Manual: Cyber Security

November 2021

FREE PRESS UNLIMITED

Disclaimer

This cyber security manual is intended for use by Free Press Unlimited (FPU) and is designed to meet the specific needs of FPU's partners, whether organizations or individuals. This manual was designed by FPU cyber security experts from the project Ethical Journalism for Syrian Media (EJSM) and is based on knowledge learned from training, consultations, and experiences aimed at building the cyber security capacities of journalists.

It is important to note that the instructions in this manual are general and should serve as guidelines rather than a thorough and comprehensive reference. Cyber risks are evolving daily; therefore, this manual will not cover all possible cyber risks, and it is always recommended to seek advice from professionals.

Contents

Introduction and Rationale

A Journalists' primary mission is to provide reliable and timely information for people to make the best possible decisions is not cost-free. The world is becoming more and more dangerous for journalists across the globe. According to the UNESCO[1], there is an increase in the number and range of physical violence against journalists over the past few years, committed mainly by governments security forces. Furthermore, Reporters without Borders have documented 49 journalists were killed in 2020, in comparison to 40 in 2019.[2]

Syria is beyond any doubt one of the most hazardous places for journalists and activists due to the situation's complexity. According to Committee to Protect Journalists (CPJ) Global Impunity Index – an index that spotlights countries where journalists are murdered and their killers go free - Syria is ranked as the second deadliest country for journalists.[3]

Day after day, digital technology is being integrated into journalists' daily work. On the one hand, this integration has allowed for timely access, faster networking, a broader audience, and many other advantages. On the other hand, the use of these digital devices has exposed journalists to new and endless threats. These cyber threats are evolving and becoming more dangerous, sophisticated, and vast, affecting not only individuals and organizations but impacting the communities and countries.

Luckily, these cyber threats can be largely mitigated by adopting appropriate policies, practices, and tools. Motivated by its mission, FPU has provided educational and technical support to increase the cyber security capacity of journalists in Syria through The Ethical Journalism for the Syrian Media program, which adopted a holistic approach by integrating physical, digital security, psycho-social health and ensuring security is an integral part of every training and coaching session.

This manual systematically presents the fundamental guidelines implemented in the training to promote cyber security awareness, knowledge, and behavior. Of course, these guidelines were intended to cover threats within the Syrian context; however, since journalists worldwide face global cyber threats, this manual can be helpful in broader contexts or countries.

What is Cyber security

In their research, Schatz et al. have defined cyber security as the is the protection of computer systems and networks from information disclosure, theft of or damage to their hardware, software, or electronic data, as well as from the disruption or misdirection of the services they provide.[4] Therefore, cyber security is basically how individuals and organizations reduce the risk of cyber-attacks.

A Culture of Awareness

It is next to impossible to have an organization where all staff has all the experience and knowledge needed to ideally master cyber security systems; moreover, the cyber risks are constantly evolving, which makes it also impossible to keep all the staff up-to-date with these risks. However, a feasible solution to overcome this challenge is to embrace a culture of cyber security awareness inside and outside the workplace.

Cyber security awareness refers to beliefs, attitudes, norms, knowledge, and the values the staff have about cyber-risks and how all of these are reflected in everyday behavior when using digital devices. Cyber security awareness is an essential prerequisite for a successful cyber security policy; if not integrated by staff in their everyday actions, no amount of education and training will save the organization from cyber risks. Such a culture of awareness will naturally improve the capacity of all the staff and enhance their confidence towards cyber threats.[5]

The importance of this approach stems from the fact that the vast majority of cyber threats are accounted for human

[1] https://unesdoc.unesco.org/ark:/48223/pf0000374206

[2] https://rsf.org/en/barometer?year=2019

[3] https://cpj.org/reports/2020/10/global-impunity-index-journalist-murders/

[4] Schatz, D., Bashroush, R., & Wall, J. (2017). *Towards a More Representative Definition of Cyber Security.* Journal of Digital Forensics, Security and Law, 12(2). https://doi.org/10.15394/jdfsl.2017.1476

[5] *Meeting the cybersecurity challenge* | McKinsey. (n.d.). Retrieved July 12, 2021, from https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/meeting-the-cybersecurity-challenge#

error, such as social engineering.[6] Staff carelessness or negligence transforms the applicable cyber security rules into abstract guidelines, therefore it is crucial to maintain a mindset of being alert for all the staff.

The cyber threats are augmented for organizations that aim at providing independent and reliable information, especially organizations of journalists working in conflict zones and authoritarian regimes. Thus, the importance of cyber-awareness culture is imperative, if not fatal.

Preparedness

Following raising awareness, comes preparedness. In this context, preparedness must be considered for two levels, organizational and individual. It is worth mentioning that while it is true that the staff and the organization have their own duties to create and maintain a cyber security culture, both staff and organization must coordinate and cooperate for successful cyber security, i.e., success is a mutual responsibility.

Organization Preparedness

As Figure 1 demonstrates, it is the duty of the organization to provide both technical and educational support for the staff to be able to protect themselves and the organization from cyber threats.

First and foremost, the organization must design, develop, and implement a holistic cyber security policy. This policy includes protection protocols, data classification, backups and data storage procedures, emergency plans, etc. When it comes to technical support, the organization must provide software, devices, cloud storage, consultations, and all other types of technical support to all the staff.

Individual Preparedness

Staff, on the other hand, also have their own duties towards successful cyber security. In fact, it is an everyday responsibility to be carried out by the staff to ensure the rules, procedures, and recommendations of the cyber security policy set by the organization are met. Furthermore, it is the responsibility of the staff to inform the organization of their cyber security needs and to attend training provided by the organization. Finally, it is also the ethical and professional duty of the staff to report any incident that might lead to a data breach, even if this incident was caused by them or might embarrass them.

Cyber security Framework

Assessment

Prior to implementing a cyber security framework, it is a must to conduct an initial assessment and evaluation for staff existing cyber security knowledge – through questionnaire for example (see Appendix A)—, digital devices, as well as data types, how it is stored, who has access to what, and how data are protected, among other things. The main purpose of this stage is to locate the

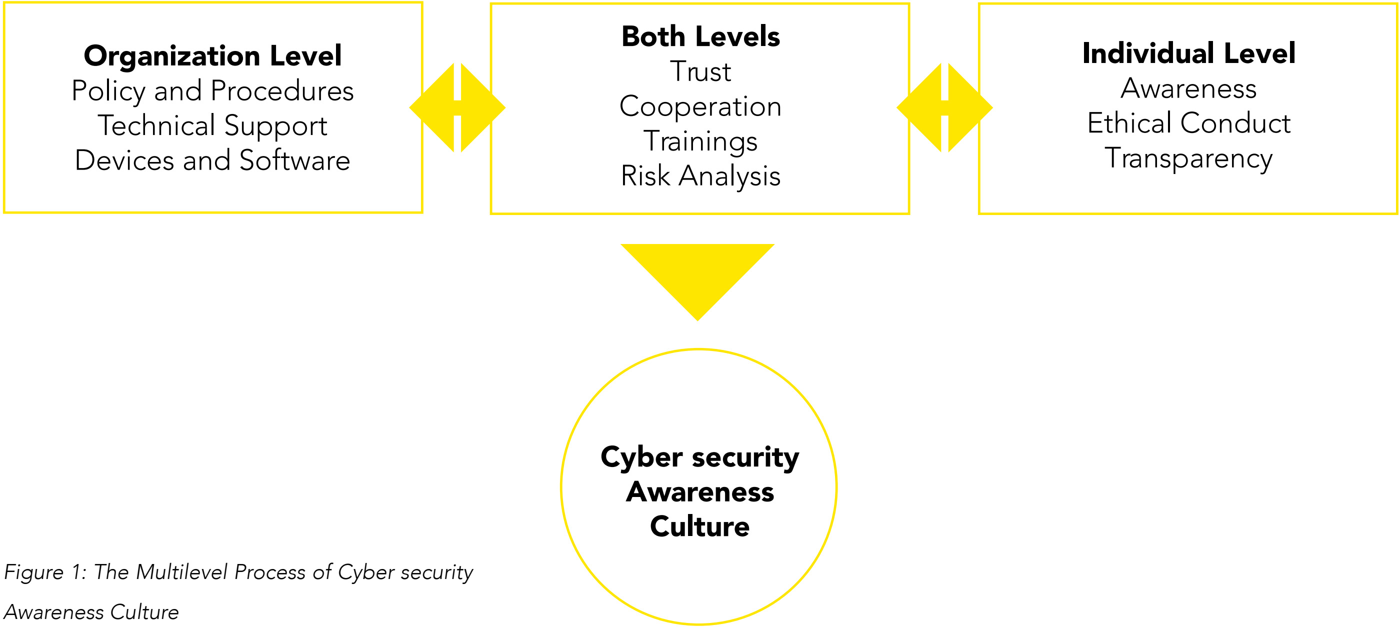


Figure 1: The Multilevel Process of Cyber security Awareness Culture

[6] Yumpu.com. (n.d.). *The-human-factor-in-data-protection-trend-micro*. Yumpu.Com. Retrieved July 12, 2021, from https://www.yumpu.com/en/document/view/27212144/the-human-factor-in-data-protection-trend-micro

strengths and weaknesses to fill the gaps when designing training and policies. It is vital to bear in mind the different needs and threats each position or department has. This assessment will also assist financial decisions related to budget, funding, and gaps. The assessment process is a fundamental key to creating an efficient and sustainable cyber framework as it is the first step that determines the rest of the framework.

Understanding Risks

Carrying out research into the potential cyber risks any organization will greatly contribute to developing the cyber security program. The research should focus on the frequency of the risks, how serious they are, what are the sources of these risks, what range they affect, and how to mitigate them. This research will allow for a profound risk analysis which in its turn will enable the organization to incorporate the necessary actions to address these risks within its cyber security program. Risk analysis is not merely an organization's duty; it needs to be embraced by staff as an everyday responsibility.

Privacy and Confidentiality

In the context of independent journalism, a holistic, unified, unambiguous, and effective policy of privacy and confidentiality is a crucial part of a successful cyber security framework. Trust is a key factor for sources, stakeholders, partners, and staff, any breach of this trust will impact lives and reputations. The privacy and confidentiality policy is the pledge that the organization makes to protect all people involved. This policy must state what information will be used, how they will be protected, what the procedures are if the policy is breached. Therefore, it is a good practice to share the policy with stakeholders and mandatory for the staff to adhere to it. This policy should also create an inventory of the data (what data the organization has) and then categorize the information per its confidentiality level shown in Figure 2.

The main step to take to ensure an adequate policy is to control access to data. It is very smart to let the person access *only* the data they need; this implies the more sensitive the data, the fewer people have access to it.

Emergency Plans

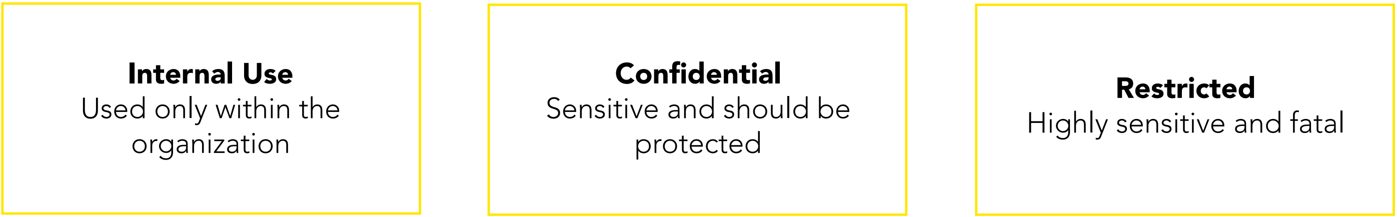
No matter how prepared an organization is, there is no such thing as a 100% cyber-safe organization. It is crucial for an organization that provides independent journalism to prepare response plans for all potential cyber-attack or breaching scenarios, e.g., data loss or data theft. Having response plans will significantly reduce the damage, save time, and make use of the incident as a lesson learned. An efficient response plan will include a clear description of each step to be taken and who has the responsibility to take it, and who should be involved in the plan. Worth mentioning here that most cyber-attacks that target independent organizations that provide reliable information are silent attacks where the attacker makes sure that the breach is not discovered as long as possible; therefore, it is brilliant to run periodical checkups for cyber safety.

Capacity Building

More importantly than digital infrastructure and policies are to build the cyber capacity of the staff in order to reduce risks, indeed most of the risks can be eliminated by providing cyber security training for the staff. It is important to design a training suitable for the amount of the knowledge of the participants so that it is not too advanced or too simple.

As part of the training of the EJSM project, participants from partner organizations had to respond to an assessment questionnaire that allows for a better-fitted training. It is a good practice to hold periodical training to keep the staff up-to-date with the latest cyber threats.

Figure 2: Data Classification



Internal Use
Used only within the organization

Confidential
Sensitive and should be protected

Restricted
Highly sensitive and fatal

7. Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems.* John Wiley & Sons.

Cyber Threats

Below listed are the most common cyber threats that organizations, as well as an individual, might face. It is important to know that these threats are evolving; therefore, the information below is not permanent but can serve as a reference.

Social Engineering

"Social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme."[7]

Fraud/Identity Theft

Internet fraud is a type of fraud or deception which makes use of the internet and could involve hiding information or providing incorrect information for the purpose of tricking victims out of money, property, and inheritance. Internet fraud is not considered a single, distinctive crime but covers a range of illegal and illicit actions that are committed in cyberspace.

Online identity theft is the theft of personal information in order to commit fraud. This can happen through your email account, but it can also be a result of online purchases or other situations where you give out sensitive information, such as your credit card information or your social insurance number. A related concern is identity spoofing, in which the victim is impersonated on social networking sites such as Facebook or Twitter. Identity spoofing may also involve spoofing someone's IP address (the unique number associated with your computer as you surf the internet). The purpose of identity spoofing on social networking sites can range from a simple prank to more serious attacks aimed at shaming or hurting someone's social networks. Internet Protocol spoofing is used by hackers to cover their tracks or to gain access to places normally closed to them.

Phishing

Phishing is used most often by cyber criminals because it's easy to execute and can produce the results they're looking for with very little effort. Commonly, they come as fake emails, text messages (Smishing), and websites created to look like they're from authentic companies. They are sent by criminals to steal personal and financial information from you. This is also known as "spoofing." They can trick you into giving them information by asking you to update, validate or confirm your account. It is often presented in a manner that seems official and intimidating, to encourage you to take action. Phishing can provide cyber criminals with your username and passwords so that they can access your accounts (your online bank account, shopping accounts, etc.) and steal your credit card numbers.

Phishing has several indicators like generic greetings such as "Dear Valued Customer"; immediate action such as "Failure to respond in five to ten days will terminate your account; Emails that requests for personal information such as social security numbers or credit card numbers; and misspellings and/or poor grammar.

Malware

Malware is one of the more common ways to infiltrate or damage your computer. Malicious software that infects your computer, such as computer viruses, worms, Trojan horses, spyware, and Adware. Indicators of malware include: It takes longer than usual for your computer to start up, it restarts on its own or doesn't start up at all; it takes a long time to launch a program; files and data have disappeared; your system and programs crash constantly; the homepage you set on your web browser is different (note that this could be caused by Adware that has been installed on your computer); web pages are slow to load; your computer screen looks distorted; programs are running without your control.

Malware can: Intimidate you with scareware, which is usually a pop-up message that tells you your computer has a security problem or other false information; reformat the hard drive of your computer, causing you to lose all your information; alter or delete files; steal sensitive information; send emails on your behalf; take control of your computer and all the software running on it.

Spyware and Adware

Spyware and Adware are often used by third parties to infiltrate your computer. It is software that collects personal information about you without you knowing. They often come in the form of a 'free' download and are installed automatically with or without your consent. These are difficult to remove and can infect your computer with viruses. Spyware can: Collect information about you without you knowing about it and give it to third parties; send your usernames, passwords, surfing habits, list of applications you've downloaded, settings, and even the version of your operating system to third parties; change the way your computer runs without your knowledge; take you to unwanted sites or inundate you with uncontrollable pop-up ads.

Indicators of spyware include: you are subjected to endless pop-up windows; you are redirected to websites other than the one you typed into your browser; new, unexpected toolbars appear in your web browser; new, unexpected icons appear in the task tray at the bottom of your screen; your browser's homepage suddenly changed; the search engine your browser opens when you click "search" has been changed; certain keys fail to work in your browser (e.g., the tab key doesn't work when you are moving to the next field within a form); random Windows error messages begin to appear; your computer suddenly seems very slow when opening programs or processing tasks.

Spam

Spam refers to unsolicited bulk messages being sent through email, instant messaging, or other digital communication tools. It is generally used by advertisers because there are no operating costs beyond that of managing their mailing lists. It could also take place in chat rooms, in blogs, and more recently within voice over internet conversation (such as Skype). Beyond being a simple nuisance, spam can also be used to collect sensitive information from users and has also been used to spread viruses and other malware. Spam is one of the more common methods of both sending information out and collecting it from unsuspecting people. Spam is the mass distribution of unsolicited messages, advertising, or pornography to addresses that can be easily found on the internet through things like social networking sites, company websites, and personal blogs. Spam can: Annoy you with unwanted junk mail; create a burden for communications service providers and businesses to filter electronic messages; phish for your information by tricking you into following links or entering details with too-good-to-be-true offers and promotions; provide a vehicle for malware, scams, fraud, and threats to your privacy.

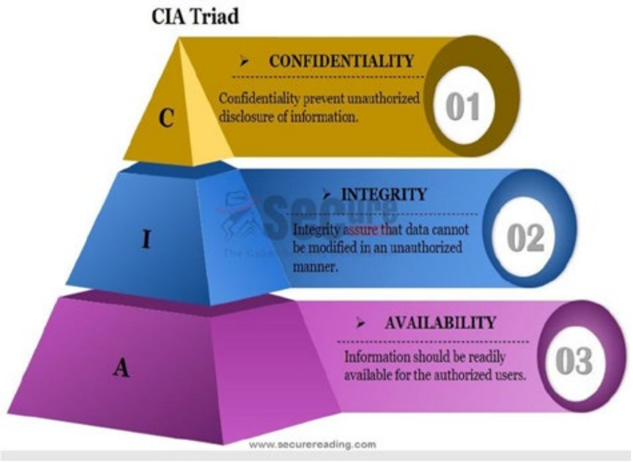

CIA Triad
C
CONFIDENTIALITY
Confidentiality prevent unauthorized disclosure of information.
01
I
INTEGRITY
Integrity assure that data cannot be modified in an unauthorized manner.
02
A
AVAILABILITY
Information should be readily available for the authorized users.
03
www.securereading.com

Figure 3: CIA Triad © securereading.com

Data Breach

A data breach is a security incident in which information is accessed without authorization. Data breaches can hurt businesses and consumers in a variety of ways. They are a costly expense that can damage lives and reputations and take time to repair.

Common causes include: Exploiting system vulnerabilities; out-of-date software can create a hole that allows an attacker to sneak malware onto a computer and steal data; weak passwords; weak and insecure user passwords are easier for hackers to guess, especially if a password contains whole words or phrases. That's why experts advise against simple passwords and in favor of unique, complex passwords; drive-by downloads. You could unintentionally download a virus or malware by simply visiting a compromised web page; a drive-by download will typically take advantage of a browser, application, or operating system that is out of date or has a security flaw. Attackers use spam and phishing email tactics to try to trick the user into revealing user credentials, downloading malware attachments, or directing users to vulnerable websites; email is a common way for malware to end up on your computer.

A common approach to guide data security is known as the Confidentiality, Integrity, Availability model, also known as CIA triad, as shown in figure 3 below.

Physical Threats

The simplest threat to your digital security is that someone will gain physical access to your computer or mobile phone. All your sensitive information would be readily accessible to anyone who seizes or steals your devices. Therefore, the first thing to think about is *where* and *how* to keep your private data, *who* has access to it, and what you will do if someone tries to take or access it.

Wi-Fi and Router

An attacker can eavesdrop on Wi-Fi communications to derive information (e.g., username, password). This type

[8] https://howsecureismypassword.net/

of attack is not unique to smartphones, but they are very vulnerable to these attacks because very often the Wi-Fi is the only means of communication; they have to access the internet. Unauthorized people can intercept anything you are doing online if the connection is not encrypted, including capture passwords and/or usernames; read emails and intercept the data you send across the not encrypted Wi-Fi connection; someone may set up a spoof hotspot (fake Wi-Fi), to fool you into thinking that it is a legitimate one. So, they can see everything you are doing on the internet; With an encrypted connection, you will be required to enter a 'key'; if you are not asked for a key, and you can just log in, the operator will know you are online in the cafe, hotel or pub and there will probably not be any encryption.

Security researchers have long warned that home and office routers can be a malicious hacker's entryway into a computer system. But router security has long been overlooked or ignored by consumers and manufacturers alike. Making matters worse, the router is often the last piece of hardware that is updated or replaced, as it's often hidden away and forgotten in cabinets and closets. When routers are compromised or aren't secure, malicious hackers can infect them with malware, re-engineer routers to direct users to spam sites or take them over for use in distributed denial of service, or DDoS attacks to overwhelm targets' networks with Web traffic.

USB

Some malware is programmed to copy itself onto every USB drive that is plugged into a computer and then install itself on every computer to which the USB is connected.

Action Plan

To overcome the previous threats, training should include theoretical and, more importantly practical instructions about the following points:

Passwords

Developing a strict password policy will add a strong layer of protection to the organization. The password policy should ensure that staff chooses strong passwords, not to repeat passwords for different purposes, not to write them on paper or on a text file, and to replace them periodically. Strong passwords must be a sequence of random words (at least 12) with numbers and symbols. To test the strength of the password, you can check samples of your choice websites like (How Secure is my Password)[8], of course, it is not recommended to check actual passwords you use now but to try samples to understand how secure passwords are composed.

It is highly recommended for journalists to use a password manager program that saves and encrypts passwords; a recommended program is LastPass[9] and Encrypt 1Password.[10]

A practice that must be included in the policy and highly emphasized is the use of Second-factor Authentication (SFA) whenever applicable; this method requires the use of another layer of security after passwords, usually through mobile phones messages, the SFA greatly decreases cyber risks. Journalists can use this method for Email, Facebook, Twitter, and many other social media websites. However, this method might not be practical for a journalist who works in areas with weak or disrupted mobile networks. Appendix B demonstrates how this method is activated.

Secure messaging

If journalists are working under repressive regimes, there is a high possibility that these regimes have authority over the internet and mobile communication providers and can access users' private data, and these regimes have the capacity to operate advanced devices that can intercept communication on different levels, including instant messaging applications. Therefore it is highly recommended to use open-source, independent, end-to-end encrypted instant messaging applications. For the time being, Signal[11] seems to be the safest free application for instant messaging, and Jitsi Meet[12] for an online meeting. It is a good idea to check Totem[13] a platform for free courses regarding secure messaging apps.

[9] https://www.lastpass.com/

[10] https://spideroak.support/

[11] https://signal.org/en/

[12] https://meet.jit.si/

[13] https://learn.totem-project.org/

Email

Using a well-known secure email service provider is a crucial first step; currently, Gmail is acclaimed when it comes to security. However, no matter how secure the email provider is, it is always a matter of human behavior that determines email security. Therefore it is highly recommended to include email use policy within the cyber security framework. In general, there are a number of widely applicable practices for more secure email, such as avoiding opening unexpected text messages from unknown senders, using strict email filtering to prevent spam, and checking links and attachments before opening them, and of course, activating second-factor authentication.

Data Safety

Apart from the aforementioned data security tips, it is imperative for journalists working in a hazardous environment to encrypt sensitive data that –if compromised— will affect people's lives; such information might include sources' names, addresses, emails, or any other identifiers. Encryption can guarantee that even in the unfortunate event of a data breach, sensitive information remains unknown. It can be done simply by using numbers or codes for these identifiers or via advanced software. It is very good practice to use built-in password protection for common office applications like Word, Excel, Access, Winrar, and Winzip.

Finally, it is important to note that backing up data and storing it in cloud services such as OneDrive and G-suite is highly recommended for organizations and individuals. It is very important to remind journalists that deleting data is also a part of a good data safety policy. Whether paper or digital, unneeded data must be properly disposed of. There are several applications such as Eraser[14] for mobiles and computers to properly erase data under hazardous incidents, and that can be very useful for independent journalists.

Network Safety

It is recommended for organizations to use wired internet instead of Wi-Fi. But since Wi-Fi is way more flexible and many organizations will still prefer it over a wired connection, it is thus a good practice to protect the router physically to prevent unauthorized people from accessing it and digitally by using strong Wi-Fi password and changing it periodically, as well as increasing protection by activating Wi-Fi Protected Access 2 (WPA2) encryption and a firewall. For more information, visit the website of your router provider, e.g., Cisco, D-Link, etc.

Browsing Safety

The organization must employ a browsing policy so that internal devices and networks are less exposed to threats. The policy must include browsing rules such as browsing the internet for work-related purposes, i.e., not to use work devices and the internet for personal browsing, e.g., Facebook or Instagram. The policy should also set safe browsing features such as incognito mode as well as installing applications for Virtual Network Proxy VPN, ads blockers.

Physical Safety

The physical safety of digital devices must be included in the cyber security policy because these threats are very common and usually overlooked. Accessing digital devices must be properly defined, as well as the use of storage devices like USB, CD's, etc. In general, it is a good practice to limit the use of portable storage devices, not to leave the computer or mobile unguarded, especially when they are running, even inside the office. For an extra layer of USB security, it is recommended to install protection applications such as USB Guard.[15]

General Cyber Security Tips

- Regularly update all applications and operating systems.
- Install only appropriate safe applications.
- Join cyber security training regularly to keep yourself familiar with the latest threats and protections methods; these training can be provided for free on platforms as the Totem project.[16]
- Do not hesitate to report any breach ASAP.
- Run regular cyber security checkups.
- Ask for professional assistance whenever needed (many organizations provide free cyber security assistance for independent journalists).
- Remember, there is no 100% cyber security.
- Remember, cyber security is a shared responsibility.

[14] https://eraser.heidi.ie/

[15] https://usbguard.github.io/

[16] https://learn.totem-project.org/