**Training Fiche Template**

|  |  |  |
| --- | --- | --- |
| **Title** | Cybersecurity and digital tools for SMEs. Be prepared to prevent and solve Cyber-attacks | |
| **Keywords (meta tag)** | Cybersecurity, Safety, Cybercrime, Cyber-attack, | |
| **Provided by** | ITSFA | |
| **Language** | English | |
| **Area** | Digital and online communication |  |
| Team and people engagement from home |  |
| Work-life balance |  |
| Self-well being |  |
| “How to boost your team productivity from home?” |  |
| Remote project management |  |
| Agile Management by Objectives |  |
| “Smart” self-efficacy |  |
| Leadership and Motivation in the Smart Working era |  |
| Teleworking: a selection of digital tools to manage your business | **X** |
| **Objectives / goals / learning outcomes** | | |
| In this course you will acquire a basic knowledge of Cybersecurity, at a business level, and also at a user/employee level. You will learn the definitions of the main cyber risks than can endanger your security and your business security; and you will learn the main tools to prevent cybercrimes whit a basic guide of cybersecurity, that will help you to know what are the basic measures to follow to protect your SME from these threats, and then to be able to work remotely in a safer way | | |
| **Description** | | |
| Due to the Covid-19 pandemic, SMEs, because of their intrinsic characteristics, have become the target of cybercriminals. The new ways of working brought about by the pandemic, teleworking, telecommuting; in other words, what is known as Smart working, have made it necessary for SMEs to acquire knowledge that will help them survive by jumping on the digitalization bandwagon and not be left behind. One of the basic training needs driven by this situation is cybersecurity.  With this course, SMEs will be able to obtain a basic knowledge of cybersecurity, and thus have the tools to prevent cyber risks that endanger the survival of their businesses, in a world that is moving unchecked towards digitalization. | | |
| **Contents arranged in 3 levels** | | |
| 2. Cybersecurity and digital tools for SMEs. Be prepared to prevent and solve Cyber-attacks  2.1 Safety at business level  -What is Cyber Security?  Due to digitalization, Cybersecurity for SMEs is a crucial issue today. Cyber-attacks are increasingly targeting small and medium-sized enterprises that are not as protected as large corporations.  Cybersecurity is a set of practices to defend computer systems and software from cybercrime. Cybercrime is any criminal activity that takes place in the digital world, involving a computer, a networked device or a network, and intended to achieve a certain purpose or benefit, which can be of different kinds. Cybersecurity covers many areas: network security, app security, information security, user security, etc. Let’s see some concepts to consider cybersecurity from a business level, to end up at the end of the course with a basic guide of Cybersecurity.  -Ransomware  Ransomware is a type of malicious software that encrypts information on different devices. Using this method, cybercriminals extort money from their victims by demanding a ransom in exchange for regaining access to their data.  Ransomware, is a type of malware that prevents users from accessing their system or personal files and demands the payment of a ransom in order to regain access to them.  -Malware  Malware means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user’s computer. Often spread via an unsolicited email attachment or legitimate-looking download, malware may be used by cybercriminals to make money or in politically motivated cyber-attacks. There are many different types of malware, like Viruses, Trojans, Spyware, Ransomware, Adware, Botnets.  -Antivirus  An antivirus is a programme that detects malware, blocked them, and eliminate them to prevent infecting the device. There exist different kinds of antivirus, to choose the most suitable one for you or your business, you will have to take in account the specifications of the device to be protected and some criteria to be taken in account.  There is plenty of antivirus software available, so, when it comes to choosing them, consider these criteria:  • Compatible with your operating system  • Protection of your device, without slowing down its speed, capacity, or performance.  • Frequent updates. Otherwise, we may be exposed to new threats.  • Versatility. Our antivirus must be as versatile as the malware.  • Ability to act. In addition to recognising the threat, it must eradicate and clean it from our device.  -Antimalware  Which is the difference between antivirus and anti-malware?  They both refer to software designed to detect, protect and remove malicious software. Despite what the name might suggest, antivirus software protects against more than just viruses; it simply uses a slightly old-fashioned name to describe what it does. Anti-malware software is also designed to protect against viruses, and simply uses a more modern name that encompasses all types of malicious software, including viruses.  Knowing this, anti-malware can prevent the occurrence of a viral infection and remove infected files. However, anti-malware is not necessarily equipped to restore files that a virus has changed or replaced.  - Security Patches. Vulnerability  It is an important part of cybersecurity in business as it helps to avoid vulnerability gaps in the company's systems, by updating all their equipment and devices. This includes computer applications and operating systems, electronic equipment firmware and anti-malware software. Patches and updates are created by the actual developers of the software and serve to improve its performance by fixing security bugs and adding new features.  - Protecting Business Data: Backup Basics  Quite simply, a data backup is nothing more than a copy of the files on your computer or device. And, as evidenced by the many threats described above, maintaining a backup of your important business files and data is essential for a number of important reasons.  Any backup is better than no backup, however, not all backup devices and technologies are equal or offer the same levels of protection. For optimal protection, it is best to safeguard your data using the 3-2-1 rule, which is as follows:  • Keep at least three (3) copies of your data (so no single event will destroy all copies);  • Store the data in at least two (2) different formats (i.e. disk, tape, cloud, etc.);  • Keep one (1) copy offsite to protect against fire, flood, theft, and other physical disasters.  Protecting Wireless Networks  Using a wireless network gives you the convenience of being able to work and use your computer virtually anywhere, and to connect to other computers on the network or access the Internet. However, if your wireless network is not secure, there are significant risks. For example, a hacker could intercept any data you send or receive, access your shared files, hijack your Internet connection and exhaust your bandwidth or download limit.  • When you buy a Wi-Fi router, it has a default name and password. These are very easy to hack, so you should change them. In addition, the router has an administrator password that allows you to change and manage the router's settings. Just like the router name and password, you should also change this password.  • To protect the information, you send over the Wi-Fi network, you can encrypt your network by updating the router software. Look for WPA3 or WPA2 settings, which offer the strongest encryption.  Training employees  Employees can make your company vulnerable to attacks, or help prevent them. Numerous studies show that a large amount of data loss comes from internal employees who, in most cases through carelessness or misinformation, give cyber criminals access to their networks.  There are many scenarios that could result in attacks in which the access routes are employees. For example, an employee losing a work tablet, giving away their login credentials, or opening fraudulent emails, which deploy viruses on the network.  To protect against insider threats, it is crucially important to invest in quality cybersecurity training for employees that gives them the tools they need to act in the face of various situations and risks.  Policies. Cybersecurity Policy. What is a cyber security policy?  To prevent cybercrime, it is important not only to train your employees in cybercrime prevention, but also to create a company cybersecurity policy. This will help clearly outline the guidelines for transferring company data, accessing private systems, and using company-issued devices. When you prepare your policy, ensure it guides your employees on:  • The type of business information that can be shared and where  • Acceptable use of devices and online materials  • Handling and storage of sensitive material  A complete cybersecurity policy template will include basic parts as follows:  • Introduction  • Purpose  • Scope  • Confidential Data  Device Security:  • Company Use  • Personal Use  • Email Security  • Transferring Data  • Disciplinary Action  2.2 Cybersecurity at user / employee level  End-user training is important because it addresses the most unpredictable cybersecurity factor - people. If good security practices are not followed, anyone can accidentally introduce a virus into an otherwise secure system. Teaching users to pay attention to risk factors is critical to the security of any organization.  Protect data on your devices  Personal data and sensitive data. Are they the same?  What is personal data?  Personal data is any piece of information that someone can use to identify, with some degree of accuracy, a living person. For example, the e-mail address of an employee of a company is considered personal data, because it indicates that that person works for the company. A physical address or a telephone number is also personal data, because this information can be used to contact the person.  Anything that can affirm your physical presence somewhere is also considered personal data. For example, recordings from security cameras are personal data, as are fingerprints.  Some examples could be:  • A first and last name  • A home address  • An e-mail address  • An identity card number  • Location data  • An Internet Protocol (IP) address  • Your phone's advertising identifier  What is sensitive personal data?  Sensitive personal data is a specific set of “special categories” that holds a stronger law protection, and must be treated with extra security, upon specific approval of the subject which that data refers to. This includes information pertaining to:  • Racial or ethnic origin;  • Political opinions;  • Religious or philosophical beliefs;  • Trade union membership;  • Genetic data; and  • Biometric data (where processed to uniquely identify someone).  Sensitive personal data should be stored separately from other personal data, preferably in a locked drawer or filing cabinet. As with personal data in general, it should only be kept on laptops or handheld devices if the file has been encrypted and/or pseudonymized.  Physical security  Cybersecurity starts with strong physical security. This includes storing documents securely, locking them in a room or cabinet, limiting the physical access to sensitive data, deleting information correctly and shredding sensitive data documents when they are no longer needed. Allow access to personal and financial information just to the staff who really need it.  • Remind your employees to never leave sensitive data documents unattended in the workplace or in public places. Failures in physical security can expose sensitive company data to identity theft, with potentially serious consequences.  All can occur due to physical security breaches, such as the loss of a laptop, the theft of a mobile phone, or the misplacement of a flash drive. As such, they are less likely to result in a data breach if the information on those devices is protected.  Here are some useful examples:  Require complex passwords: Require long, complex and unique passwords. And make sure these passwords are stored securely. Consider using a password manager.  Use multi-factor authentication: Require multi-factor authentication to access areas of your network with sensitive information. This requires additional steps beyond logging in with a password, such as a temporary code on a smartphone.  Limit login attempts: Limit the number of incorrect login attempts allowed to unlock devices. This will help protect against intruders.  Encrypt: Encrypt portable devices, including laptops and thumb drives, that contain sensitive information. Encrypt any sensitive data you send outside the company, such as to an accountant or lawyer.  -Email security  In the case of the user/employee using personal devices to access the company's systems, or for personal use, certain security measures should be taken regarding the use of email, as it can also be a gateway for criminal actions. In the event that employees must use their personal devices to access company systems, employees should report this information to management for logging purposes.  To ensure the protection of company systems, all employees should:  • Ensure that all personal devices used to access company systems are password protected (minimum 8 characters).  • Install comprehensive anti-virus software.  • Regularly update anti-virus software.  • Lock all devices if left unattended.  • Ensure that all devices are protected at all times.  • Always use secure, private networks.  Protecting email systems is a high priority, as emails can lead to data theft, scams and carry malicious software such as worms and bugs. Therefore, users/employees are advised to:  • Verify the legitimacy of each email, including the email address and name of the sender.  • Avoid opening suspicious emails, attachments and clicking on links.  • Look for any significant grammatical errors.  • Avoid titles and links that encourage clicking.  • Contact the IT department regarding any suspicious emails.  Phishing  Also known as electronic fraud. Knowing a little more about the most common and dangerous frauds will help us to avoid falling into them.  Through these methods, 'phishing' and 'smishing', the attacker seeks to obtain private information such as passwords or credit cards. In this attack, the victim is asked for vulnerable data, such as passwords or access codes, by email, pretending to be the legitimate website or entity, so that the victim provides the data requested by the attacker.  Smishing  This threat is similar to phishing, the only difference is that it is sent via SMS to phones. The hacker sends a message to our phones, opening the message is not dangerous. The danger lies in clicking on the link, that is when the attack begins.  2. 3 Most common cyber risks to be aware of. The basic guide of Cybersecurity  After familiarizing ourselves with the concepts mentioned above, let's take a look at the most frequent risks faced by SMEs, according to studies based on the European Union Cybersecurity Agency (ENISA) survey, with phishing and web-based attacks topping the list.  1) Phishing Attacks  This type of attack has become extremely popular due to remote working. One careless click on a link is all it takes for a cybercriminal to gain access to sensitive business information.  2) Web-based Attacks  Cybercriminals will use almost any vulnerability - within an operating system (OS) or application - to carry out an attack. However, most cybercriminals develop web threats that deliberately target some of the most common operating systems and applications  3) General malware Attacks  Many SMEs underestimate the possibility of cyber-attacks due to their size. However, this is precisely what hackers are looking for, as they can quickly profit from a ransomware threat to less secure SMEs.  4) Malicious insiders  This type of threat refers to the existence of persons within an organisation (whether internal employees or external suppliers, among others) who through carelessness, ignorance and/or bad faith, perform an "action" that affects the security of processes, systems or facilities of an industrial operating environment or critical infrastructure.  5) Denial of service attacks  The aim of these attacks is to disrupt a company's website so that it is inaccessible, which is done for various reasons by the cybercriminal. A stopped website can lead to loss of revenue, data breaches, customer distrust, and paralysis of the company's activity.  The basic guide of Cybersecurity  1. Determine your vulnerabilities  The first thing to do is to identify your vulnerabilities, so that you know which data to protect. Ask yourself questions such as: ¿What is the most important data that my company stores? ¿Where do you store this data? Once you have the answers, you can start assessing the risks.  2. Protect your devices  Work devices are crucial to the performance of your business. Their internet connection makes them vulnerable to cyber-attacks. Here are some tips to protect them  A. Update your software  B. Protect yourself from Viruses  C. Set up a Firewall  D. Special precautions for laptops and other mobile devices  3. Protect your data  No matter what type of business you are in, data is an essential part of it. Data can be damaged in a thousand different ways, one of which is through cyber-attacks. Here are some useful tips on how to protect your data.  A. Implement a procedure for backing up critical data  B. Encrypt confidential company information that you store in the cloud  C. Protect your passwords  D. Set permissions  E. Protect your wireless networks  F. Surf the internet safely  G. Protect confidential information created by remote workers  H. Protect your customer data  4. Instill cybersecurity in the workplace  The security measures mentioned in this basic guide can help you to significantly reduce the risk of a cyber-attack. But this will be of no use if your company's employees do not have the necessary awareness and training to be able to contribute to the prevention of them. Include this type of training in your company, and don't forget to create a company cybersecurity policy that all team members can follow. | | |
| **Contents in bullet points** | | |
| 2. Cybersecurity and digital tools for SMEs. Be prepared to prevent and solve Cyber-attacks  2.1 Safety at business level  2.2 Cybersecurity at user / employee level  2.3 Most common cyber risks to be aware of. The basic guide of Cybersecurity | | |
| **5 glossary entries** | | |
| Cybersecurity: Is a set of practices to defend computer systems and software from cybercrime. Cybersecurity covers many areas: network security, app security, information security, user security, etc.  Cybercrime: Is any criminal activity that takes place in the digital world, involving a computer, a networked device or a network, and intended to achieve a certain purpose or benefit, which can be of different kinds. **5 glossary entries**  Ransomware: Is a type of malicious software that encrypts information on different devices. Using this method, cybercriminals extort money from their victims by demanding a ransom in exchange for regaining access to their data.  Malware: It means malicious software. One of the most common cyber threats, malware is software that a cybercriminal or hacker has created to disrupt or damage a legitimate user’s computer. There are a many different types of malware, as: Virus, Trojans, Spyware, Ransomware, Adware, Botnets.  Backup: Quite simply, a data backup is nothing more than a copy of the files on your computer or device. And, as evidenced by the many threats described above, maintaining a backup of your important business files and data is essential for a number of important reasons.**5 glossary entries** | | |  |
| **Bibliography and Further References** | | | SWIFTSME\_Course 2\_Cybersecurity and digital tools for SMEs. Be prepared to prevent and solve Cyber-attacks\_EN |
| <https://atlasvpn.com/blog/phishing-and-web-based-attacks-were-the-most-common-among-europes-smes>  <https://www.kaspersky.com/resource-center/preemptive-safety/protecting-wireless-networks>  <https://www.pandasecurity.com/es/mediacenter/seguridad/parches-brechas-datos/>  <https://searchsecurity.techtarget.com/definition/cybercrime>  <https://es.malwarebytes.com/antivirus/>  <https://ciberseguridad.com/normativa/espana/medidas/actualizaciones/>  <https://www.betterteam.com/cyber-security-policy>  <https://business.gov.au/online/cyber-security/create-a-cyber-security-policy>  <https://www.daemon4.com/empresa/noticias/las-principales-amenazas-de-ciberseguridad-para-pymes/>  <https://www.itgovernance.co.uk/blog/the-gdpr-do-you-know-the-difference-between-personal-data-and-sensitive-data>  <https://www.bbva.com/es/phishing-y-smishing-que-son-y-como-evitarlos/>  <https://www.acronis.com/en-us/articles/data-backup-for-business/>  <https://www.ciberseguridadlogitek.com/la-amenaza-del-malicious-insider-en-los-entornos-de-operacion-industrial-y-de-infraestructuras-criticas/>  <https://usa.kaspersky.com/resource-center/threats/web>  <https://expertinsights.com/insights/the-top-5-biggest-cyber-security-threats-that-small-businesses-face-and-how-to-stop-them/>  <https://es.vpnmentor.com/blog/la-guia-completa-de-ciberseguridad-para-pequenas-y-medianas-empresas/>  <https://www.ncsc.gov.uk/collection/small-business-guide>  <https://insights.ascentor.co.uk/blog/2019/11/12-practical-cyber-security-tips-for-smes>  <https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf>  <https://www.kaspersky.com/resource-center/preemptive-safety/small-business-cyber-security>  <https://ciberseguridadbidaidea.com/ciberseguridad/6-principales-amenazas-de-una-empresa-en-ciberseguridad/>  <https://www.widefense.com/recursos/ciberseguridad/pequenas-empresas/>  <https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security>  <https://latam.kaspersky.com/resource-center/preemptive-safety/antivirus-choices>  <https://www.incibe.es/protege-tu-empresa/herramientas/servicio-antiransomware>  <https://internetpasoapaso.com/antimalware/>  <https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/virtual-patching-patch-those-vulnerabilities-before-they-can-be-exploited>  <https://me-en.kaspersky.com/blog/how-to-set-up-wifi-router/4390/>  <https://blog.walkme.com/5-employee-training-fails/>  <https://almamate.in/importance-of-selecting-the-best-salesforce-institute-in-noida/>  <https://cmitsolutions.com/blog/6-ways-protect-data-devices-digital-identity/>  <http://www.rbntechnologies.com/products.html>  <https://memoori.com/physicalsecurity-2016-rounded_v1/>  <https://www.djcs.com.ve/djcsnews/1901-automationedge-password-reset>  <https://www.datacenterknowledge.com/security/managing-encryption-data-centers-hard-and-it-will-get-harder>  <https://nakedsecurity.sophos.com/es/2016/08/09/email-how-secure-is-yours-survey/>  <https://www.valoradata.com/blog/que-es-el-phishing/>  <https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/>  <https://www.keepnetlabs.com/7-ways-to-prevent-phishing-attacks-in-2021/>  <https://www.teceze.com/what-is-vmdr-vulnerability-management>  <https://cypheradda.blogspot.com/2019/05/5-cybersecurity-tips-for-workplace.html>  <https://molinaoposiciones.com/2021/03/22/por-fin-fecha-definitiva-de-auxilio/>  <https://unaaldia.hispasec.com/2021/04/malware-en-plantillas-empresariales-de-descarga-gratuita.html> | | |  |
| **5 multiple-choice self-assessment questions** | | |  |
| 1) What is personal data?  **a) Personal data is any piece of information that someone can use to identify, with some degree of accuracy, a living person. For example, the e-mail address of an employee of a company is considered personal data, because it indicates that that person works for the company.**  b) Personal data is a specific set of “special categories” that holds a stronger law protection, and must be treated with extra security, upon specific approval of the subject which that data refers to.  2) Select the correct answer related to the concept of Security Patches.  **a) It is an important part of cybersecurity in business as it helps to avoid vulnerability gaps in the company's systems, by updating all their equipment and devices. This includes computer applications and operating systems, electronic equipment firmware and anti-malware software.**  b) It is an important part of cybersecurity that includes storing documents securely, locking them in a room or cabinet, limiting the physical access to sensitive data, deleting information correctly and shredding sensitive data documents when they are no longer needed.  3) Regarding to Cybersecurity at user level, why is important an End-user training?  a) It is not that important, as the end-user is only the one affected by cybercrime and has no choice but to install a good antivirus.  b) **End-user training is important because it addresses the most unpredictable cyber security factor - people.**  4) Which is the difference between antivirus and anti-malware?  a) They both refer to software designed to detect, protect and remove malicious software.  b) Just an anti-malware can detect malicious software, an antivirus is specifically designed to just remove the threat from the computer    5) Select the correct option about Protecting Wireless Networks.  **a) If your wireless network is not secure, there are significant risks. For example, a hacker could intercept any data you send or receive, access your shared files, hijack your Internet connection and exhaust your bandwidth or download limit.**  **b) When you buy a Wi-Fi router, it has a default name and password. These are very easy to hack, so you should change them. In addition, the router has an administrator password that allows you to change and manage the router's settings, you should also change this password.** | | |  |
| **Related Material** |  | |
| **Related PPT** | SWIFTSME\_Course 2\_Cybersecurity and digital tools for SMEs. Be prepared to prevent and solve Cyber-attacks\_EN | |
| **Reference Link** |  | |
| **Video in YouTube format (if any)** |  | |