Cyber MSME

Cybersecurity for Micro, Small & Medium Enterprises

Training module title:

Basics of Cybersecurity. Comprehending the Fundamental Rules of Cybersecurity

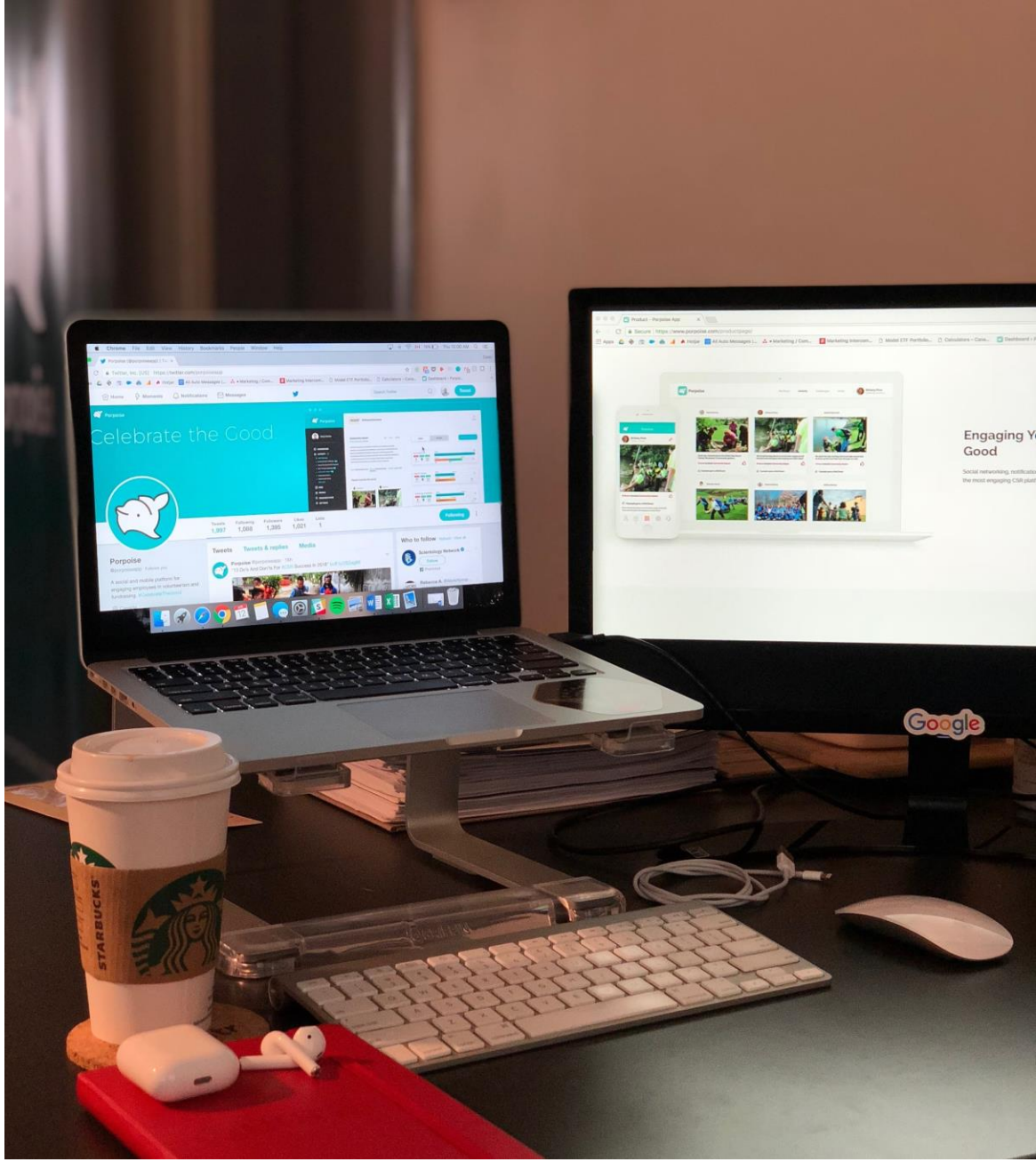
By Internet Web Solutions.

Erasmus+

Objectives and Goals:

At the end of this module you will be able to:

- Understanding the main cyber threats our small business faces.
- To know in detail the development of a cyber-attack to deal with it successfully.
- To Know what to do before, during and after an attack.



Index

Unit 1 **Main threats for companies.**

Unit 2 **The seven stages of a cyber-attack**

Unit 3 **Rules to protect against external threats**

Erasmus+

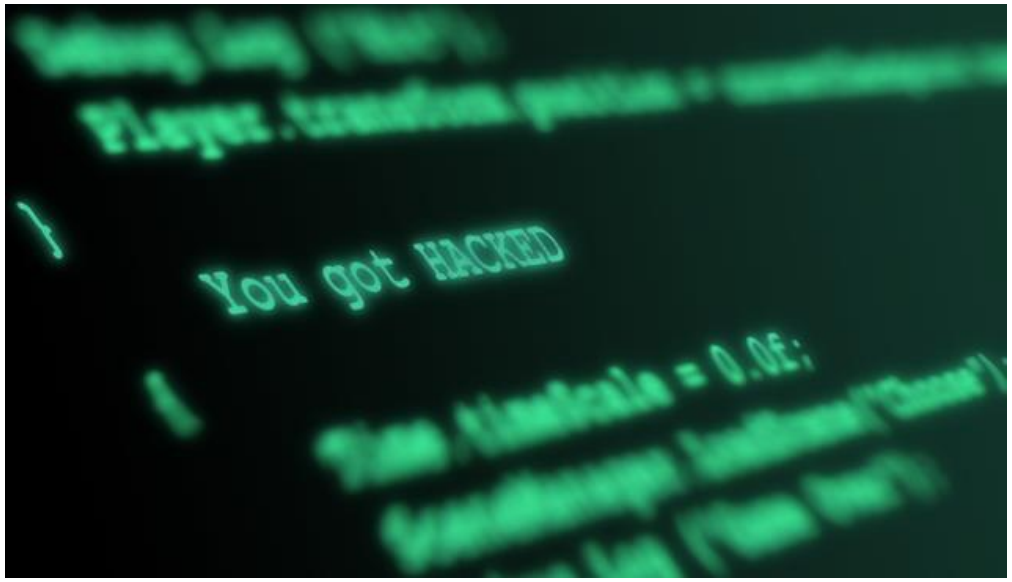
The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.1: Introduction

Technology has taken over our work environments.
The Internet, e-commerce and mobility bring us improvements in productivity and communications with our clients, collaborators and suppliers. But as in the real world, this new virtual scenario also presents risks that we need to be aware of.

Guaranteeing the company's information security is, now more than ever, vital for the business.
The following are some of the most common threats. This information is very useful for detecting threats, so we can prevent them from occurring. And if the attack has occurred, to recognize them and act correctly.



Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.2: Phishing

Phishing is a type of fraud generally committed through email, although other means can also be used, such as SMS (Smishing), social networks, instant messaging applications or phone calls (vishing). The goal of cybercriminals is to steal confidential information and login credentials. For that purpose, cybercriminals often impersonate well-known companies and organizations, such as banking or public entities, energy or logistics companies, etc.

Phishing cyber-attacks contain a link in the body of the message that leads to a fraudulent web page, generally with the same aesthetics as the legitimate web page it is trying to impersonate (web spoofing). On this website, the confidential information that the cybercriminals wish to steal is requested, generally personal information, access credentials and financial information. To make the fraud more truthful, the fraudulent website usually uses a domain name similar to the legitimate one, always aiming to trick potential victims into falling for the scam.

Unit 1: Main threats for companies

1.2: Phishing

Once the victim of the attack has provided all the information requested by the cybercriminals, they are usually redirected to the legitimate website of the impersonated company, so that the fraud goes unnoticed for as long as possible, until the victim becomes aware of it and reports it.

How to identify a phishing campaign?

Phishing campaigns usually have several common factors that we can detect and prevent them from compromising the security of the company:

- Analyse the sender. Phishing emails sometimes contain senders that do not match the organization they supposedly represent. This is the first indicator to check. In other cases, cybercriminals use the email spoofing technique, which consists of falsifying the sender, so that it appears to come from the legitimate entity when it does not.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.2: Phishing

- Generate a sense of urgency. The cybercriminal scares us with the consequences we will suffer if we do not follow the instructions to access a fraudulent web page and enter confidential information. Cybercriminals try to trick us with relevant issues such as service or account cancellation, fines, penalties for not accessing on time, etc. During the COVID-19 pandemic, cybercriminals have adapted to use lures based on this theme and any aspect that could encompass it, such as health warnings or government aid.

- Look for false links. Links often look genuine and ask us to click on the corresponding text.
- **To check where the link actually points, you can hover your mouse over it and see the dialogue box at the bottom of the screen with the real link address**, or use online tools.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.2: Phishing

- Pay attention to impersonal communications. Communications from legitimate entities usually refer to their recipient using first and last names. In contrast, cybercriminals usually do not know these personal details, so communications are impersonal.

- Check spelling and grammatical errors. A genuine communication from any entity will not contain spelling or grammatical errors, since communication with its customers is a very careful aspect.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.3: Man-in-the-Middle attacks (MitM)

The MITM attack is very popular among cybercriminals because of the amount of information they can access if they are successful. The attack is based on intercepting communication between 2 or more interlocutors to impersonate one or the other, to see the information and modify it, in such a way that the responses received at the ends can be of the attacker and not of the legitimate interlocutor.

We can find different attack conditions.

Public or low-security Wi-Fi access points can pose a risk where an attacker deliberately allows a connection to be established to carry out a "man in the middle" attack.
Another method is to imitate the name of a nearby network (SSID) to create confusion so that some people mistakenly connect to it, and many devices are configured by default to connect without asking, automatically connecting to the nearest open networks or whose SSID name is the same.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.3: Man-in-the-Middle attacks (MitM)

Local Area Network (LANs) are also vulnerable to this type of attack. The attacker must have access to the local corporate network, where he can launch an attack that consists of tricking the computers on the local network into believing that it is a legitimate device on the network and forcing all the traffic generated to pass through the device controlled by the cybercriminal.
Access to local networks can be carried out physically, for example with a computer, or using malware, for example by infecting certain servers and being able to manipulate their responses.

On the other hand, attackers also exploit vulnerabilities in **outdated browsers**, so we must pay special attention.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.3: Man-in-the-Middle attacks (MitM)

Usually, it is very difficult to detect when you are suffering a Man in The Middle attack, therefore, prevention is the first measure of protection. In order to minimize the risk of becoming a target of such an attack, we can take some specific actions:

tip Access to secure websites with certificates (those that start with HTTPS, verifying that the certificate belongs to the corresponding company or entity)

tip Protect the company's Wi-Fi network. Our network should be at least WPA2-AES with strong, non-guessable passwords. If clients must connect to a network in our company, enable a guest network with restricted access to the corporate network.

tip Keep the software of our equipment up to date, especially the operating system and browser.

tip Use strong passwords and enable two-step authentication whenever possible.

tip Avoid connecting to open Wi-Fi networks (in cafes, hotels, airports, etc.); if you must connect, use a virtual private network or VPN.

Erasmus+

Unit 1: Main threats for companies

1.3: Man-in-the-Middle attacks (MitM)

tip If you need to connect through public networks without using a VPN, avoid disclosing personal information by using social networks or online banking.

tip Avoid using free VPNs, as it is unknown who is behind them and how they may use the information.

tip Avoid opening e-mail links from unknown sources.

tip Use security software such as antivirus and antimalware on corporate computers and keep it up to date.

tip Keep the software firewall enabled on those systems that allow it.

tip Secure the corporate website with an SSL certificate.

tip If we have suffered any infection in our computers, or we suspect it is happening (because of strange actions pop-ups, advertising, etc.), we must clean the computer before transmitting any sensitive information.

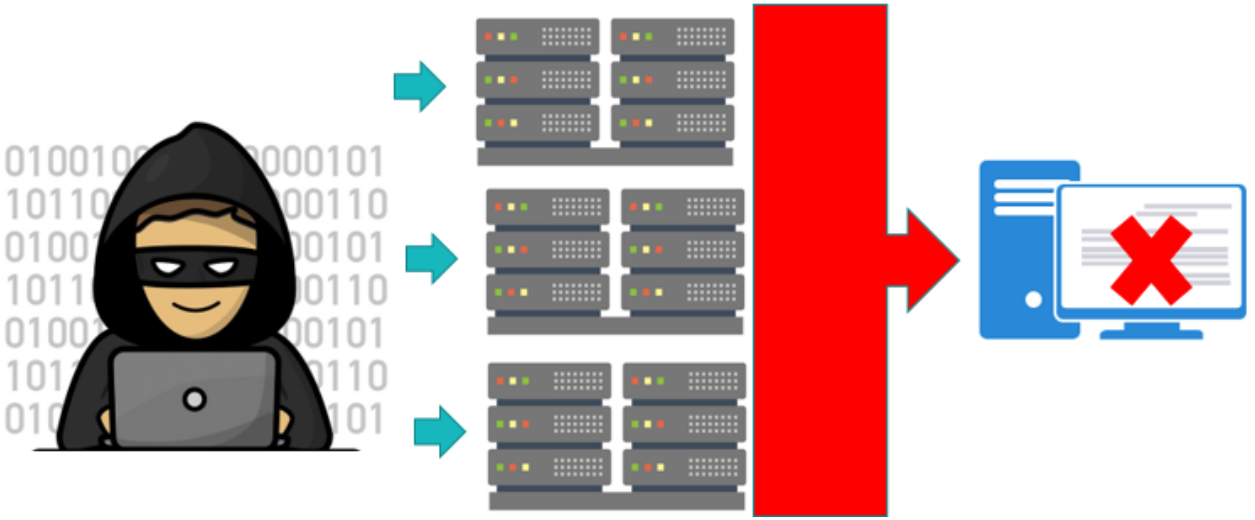
Erasmus+

Unit 1: Main threats for companies

1.4: Denial of Service Attack (DOS)

One of the most important assets for many companies is their website, whether it's a simple informational page or something essential to the business such as an online store. Competitors, cybercriminals, angry employees or ex-employees, etc. can all put your company's website out of business. One of the most common attacks they can carry out is a denial of service (DoS)

What is a denial of service attack?
This type of attack aims to reduce the quality of a service, for example, a web page, leaving it in a non-functional state. To achieve this, cybercriminals saturate the system resources hosting the service to be interrupted by sending them an avalanche of requests that the system is not able to handle.



Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.4: Denial of Service Attack (DOS)

Denial-of-service attacks have severe consequences for the systems under attack. Implementing preventive measures will be essential because we will only know that we have been victims of this attack when the service stops working.

tip

Protection measures in the internal network:
Locate the web server in a demilitarized zone (between firewalls), also called DMZ, thus preventing an intruder from accessing the internal network if he breaches the web server

Implement an intrusion detection and prevention system (IDS/IPS) that monitors connections and alerts us if it detects unauthorized access attempts or protocol misuse;

tip

Protection measures in the hosting:
If you have contracted a hosting service, you should find out about the security measures implemented by the provider. Verify with the provider who will be in charge of its configuration and administration.

tip

Bandwidth:
It may be the most basic form of protection, but it is not the least effective. We need to have as much bandwidth as possible. In this way, the traffic peaks that cause denials of service can be better managed.

Erasmus+

Unit 1: Main threats for companies

1.4: Denial of Service Attack (DOS)

tip

Redundancy and load balancing:

Redundancy consists of having the asset duplicated on more than one server.

Load balancing allows work to be assigned to one server or another depending on the workload it is supporting. This measure reduces the risks of suffering one of these attacks, since having more than one server will reduce the possibility of it stopping due to overload.

tip

Cloud-based security solutions:

One of the solutions that any critical web service should have is a Web Application Firewall. WAFs act as intermediaries between our web service and users, also interposing themselves to cybercriminals or bots. In case of attack, the WAF will act and prevent malicious connections from reaching the website, thus avoiding denials of service.

tip

Updated systems:

Some of the denials of service attacks originate from outdated systems, as these are more vulnerable. Keeping software (servers, web content management systems, etc.) up to date is essential to avoid any type of attack.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.5: Zero-day exploitation 

When the developer of an application or web service discovers a security flaw in its system quickly applies an update or patch to fix it. But what happens if a cybercriminal discovers the vulnerability earlier and exploits it? This is what is known as a Zero-Day vulnerability.

The main threat is until a patch is released and users install it on their computers, cybercriminals have a free hand to exploit the vulnerability and take advantage of the security flaw.


tip

When it comes to vulnerabilities, the most important measure to protect our security is to keep all protection tools activated. **An updated antivirus can mean the difference between an infected device and a contained threat.**

In addition, another fundamental measure is **to keep all the software we use up to date**. 
tip

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.6: Corporate social networks: threats and security measures

Nowadays, social networks have become a very important tool for companies, allowing them to publicize their products or services and have a closer relationship with customers or potential customers.

Generating a company's image and reputation on social networks is not an easy task, and many times companies lose all the effort and time to create an ideal image due to poor management.

Risks for the company:

Human error

- Value judgments
- High tone
- Disclosure of confidential or private information

Weak privacy settings

- Weak passwords
- Publications
- Third-party applications

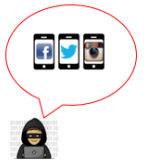
Fraud campaigns

- Spoofing
- Malware
- Phishing

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies



1.6: Corporate social networks: threats and security measures

To avoid the above risks, we will follow a series of security measures and good practices in the use of social networks:

Password

Strong

Two-factor authentication

Password is the key to access the social network. If an unauthorized person accesses our social network profile, they could publish in our name or access our followers through direct messages, damaging the company's image.

Common Sense

Think before publishing

Before publishing any information about the company or on behalf of the company, we have to think about whether it can be used against or negatively affect the company's image.

Setting privacy options

Correctly configuring privacy settings

Privacy options should be configured as restrictively as possible, without affecting the objective set by the company for the social network, such as communicating with customers and establishing a closer relationship.

Malware and links

Malicious attachments and links

Any type of attachment or link sent by the social network will be considered a potential threat. If in doubt, do not execute the attachment or open the link.
In addition, devices with access to social networks will always have antimalware.

Erasmus+

Unit 1: Main threats for companies

1.7: Cybersecurity in teleworking

When the company allows employees to telework, it is recommended to develop a policy for this purpose, to specify the technical and organizational aspects that define teleworking in the company. It is a good practice to establish the permitted uses of business services, and the characteristics and configurations of the technologies to be used for remote access, such as type of device, permitted networks, time slots, home Wi-Fi, etc.

The key points of a good security policy for SMEs are:

Raise employee awareness before starting to telework. Employees must be trained in cybersecurity before they start teleworking and are aware of the policies and measures that will be implemented in the company.

Remote workstation protection regulations. A specific regulation that includes all the necessary measures to protect the workstation, the devices allowed, the systems installed or the applications and programs considered necessary to perform the daily work.

List of users who have the option to work remotely.

Procedures for requesting and authorizing teleworking

Implementation and testing period. It is necessary to evaluate different scenarios and configurations before starting teleworking. Hasty implementation of teleworking can jeopardize the company's confidential information.

Erasmus+

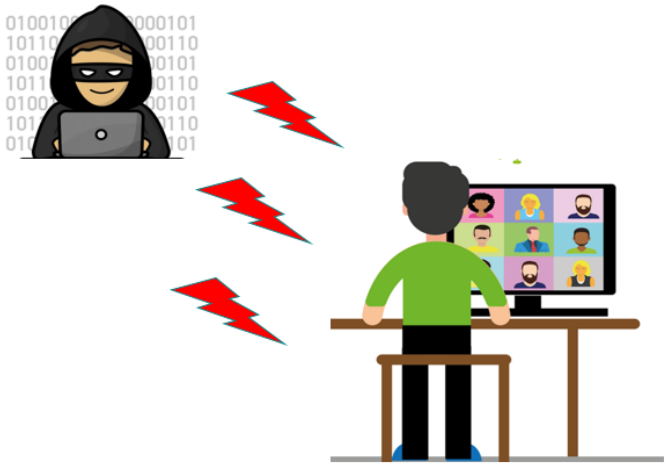
The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 1: Main threats for companies

1.7: Cybersecurity in teleworking

Load testing in simulated scenarios. If a large number of employees are going to telework, we must assess the load that will occur in the company's internal systems.

Applications and resources that can be used by each user.



Secure access. Strong passwords and two-factor authentication will be used for access credentials.

Configuration of teleworking devices. The devices used by the employee to telework will be previously configured by the organization's technicians.

Encryption of information media.

Planning for backups of all media

Use of secure connections through a virtual private network (VPN)

Internet connection. When it is not possible to use the home, or any other network for teleworking, use the 4G or 5G mobile data network always avoiding connection to public Wi-Fi networks.

Erasmus+

The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

Unit 2: The seven stages of a cyber-attack

The key to detecting, stopping, disrupting and recovering from a cyber-attack is to understand its life cycle and thus develop and implement all the necessary operations to ensure the highest degree of security and protection. This life cycle is known as the **Cyber Kill Chain**.

Cyber Kill Chain consists of seven steps, each of which represents a stage of the attack. Knowing the cybercriminal's steps to achieve his goal, we can stop the attack in any of its phases and break the attack sequence by blocking it.

Unit 2: The seven stages of a cyber-attack

2.1: Reconnaissance

The cybercriminal gathers information about his target by looking at the details the organization publishes and seeks information about the technology it uses and data on social networks, and even contact via email interactions.

With that information, the cybercriminal assesses which attack methods might work successfully. For this reason, to prevent the cyber attacker from having this data, employees must be aware and develop an authentic security culture, reviewing and limiting the information shared on the web and social networks or carrying out measures that make it inaccessible.

Unit 2: The seven stages of a cyber-attack

2.2: Weaponization

In this stage, the attack is explicitly prepared on a target. The cybercriminal could create a PDF or Microsoft Office document and include it in an email that impersonates a legitimate person the company interacts typically with. Again, **being cybersecurity aware will be the best mechanism to stop the attack at this stage.**

2.3: Delivery

In this phase, the attack is transmitted, for example, by opening the infected document that has been sent by email, accessing a phishing site, etc. **Being aware of these types of attacks and learning to identify them will be our first line of defence.**

Unit 2: The seven stages of a cyber-attack

2.4: Exploitation

This phase consists of the attack "detonation", compromising the infected computer and the network it belongs to. This usually occurs by exploiting a known vulnerability, such as a remote desktop vulnerability, which, if not patched, would allow computers to be accessed from the outside.
For this reason, **it is essential to have security solutions** in place **and to keep all systems, including the antivirus, updated to the latest version.**

2.5: Instalation

At this stage, the attacker installs the malware on the victim's system. It also often happens that no installation is required, as in credential theft or CEO fraud. In any case, cybersecurity training and awareness will be our primary weapon to stop any attack in this phase, along with technical measures such as system monitoring, using our own infrastructure or outsourcing personnel or services.

Unit 2: The seven stages of a cyber-attack

2.6: Command and control

At this point, the attacker has control of the victim's system. He can perform or launch his malicious actions directed from a central server known as C&C (Command and Control), steal credentials, take screenshots, takes confidential documentation, install other programs, know what the user's network is like, etc.

2.7: Action on objective

This is the final phase in which the attacker gets hold of the data and tries to expand his malicious action to more targets. The kill chain is not linear but cyclical since each of its phases would be executed again to infect more victims. Therefore, to break the chain and prevent an attack from achieving its objectives, it will be necessary to be truly committed to cybersecurity.

Unit 2: The seven stages of a cyber-attack

An organization where employees have the necessary cybersecurity skills, that keeps all systems and equipment up to date, uses the right security solutions and monitors its communications activity will significantly increase its ability to detect and respond to these types of security incidents, making it much more difficult for criminals and preventing systems and the information stored on them from being compromised. Keeping up to date and training and raising awareness among your employees will be the main barrier against any threat or targeted attack. Protect your company!

Unit 3: Rules to protect against external threats

3.1: Before the cyber-attack

Being proactive is essential to partially or totally avoid the damage that a security incident can cause. Moreover, if it is not possible to avoid it, you will be better prepared to provide an effective response to minimize its effects.

Risk analysis and assessment. The first step is to review your information assets, what threats you are exposed to and where you need to start taking care of your business cybersecurity.

We can analyse:
Technologies we use (email, web, telework, mobile devices).
Updating our devices and systems
Use of antivirus
Training of employees in cybersecurity
Passwords management, etc.

Operational and ALWAYS updated

Antivirus
Antimalware
Backups
Updated equipment
Access control to relevant data

Cyber-insurance

Cyber insurances are indicated for risks of lower probability and greater impact, those for which taking other measures is less profitable than taking out insurance to cover losses in the event of an occurrence.

Awareness and training.

Ensure that, at all times, employees are aware of, understand and comply with the cybersecurity rules and protection measures adopted, warning them of the risks that may arise from the misuse of the technological devices and solutions available to them.

Unit 3: Rules to protect against external threats

3.2: During the cyber-attack

Preparation: the necessary tools for the incident treatment are gathered (anti-malware, file or device integrity checkers, vulnerability scanners, log analysis, recovery and backup systems, forensic analysis, etc.).

Identification: the incident is detected, the scope is determined and a solution is devised. This phase involves business, operations and communication managers (contacts with technical support, CERT, forensic experts, police or legal advisors if necessary, etc.).

Containment: preventing the incident from spreading to other resources. As a consequence, its impact will be minimized (separating computers from the affected network, disabling compromised accounts, changing passwords, etc.).

Mitigation: the compromised elements are eliminated, if necessary and possible, and the affected systems are reinstalled or backed up. In any case, mitigation measures will depend on the type of incident.

Recovery: the aim is to return the level of operation to its normal state so that the affected business areas can resume their activity.

Recapitulation: the details of the incident are documented. For this purpose, the data collected will be archived and lessons learned will be discussed. Employees will be informed and taught the recommendations aimed at preventing future risk situations.

Unit 3: Rules to protect against external threats

3.3: After the cyber-attack

Managing an incident is not just a matter of restoring the affected systems and services or applying the necessary security measures to prevent it from happening again. It is just as important to recover the daily activity of the organization as it is to correctly document everything that happened, assess the damage or review the company's policies. With these "lessons learned," we will be better prepared to stop a similar incident.

Report your incident

Contact the authorities.

Learn from the incident.

To prevent it from happening again in the future and to fix it if it happens again

Document the details

It will help us learn from what happened and evaluate the actions taken.

Assess in detail the costs of the incident.

Will be evidence in case of trial.

Review the company's policies.

Lessons learned.

Erasmus+

Bibliography and relevant links

Incibe. National Institute of Cybersecurity> **Awareness kit for companies.**

https://www.incibe.es/protege-tu-empresa/kit-concienciacion

Cisco > **What is Phishing?**

https://www.cisco.com/c/en/us/products/security/email-security/what-is-phishing.html

Norton > **What is a man-in-the-middle attack?**

https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html

Cybersecurity & Infrastructure Security Agency> **Understanding Denial-of-Service Attacks**

https://us-cert.cisa.gov/ncas/tips/ST04-015

Kaspersky > **What is a Zero-day Attack? - Definition and Explanation**

https://www.kaspersky.com/resource-center/definitions/zero-day-exploit

Business2Community> **The Social Media Security Risks Hidden in Your Shadow IT**

https://www.business2community.com/cybersecurity/the-social-media-security-risks-hidden-in-your-shadow-it-02354072

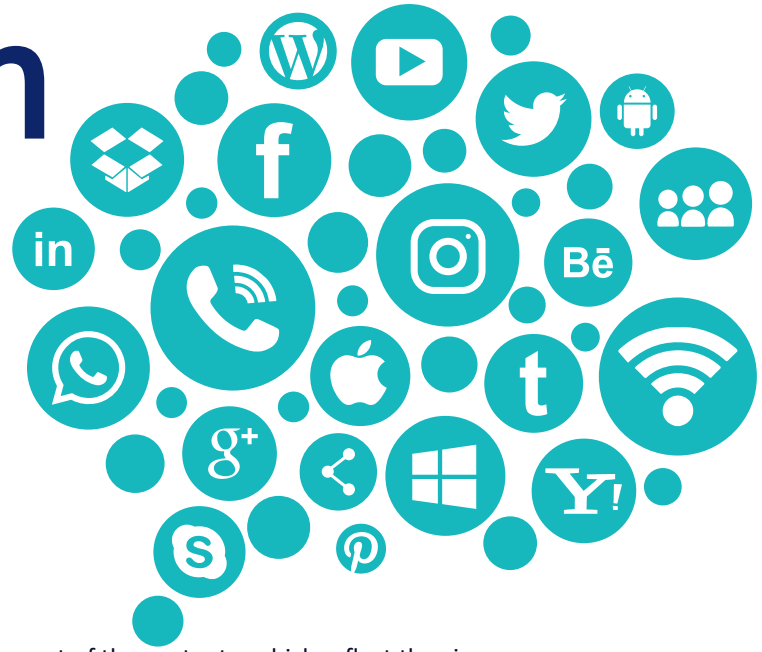
Forbes > **Four Practical Tips For Maintaining The Cybersecurity Of Your Remote Company**

https://www.forbes.com/sites/forbestechcouncil/2021/05/04/four-practical-tips-for-maintaining-the-cybersecurity-of-your-remote-company/?sh=3041c9e95c73

Thomson Reuters > **Kill Chain: The 7 Stages of a Cyberattack**

https://tax.thomsonreuters.com/blog/kill-chain-the-7-stages-of-a-cyberattack/

Thank you for your attention



The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.