**Training fiche**

|  |  |  |
| --- | --- | --- |
| **Title** | | Cybersecurity in the (home) office |
| **Keywords (meta tag)** | | cybersecurity, safety, malware, phishing, sensitive information |
| **Provided by** | | Internet Web Solutions |
| **Language** | | English |
| **Training area (X where applicable)** | | |
|  | Innovation & Servitization | |
| **X** | Digital Transformation | |
|  | Localization | |
|  | Sustainability | |
| **ESCO competencies and skills** | | |
| * Transversal skills and competences   + Social and emotional skills   + Critical thinking   + Analytical thinking   + Problem-solving   + Self-management   + Business management   + Adaptability   + Resilience   + Creativity   + Networking   + Initiative   + Flexibility   + Openness   + Understanding complexity   + Cooperation   + Empathy   + Innovation   + Leadership      * Skills   + Technological skills   + Product marketing   + Digital marketing   + Digital skills   + Communication   + Cooperation   + Emotional intelligence      * Knowledge   + Business management   + Online learning and training   + Advertising   + Cloud computing   + Big data   + E-commerce   + Artificial intelligence   + IoT   + Digital literacy   + Cybersecurity   + Data mining and analysis   + Sustainability   + Well-being   + Climate change   + Social media management | | |
| **Teaser** | | |
| “Did you know 85% of European MSMEs consider cybersecurity to be a key concern for their business?” | | |
| **Objectives / goals / learning outcomes** | | |
| In this module you will learn about what cybersecurity is, familiarise yourself with the most commonly used terminology in this field and find out about the most common cyber-attacks when working from home and from the office. In this way, you will be able to prevent the main cyber risks and to navigate safely, not only when working from home but also when doing everyday tasks on the Internet, thus increasing your skills and knowledge about computer security. | | |
| **Description** | | |
| Most European MSMEs see cybersecurity as a key business concern. However, in a post-pandemic context, not all companies have implemented new security measures to fight risks arising from remote working due to lack of awareness and lack of cybersecurity skills. This module will enable MSME staff and entrepreneurs to improve their cybersecurity skills and knowledge in order to increase their digital skills and cyber resilience. | | |
| **Checklist of benefits for entepreneurs** | | |
| ✓ The implementation of cybersecurity strategies in MSMEs reduces the risk of information loss and leaks, while maintaining data integrity.  ✓ By keeping customer information confidential, the company's reputation and corporate image is also enhanced in the public eye.  ✓ Cybersecurity increases the resilience and recovery capacity of companies, with backups that allow them to resume business after an unexpected incident.  ✓ By reducing information loss due to cyber-attacks or internal issues, there is also an increase in productivity.  ✓ Cybersecurity is an essential tool for employers and employees, not only in working life but also in personal life, by raising awareness and preventing cyber risks (e.g., in online shopping). | | |
| **Contents arranged in 3 levels** | | |
| **Module: Cybersecurity in the (home) office**  **Unit 1: Fundamentals of cybersecurity**  **Section 1.1: What is cybersecurity?**  The term "**cybersecurity**" was born in the 1970s because of the need for companies to **protect their computer systems** from malicious attacks that could compromise their proper functioning by misusing information.  Cybersecurity includes the application of tools, technologies, policies, controls and procedures in protecting or recovering networks, systems, devices and applications from **cyber attacks** aimed at accessing, destroying or altering sensitive information, disrupting workflows, or extorting money from organisations or individuals.  According to a 2021 report by the European Union Agency for Cybersecurity (ENISA), out of a total of 249 European MSMEs surveyed, **85% consider cybersecurity to be a key concern for their business**. In a post-pandemic context, 45% of MSMEs implemented new technologies in response to the pandemic, yet 90% did not include new security measures.  The same report, which provides valuable information on the cybersecurity of European MSMEs, shows the **main cybersecurity incidents suffered by European MSMEs based on their origin**, as shown in the graph.  Source: <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes> (own elaboration)  **Section 1.2: Main definitions**  General security:   * **Backup**: a copy of files and programs that is stored on other devices or other media, in order to recover information in the case of failure, loss or theft. * **Sensitive information**: information containing private or confidential data, such as personal or bank details. * **Software**: software is a computer program designed to perform specific tasks, for example a browser, a game, etc. It is the opposite of "hardware", which is the physical components of the device, such as the motherboard or the processor. * **Encryption**: is a process that converts a document or file into information that is unreadable to people who do not have the key to decrypt it. It serves to protect information from people who should not have access to it. * **HTTP / HTTPS**: one of the most widely used protocols for Internet browsing. HTTPS (HyperText Transfer Protocol Secure) is the secure version, and ensures that the information transmitted between your device and the website is encrypted and protected. * **Firewall**: when navigating the web and accessing a website, it communicates with your computer to establish the connection. The firewall analyses this type of connection to prevent access to those that could constitute a risk.   Threats:   * **Social engineering**: social engineering does not require high computer skills, as it involves the manipulation of people through psychological techniques and social skills, and is often used to obtain sensitive information, such as passwords or bank details. Phishing techniques are based on social engineering. * **Phishing**: the technique of pretending to be another person or entity via email, leading the user to perform some action on a fraudulent page in order to obtain passwords or download an infected file. * **Smishing**: SMS + phishing. Similar to phishing, this technique uses SMS messages for the same purpose. * **Vishing**: voice + phishing. In this case, the attacker pretends to be someone else on a phone call, often posing as technical support for the device or the phone company. * **Web based attacks**: these complex attacks act when you use the Internet, making use of malicious software to infect devices that do not have the necessary security or are outdated.   Types of malwares:   * **Malware**: malware is malicious software that can take various forms (as executable code, scripts, etc.), and can perform actions such as encrypting or deleting sensitive data, altering the basic functions of the device, spying on user activity, and more. Anti-malware is software whose function is to detect, protect and remove this type of malicious software. * **Computer virus**: this type of malware aims to alter the functioning of the device, and requires user interaction to spread to other files and systems.. * **Computer worm**: is able to replicate and move from one infected device to others across the network. It often comes from infected USB drives, email attachments, or even websites. * **Trojan**: this type of malware enters the system as a harmless file or software, and performs unwanted actions in the background, such as deleting files or downloading other malware. * **Spyware**: as the name suggests, this type of malware spies on the infected device, collecting information about the user's activity. It usually comes from spam or fraudulent download websites. * **Adware**: malware that tracks the user's browser and download history in order to display unwanted ads or banners for the user to click on. They usually infect devices via infected websites or fraudulent download websites. * **Ransomware**: a dangerous type of malware that encrypts files on the device's hard drive and restricts access to the user, demanding a ransom, usually in cryptocurrencies, in exchange for decrypting the files. A well-known case is that of [**WannaCry**](https://www.europol.europa.eu/wannacry-ransomware).   **Unit 2: Cybersecurity…**  **Section 2.1: …in the workplace**  **Cybersecurity is the responsibility of everyone in a company**, both management and employees, so it must also be part of the company's working culture.  Both in the office and at home, it is absolutely necessary to comply with a series of **basic measures within the framework of a cybersecurity plan** for the proper functioning of the business.  The following is a **basic cybersecurity plan** to follow to maintain the integrity of the company's information:   1. **Inform about the company’s cybersecurity policies.** Each company has unique needs, so cybersecurity policies should be developed and followed by all employees and managers to create a culture of cybersecurity. 2. **Update the software of the devices.** Keeping all applications and operating systems up to date prevents vulnerabilities. 3. **Setting up a firewall.** A firewall will provide additional protection when navigating the Internet. 4. **Make regular backups.** In case of data loss, backups will help restore normality quickly. 5. **Securing wifi networks.** Wifi networks used in day-to-day activities shall be properly configured to be sufficiently secure against third parties. 6. **Install anti-malware software.** To protect against possible attacks. 7. **Develop an action plan for mobile devices.** Cybersecurity is not only for computers, but also for mobile devices such as smartphones and tablets, which must also be protected. 8. **Implement procedures for the protection of information.** Procedures to be followed in case of cybersecurity incidents should be established. 9. **Use strong passwords.** They should combine numbers, letters and special characters. One way to check if passwords are secure is the website <https://password.kaspersky.com/>. 10. **Restricting permissions for software installation.** Employees should have limited access when installing new software, in order to prevent the installation of fraudulent applications that could infect network devices.   **Section 2.2: …in remote work**  **When working remotely, cybersecurity is even more important**,as when working from home there is not the same control over the company's cybersecurity procedures and policies, networks are less secure, there may be configuration errors, lack of training, among others.  This is why new measures must be considered to ensure that the following **cybersecurity objectives for remote access to information** can be met:   * **Availability**. Authorised users must have access to the information when necessary. * **Confidentiality**. It must be ensured that only authorised users can access the information. * **Authenticity**. It must be ensured that authorised users (with access to information) are who they claim to be. * **Traceability**. It must be possible to track improper or unauthorised access to information. * **Integrity**. It must be ensured that the information and its processing methods are accurate and complete.   In addition to the aforementioned cybersecurity plan, the use of a **VPN** (**Virtual Private Network**) is highly recommended. This network technology allows a secure connection between the local network and the Internet, so that **the integrity and confidentiality of the information is guaranteed**.  In addition, **remote desktop access applications** will allow teleworkers to remotely control computers that are physically located in the office, such as the TeamViewer tool.  **Cloud solutions** and **collaborative tools** are also important tools for cybersecurity in remote work, **enabling accessibility to information in a fast and coordinated manner**.  Some examples of tools for remote work are:  **VPN:**   * **hide.me**. This VPN service allows to navigate in a private way, without geographical restrictions. It counts with more than 2000 servers and 75 locations. <https://hide.me/> * **PrivadoVPN**. Based in Switzerland, its free version allows to protect up to 10 GB of data every month. <https://privadovpn.com/>   **Remote desktop:**   * **AnyDesk**. This is another remote desktop software that is also available free of charge for personal use. This type of tool allows access to information from anywhere, which improves internal communication. <https://anydesk.com/> * **TeamViewer**. This tool focuses more on remote access to information, as it allows access to any device from anywhere. It allows secure file sharing and access to other devices, and is free for personal use. <https://www.teamviewer.com/>   **Cloud solutions:**   * **Dropbox**. The free plan provides 2 GB of storage, and the paid plans go up to 3 TB of storage. <https://www.dropbox.com/> * **MEGA**. This platform includes 20 GB for free, and has paid plans for individuals up to 16 TB, and for companies up to 10 PB, making it one of the solutions with the largest capacity. <https://mega.io/>   **Collaborative tools:**   * **Slack**. This instant messaging platform allows integration with other tools, and simplifies team communication. The free version allows access to the history of the last 10,000 team messages, video calls with colleagues, and integrates with 10 applications. <https://slack.com/> * **Trello**. This tool works with the Kanban card system, and allows you to include notes, files, deadlines and other items. It is easy to manage by dragging the cards, and is available in several languages. This tool is free up to 10 boards per team. <https://trello.com/>   **Unit 3: Recommendations for entrepreneurs and staff**  **Section 3.1: Recommendations for entrepreneurs**   * Make sure your company has a **cybersecurity plan** that is appropriate to the needs and potential vulnerabilities of your business. * Establish policies and procedures for **secure information management**, e.g., no personal devices, secure destruction of documents. * **Train your employees in cybersecurity** so they can comply with policies and procedures. * **Improve your digital and cybersecurity skills**; remember that you handle very sensitive information. * Also compy with the **recommendations for staff**! ☺   **Section 3.2: Recommendations for staff**   * Cybersecurity starts with the **physical security of information**: keep your desktop free of confidential information, post-its with passwords, emails, etc. * Do not connect **USB devices** that come from untrusted people, as they could infect your computer. * **Encrypt sensitive information before sending it**, e.g. through a password-protected compressed file. * Remember to **empty your computer's trash** regularly. * Make regular **backups**. * Outside the company, **keep a close eye on your mobile devices**. * If possible, **avoid connecting to open wifi networks** with work devices. If you need to do so, use a VPN for security. * **Lock your computer** when you are away from your desk. * Use **passwords that are secure**. You can check the security of your passwords on dedicated password checking websites such as <https://password.kaspersky.com/>. * **Don't always use the same passwords**, as you will be more vulnerable in case they are leaked. * **Do not download attachments from unknown senders**, be wary of **suspicious messages** and **report any incidents** to your supervisors. | | |
| **Contents in bullet points** | | |
| * Cybersecurity emerged out of the need for companies to protect their computer systems from malicious attacks. * The most common cybersecurity incidents suffered by European MSMEs are related to phishing. * Cybersecurity is everyone's responsibility in a company, and it is necessary to have a cybersecurity plan that is properly followed by managers, directors and employees. * In remote work, cybersecurity is complemented by the use of ICT tools that enable the five objectives of cybersecurity in accessing information to be met. * The employer must ensure that a cybersecurity plan is in place, and that employees have the necessary skills to comply with it. * Workers should be committed to the secure management of information in the course of their work. | | |
| **5 glossary entries** | | |
| **Cybersecurity.** The application of tools, technologies, policies, controls and procedures in the protection or recovery of networks, systems, devices and applications from cyber attacks aimed at accessing, destroying or altering sensitive information, disrupting workflows, or extorting money from organisations or individuals.  **Phishing.** The technique of pretending to be another person or entity via email, leading the user to perform some action on a fraudulent page to obtain passwords or download an infected file. Similar are vishing (voice + phishing) or smishing (SMS + phishing).  **Malware.** Malicious software that can come in different forms (as executable code, scripts, etc.), and can perform actions such as encrypting or deleting sensitive data, altering the basic functions of the device, spying the user's activity, among others. Viruses, worms, adware, trojans, spyware and ransomware are also malware.  **Backup.** Copy of files and programs that is stored on other devices or other media, in order to recover information in case of failure, loss or theft.  **Sensitive information.** Information containing private or confidential data, such as personal or banking details. | | |
| **Bibliography and further references** | | |
| <https://www.redseguridad.com/especialidades-tic/como-definir-la-ciberseguridad-en-un-entorno-laboral-hibrido_20210928.html>  <https://www.enisa.europa.eu/publications/report-files/ETL-translations/es/etl2020-web-based-attacks-ebook-en-es.pdf>  <https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes>  <https://www.enisa.europa.eu/publications/enisa-report-cybersecurity-for-smes>  <https://www.incibe.es/sites/default/files/contenidos/guias/doc/ciberseguridad_en_el_teletrabajo.pdf>  <https://www.microfocus.com/en-us/what-is/cyber-security>  <https://www.osi.es/es/actualidad/blog/2021/06/28/conceptos-basicos-de-ciberseguridad-que-debes-conocer>  <https://es.linkedin.com/pulse/recomendaciones-de-ciberseguridad-en-el-puesto-trabajo-pizarro>  <https://www.redseguridad.com/actualidad/cibercrimen/que-es-el-malware-tipos-y-maneras-de-evitar-ataques-de-este-tipo_20210410.html>  <https://openwebinars.net/blog/origen-e-importancia-de-la-ciberseguridad/>  <https://uniserveit.com/blog/10-step-cybersecurity-plan-for-your-small-business>  <https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes>  <https://www.europol.europa.eu/wannacry-ransomware> | | |
| **Five multiple-choice self-assessment questions**  Upon completion of the validation mechanism, users will be able to generate customised Certificate of Attendance and Certificate of Completion. | | **Question 1. What is meant by "cybersecurity"?**  Option a: Tools to protect devices from malware attacks.  Option b: Procedures designed to protect sensitive information from malicious attacks.  Option c: The protection of company IT systems.  Option d: All answers are correct.  **Correct option: d**  **Question 2. What should you do to prevent phishing?**  Option a: Be wary of unsolicited emails to change a password.  Option b: Click on the links in the emails.  Option c: Download spam email attachments.  Option d: Taking phone calls from unknown numbers.  **Correct option: a**  **Question 3. What is the most common attack on European MSMEs?**  Option a: Denial of service.  Option b: Ransomware.  Option c: Phishing.  Option d: None is correct.  **Correct option: c**  **Question 4. Which of the following are cybersecurity objectives for remote access to information?**  Option a: Availability, confidentiality.  Option b: Traceability, publicity.  Option c: Confidentiality, corruption.  Option d: Integrity, measurability.  **Correct option: a**  **Question 5. What would you do with a USB drive you find on an office desk?**  Option a: Connect it to my computer to see what's in it so I can return it to its owner.  Option b: I would try to find its owner without connecting it to any computer.  Option c: Report it to the police.  Option d: Throw it away.  **Correct option: b** |
| **Related material** | | RESTART\_PR3\_COU\_03\_IWS\_Cybersecurity\_EN.pptx |
| **Reference link** | | - |
| **Video in YouTube format (if any)** | | <https://www.youtube.com/watch?v=PSrnvEEDpuY> |