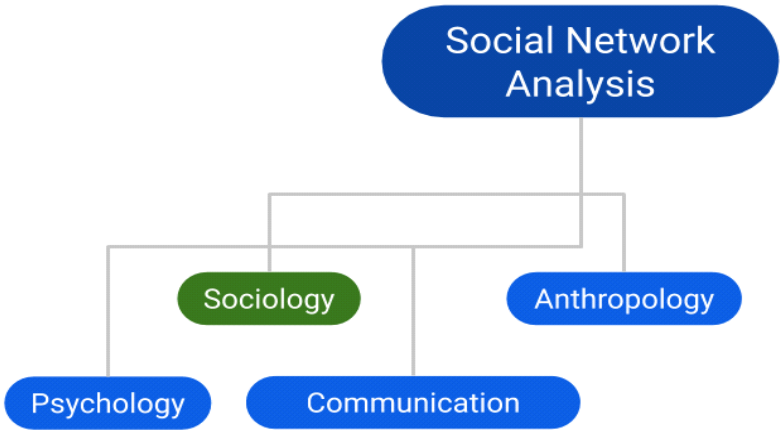


Figure 8: Relationships between fields in SNA (https://bookdown.org/omarlizardo/_main/1-2-what-is-a-social-network.html)

Questions:

Questions Discussion Forum to be answered with a short explanation. Answers will be discussed with the mentor during the mentoring sessions

1. Social networks roles
2. Social networking sites
3. Interdisciplinary fields in connection with social networks

Attachments:

1. Presentation
2. Video movies

References:

References

Aggarwal A., Rajadesingan A & Kumaraguru P. (2012). PhishAri: automatic realtime phishing detection on twitter. eCrime Res. Summit, eCrime. 1–12.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

Co-funded by the Erasmus+ Programme of the European Union

Ankit Kumar J., Somya Ranjan S. & Kaubiyal J. (2021). Data breach causes worldwide. URL: https:// www.s tatista.c om /statis tics /263303 /p roportion-o f -the-m ost -com https://www.statista.com/statistics/263303/proportion-of-the-most-common-causes-for-possible-identity-theft/mon- causes- for- possi ble- ident ity- theft/.

Cutillo, A., Manulis, M. & Strute, T.(2010). Security and Privacy in Online Social Networks. EUROCOM. TU Darmstadt.

Gupta B. & Sahoo, S. (2021). Online social networks security: principles, algorithm, applications, and perspectives. CRC Press.

Jain A. &Gupta B. (2018). Detection of phishing attacks in financial and e-banking websites using link and visual similarity relation. Int J Inf Comp Secur 10(4):398–417.

Jain, A., Sahoo, S.R. & Kaubiyal, J. (2021). Online social networks security and privacy: comprehensive review and analysis. Complex Intell. Syst. 7, 2157–2177.

Kangur, K. (2022). The 15 Biggest Social Media Sites and Apps. URL: https://www.dreamgrow.com/top-15-most-popular-social-networking-sites/.

Mislove A., Viswanath B., Gummadi K. & Druschel, P. (2010). You are who you know. In: Proceedings of the third ACM international conference on Web search and data mining—WSDM '10, 251.

Rydstedt, G. (2018). Clickjacking – OWASP. URL: https://owasp.org/www-community/attacks/Clickjacking.

Sahoo SR, Gupta BB (2020). Fake profile detection in multimedia big data on online social networks. Int J Inf Comput Secur 12(2–3), 303–331.

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.