Funded by the Erasmus+ Programme of the European Union

Overview of Understanding and Handling Cyber-Attacks

Handling of Cyber-Attacks

Safeguarding against Phishing in the age of 4th Industrial Revolution
www.cyberphish.eu
This project has been funded with support from the European Commission.
This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

CyberPhish
Safeguarding your digital future

Learning Goals

Explain and understand the ways how the cyber attacks could be handled out

Understand how the cyber attacks could be avoided or the damage could be minimized

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

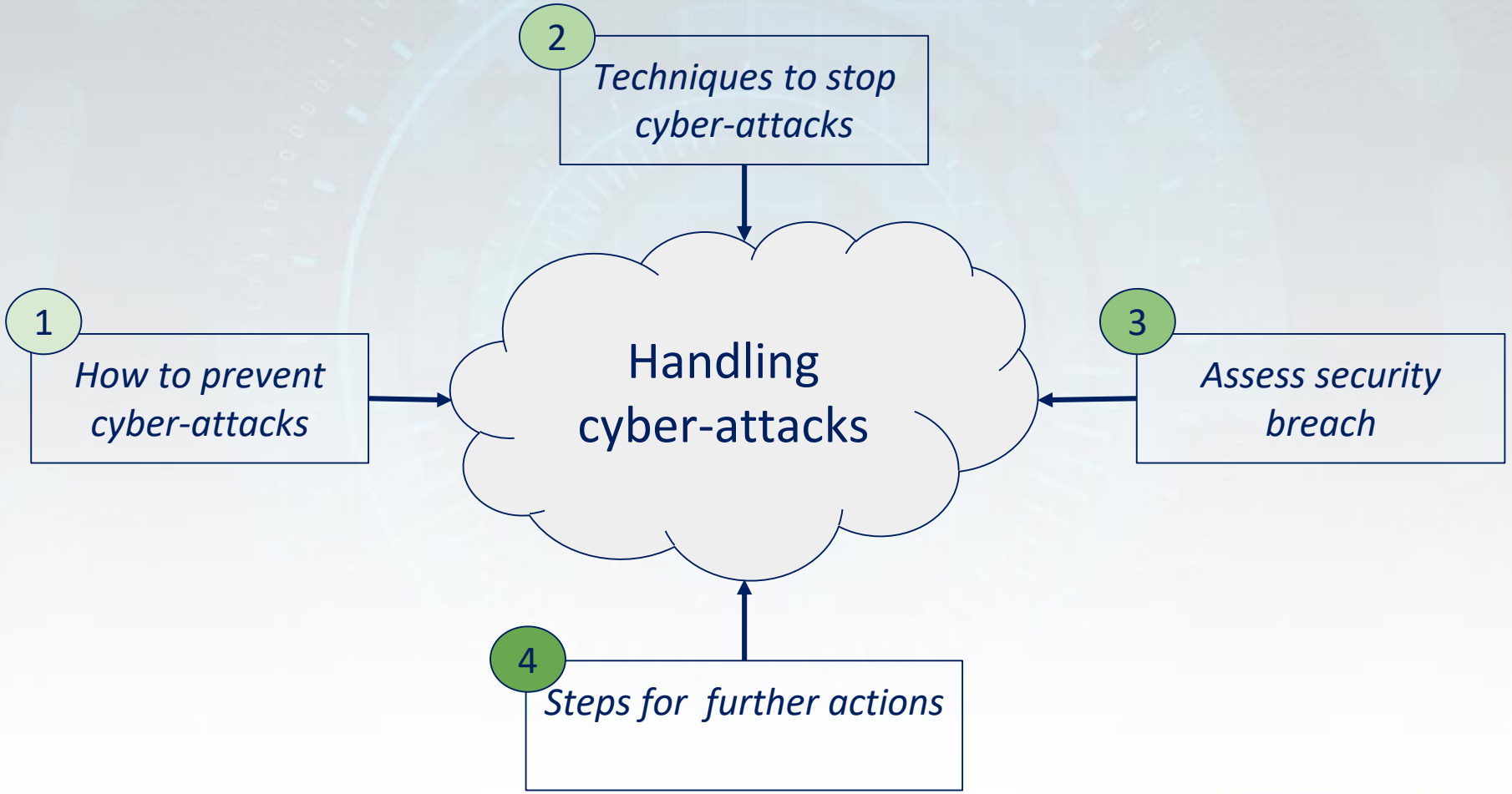
Student Workload

Lecture	5 h
Audio and video material	2 h
Case studies	2 h
Further reading	4 h
Preparation for exam	2 h

CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Contents


2
Techniques to stop cyber-attacks
1
How to prevent cyber-attacks
Handling cyber-attacks
3
Assess security breach
4
Steps for further actions

Avoiding Cyber-Attacks

- The most effective way to combat cyber-attacks is to use appropriate preventive measures
- *No successful attack - no losses.*

- To avoid or mitigate the attack, you need to develop some habits which are often called ***security hygiene*** or ***cyber hygiene***.

- *If you and your staff will follow security hygiene the **probability** to become a victim of the cyber attack could be reduced at least **by 90 percent** !*

Funded by the Erasmus+ Programme of the European Union

Awareness Training

- The first and one of the most important tips to handle cyber-attack is **awareness training**.
- This will ensure that all employees, according to their positions, or citizens will be able to handle cyber incident.

- Training is also one of the main tools to reduce the risk.
- *They can't guarantee the 100% security anyway but can reduce the risk*

Funded by the Erasmus+ Programme of the European Union

Best Practices to Avoid Cyber-Attacks

1. Top-down policies for improving your security posture.

Best practices always need to be backed by the right policies. This means that cyber security should be an integral part of corporate governance.

2. Bottom-up practices for cybersecurity teams.

Backed by well-developed policies a number of practices can be adopted to help prevent, limit or mitigate cyber attacks.

3. Adopt proactive measures to detect and respond to advanced cyber threats.

Perhaps the most important best practice is taking a proactive approach to cyber security.

Funded by the Erasmus+ Programme of the European Union

Steps to Handle Potential Attack

- *Step 1: Know which are the most usual cyber threats*
- *Step 2: Move into cyber security action mode*
- *Step 3: Assess risk exposure*
- *Step 4: Develop protection and detection measures*
- *Step 5: Establish contingency plans*
- *Step 6: Recovery*

Funded by the
Erasmus+ Programme
of the European Union

Avoiding Cyber-Attacks

- To avoid the cyber-attack is strongly suggested to follow several steps presented below:

1. Train your staff.

- One of the most efficient ways to combat against cyber-attacks and all types of data breaches is to train your employees

- To prevent phishing they need to:

Check links before clicking them

Check email addresses from the received email

Use common sense before sending sensitive information. It's better to check via a phone call with the person in question before actioning the "request"

Funded by the Erasmus+ Programme of the European Union

Avoiding Cyber-Attacks

To avoid the cyber-attack is strongly suggested to follow several steps presented below:

2. Keep your software and systems fully up to date.

- often hackers exploit software weaknesses which became known to hackers' community;

- it’s smart to invest in a patch management system;

- leaf offer patch management as part of their managed security solution.

Funded by the Erasmus+ Programme of the European Union

Avoiding Cyber-Attacks

To avoid the cyber-attack is strongly suggested to follow several steps presented below:

3. Ensure Endpoint Protection.

- endpoint protection protects networks that are remotely bridged to devices. Mobile devices, tablets and laptops that are connected to corporate networks give access paths to security threats.

4. Install a Firewall.

- putting your network behind a firewall is one of the most effective ways to defend yourself from any cyber-attack.

Funded by the Erasmus+ Programme of the European Union

Avoiding Cyber-Attacks

To avoid the cyber-attack is strongly suggested to follow several steps presented below:

5. Backup your data

- in the event of a disaster (may be caused by cyber-attack) you must have the copy of your data.

6. Control access to your systems

- *the attacks can be physical.*
- *having control over who can access your network is important.*

Funded by the Erasmus+ Programme of the European Union

Avoiding Cyber-Attacks

To avoid the cyber-attack is strongly suggested to follow several steps presented below:

7. Wi-Fi Security.

- do not forget enter password for each Wi-Fi connection used.

8. Personal accounts for each employee.

- each employee needs to use personal account;

- account sharing needs to be prohibited.

Funded by the Erasmus+ Programme of the European Union

Avoiding Cyber-Attacks

To avoid the cyber-attack is strongly suggested to follow several steps presented below:

9. Access Management

- employees need to have installed only authorized software;

- the use of unauthorized software needs to be prohibited.

Funded by the
Erasmus+ Programme
of the European Union

Avoiding Cyber-Attacks

Tips for increasing of your security:

1. Reduce Data Transfers and Unnecessary Communications;

2. Follow cybersecurity landscape;

3. Survey Data Leakage;

4. Develop and implement Incident Response Plan.

It’s not easy to follow all of them every day but you need to think about them.

Funded by the
Erasmus+ Programme
of the European Union

Avoiding Cyber-Attacks

If you will follow these guidance, you will significantly reduce the risk of cyber-attack.

But not forget:

- It can be difficult to know where are the weakest points.

- There's so much information out there which is even conflicting sometimes.

- You need a solution fitted to you.

Funded by the Erasmus+ Programme of the European Union

Safely Browsing Internet

- While you are browsing the Web, you could be picking up spyware, downloading malware, or even visiting fraudulent sites.
- Often you can be unaware that you are doing something unsafe.
- This does not mean that you need to be afraid every time when clicking on any link.
- Some simple precautions can help you be significantly safer while you're browsing.

Funded by the Erasmus+ Programme of the European Union

Safely Browsing Internet

- **Protecting your computer against malicious sites:** every browser has security features that protect you against visiting malicious sites. Enable these features !

- **Keeping your browser updated:** new malware and phishing threats are regularly created. It is important to keep browser updated.

- Make sure you have the latest version of your browser.

- Make sure you have installed all recent updates.

Safely Browsing Internet

- **Domain checking**: Malicious sites often use deceptive domains to trick users into believing they are on a legitimate site. Most browsers has features enabling domain checking or you can use special web sites to check the domain (less convenient).

- **Download only from trusted sites**: one of the easiest ways malware, spyware, and adware can access your computer is through downloads:

- Be cautious of freeware;
- Avoid illegal downloads;
- Be cautious of P2P file sharing.

Funded by the Erasmus+ Programme of the European Union

Safely Browsing Internet

- **Clear your cache regularly**

- The browser can speed up access by loading pages from the cache.
- With a high-speed Internet connection, you may not notice the difference.
- Cache can take up space over time, causing your browser to slow down.

It’s a good idea to clear the cache on a regular basis to help free up space on your computer and ... remove possible malicious files.

Funded by the Erasmus+ Programme of the European Union

Safely Browsing Internet

- **Block pop-ups**
  - Pop-ups are small browser windows that automatically pop up when you visit certain sites.
  - Pop-ups may be part of the legitimate functioning of a site.
  - Some pop-ups may contain malware.

- **It's a good idea to block pop-ups**

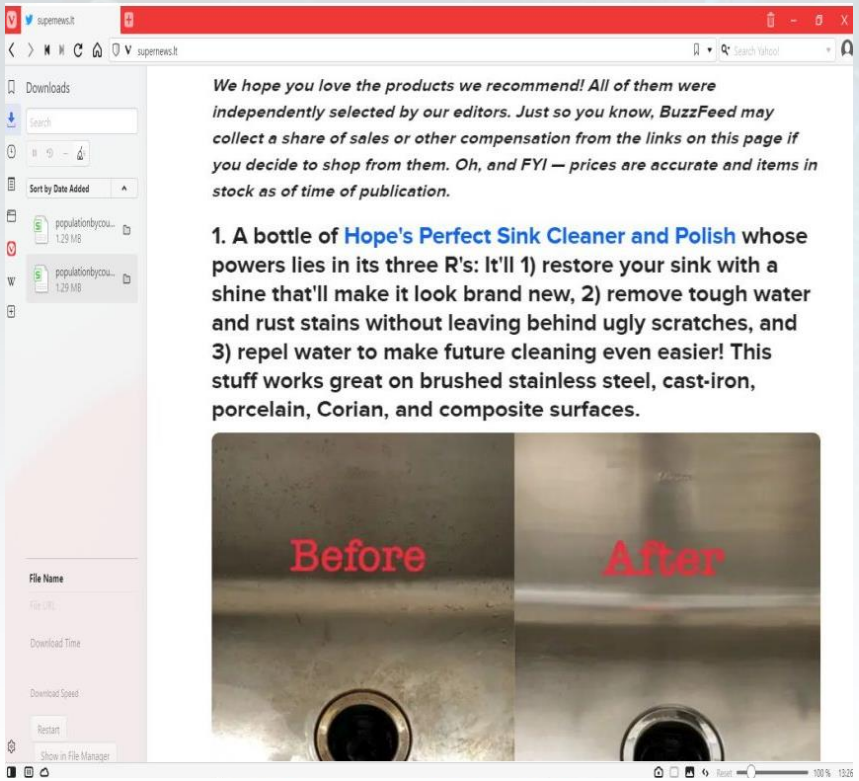
Most browsers has special pop-up blockers.

Funded by the Erasmus+ Programme of the European Union

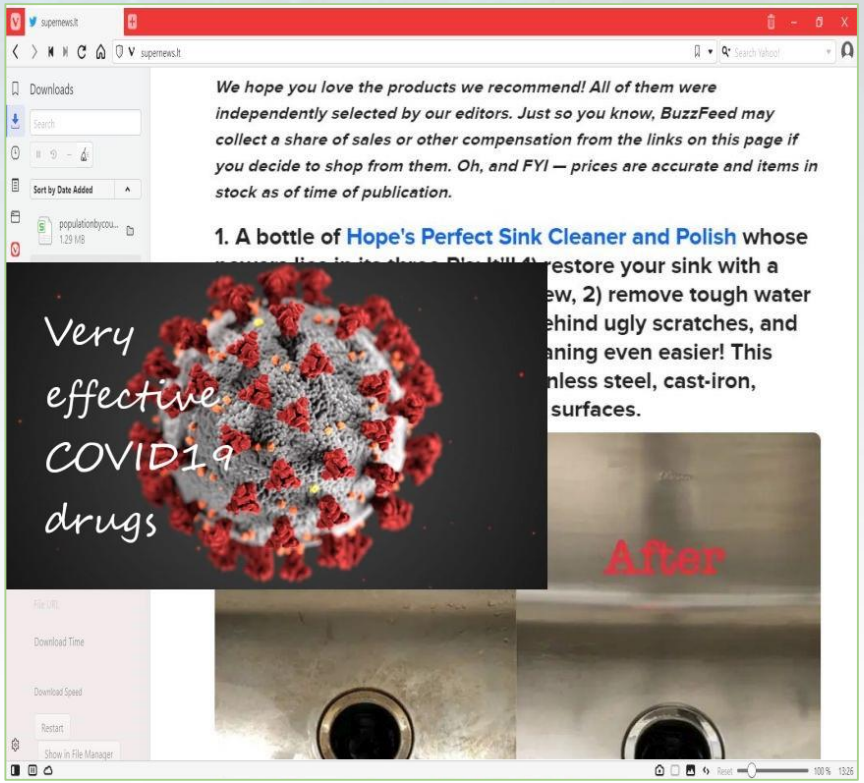
Safely Browsing Internet:

examples with pop-up and without pop-up

Mary blocked pop ups



Jane not ...



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Installing Security Software

- **Security software is essential element** of securely working in cyberspace.

- Pay the attention:

1. Install Internet Security Software;
2. Install a Firewall;
3. Create a Boot Disk;
4. Configure Strict Web Browser and Email Security Settings;
5. Don't Install/Run Unknown Programs;
6. Disable Hidden Filename Extensions.

Funded by the Erasmus+ Programme of the European Union

How is your Browsing Activity Tracked

- Some websites (Amazon, eBay, Netflix and many others) collect data about your preferences: they want to suggest products you might like.
- Google tracks and analyses activity to provide statistical data to companies.
- Some governments collect data about your online activity in case it is needed for criminal investigations or national security purposes.
- **Some criminals may try to track your activities too.**

- It is important to be aware of this tracking to develop safe browsing habits.

Funded by the Erasmus+ Programme of the European Union

Creating Strong Passwords

Password - usually the main tool that ensures your security in modern IT systems.

Password needs to be strong to ensure high level of security.

What is strong password ?

A strong password is one that's easy for you to remember but difficult for others to guess.

Funded by the Erasmus+ Programme of the European Union

Tips for Creating Strong Passwords

Bad practice: to use the same password for each account.

The reason: if someone discovers your password for one account, all your other accounts potentially will become vulnerable.

Tip: to use numbers, symbols, and both uppercase and lowercase letters in your password. This will make harder to hack the password using brute force attack.

Funded by the
Erasmus+ Programme
of the European Union

Tips for Creating Strong Passwords

Bad practice: use of personal information such as your name, birthday, user name, or email address.

The reason: this type of information is often publicly available, which makes it easier for someone to guess your password.

Use a longer password
Rule of thumb: the longer the password is the better (Harder to remember too). Although for extra security it should be even longer.

Funded by the Erasmus+ Programme of the European Union

Tips for Creating Strong Passwords

Bad practice: to use words that can be found in the dictionary.

The reason: many hacking tools are doing so called vocabulary-based attacks. First are trying to check known words in the vocabulary.

E.g., **player2002** would be a weak password (word from vocabulary and the digit meaning the year of birth).

Random passwords are the strongest. Think about using password generator.

Funded by the
Erasmus+ Programme
of the European Union

Common Password Problems

Most commonly used passwords are based on family names, hobbies, or just a simple pattern. Easy to remember but also easy to guess.

Some examples with bad passwords

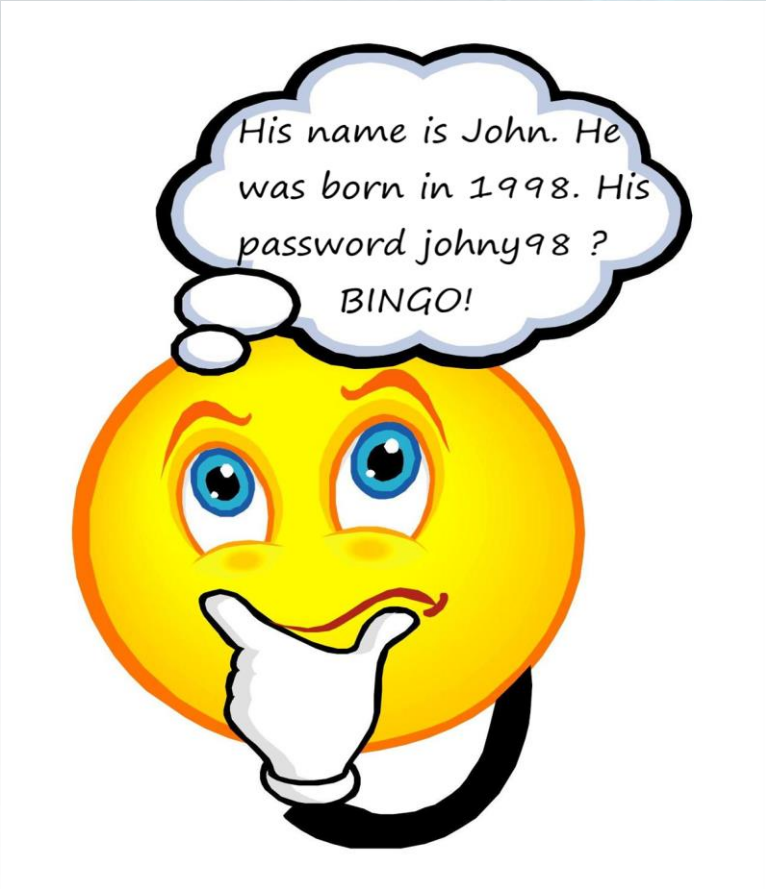
Password: *nick1995katie1997*

Problem: looks long but easy to guess because using two names (boyfriend and girlfriend) with their birth years. Easy to guess if you know info about the targets.

Solution: insert random symbols, use uppercase - lowercase combinations, e.g. ***ni%k199oK$tie199x***

Funded by the Erasmus+ Programme of the European Union

Tips for Creating Strong Passwords



Common Password Problems

Password: *w@kLx*

Problem: looks random and hard to guess but contains only 5 symbols. Too short...

Solution: stronger version needs to be much longer preferably at least 10 symbols.

Password: *123abc456cba789*

Problem: easy to remember but the combination of symbols used will be among the first to check

Solution: random password generator , e. g. *#eV$pIg&qf*

Funded by the Erasmus+ Programme of the European Union

Common Password Problems

Password: *Gmail Bd458$%Kl!df; eBay Bd458$%Kl!df; Amazon: Bd458$%Kl!df*

Problem: password OK but using it on different sites is bad practice.

Solution: use different passwords for each site.

Instead of writing your passwords on paper, you can use a **password manager** to store them securely.

Password managers can remember and enter your password on different websites, which means you won't need to remember longer passwords.

Funded by the Erasmus+ Programme of the European Union

Multi Factor Authentication

Multi Factor authentication (MFA) is an even better way to protect your sensitive data.

What is multi-factor authentication?

Multi-factor authentication is a method of verification where **at least two different factors** of proof are required.

MFA sometimes is called 2FA (stand for two-factor authentication).

In principle it adds additional layer of security.

Funded by the Erasmus+ Programme of the European Union

Types of Multi Factor Authentication

There are generally three recognized types of authentication factors:

Type 1: Something You Know – includes passwords, PINs, code words, etc.

Type 2: Something You Have – includes all items that are physical objects (keys, smart phones, smart cards, USB drives).

Type 3: Something You Are – includes biometric (fingerprints, palm scanning, facial recognition, retina scans, iris scans, voice verification).

Funded by the Erasmus+ Programme of the European Union

Multi Factor Authentication

Combining at least two factors from these three categories we obtain multi-factor authentication.

Multi-factor authentication is much more difficult for an intruder to overcome.

With multi-factor authentication, the attacker must have more skills and be able to carry out multiple attacks simultaneously.

Very often this is extremely difficult.

Well known example of multi-factor authentication supporting online service is PayPal.

Funded by the Erasmus+ Programme of the European Union

Popular Multi Factor Authentication Tools

There are many multi factor authentication tools available.

Common authenticator apps can be found in your mobile device app store:

- Google Authenticator;
- LastPass Authenticator;
- Microsoft Authenticator;
- Authy;
- and many others.

Funded by the
Erasmus+ Programme
of the European Union

File Encryption

- *What is File Encryption?*

  File encryption is a method of encoding data in order to transfer files securely.

- *What File Encryption Do ?*

  Encrypting files helps to prevent tampering or unauthorized access.

- *How File Encryption Works ?*

  Works by using complex algorithms to jumble the data being sent.

Funded by the
Erasmus+ Programme
of the European Union

File Encryption

Important:

you need to have a key to be able get access to the information contained in file !

Funded by the
Erasmus+ Programme
of the European Union

How are Files Encrypted

Two of the most popular encryption standards are:

- ***Open PGP*** - allow you to encrypt and decrypt files using public and private keys.
- ***ZIP with AES*** - compress and encrypt files with AES encryption using ZIP and GZIP standards.

Funded by the Erasmus+ Programme of the European Union

Why to Use File Encryption Software

- Layered data protection

- Security across many devices

- Data transfers secured

- Integrity maintained

- Ensured compliance

Funded by the
Erasmus+ Programme
of the European Union

How to Choose Encoding Software

- What encryption standards does you need to support?

- How sensitive is the data?

- Are large files being exchanged ?

- Should the files be encrypted, or should the connection be encrypted?

- How will the data be transported?

Funded by the
Erasmus+ Programme
of the European Union

Encoding Software

- AxCrypt Premium
- Folder Lock
- CryptoForge
- NordLocker
- Steganos Safe

Funded by the Erasmus+ Programme of the European Union

Tips to Identify Cyber Attack

If you already opened suspicious email or link check to following things:

- *Unusual activity on your device or network.*
- *suspected use of password on your account.*
- *Identify suspicious pop-ups.*
- *Monitor a slower-than-normal network.*
- *Keep software up-to-date.*
- *Unexpected or sudden changes in available disk space or memory.*

Funded by the
Erasmus+ Programme
of the European Union

Some Tips for Safe Online Shopping

- Online shopping is very convenient and often economic ways to buy something.
- But also very dangerous: FBI *Internet Crime Complaint Centre* (IC3) found that **half of cybercrime** in 2019 was related to online shopping.
- Situation not better elsewhere.
- Various sources of misbehaviour:

- not received goods;

- not paid for goods;

- steal the sensitive data, in particular financial data, e. g. credit card data.

Funded by the Erasmus+ Programme of the European Union

Some Tips for Safe Online Shopping

- **Tip 1: use only familiar or trusted online shops**

- This is safety precaution number one;

- Look for the customer's opinion about the online shop;

- Look how long the shop is active (usually the longer is active more reliable is);

- Try avoid using the shops that you heard about from pop-up advertisements or email commercials;

- Report Cyber Crime if you felt victim !

Funded by the Erasmus+ Programme of the European Union

Some Tips for Safe Online Shopping

- **Tip 2: never buy anything online using your credit card from a site that doesn't have SSL (secure sockets layer) encryption installed**

- the site has SSL because the URL for the site will start with HTTPS — instead of just HTTP;

- an icon of a locked padlock will appear, typically to the left of the URL in the address bar or the status bar down below;

- HTTPS is almost standard now even on non-shopping sites.

Funded by the Erasmus+ Programme of the European Union

Some Tips for Safe Online Shopping

- **Tip 3: don't overshare personal information**

- no online shopping site needs your personal code, passport data, etc.;

- your credit card data needs to be approved by your bank online;

- enable secure shopping option on your e-bank;

- being not registered buyer often has advantages from the security point of view.

Remember: the less scammer knows about you the more difficult to hack you.

Funded by the Erasmus+ Programme of the European Union

Some Tips for Safe Online Shopping

- **Tip 4: properly protect your account**

- use strong passwords (see above);

- change passwords regularly (only 25% of people are doing this if not required);

- use different passwords on different shopping platforms;

- use multi factor authentication where possible;

- use anti-malware software;

- avoid shopping using not-private computer.

Funded by the Erasmus+ Programme of the European Union

Some Tips for Safe Online Shopping

- **Tip 4: think mobile**

- don't be afraid to buy using mobile apps: they are not less safe than desktop shopping;

- but use only apps provided by the retailer or other online shopping platform;

- hide your device screen when making payment in public place;

- properly protect your mobile device.

Remember: you need to think a little bit like a gangster when making safe shopping or payment in public.

Funded by the Erasmus+ Programme of the European Union

Some Tips for Safe Online Shopping

- **Tip 5: skip the card, use the phone**

- paying for items using your smartphone is standard;

- are in fact even more secure than using your credit card;

- mobile payment apps like Apple Pay generates a one-time-use authentication code for the purchase that no one else could ever steal and use;

- you do not need to have the credit card with you: this is also a measure of precaution !

Funded by the Erasmus+ Programme of the European Union

Dealing With Cookies

- Cookies are essential element to the modern Internet but a vulnerability to your privacy.
- Cookies help web developers give you more personal, convenient website visits.
- Cookies let websites remember you, your website logins, shopping carts and more. But they can also be a treasure trove of private info for criminals to spy on.

- Even a basic understanding of cookies can help you keep unwanted eyes off your internet activity.

Funded by the Erasmus+ Programme of the European Union

What are Cookies ?

- In the basic form: cookies are text files with pieces of data (e.g., username and password)
- They are used to identify you as you using Internet.
- HTTP cookies are used to identify specific users and give more convenience for browsing.

- Data stored in a cookie is created by the server upon your connection. This data is labelled with an ID unique to you and your computer.
- The server reads the ID and knows what information to specifically serve to you.

Funded by the Erasmus+ Programme of the European Union

Types of Cookies

Two basic types:

- Magic Cookies
- **HTTP Cookies**

- **Magic cookies** are term that refers to packets of information that are sent and received without changes.
- Most often used for a login to computer database systems, such as a business internal network.

Funded by the Erasmus+ Programme of the European Union

Types of Cookies

Two basic types:

- Magic Cookies
- **HTTP Cookies**

- **HTTP cookies** are a modified version of the “Magic cookie” built for internet browsing.
- **HTTP cookie** is used to manage our online experiences.
- Malicious people can use them to spy on your online activity and even steal your personal info.

Funded by the Erasmus+ Programme of the European Union

What are Cookies Used for?

- **Session management**. For example, cookies let websites recognize users and recall their individual login information and preferences, such as sports news versus politics.

- **Personalization**. Customized advertising is the main way cookies are used to personalize your sessions.

- **Tracking**. Shopping sites use cookies to track items users previously viewed, allowing the sites to suggest other goods they might like and keep items in shopping carts while they continue shopping.

Funded by the
Erasmus+ Programme
of the European Union

Different Types of HTTP Cookies

- **Session cookies** are used only while navigating a website. They are stored in random access memory and are never written to the hard drive. When the session ends, session cookies are automatically deleted.

- **Persistent cookies** remain on a computer indefinitely, but often many include an expiration date and are deleted after predefined period

Funded by the
Erasmus+ Programme
of the European Union

Persistent Cookies

- Persistent cookies are used for two primary purposes:

- **Authentication**: track whether a user is logged in and under what name. They also streamline login information, so users don't have to remember site passwords.

- **Tracking:** track multiple visits to the same site over time.

Funded by the Erasmus+ Programme of the European Union

How can Cookies be Dangerous

- Since the data in cookies doesn't change, cookies themselves aren't harmful.
- However, some cyberattacks can hijack cookies and enable access to your browsing sessions.
- The danger lies in their ability to track individuals' browsing histories.
- Sometimes they could be used to infect your computer with malware.

Funded by the Erasmus+ Programme of the European Union

First-Party vs. Third-Party Cookies

- First-party cookies are directly created by the website you are using. These are generally safer, as long as you are browsing reputable websites or ones that have not been compromised.

- Third-party cookies are generated by websites that are different from the web pages users are currently surfing, usually because they're linked to ads on that page.
- Visiting a site with 10 ads may generate 10 cookies, even if users never click on those ads.
- Third-party cookies let advertisers or analytics companies track an individual's browsing history across the web on any sites that contain their ads.

Funded by the Erasmus+ Programme of the European Union

First-Party vs. Third-Party Cookies

- Zombie cookies are third-party cookies and permanently installed on users' computers, even when they opt not to install cookies.
- They tend to reappear after they've been deleted.
- Like other third-party cookies, zombie cookies can be used by web analytics companies to track unique individuals' browsing histories.
- Websites may also use zombies to ban specific users.

Funded by the
Erasmus+ Programme
of the European Union

Tips to Deal with Cookies

- EU law requires user's consent to use the cookies.
- To comply with the regulations governing cookies under the GDPR and the ePrivacy Directive you must:
- *Receive users' consent before you use any cookies except strictly necessary cookies.*
- *Provide accurate and specific information about the data each cookie tracks and its purpose in plain language before consent is received.*
- *Document and store consent received from users.*
- *Allow users to access your service even if they refuse to allow the use of certain cookies*
- *Make it as easy for users to withdraw their consent as it was for them to give their consent in the first place.*

Funded by the Erasmus+ Programme of the European Union

Tips to Deal with Cookies

- Most modern browsers allow you to manage cookies saved on your computer.
- E.g., you may wish to accept all cookies, delete specific website cookies or reject all cookies.
- You need to look for the browser manual or help system to find the possibilities that browser provides to manage the cookies.

Funded by the Erasmus+ Programme of the European Union

Dealing with Malware

- Malwares are malicious software that enables the attacker to have full or limited control over the target system once it enters.
- They can damage or modify information in the system and steals the information from the system.
- There are various types of malware such as – Virus, Trojans, Worms, Rootkits, Spyware and Ransomware.

- A malware might enter the system through emails, file transfers, installation of random third - party software, non-usage of quality anti-virus software.

Funded by the Erasmus+ Programme of the European Union

*Difference Between **Virus** and **Worm***

Virus

- attaches to a program or file and keeps spreading from one system to another.
- replicates and executes itself.
- alters the system without the knowledge of user.
- spreads in the same speed as programmed.

Worm

- subclass of virus which is similar in design, replicates from one computer to another.
- exploit the OS which has weak security.
- causes the system or network to stop responding.
- spread faster than virus.

Funded by the Erasmus+ Programme of the European Union

Antivirus Sensing Software

- An antivirus or antimalware is used to identify, prevent or remove the malware present in the system.
- Can perform system checks and update the security of the system in regular basis.
- Various antivirus software are available in the market for free or not for free.

- Not using antivirus software is a "type of cyber crime"! You can not only fell the victim of attack but your computer may be used as a tool for cyber attack.

Funded by the Erasmus+ Programme of the European Union

Tips to Prevent Malware

- Similar to about what we talked before but needs to be remembered anyway:

- *Keep your computer and software updated.*
- *Use a non-administrator account whenever possible.*
- *Think twice before clicking links or downloading anything.*
- *Be careful about opening email attachments or images.*
- *Don't trust pop-up windows that ask you to download software.*
- *Limit your file-sharing.*

Funded by the Erasmus+ Programme of the European Union

Assess the Security Breach

Two important issues:

- **Follow trusted sources:** *If you are one victim of a broader attack that's affected multiple businesses or persons, follow updates from trusted sources charged with monitoring the situation*

- **Determine the cause of the breach:** *whether you're part of a broader attack or the sole victim, you'll also need to determine the cause of the breach within your specific facility so you can work to help prevent the same kind of attack from happening again.*

Funded by the Erasmus+ Programme of the European Union

Assess the Security Breach

Try to find the answers to the next questions:

- How was the attack initiated?
- Who has access to the servers that were infected?
- Which network connections were active when the breach occurred?

Funded by the
Erasmus+ Programme
of the European Union

Assess the Security Breach

- E.g., you may be able to pinpoint how the breach was initiated by checking your security data logs through your firewall or email providers, your antivirus program or other way.
- You may need to ask support of cybersecurity professionals.
- Do not hesitate to seek for advice if you feel lack of knowledge.

Funded by the
Erasmus+ Programme
of the European Union

Assess the Security Breach

Identify those affected by the breach:

- It is very important to find out who may have been affected by the breach, including your employees, customers, and third-party vendors.

- Assess how severe the data breach was by determining what information was accessed or targeted, such as birthdays, mailing addresses, email accounts and credit card numbers.

Funded by the Erasmus+ Programme of the European Union

Assess the Security Breach

Initiate your cyber-attack protocol:

- Your employees should be aware of your policies regarding data breaches.
- After discovering the cause of the breach, adjust and communicate your security protocols to help ensure the same type of incident doesn't occur again.
- Consider restricting your employees' access to data based on their job roles.

Funded by the Erasmus+ Programme of the European Union

Manage the Fallout from Cyber-Attack

If attack was on company: notify the managers and employees of the breach and all others who may be affected by the attack on you.

This includes:

- Communicate with your colleagues to let them know what happened.

- Define clear authorisations for team members to communication on the issue both internally and externally.

- Remaining in close contact with your team is crucial while recovering from a data breach.

- You may need legal advice on the judicial aspects of the incident.

Funded by the Erasmus+ Programme of the European Union

Manage the Fallout from Cyber-Attack

If attack was on company: notify the managers and employees of the breach and all others who may be affected by the attack on you.

This include:

- If you have cyber liability insurance, notify your carrier. If not try to consider if obtaining the insurance may be useful.

- Cyber liability insurance is designed to help you recover from a data breach or cyber security attack.

- Contact your carrier as soon as possible to see how they can help assist you with what to do after a cyber-attack.

Manage the Fallout from Cyber-Attack

If attack was on company:

notify customers

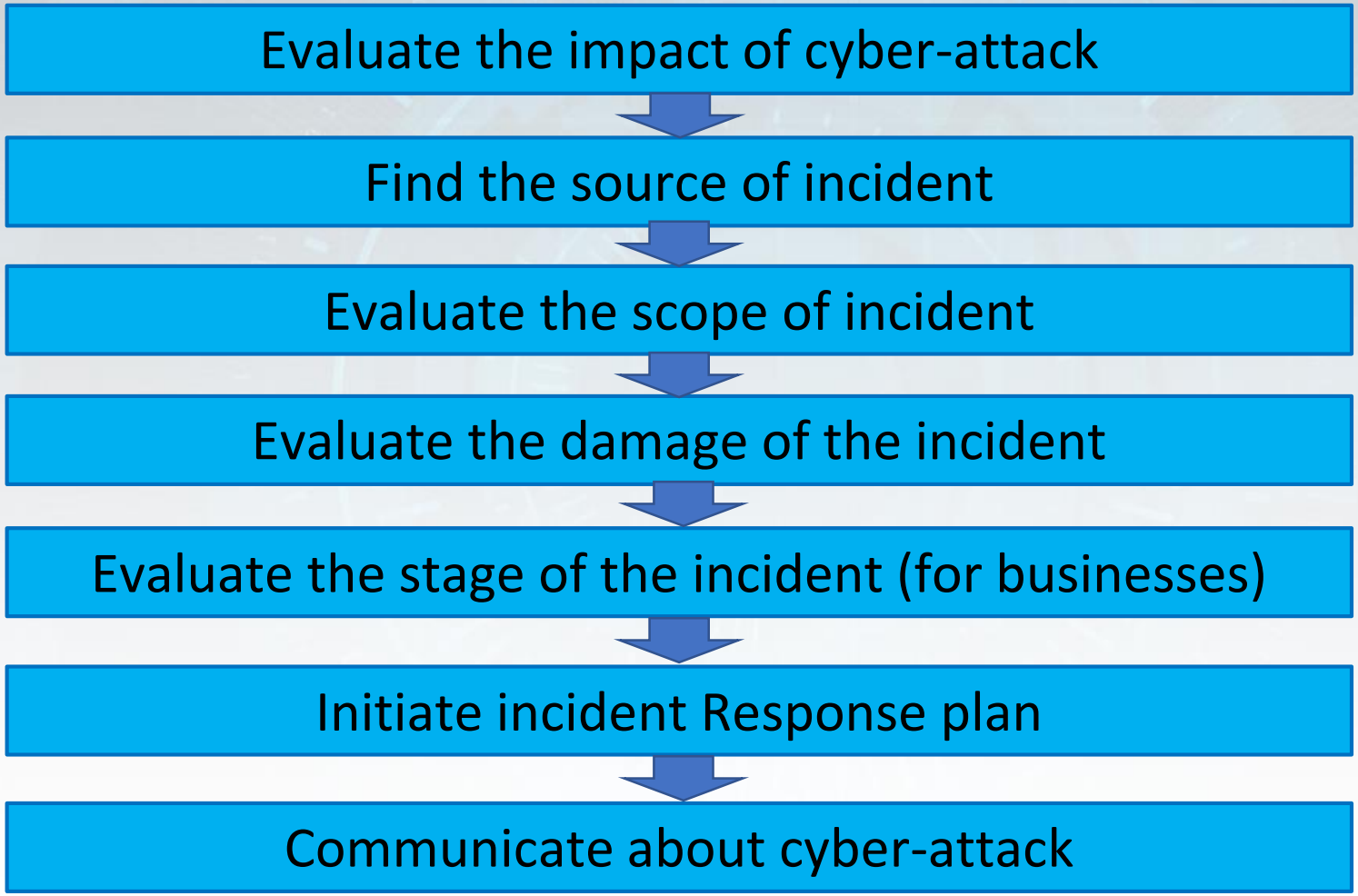
This includes:

- Emphasize your willingness to be transparent with your customers by considering a special action hotline specifically to address questions from affected individuals.

- Communication can be key to maintaining positive, professional relationships with your patrons and minimize potential losses.

Funded by the Erasmus+ Programme of the European Union

Evaluation of Cyber-Attack



Funded by the Erasmus+ Programme of the European Union

Report Cyber Crimes

- Report the attack to the responsible body :
  - each country has responsible body like CERT.
- Depending on the type of cyber attack and local and international regulatio ns you may need to inform law enforcement agencies.
- You may need contact your credit card company if you fear that sensitive financial data may be compromised.
- Tell financial organization that you’re disputing unauthorized charges made by scammers on your card or if you suspect your card number was compromised.
- Discuss further actions with financial organization.

Funded by the Erasmus+ Programme of the European Union

Report Cyber Crimes

- This is especially important if you observed activities related with criminal activities:

- you see this was not the case of *ego hacking* (e.g. young hacker trying to test himself/ herself).

- If you discover you are the victim of a fraudulent incident:

- Contact your IT/security department, if you have one;

- Immediately contact your financial institution to request a recall of funds;

- Contact your employer to report irregularities with payroll deposits.

Funded by the Erasmus+ Programme of the European Union

Steps After Immediate Threat was Removed

- Upgrade your software. Install necessary patches.
- Change the passwords across the system.
- Change the passwords on other systems as the measure of precaution.
- Implementing two-step verification methods to access vulnerable accounts.

- Putting a WAF (*web application firewall*) in place to safeguard your website it you are website administrator or have your website.
- Ensuring your e-commerce platform is PCI-DSS (*Payment Card Industry Data Security Standards*) Level 1 compliant.

What to Do Next

- “Sixty percent of small business and personal breaches in the past 3 years were the result of external factors. Consequently, employee education training sessions should be also regularly occurring and comprehensive. Ensure that staff can identify warning signs of suspicious emails and attachments and know how to report any they receive. Train them on how to encrypt personal or sensitive information, too.”
- *Mike Tanenbaum, executive vice president and head of cyber for Chubb North America*.

Funded by the Erasmus+ Programme of the European Union

If Your Gmail or YouTube Account Has Been Hacked

- If you notice unfamiliar activity on your Google Account, Gmail, or other Google products, someone else might be using it without your permission.

Step 1: Sign into your Google Account

Step 2: Review activity & help secure your hacked Google Account

Step 3: Take more security steps

For more details see: https://support.google.com/accounts/answer/6294825?hl=en

Funded by the Erasmus+ Programme of the European Union

If Your Facebook Account Has Been Hacked

According Facebook suggestions your account may have been hacked if you notice:

- Your email or password have changed.
- Your name or birthday have changed.
- Friend requests have been sent to people you don't know.
- Messages have been sent that you didn't write.
- Posts have been made that you didn't create.

- If you think your account has been hacked or taken over, you should visit page: https://www.facebook.com/hacked

Funded by the Erasmus+ Programme of the European Union

What to Do if Your Other Account Has Been Hacked

- There are huge variety of systems that could be hacked
- It is impossible to provide details for any system

- General suggestions are:

- look for the advices in help system
- try to contact the company responsible for the product

Funded by the
Erasmus+ Programme
of the European Union

Summary

Avoiding cyber-attacks is feasible.

- Train and develop awareness;
- Develop necessary habits;
- Use appropriate tools;
- Have a plan how to behave in case of cyber-attack.

Assignment

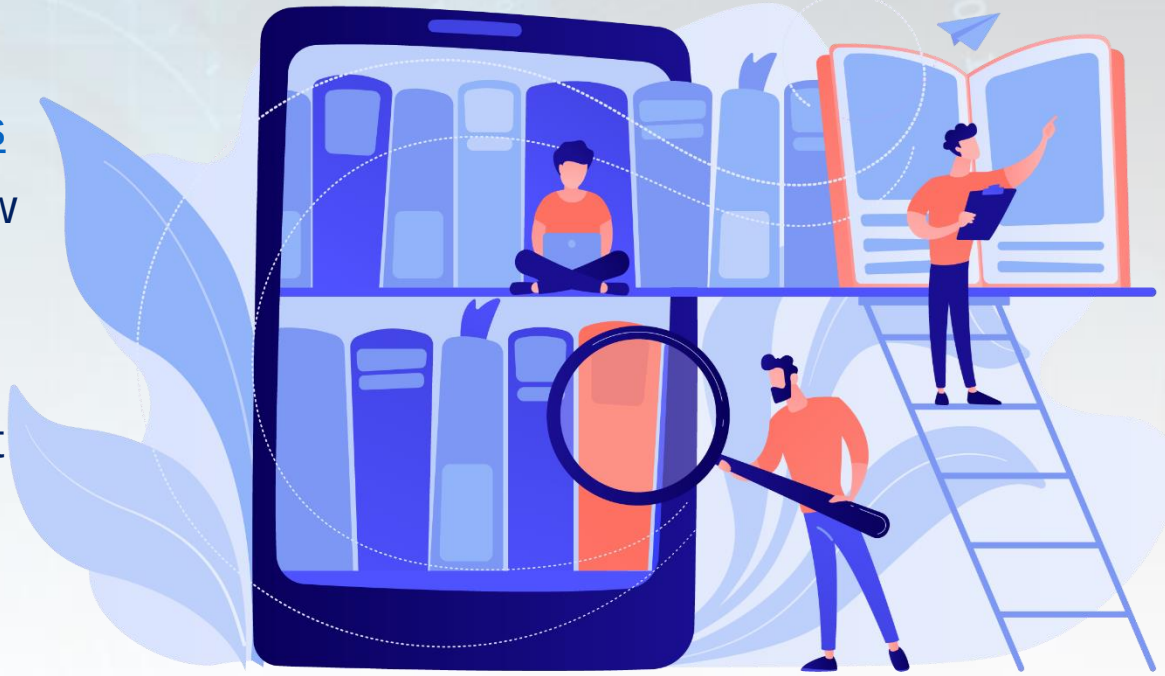
Evaluate the state of the cyber security in enterprise

- State of readiness
- Quality of the tools used
- Quality of passwords
- Reactions
- Post attack changes

Funded by the Erasmus+ Programme of the European Union

Further Reading

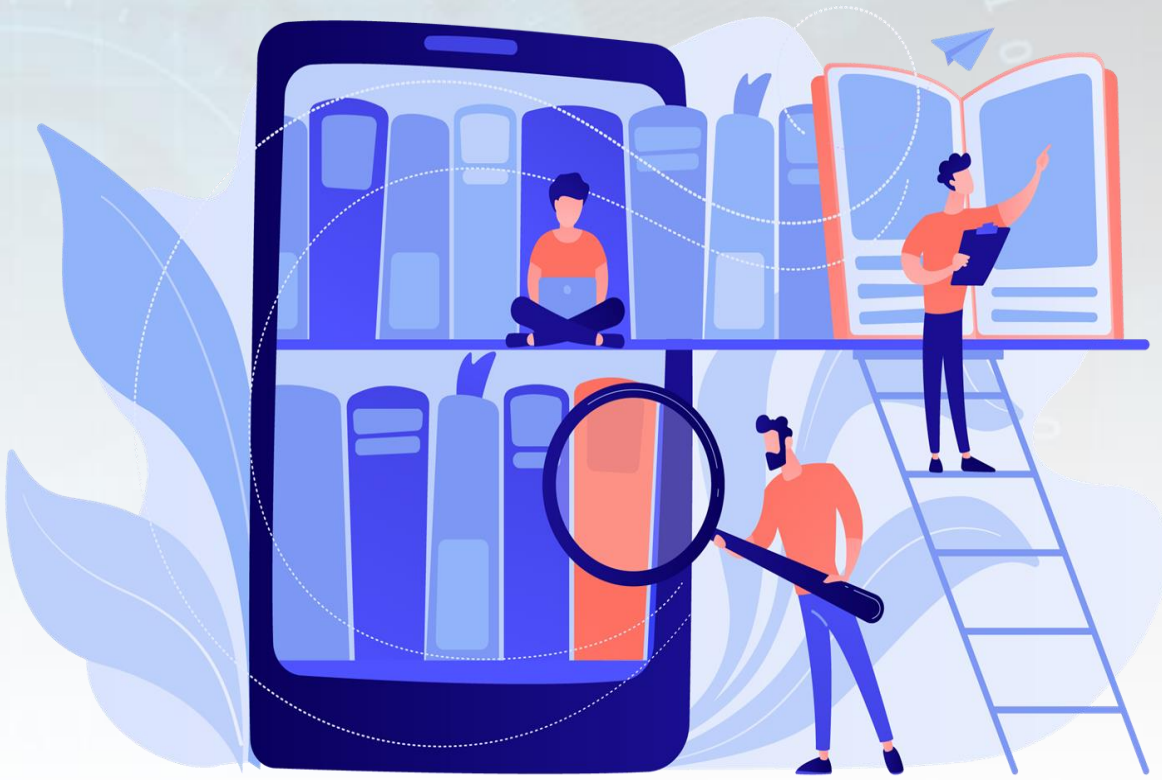
- Protect your business from cyber threats. Australian Government Guidelines. https://business.gov.au/online/cyber-security/protect-your-business-from-cyber-threats
- Yuchong Li, Qinghui Liu. A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments. Energy Reports, September 2021
- Atul S Choudhary; Pankaj P Choudhary; Shrikant Salve. A Study On Various Cyber Attacks And A Proposed Intelligent System For Monitoring Such Attacks. In Proc. of IEEE 2018 3rd International Conference on Inventive Computation Technologies



Funded by the Erasmus+ Programme of the European Union

Further Reading

- Federal Communications Commission. Cybersecurity for Small Business. https://www.fcc.gov/general/cybersecurity-small-business
- State of Cybersecurity in Local, State & Federal Government. Ponemon Institute Research Paper. https://www.ponemon.org/local/upload/file/State%20of%20Cybersecurity%20in%20Government%20FINAL2.pdf
- NCSS Good Practice Guide. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/ncss-good-practice-guide



CyberPhish
Safeguarding your digital future

Funded by the Erasmus+ Programme of the European Union

Thank you!