TOOLS AND METHODS TO PROTECT INFORMATION AND PERSONAL DATA ONLINE

INTRODUCTION

The inevitable fact of today's landscape is that every time a new device comes online or interacts with another device, the potential attack surface increases. The exponential growth of online solutions for everyday life has resulted in the growth of vulnerabilities, and the most common victim is the everyday user, who's personal data and privacy are at stake every time they connect to the internet, use cloud storage, open their e-mail and interact with the online-enabled software product.

Regardless of the ingenuity and the growing sophistication of the cyberattacks we come across every day, still, the most unprotected and vulnerable user is the user who is not taking the basic safety measures when online. Ignorance, unawareness or pure stubbornness, and lack of time are the most exploited vulnerabilities within the online world.

Inattentive users can easily be tricked into unwillingly performing an action or disclosing confidential information. This can be used for data theft or cyber espionage the consequences of which more often than not lead to financial loss, anxiety, further damage, or humiliation. There are different ways to exploit a user with risky online behavior, however, among the most common methods are online-enabled, be it phishing, where e-mails that appear to be sent from trusted sources manipulate unsuspecting users into revealing sensitive information or clicking on links or downloading content that will infect their devices with various types of malware, or be it sheer the exploitation of laxly secured profiles online or piece-of-cake passwords.

Cybersecurity for the everyday user mostly comes to preventing, detecting, and recovering from cyber incidents. The average web user will not have the skill set to respond to cyber threats, fight cybercriminals, and safeguard entire network infrastructures. This is why the Be@CyberPro Project Consortium developed this lesson to provide you with brief outlines of cyber incident prevention in the online space.

The objective of this lesson is to provide an overview of the most basic principles related to protecting your data and privacy online. In this lesson, we will briefly discuss password protection, digital identity, and identity management. We will go over some of the basics of e-mail communication and some of the most important aspects of website certificates, what to look for when you are opening websites, and some hints on how to recognize sketchy websites.

Remember that this lesson only provides the basic "survival" tips and will not substitute for your vigilance, attention and caution.

Photo 1 by TheDigitalWay from Pixabay (www.pixabay.com)

Co-funded by the Erasmus+ Programme of the European Union

This project has been funded with support from the European Commission.
This publication reflects the views of its authors only, and the Commission cannot be held responsible for any use which may be made of the information contained therein.

PASSWORDS

As a society, we are really bad with passwords. You can read some of the more famous showcases of that statement here [1] if you are curious. However, most of us still continue to use weak passwords, create profiles in insecure websites, use the same password for more than one profile, and rarely changing our passwords, although we know better. Without further ado, we will offer you some useful tips related to your password habits that can potentially spare you headaches.

1. Basic principles

We know that creating simple passwords is plain suicide. Password basics have changed with time and what was considered a sophisticated password a few years back might not be categorized as secure today.

A few years ago, long passwords were considered more secure than short passwords. However, what password would you consider more secure: 1) 7D*K2#c or 2) abcdefghijklmnopqqq. **It is not only about the length of a password but you have to consider the quality of it as well**. You have to know that password cracker algorithms look for patterns, such as the one in the second example from above and it is much easier to crack the second password, as it is the first. Creating high-entropy passwords is not easy, however, most password managers will offer to generate a secure password for you to meet the criteria of the service you want to be using. However, be careful when using an app to select a strong password for you and use only legitimate software for that, and not a random online tool that pops up after a “generate a secure password” Google search.

Let us give a third example of a password: 3) mycatisgreenandilovepizza. The thing is that there password-crackers are frighteningly good at guessing full words and common phrases and depending on the quality of the cracker and the speed of the processor, this password could be cracked in less than 30 minutes.

Furthermore, as we will discuss in the next chapter of this lesson, which deals with the topic of digital identity, you have to assume that things such as your favourite music, the city you live in, and much more, are known facts. Social engineering is a very curious topic in cybersecurity which gains increasing recognition and is also an increasingly widespread way to crack passwords. This type of social engineering is called a heuristic-based attack – your password could be something related to your personal interests and your personal interests are most likely online.

Another type of heuristic social engineering attack Is the human behavior heuristic attack. Those became popular when platforms began to oblige users to add a capital letter, a number, and a symbol to the passwords they are choosing. A “hacker” or the algorithm of their cracking software is going to assume first that you will be putting the required symbols, capital letters, and numbers at the beginning of the end of the password to meet the requirements of the platform. This makes “P@ssword1” not much more of a stronger password than “passwordpassword” to a malicious party. Cybersecurity and cybercrime both have a lot to do with knowing human psychology and recognizing vulnerable behavioral patterns, so don’t fall into this trap.

2. Change your passwords frequently

It is recommended that you change your password every several months. Of course, it is more important to keep your password safe and secretive and not using it for multiple websites, but changing your passwords is not a bad habit by itself. Some services, such as AWS, will remind you if you have not changed your password for a while and will prompt you to change it. However, this sort of engagement will require you to absolutely have a password manager and some people consider it a risk, as this sort of “pressure” to change the password frequently could potentially lead users into risky behavior, such as using one password for multiple services or wring passwords down to their phones or even worse, on paper. We recommend that you update your passwords from time to time only if you have a secure way of storing them.

3. Multi-factor authentication

Multi-factor authentication requires a user to use two or more separate methods to verify their identity and if one of the methods fails, the user will not be let to use the service. It is most usually a password, followed by something else, such as a text with a code, or a call via an automated phone call, biometrics, security tokens, e-mail verifications and others.

This is a good way to protect your more important profiles, such as your e-banking profile or your e-mail, however still, regardless that many platforms begin to integrate multi-factor authentication, it is not enabled by default. We recommend that you start using it, especially for crucial profiles, as mentioned above.

4. Do not reuse

There are little things worse than an easy-to-guess-password, and one of them is reusing a password. Reusing your passwords is a very warm welcome to any malicious party that wants to gain access to more than one of your profiles. Let us explain why. Most people use one or two e-mails to register for most services they use for personal purposes. Imagine you are registered to website “F” with the same e-mail and password you are using for website “G”. A hacker gains access to website “F” that stores their passwords protecting them with SHA1 encryption, which makes it only a little bit harder for the hacker to read it as if it were plain text. The hacker sees your e-mail and

has decrypted your password and becomes curious about whether you have created a profile with the same e-mail on the website “G”. Guess which password they will be trying first? It is an added “bonus” for the hacker if you are using this same password to protect your e-mail – then you are in a very, very unpleasant situation.

If you are using different passwords for all your different profiles, if website “F” exposes your password in any way, the damage you will suffer will be isolated to this particular website and does not extend to other services that you use.

5. Password managers

Password managers are a great tool to use, as they take away the burden of remembering all your passwords and profiles. A password manager is a service, that stores your passwords, usernames, and other relevant information in them. There are a lot of good, free services that you can use. The way they work is that they protect all your passwords with a master password, usually, and when you enter the master password, you have access to your password vault.

However, as password managers store all your passwords and profiles, so they become a very “juicy” target for attacks. This is why we recommend that if you choose to use a password manager, to choose a legitimate one, that has potentially been recommended to you by someone you trust.

When using a password manager, however, be twice as careful when opening links and learn how to check certifies. A fake website with a fake certificate that is trying to get a hold of your passwords will look exactly the same as the legitimate one. You need to know how to identify a phishing site. More information about website certificates is available in this lesson, in the chapter about “Safe Websites and Networks”.

---

[1] https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html

DIGITAL IDENTITIES

The term **Digital Identity** (or DI) is commonly defined as the digital representation of the information known about a specific person, company, or entity. Now, let's translate that. Your Digital Identity is made up of all the information or sets of claims, that you have made online for yourself or are made by somebody else in reference to you. Such claims might be that you study at a certain place – your classmates might have managed your name as a student in their school on a social media website, or you may have mentioned your affiliation to the school yourself through your Facebook page, for instance.

A claim is an assertion of truth about something. A photo, a video, or a voice recording, in cybersecurity, are also recognized as claims – claim what you look like or claim about your surroundings. A claim might also be a simple written statement that you post on Facebook, such as "I'm happy today". In cybersecurity terms, a claim can stand for something more technically complex. Cybersecurity recognizes a claim as an identity record that unambiguously asserts one or more attributes to an identity. Such an identity record might be your username. A claim which asserts more than one attribute in a single identity is referred to as a **credential** – such as username and password, or in non-technical terms, you might consider your school diploma as a credential as it is a complex claim record that includes multiple claimed attributes, such as your name, your date of birth, your major, etc.

Why is this important – all claims, made by yourself or by somebody else about you, are interrelated and comprise a digital identity, which relates back to you. In the online world, much like the real one, your identification credentials are stored in databases and are often compared against or collated to other data, which is stored indefinitely for further use. The bits and pieces of information that is posted with relation to you online is being collected about by third parties, and this data is being used in various ways – for instance, the browsing data, related to your digital identity might be used to improve your browsing experience by suggesting relevant advertisements to you. This is not, by all means, bad, but it can be. Everything you or someone else, shares about you and can be attributed to your identity, comprises what a digital identity is and this could leak or be exploited to harm you economically, psychologically, or in otherwise unpleasant ways.

We don't mean to scare you, but we call for your vigilance on what information you post, where, in what way and for what purposes. Furthermore, in cybersecurity, we recognize that a digital identity is not only comprised by claims but with other things as well, such as user-generated behavior, data produced by your actions online, or data assigned to you by a platform that you may be using. This means that you have to be careful not only when you post something online, but what your behavior is online, what places do you go to online, and what you are doing there.

For instance, when using a service online, you might be assigned a **cryptographic identifier (CID)**, that comprises part of your digital identity. All these identifiers about your actions online serve not only as a way to identify you online, but also to ensure non-repudiation, authorization, authentication, etc. – identifying you online is at the core of what online is and why we use it. This means that the online world has some mechanisms that ensure to a certain extend that you are you or that if you share something, you will have a hard time denying that it was you who shared it.

In cybersecurity, we use with relation to digital identity**, the term "nym".** Nyms are identities that are given to the user when interacting with other parties, or where the actions of a user are recorded by a software product, a platform, or something else. A common nym is a pseudonym that you would often give to yourself. Nyms could be linked to you or created to you to bind you with a meaningful context, for instance, your profile on Facebook, but could be something that is meaningful only within the context of a specific application or online transaction. The meaningless types of nyms are called unbound nyms, which simply put is an identifier that is very application-specific and might not necessarily reveal your actual identity. However partial identities, such as your profile on Facebook, might reveal more about you and more specifically, could reveal identity attributes – your birthday, or something else. This is very important, as partial identities are often bound together by different services and further attributed to a specific human being – in your case – this is you.

You are likely to be juggling various identities. A personal digital identity, a school digital identity, a sports digital identity, and many others. We call these contextual identities and they are great – the online world is a complex environment that allows you to do that so that you can create content, share it with specific target groups and interact with different stakeholders. This is much likely a mimicry of the real world – you talk to your cat in one way, and you talk to your teacher in another way.

Unlike the analog world, however, digital connections are very quick to be established and are characterized by a very high permanence of memory. This means that data travels very fast and a lot of it is stored for a long period of time with very high chances to prove the origin of this data. This requires your vigilance on issues such as identity, security, privacy, trust, and risks related to the disclosure on more than what is needed.

Managing your digital identity has a lot to do with the granulation of your different digital identities and creating as little of a mixture as possible. A few tips for you:

1. **Use different devices whenever possible for different identity roles.**

We don't mean that you should use a different computer for every different website you visit. Vulnerabilities in your personal computer may result in leakage of information, related to your school identity and information and vice versa. Using a school computer to check your Facebook profile might expose personal information.

2. **Use different accounts whenever possible for different identity roles.**

An example of this might be using your school e-mail (if you have one) for personal communication, which is a big no. Or using a personal e-mail account for school. With your personal e-mail, you might be registered on various websites revealing other digital identities you might have. Make sure to protect your privacy by following this strictly.

3. **Secure your documents – both on and offline.**

Secure any personal data you might have by any means that you have. Shred, encrypt, and protect with a password anything you don't want to be leaked, and remember to pay attention to what you upload and where.

4. **Power up your passwords.**

We can agree that a password is not safe if you are using it for protecting multiple profiles. Protect your digital identities by using strong passwords, with a different password assigned to protect a different thing. Do not use one password for more than one account, especially when it concerns multiple digital identities you might have. It's true, of course, that a single breach can expose quite a lot already, but you can minimize potential damage by using strong passwords and creating profiles in secure places only. For this, you will need a password manager. More information about password managers is available in the previous chapter of this lesson.

5. **Don't share more than you need to.**

You will inevitably share quite a lot only by signing in for a certain service that you need to use to live your life normally. Don't share too much, especially if it is not needed. Of course, in social media, you might like to share photos, stories, and personal details, but remember that once online – it is always online. Think twice before sharing details about yourself that you might not be happy people beyond your circle of friends seeing. By the same token, abstain from sharing too much information about people related to you – such as your friends, your parents, etc., such as where they go to school, where they work, etc. They can share this themselves, if they want but really unless you deem it important, think twice. It might be a good idea to cultivate the habit of asking whether it is alright to share something, such as photos revealing somebody else's face, or information that concerns them. If you want to share something that reveals the identity of your classmates, you must ask for their explicit consent.

6. **Stay vigilant and educate yourself**

Keep track of your debit cards (if you have such), your phone bills, your computer, and your friends' behavior online. React if you see something that bothers you, ask questions, and demand answers. Track your browsers' behavior, the loading speed, the speed of your computer, and upon significant change, take some action, such as re-installing, backing up information, running an anti-virus check, securing your accounts. Be mindful of your online habits and your cybersecurity hygiene and stay on track.

You don't have to completely change your life in order to manage your digital identities, however, if you are not following those basic tips already, we recommend that you start from them and build up. There is a lot of risks involved with identity theft and identity-based harassment and even the simplest measures could help you out significantly.

E-MAIL COMMUNICATION

Here, we will attempt at giving you some of the most basic tips to secure your e-mail communication. However, you need to know that e-mail communication will require a lot of your attention and any tools you can employ to further secure yourself, although helpful, will not substitute a vigilant mindset.

1. E-mail provider

Our first tip to securing your e-mail communication is choosing wisely your e-mail provider. This might seem obvious, but a lot of users, especially the older ones, who have created their e-mail accounts at the dawn of the Internet, might still be using their old and sketchy e-mail providers because back in the day, they were easier to use, widespread and accessible. This is understandable, as when you have an e-mail address for a long time, you might not feel like changing it. However, all measures you can take to protect yourself when communicating through e-mail will largely depend on whether your e-mail provider is up-to-date with security practices. A lot of the smaller e-mail providers will also most likely not invest as much in cybersecurity as the larger ones will. Back in the day, this might have been different, but today it is pretty much a thing.

If you are considering changing your e-mail provider or considering creating a new e-mail account to use as a primary account, we recommend that you do your research and take a bit of time to make yourself familiar with the privacy policies of the e-mail providers that catch your eye, as well as make sure that they have decent spam filtering capabilities and support end-to-end encryption or at least some form of transport layer encryption. It might seem obvious, however, there are still some small, local e-mail providers that do not offer those and your private communication might easily become exposed.

The majority of web-based clients use TLS to encrypt messages, which, unfortunately, comes with some downsides (check out this article[1]). End-to-end encryption is a far more secure method of communication, but it’s also difficult to set up for a single user. Businesses, on the other hand, may be able to utilize end-to-end encryption in a meaningful way. If you’re simply looking to secure your personal inbox, it’s good to install an antivirus, use a password manager continue through the tips below.

We recommend that you choose e-mail providers that offer multi-factor authentication and where you can further, enhance your security settings.

2. Custom filters

Most e-mail providers will allow you to set custom filters that will fight alongside your spam filter against unwanted messages. You can set your email to filter messages that contain certain words, that will be natively used by scammers or spammers.

3. Anti-virus

Installing an anti-virus might be useful for you to help protect you against phishing scams and save you a bit of time. Some anti-virus software will scan your landing pages and will warn you if you attempt to open one. Anti-virus programs refer to large databases with phishing URLs and will first attempt to match a website you are trying to open against this list. If there is a match you will be warned. Some anti-virus software will analyze the text and the contents of the websites for some warning signs and warn you. Those two features are particularly useful if you click on a fishy link by accident.

Of course, there are corporate versions of most of the anti-virus software that will allow for e-mail server protection. However, on a personal level, installing an anti-virus software, even the free edition, can help scan your e-mails and prevent you from opening sketchy web pages.

4. Secure your account

We recommend that for your personal correspondence and a primary e-mail account, you use a provider that offers multi-factor authentication and set up strong, highly entropic passwords. Use a password manager if you choose, however, be careful. Also, make sure you set up a backup e-mail address, from which you can recover the former should something happen.

We also recommend that you check your personal mailbox daily, so as to be able to identify quickly if something odd has been going on – for instance, if you can’t access your mailbox all of a sudden, if your spam e-mails count increase or if you notice any sort of odd activities and take measures immediately.

5. Separate accounts

As mentioned above, avoid using the same address for personal and formal or school-related communication. Most probably, your school’s system administrator has made the effort to secure your school e-mails well enough, so do not use your personal e-mail to exchange sensitive or school-related information. Furthermore, you probably use your personal e-mail address to register for multiple services and websites, so consider it sensitive and share it only with your personal contacts. Do not include your e-mail, both the school one and the personal one, in plain text on websites or in presentations or other documents that will be available online.

The reason behind this is that there are a lot of “spambots” that crawl the online space to harvest e-mail addresses. Often you have no choice but to include a mailto link with an email address on a web page. Use e-mail obfuscation tools and plugins, which are available for free for most content management systems, like Drupal, WordPress and others. Those tools use obfuscation to generate a "mailto:" link which will confuse most spambots but will still work in standard browsers, as most of these spambots do not seem to have complete HTML parsers and most do not execute JavaScript. If you don’t feel like obfuscating e-mails in web pages, the least you can do is to substitute the “@” with “at” and the “.” with “dot”. This will still make the address human-readable but might confuse the spambots.

In presentations or documents you can include your e-mail address as a picture, which will most likely prevent spambots from harvesting it.

6. Think before you send

Last but not least, always think before you send something, especially if it contains sensitive information. Even if you trust the receiver of your e-mail, this e-mail can be resent to someone else, or the contents of it could become exposed in other ways. We recommend, as mentioned above, to send sensitive information encrypted only and share the encryption key personally or by other means (do not include the encryption key in the same e-mail as the encrypted container) with the receiver. Be mindful when forwarding e-mails and protect the e-mail addresses of the receiver. If you are sending a mass e-mail to people who do not know each other, use BCC instead of To or CC. Cc stands for carbon copy which means that whose address appears after the Cc: header would receive a copy of the message. Also, the Cc header would also appear inside the header of the received message.

Bcc stands for "blind carbon copy", which is similar to that of Cc except that the Email address of the recipients specified in this field do not appear in the received message header and the recipients in the To or Cc fields will not know that a copy sent to these address.

---

[1] https://www.cloudwards.net/email-security/

SAFE WEBSITES AND NETWORKS

One of the most important things that we do online, besides communicating and sharing our own ideas and thoughts, is to browse for content. It is the Information era – whether we share information or receive information, the Internet is all about the exchange of it. This makes two important aspects of cybersecurity when online stand out – what networks do we connect to and what websites and platforms we go to.

It is important to be able to recognize an insecure website and modify our behavior according to our observations, as much as it is important to have the basic knowledge to assess if a network is too unsecured to connect to and what we should never do on an unknown network.

Here, we will not discuss how you can secure your own network, as this is a huge topic on its own. Most of the content in this chapter will be an overview of what consists of an unsecured network and what we can and what we should not do in it.

When we talk about unsecured networks, more often than not, we refer to hotspots that we do not know, but that we can connect to. Such networks could be coffeehouse networks, free Wi-Fi (wireless) networks. They might have no special login requirements or screening process, or they might have some but could be used by many people.

We all have probably used free Wi-Fi at one point or another. In fact, we appreciate the fact that we can go to a mall or airport and with just a few clicks on the establishment's Wi-Fi network link, we can be connected to the Internet. What unsecured Wi-Fi means for you, however, is that you are not secured while using this network. If you are connected to this network and someone would have some malicious intentions and is over the same network, there is very little you can do to stop them – they can intercept your traffic, they can see what you are doing and eavesdrop, they might even get themselves familiar with passwords you might be entering.

There are, of course, many hotspots that require you to enter some form of credentials and/or will present a "terms and conditions" page to click on before you can access the network, but that's almost nothing more than a welcome page, and it doesn't mean that you are safe. Some places might have a password of the day, but that doesn't mean their security measures are strong – we will expand on that in the next lesson, however, passwords aren't the only measure you need to take to secure your network. And is there always going to be something that is listening to your traffic – most probably no, but as cybersecurity professionals, we all have that one person in our lives that when bored in a coffee house will snoop on other people's business online or will set up their own "Free Wi-Fi" to see what you are doing online. So, without further ado, some general rules of conduct.

1. **Avoid using free Wi-Fi networks when possible.**

With your personal data and privacy at risk, make sure you use public Wi-Fi networks only when you urgently need it. Don't use it just because you are bored or you need to order that one thing online. Those networks really are not safe.

2. If you absolutely have to use it, **make sure you connect to the right network**

A lot of tech-savvy people, when bored in coffee places, would set up their own "Free Wi-Fi" or "Free CoffeeHouse Wi-Fi" as a trick to bait you to log in and see what information they can get out of you. Make sure you always ask the staff of the place where you are at what is the name of the open network of the place, maybe show them the names of the networks on your device and ask them to confirm which one is theirs. When in hotels, ask explicitly at reception or better yet, whenever you can use your own mobile data to connect or provide a hotspot for your other devices – it could be worth the investment.

3. **Do not use any services that require you to enter your passwords**

The danger here is two-fold. On the one hand, there are software tools that can be used to capture keyboard activity, so you can basically tell them your password. On the other hand, on free networks, one can easily set up a fake website that could much resemble the real website that you use and bait you into typing in your credentials.

4. **Do not work with any sensitive information** when logged in on a public network

Especially, do not enter credit card details, do not order things online, by all means, avoid online banking (if you have a bank account already) or online shop (if you have your own credit or debit card). Save those things for later and don't take any chances – you don't know who else is connected to the same network.

5. **HTTPS**

If an organization wants to have a secure website that uses encryption, it needs to obtain a site, or host, certificate. There are two elements that indicate that a site uses encryption: 1) a closed padlock, which, depending on your browser, may be located in the status bar at the bottom of your browser window or at the top of the browser the window between the address and search fields and 2) a URL that begins with "https:" rather than "http:"

Any time you are over the internet, take the habit to look at the address bar of the webpage and the webpage name. If you see "https" right in front of the address, it means that this website is encrypted, which means your data can't be read in transmission. If you see only "http," that site isn't secure. You might also see a small "padlock" symbol in front of the web address. HTTPS stands for Hypertext Transfer Protocol Secure which is basically an extension of the Hypertext Transfer Protocol (HTTP). HTTPS is used for secure communication because in HTTPS the communication protocol is encrypted using Transport Layer Security (TLS), or, formerly, Secure Sockets Layer (SSL).

What Wikipedia[1] says about HTTPS is that the principal motivation for HTTPS is authentication of the accessed website and protection of the privacy and integrity of the exchanged data while in transit. It protects against man-in-the-middle attacks. The bidirectional encryption of communications between a client and server protects against eavesdropping and tampering of the communication. In practice, this provides a reasonable assurance that one is communicating without interference by attackers with the website that one intended to communicate with, as opposed to an impostor.

6. Check website certificates

By making sure a website encrypts your information and has a valid certificate, you can help protect yourself against attackers who create malicious sites to gather your information. You want to make sure you know where your information is going before you submit anything.

One thing that you can get in the habit of doing and we recommend that you do, is taking the time to check the certificates on the websites you are visiting. Checking SSL certificates' expiration date on modern browsers is fairly easy. Depending on which browser you are running, it can be done within just a few clicks. Here is a tutorial[2] on how to check an SSL certificate's expiration date on Google Chrome.

If you are not familiar with web certificates and what they stand for, here are a few words of explanation. Trusted certificates can be used to create secure connections to a server via the Internet. A certificate is essential in order to circumvent a malicious party that happens to be on the route to a target server, which acts as if it were the target. Such a scenario is commonly referred to as a man-in-the-middle attack. The client uses the Certificate Authority (CA) certificate to authenticate the CA signature on the server certificate, as part of the authorizations before launching a secure connection. Usually, client software — for example, browsers — includes a set of trusted CA certificates. This makes sense, as many users need to trust their client software. A malicious or compromised client can skip any security check and still fool its users into believing otherwise.

If a website has a valid certificate, it means that a certificate authority has taken steps to verify that the web address actually belongs to that organization. When you type a URL or follow a link to a secure website, your browser will check the certificate for the following characteristics:

- the website address matches the address on the certificate
- the certificate is signed by a certificate authority that the browser recognizes as a "trusted" authority

If the browser senses a problem, it may present you with a dialog box that claims that there is an error with the site certificate. This may happen if the name on the certificate is registered to does not match the site name if you have chosen not to trust the company who issued the certificate, or if the certificate has expired.

You will usually be presented with the option to examine the certificate, after which you can accept the certificate forever, accept it only for that particular visit, or choose not to accept it. The confusion is sometimes easy to resolve (perhaps the certificate was issued to a particular department within the organization rather than the name on file). If you are unsure whether the certificate is valid or question the security of the site, do not submit personal information. Even if the information is encrypted, make sure to read the organization's privacy policy first, so that you know what is being done with that information.

When checking the certificate of a given website, make sure you pay attention to the 1) issuer of the certificate, 2) the expiration date of the certificate, and 3) who the certificate is issued to.

If you have any doubt, do a Google search and find out more about the certificate authority, or whether the company, that has issued the certificate really owns the website – if there is any discrepancy between the organization on the certificate that the certificate has been issued by or to, and the information you find online about the owner of the website or the certificate authority, we recommend that you revise your intentions on using this website.

7. **VPN** (Virtual Private Network)

You probably hear a lot about VPN for work and travel. This is because it is a good decision if you want to stay safe online but still you need to be away from your trusted networks. A VPN allows you to change your device's IP address, secure your internet traffic, and protect your online anonymity, all at the same time. A virtual private network (VPN) extends a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

If you don't want to limit your online activity but still want to be safe, look into using a VPN. By using VPN, you most probably will have to pay a small fee for the service, but you are protected – this is if you choose to buy a VPN service. You can also set up your own VPN server at home.

There is a lot of dispute against buying VPN services, as using paid VPN means that your traffic goes through your VPN service provider and they can log your online activity. Of course, this is safer than a random person snooping on your traffic and VPN providers offer non-disclosure agreements and privacy policies, as opposed to the person intercepting your traffic at that random coffee place. However, it is safe to assume that every VPN provider will log your activity, so as to it lets them deflect blame to the customer if they ever were to get into legal trouble or if you are doing something illegal online while using their service – it is in their best interest. Your home network provider would also do that. Check out this article[3] for the point of view of a precautious user who does not support the idea of payed VPN services. If you are concerned about paying for a VPN service, then you should consider setting up your own VPN server. Setting up your own VPN server at home may sound like a daunting task and it is more technically advanced, but there are a lot of free online resources showing you how to do that and you will most likely learn new things in the process.

You can also set up your VPN server in the cloud with services like Amazon AWS offers a range of options supporting the OpenVPN protocol, one of the fastest and most stable encryption protocols in the world. Another option is to set up a VPN server directly on your router.

There are a lot of things to look out for when online. However, the most important thing you can start doing if you haven't already, is to start cultivating online security habits. There is nothing worse than knowing that you are not doing the best you can to protect yourself and still not doing it.

Online security is an amazing topic to do your own research on. There are a lot of things that you will probably learn in the process and that will help you learn how things work. Even if you are a computer science teacher, you will most likely benefit a lot from things, such as setting up your own VPN server on a cloud technology that is new for you – you may try DigitalOcean if you have not already or AWS. There are plenty of projects you can start implementing to further your knowledge on the subject, but most importantly, that will give you ideas on how to communicate those topics with your students, what new projects and assignments you can do in school and what are your own knowledge gaps in the field of online security that you can fill in.

---

[1] https://en.wikipedia.org/wiki/HTTPS

[2] https://www.thesslstore.com/knowledgebase/ssl-support/how-to-check-a-certificates-expiration-date-chrome/

[3] https://schub.io/blog/2019/04/08/very-precarious-narrative.html

SUMMARY

Cybersecurity often is understood to refer to the Internet and the online space. However, not only is the notion of cybersecurity complex, but it is also closely connected to the fundamental rights of people, such as personal data and privacy, sensitive data protection, freedom of expression, rights to safety, the values of peace. Cybersecurity is the protection of systems and humans and more often than not, in literature, people are identified as the weakest link in cybersecurity as any given technical solution is still prone to failure due to human misconduct (Gratian, Bandi, Cukier, Dykstra, & Ginther, 2017).

How do we protect people in the online space and how do we stop cyberattacks from disrupting the supply of essential services for our society, when human fault-based cybersecurity vulnerabilities are so prevalent? The Internet allows users to gather, store, process, and transfer vast amounts of data, including proprietary and sensitive business, transactional, and personal data – how do we protect all that, and is it our job to do so?

Cybersecurity is a shared responsibility. As cyberspace and the physical space come closer, risks and threats in cyberspace increasingly affect physical space and individuals' livelihoods (European Commission, 2016) and we all bear the responsibility of starting by protecting ourselves online, by taking at least the basic measures.

In this lesson, we went through some of the basics related to staying safe online and we gave outlines of some of the most important attention areas, along with useful tips, ideas and preventive measures for the reader to take home.

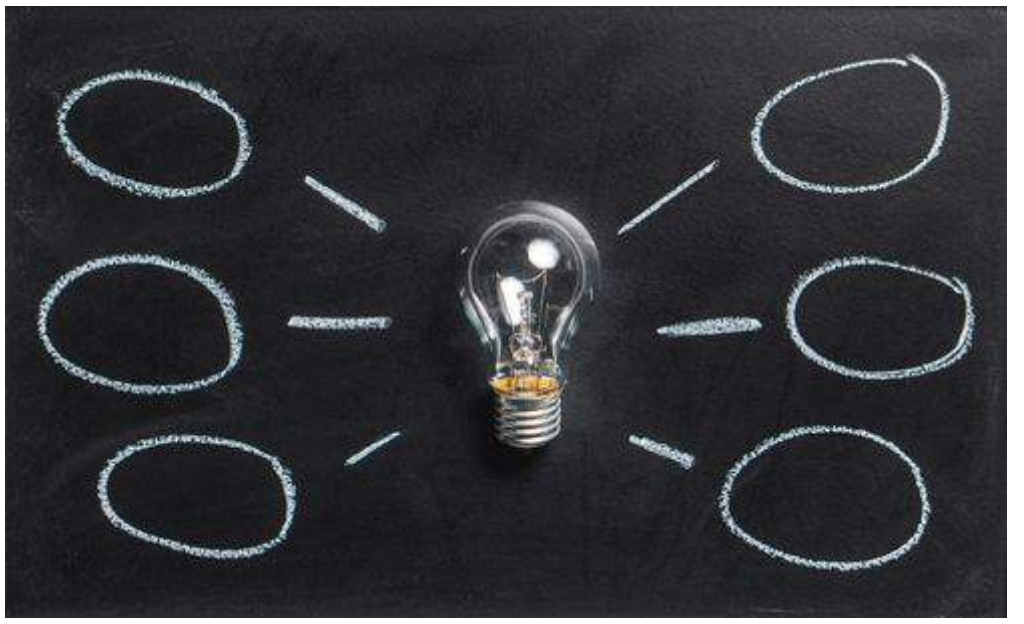

Photo 2 by Pixabay from Pexels (www.pexels.com)

[1] https://www.idtheftcenter.org/2018-data-breaches/

REFERENCES AND FURTHER INFORMATION

Ahson, S. A., & Ilyas, M. (2011). *Near Field Communications Handbook*. Auerbach Publications.

European Commission . (2016). Cybersecurity. *Scientific Advice Mechanism*, Scoping Paper.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2017). Correlating Human Traits and Cybersecurity Behavior Intentions. *Computers & Security*, 345–358. doi:10.1016/j.cose.2017.11.015.

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL. (2016, April 27). Protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Da. https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1552662547490&uri=CELEX%3A32016R0679.

1. https://schub.io/blog/2019/04/08/very-precarious-narrative.html
2. https://www.cloudwards.net/email-security/
3. https://en.wikipedia.org/wiki/HTTPS
4. https://www.thesslstore.com/knowledgebase/ssl-support/how-to-check-a-certificates-expiration-date-chrome/
5. https://schub.io/blog/2019/04/08/very-precarious-narrative.html
6. https://www.youtube.com/watch?v=QoQ-GS57sQE
7. https://www.youtube.com/watch?v=mmslC_JEk7s
8. https://www.youtube.com/watch?v=5GWIHv94KPM
9. https://www.youtube.com/watch?v=6ZCiXx6KYtA
10. https://www.youtube.com/watch?v=nENfIjvb5P4