**JUST Training Fiche: Interacting safely in a digital setting**

|  |  |  |
| --- | --- | --- |
| **Title** | Interacting safely in a digital setting | |
| **Keywords** | Cybersecurity, The Cloud, Privacy, Netiquette | |
| **Provided by** | Internet Web Solutions | |
| **Language** | English | |
| **Objectives** | The objectives of this module are to **explain the importance** of maintaining good **cybersecurity practices**, to highlight the importance of **protecting personal information**, and to provide a general idea of the **handiest and effective cybersecurity tools**. | |
| **Learning outcomes** | * Getting familiar with cybersecurity: Protocols are as important as applications * Developing responsibility: Netiquette and common sense are especially important * Understanding how to maintain privacy: Being very mindful of the content shared online. * Understanding the utility tools, such as VPNs, Antimalware and cloud apps | |
| **Training Area** | **Business Etiquette** |  |
| **Digital Skills** | **X** |
| **Soft Skills** |  |
| **Smart Working** |  |
| **Content index** | **Interacting safely in a digital setting**  **Unit 1: Cybersecurity tips and tricks**  Section 1.1: Introduction  Section 1.2: Keep yourself updated  Section 1.3: Use backups!  Section 1.4: Passwords and Multi-factor authentications  **Unit 2: Safe practices**  Section 2.1: Safeguard your privacy  Section 2.2: Watch your netiquette  **Unit 3: Tools to enhance ICT security**  Section 3.1: VPNs  Section 3.2: Antimalware  Section 3.3: The Cloud | |
| **Training content** | **Interacting safely in a digital setting**  **Unit 1: Cybersecurity tips and tricks**  **Introduction**  We live in an increasingly interconnected world. This comprises the feeling of the need to share the best of our last trip to our Instagram circle or shifting the topic from leisure to work, every call or email exchange we participate in during our educational and/or work life.  Unknowingly, these information exchanges contain plenty of data about us, often sensible, which can be stolen and collected by people who want to take advantage of it illegally.  This is why having cybersecurity protocols or just practices (which does not only mean installing an antivirus and then stopping caring) is essential for our online life.  **Keep yourself updated**  Our devices usually bother us with inconvenient “new software update” notifications. Despite sometimes not changing anything at first glance, these updates are very useful, as they patch recently discovered bugs and security issues that might pose a risk to our devices and the information they contain.  However, these software updates might be short-lived since hackers are always on the lookout to find software vulnerabilities, which stresses the importance of keeping our devices updated.  **Use backups!**  Keeping a separate, additional copy of your files is a safe bet when, despite our efforts, the worst happens and the files get corrupted or our system suffers a cyberattack. To avoid it, our files can be safely stored in an external drive and/or online cloud applications.  Contrary to common belief, backup versions should be created during the elaboration process and not only once the file is finished. In this way, you can easily circle back to previous iterations of the file in case something goes wrong with the mid-draft.  **Passwords and multi-factor authentication**  Often overlooked, passwords are a vital part of cybersecurity. Despite the hassle of remembering and introducing them character-perfect, long passwords with as m4nY! types of characters as possible are a must. Needless to say, using your date of birth (and the like) is not an option.  Also, due to frequent security breaches, passwords can be easily compromised, so keep different passwords on every device or account and remember to change them regularly!  Multi-factor authentication is a system that makes it harder for cybercriminals by requiring additional credentials beyond the password to enter your account e.g., an SMS code, a call or using a specific app.  **Unit 2: Safe practices**  **Safeguard your privacy!**  We tend to associate cybersecurity with hackers using state-of-the-art tools to break into our accounts. The truth is that most of their success comes from googling and gathering “public information” from social media, blogs and forums.  In this way, if we like to use a combination of our pet’s name, mother’s surname, door number, etc., for our passwords, it is a matter of time before a hacker can gather it all from here and there, recombine it and break in.  Reconsider what “private information” means to you. Go back on your timeline(s), look for any pictures of your ID/credit card/personal documents (could be goodbye, appreciation or mock posts) and delete them. Also, pay attention to any profiles having too much unnecessary personal information.  Remember: if you don’t want any information to be seen by strangers, just don’t post it!  **Watch your netiquette**  “Netiquette” is a set of rules of courtesy designed to ease online coexistence, just as we have social conventions for the offline world, such as waving, greeting and saying “please”.  Also, as in real life, bear in mind that this code of conduct is not immutable and depends on the context. A good example of this is the set of rules usually sticky posted on Facebook groups or forums.  The original “netiquette” rules by Virginia Shea (1994) are still valid with some updates, such as in the following example:   * Avoid using online communities as Google substitutes – Basically, try to look for previous posts/threads that already answered the issue. * Restrict the use of extra punctuation marks, abbreviations, emojis, capital letters and alternative spellings – C0Z N0B0DY wantz T0 R3AD MESSAG3S L1KE th1s, rite???? 😃😃😃 * Do not spam your own products or services – Usually, there are separate, specific spaces for that. If you can’t see them, you’re not at the right place. * Do not send any personal or private information – Please refer to the previous section. * Give authors due credit – Not only from a legal point of view but also because, while people hate being plagiarised, they do love seeing their work shared.   **Unit 3: Tools to enhance ICT security**  **VPNs**  Not everything is going to be measures, rules and habits. Fortunately, there are plenty of tools designed to combat cyber threats, like VPNs, Antimalware and Cloud apps.  VPNs are filters that mask your online identity and encrypt your data. It does so by connecting to a private server that scrambles your data, blocking external access to them and making them unreadable if stolen.  Additionally, most VPNs have servers in several countries, which means we have plenty of options to disguise our IP as a foreign one and access geo-blocked contents unavailable in our country:   * NordVPN and Access are two reasonably paid options that let us browse safely. * Moreover, Surfshark and Tunnelbear also offer attractive and reliable free plans.   **Antimalware**  Despite being commonly called “Antivirus”, Antimalware software is designed to detect, quarantine and eliminate any cyber threats, not only viruses.  While viruses are designed to replicate themselves and make devices malfunction, malware is an umbrella term for any kind of malicious software that spreads spam and ads and steals information and passwords (and might even ask for a ransom!).  Nowadays, it is true that most antimalware software has an antivirus app and vice versa, with a big range of functionalities and modalities:   * As per paid options, ESET, Norton, and Avast stand out. * Moreover, the free versions of Malwarebytes and Bitdefender also offer a first-rate service.   **The Cloud**  “The Cloud” is an online hosting service that allows users to upload, modify, store and share their files.  Storing your files online in private servers safeguards said files against any local attack or corruption and prevents problems with physical hard drives, such as lack of space, losses or deterioration. Despite its name, “the Cloud” is not a unique entity, but every provider has their own, and that is why there are several options:   * A popular option despite veering to paid plans, Dropbox offers a 2 GB free plan. * With 5 GB and 15 GB, respectively, Microsoft’s OneDrive and Google Drive also offer full integration within their environments. * Finally, though mainly used for file sharing, MEGA allows free users to store up to 20 GB. | |
| **Glossary** | **Backup**: digital copy of a file stored separately and used in case the original is lost or damaged.  **Multi-factor authentication:** An access modality that requires presenting two or more pieces of evidence for extra security.  **VPNs:** filters that mask your online identity and encrypt your data. It does so by connecting to a private server that scrambles your data, blocking external access to them and making them unreadable if stolen.    **Antimalware:** software designed to detect, quarantine and eliminate any cyber threats, not only viruses.    **The Cloud:** Online hosting service that allows users to upload, modify, store and share their files away from local attacks or corruption. | |
| **Self-evaluation (multiple choice queries and answers)** | 1. Netiquette does not advocate for:   1. Looking for previous replies that might help you. 2. **Using plenty of abbreviations.** 3. Giving authors due credit.   2. Posting personal information is the safest if:   1. Posted privately. 2. **It is not posted.** 3. Uploaded to the cloud.   3. Hackers gather most of their information on average users by:   1. **Googling their names.** 2. Using sophisticated software. 3. Extorting them.   4. Are viruses and malware the same?   1. Yes, they are synonyms. 2. Not at all. 3. **Viruses are just a type of malware.**   5. Which one has the most space?   1. Google Drive 2. Dropbox 3. **Mega** | |
| **Bibliography** | * <https://www.ionos.es/digitalguide/online-marketing/redes-sociales/netiquette/#:~:text=Este%20t%C3%A9rmino%20hace%20referencia%20a,t%C3%A9rmino%20netiqueta%2C%20su%20traducci%C3%B3n%20directa> * <https://www.avast.com/es-es/c-malware-vs-virus#:~:text=%C2%BFCu%C3%A1l%20es%20la%20diferencia%20entre,que%20un%20tipo%20de%20malware> * <https://www.trellix.com/en-au/security-awareness/ransomware/malware-vs-viruses.html#:~:text=Malware%20is%20a%20catch%2Dall,its%20code%20into%20other%20programs> | |
| **Resources (videos, reference link)** |  | |