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)

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.

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.

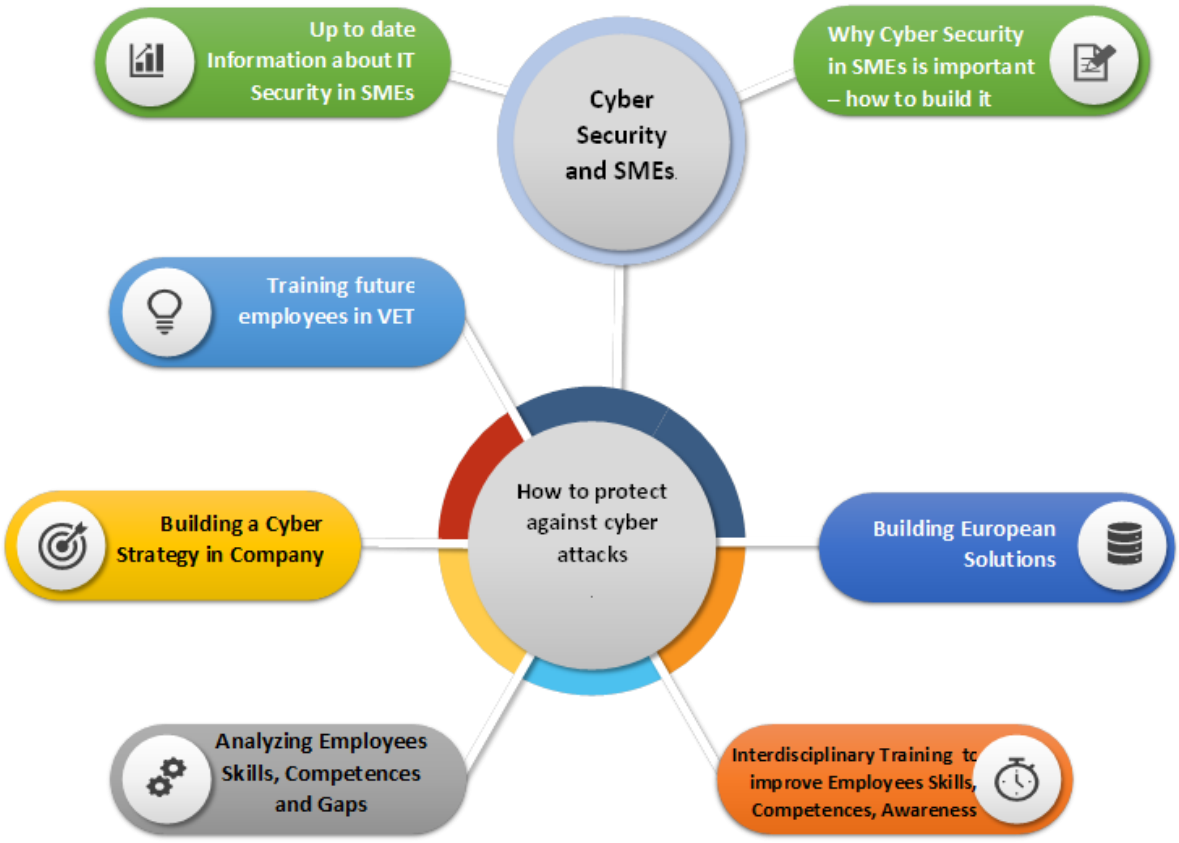

Figure 1: Activities supported by the InCyT project

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 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, 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 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 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.

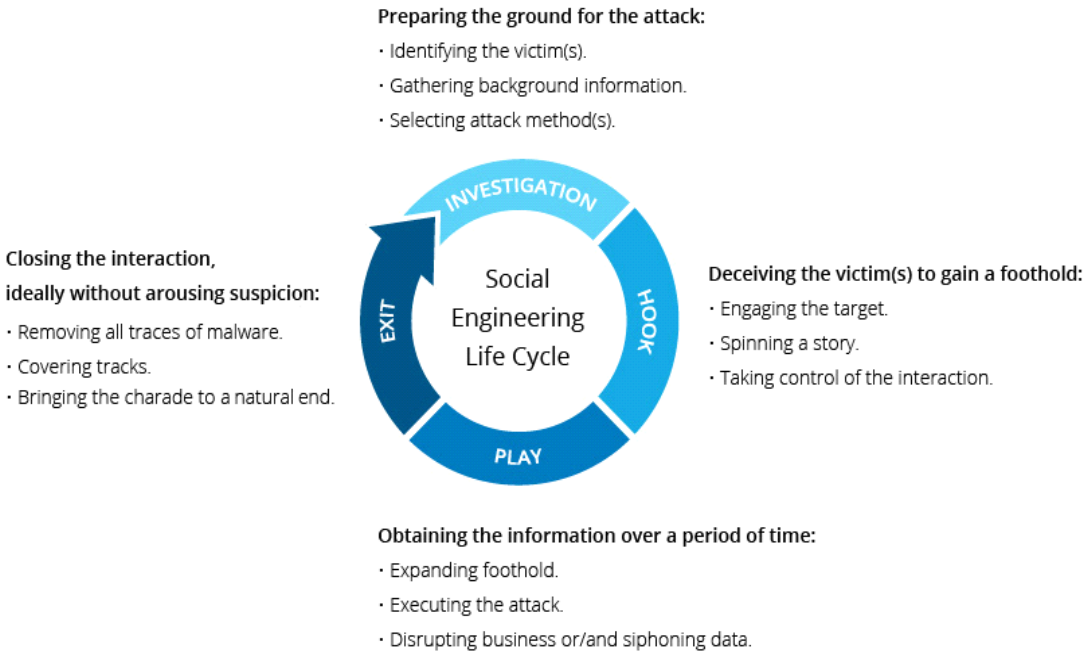

Figure 2: Life cycle of an attack

Social network

- 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

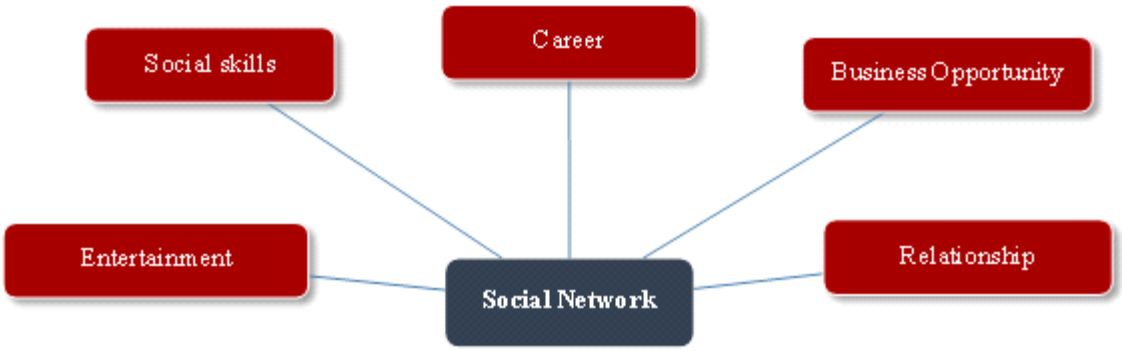

Figure 3: Roles in the Social Network

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:

- 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 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 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
- 19 Social Media Security Best Practices