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

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.

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:

- 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 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 — I**nformation 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 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.
- 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 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 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;

- 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 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

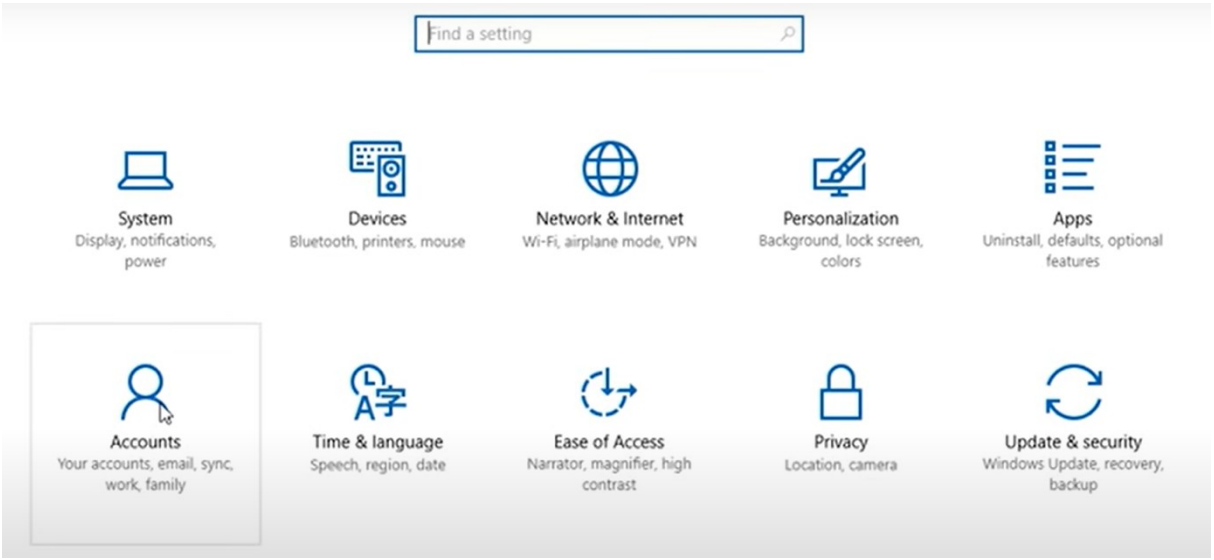
1. Lock your session: Strengthen your online accounts by activating the strongest authentication tools available, such as biometrics (a person's measurable biological traces), security keys, or a unique one-time code generated by an application tool on your mobile device. Your usernames and passwords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

Exercises-1:

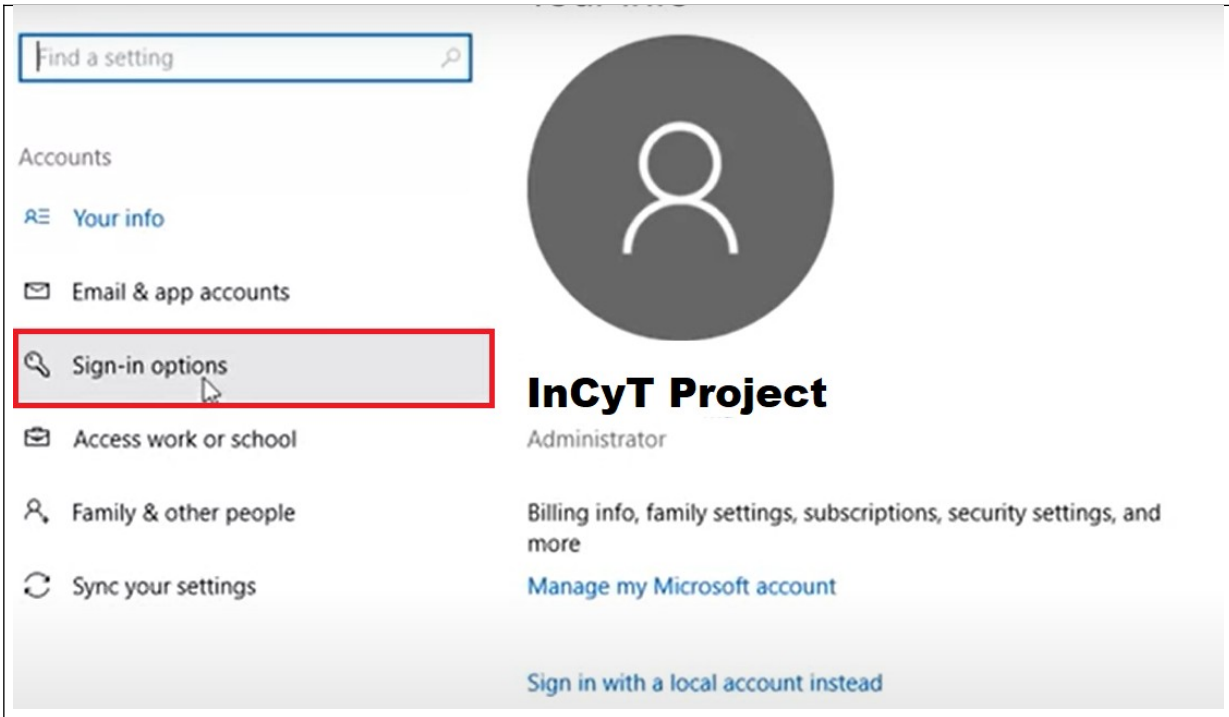
To have the computer lock automatically when you get up from the computer.

Step-1: Click the Windows Settings button.

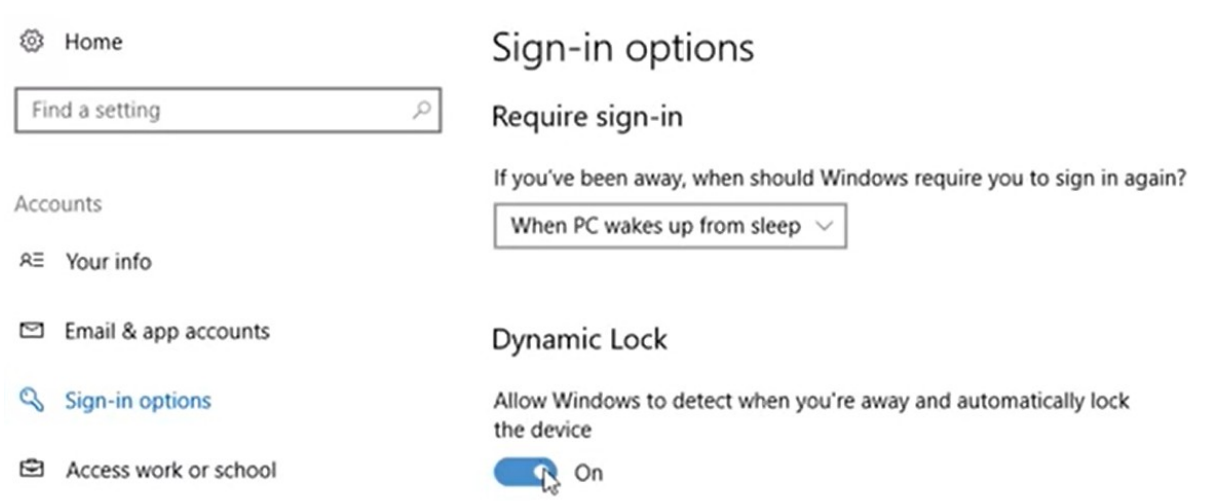
Step-2: Click the Accounts tab.



Step-3: Click on Sign-in section.



Step-4: Enable to the Dynamic Lock speficication.



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

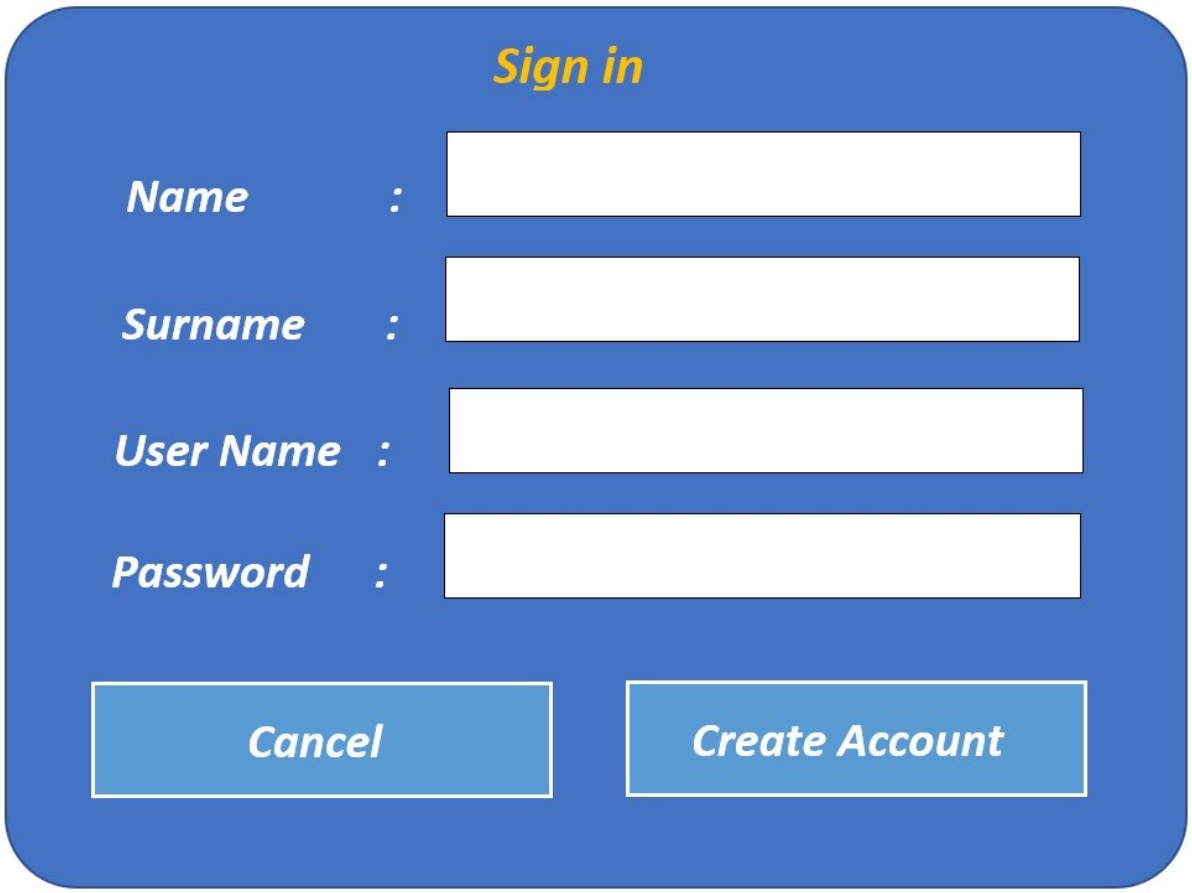
guessable. Passwords should be created according to the following criteria:

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.
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 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 **c**ybersecurity **p**roject **i**s **s**upported **b**y **E**rasmus**+ 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.

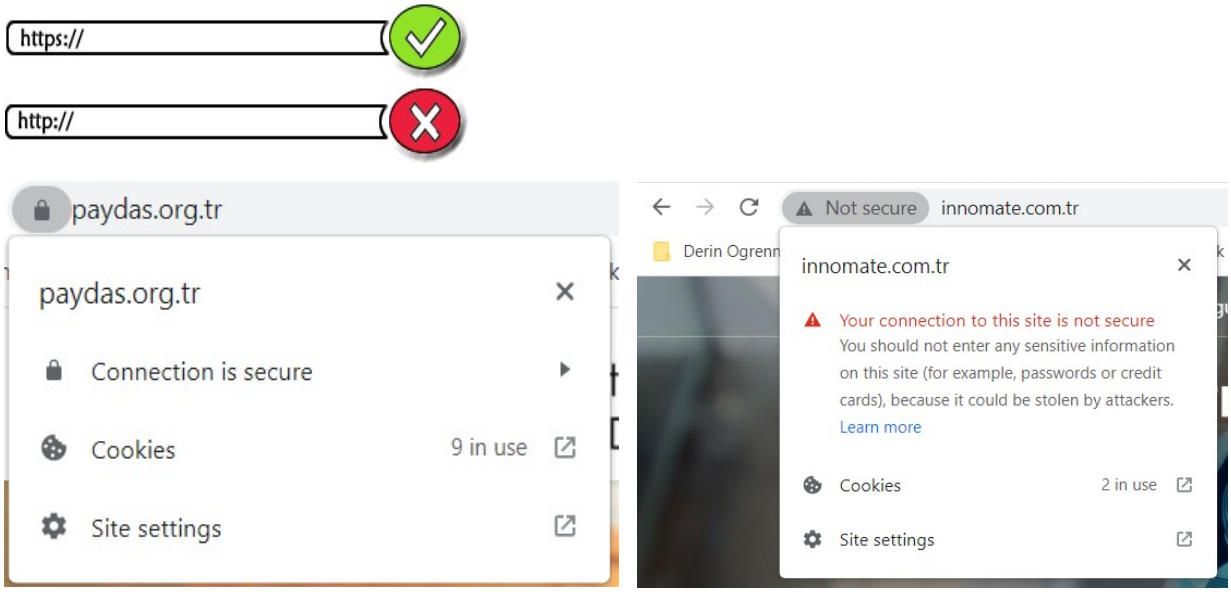


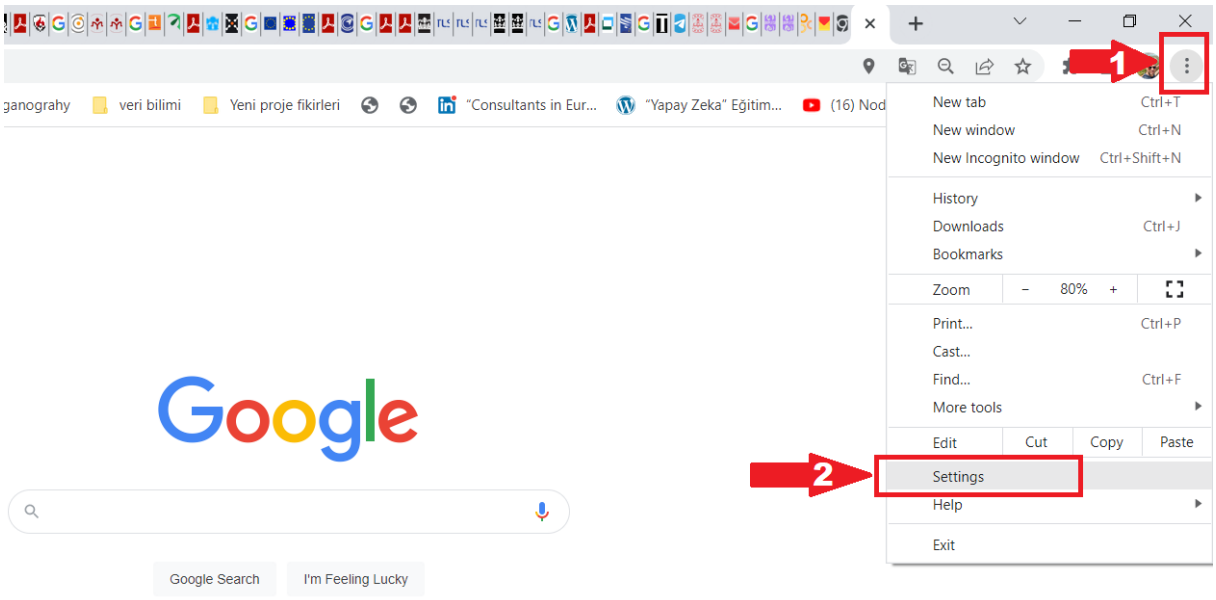
Figure 2. Secure and Not secureweb sites

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.

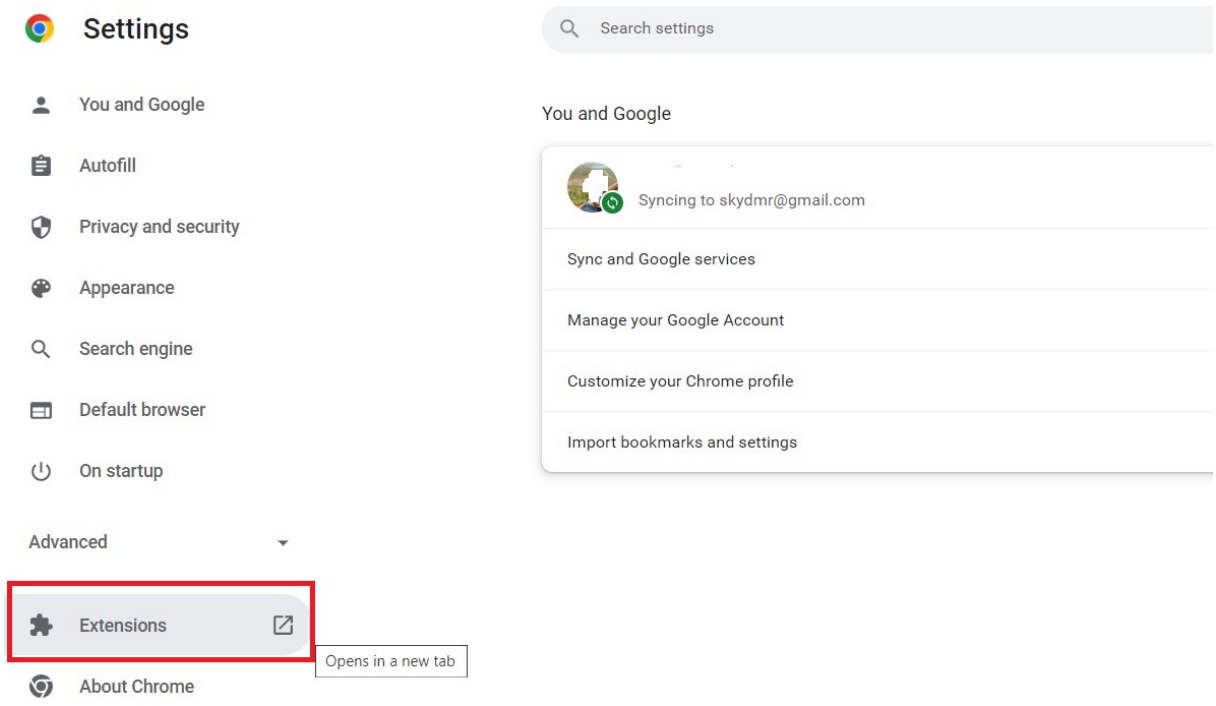
Exercises-3:

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

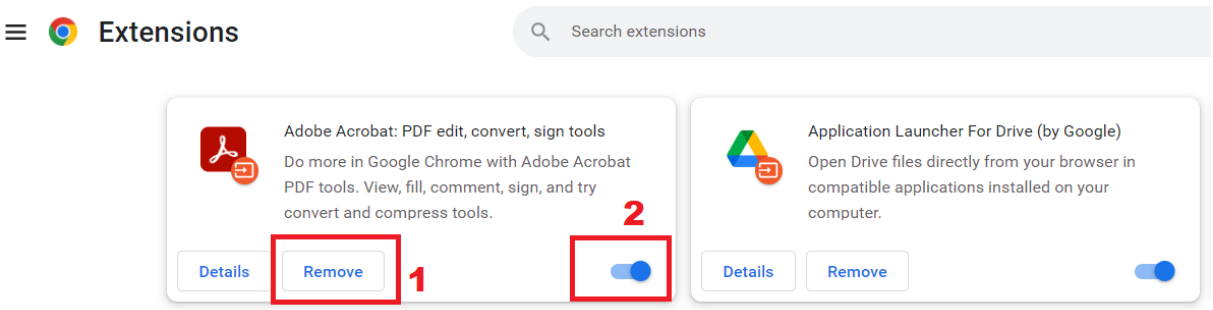
Step-1: Open your web browser and click the “Costume and Control…” button in the upper left corner (1). Click on the “Settings” tab from the drop-down menu (2).



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).



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:

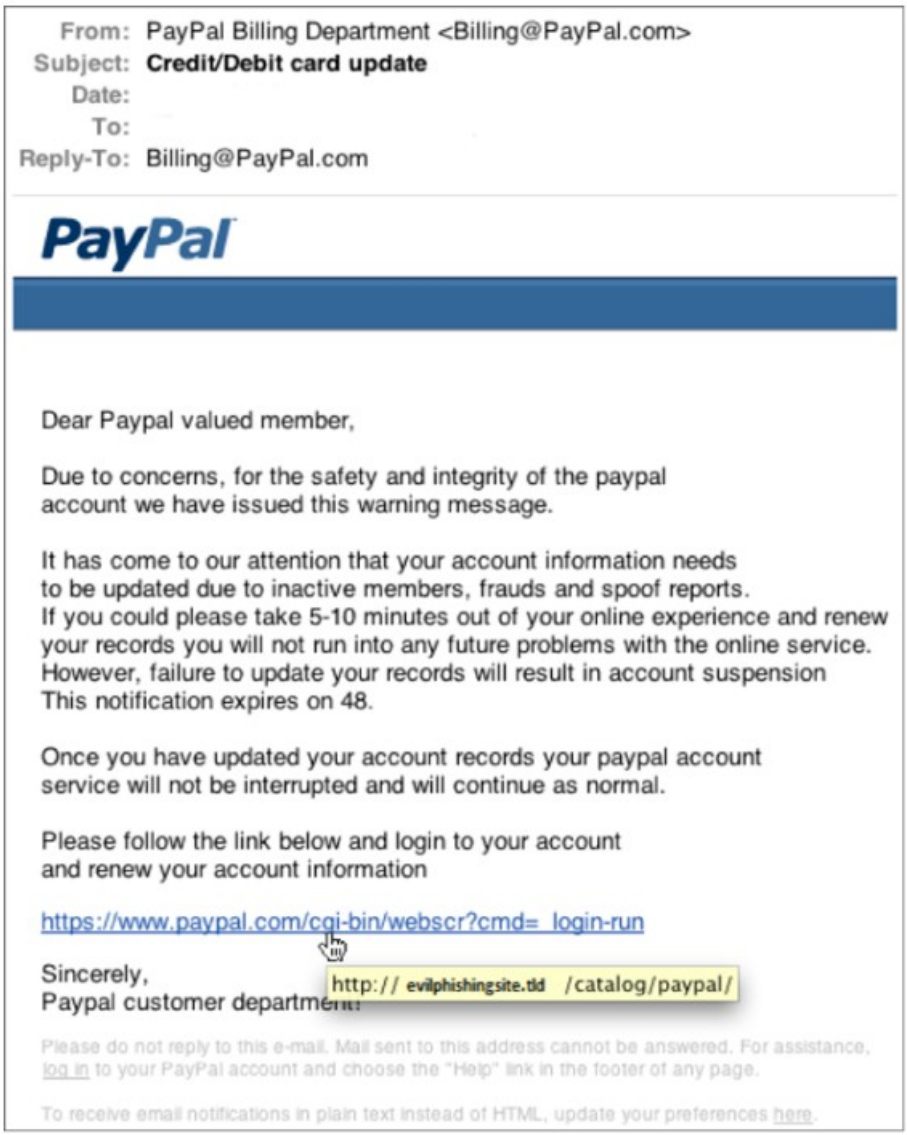
- Messages beginning with "Dear Customer" or other general greeting entries.
- Messages that require immediate action or create a sense of urgency, such as threatening to close your account.
- Messages that claim to be from an official organization but have grammatical or spelling mistakes or use a personal 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 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.



From: PayPal Billing Department <Billing@PayPal.com>
Subject: **Credit/Debit card update**
Date:
To:
Reply-To: Billing@PayPal.com

PayPal

Dear Paypal valued member,

Due to concerns, for the safety and integrity of the paypal account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take 5-10 minutes out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension This notification expires on 48.

Once you have updated your account records your paypal account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

https://www.paypal.com/cgi-bin/webscr?cmd=_login-run

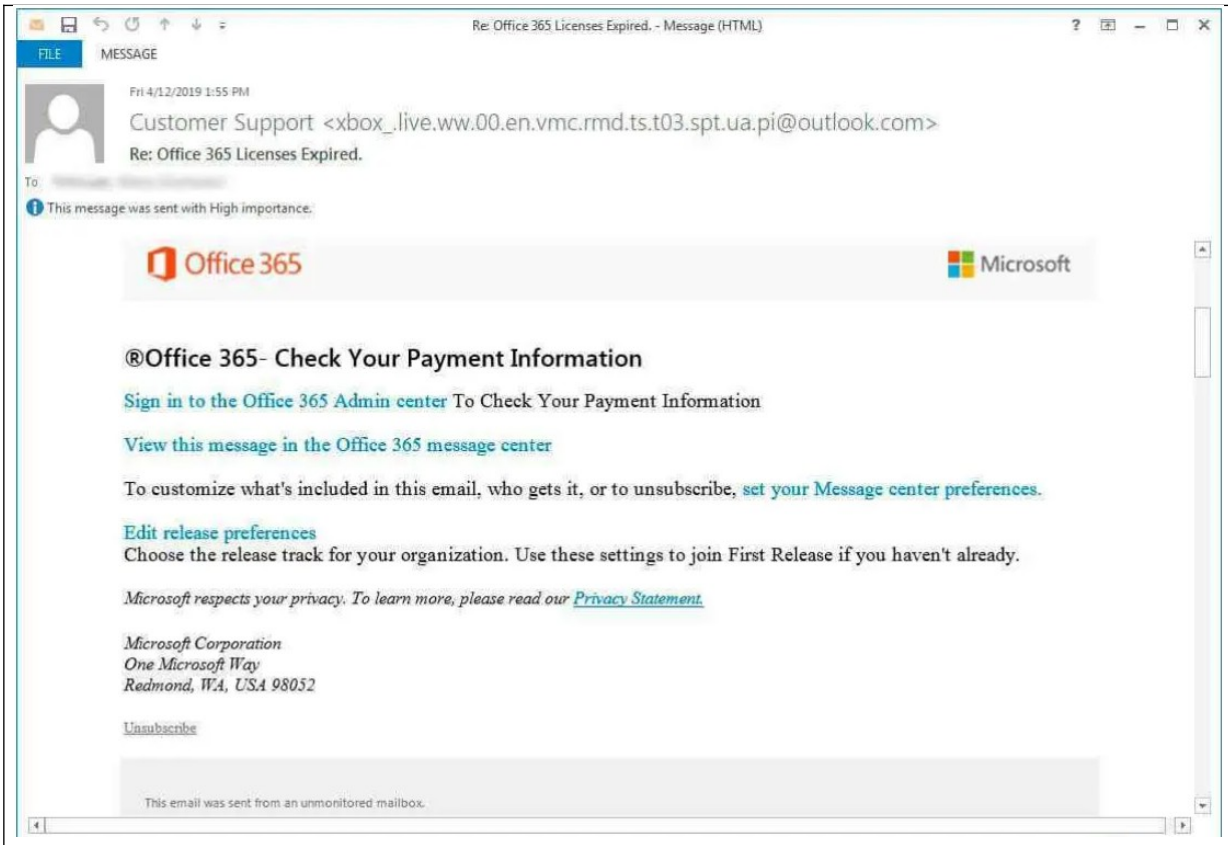
http:// evilphishingsite.tld /catalog/paypal/

Sincerely,
Paypal customer department

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences here.

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.



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 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.

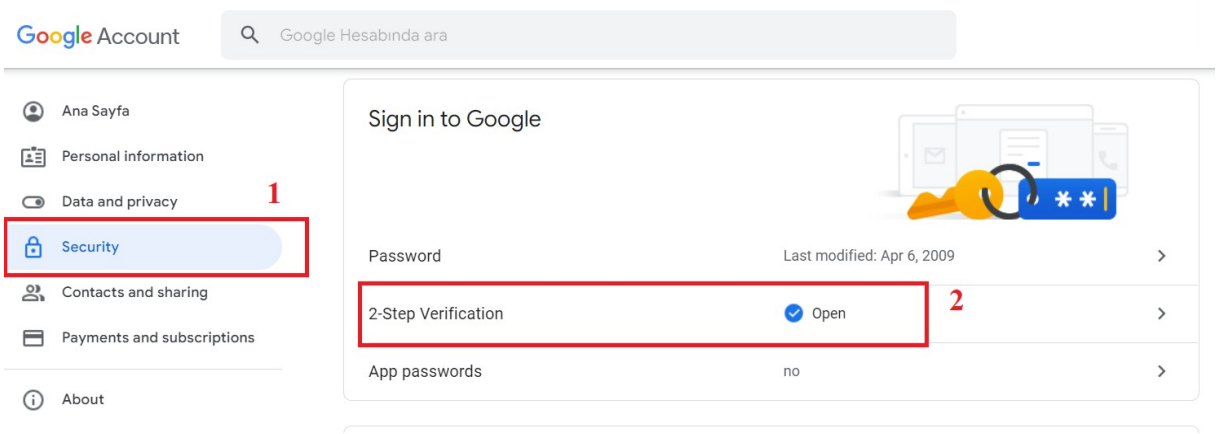
The screenshot below shows how to activate the two-factor authentication feature of the Gmail account.

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 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:

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

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/