LESSON 2.1 - THE IMPORTANCE OF PROTECTION OF DATA AND PERSONAL INFORMATION

INTRODUCTION

Nowadays, we live in an increasingly interconnected society where we find ourselves relying on various software products and services, both internet-enabled and offline, to lead our day-to-day lives. Our medical records are digitally stored, our identity is all over the internet through the various profiles we create every day, we are managing our finances online, we rely on technology to connect with friends and relatives, we book our trips online.
Ofcom's Communications Market Report of 2018[1] reports that "people in the UK now check their smartphones, on average, every 12 minutes of the waking day. Two in five adults (40%) first look at their phone within five minutes of waking up, climbing to 65% of those aged under 35. Similarly, 37% of adults check their phones five minutes before lights out, again rising to 60% of under-35s".

Of course, the benefits of a digitally enabled society are numerous. Software solutions nowadays help our productivity, maximize customer value and allow us to dedicate more time to our well-being while cutting down on bureaucracy. This advancement makes data and information a critical asset to our way of life and to our economy. This also makes data and information an attractive target to malicious parties because of the value this information has for our ability to maintain a normal standard of life.

Along with the phenomenal growth of technology, cybercrime opportunities have been dramatically increasing day by day using this same technology and this has a disastrous financial and psychological reflection. Cybersecurity Ventures predicts cybercrime damages will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015[2]. Cybercrime reports are relentless and committing cybercrime is becoming increasingly rewarding. Cybercriminals have proven to be resilient, adaptive, fast-learning and have moved quickly to adopt new technologies.

The main reason, why cybercrime is so prevalent, besides being very rewarding, is that it is far too easy. Many average users of technology would not take even the basic precautions to protect themselves. Users often lack adequate cyber hygiene, they leak sensitive data and information themselves, out of ignorance or carelessness, they lack the adequate cyber hygiene to protect themselves. Against

[1] https://www.ofcom.org.uk/research-and-data/multi-sector-research/cmr/cmr-2018
[2] https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

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.

this backdrop, cybercriminals are able to apply basic mechanisms to identify easy targets.

In this lesson, we will discuss the basics of why data protection should be important to you, not only as a teacher, but as an individual in nowadays' society. We will attempt at convincing you that this is an important topic to discuss with your students and their parents. We hope that this lesson will inspire you to put your defenses higher up and to research further on how you could start taking care of your data if you haven't already or deepen your knowledge about it.

Photo 1 rawpixel.com from Pexels (www.pexels.com)

LEGAL STANDPOINT

Privacy and the right over one's own data are among the core principles that lay in the foundations the European Union. We, as teachers in the European Union are required to abide by the laws of the Union to protect and respect our students' rights over their own data and identity. This is among the European Convention on Human Rights'[3] core statements and is part of the EU legislation that member countries have to respect.

Furthermore, the principles of control over one's own data lie at the heart of the GDPR (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2016), which we all have heard about. The GDPR sets out a number of principles and regulations that are set out right at the start of the legislation. Article 5(1)(f) of the Regulation requires that personal data shall be "processed in a manner that ensures appropriate security of the personal data, including protection

[3] https://en.wikipedia.org/wiki/European_Convention_on_Human_Rights

against unauthorized or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organizational measures (‘integrity and confidentiality’).”

Failure to comply with the principles may leave you open to substantial fines. Article 83(5)(a) states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or 4% of your total worldwide annual turnover, whichever is higher.

The GDPR specifically requires you to take responsibility for complying with the principles, and to have appropriate processes and records in place to demonstrate that you comply. A key principle of the GDPR is that you process personal data securely by means of ‘appropriate technical and organizational measures’ – this is the ‘security principle’ of the regulation. This means that your school is required to come up with a set of organizational policies and appoint a Data Protection Officer (DPO) who will proactively take measures to ensure that all employees of the school are familiar with the processes related to ensuring the security of the personal data stored.

You, as employee of your school, are also required to abide by the law and are held responsible for the mistreatment of personal data. This means that you should have a good grasp of some basic cybersecurity principles. For instance, Article 32 of the GDPR includes encryption as an example of an appropriate technical measure, depending on the nature and risks of your processing activities. The reasons behind this recommendation are multiple, however, apart from being recognized a secure way to treat data, encryption has been identified as a widely-available measure with relatively low costs of implementation. There is a large variety of solutions available and this is only one of the measures you are recommended to take to protect the data you store.

This module will present some tools to protect personal information and privacy, and we hope that this will be useful for you if you wish to apply some security recommendations.

Another thing you have to know about the processing, analyzing, obtaining and storing of personal data is that you, as an employee of the school, have to respect key legislation principles regarding to data processing, such as fair and lawful processing, purpose limitation, data minimization and retention.

In the case of processing on the basis of the law, this law should already ensure that these principles are observed (e.g. the types of data, storage period and appropriate safeguards). Prior to processing personal data, individuals must be informed about the processing, such as its purposes, the types of data collected, the recipients, and their data protection rights[4].

If parts of the processing are outsourced to an external organisation (so-called ‘processor’) there must be a contract or another legal act guaranteeing that the processor provides sufficient guarantees to implement appropriate technical and organisational measures that meet the standards of the GDPR.

Last but not least, legally in case of a data leak or accidental disclosure of data to unauthorized parties, your school is required to inform the affected people and the Data Protection Authority (DPA) without undue delay and at the latest within 72 hours after having become aware of the breach. This means if you are the one to identify mistreatment of data, security breach or data leak, that you are required to immediately inform the Data Protection Officer of your school. Further assistance may be required on your part depending on the case and the structure and administrative role-distribution in your school.

ETHICAL STANDPOINT

This chapter of the lesson will focus on why it is important to protect yours and your students’ personal data from an ethical standpoint and will discuss, without entering in philosophical details, why personal data and identity matters.

Firstly, we have to admit that nowadays, especially when it comes to learning with technology and software, that collect various data and information, collecting personal or sensitive data (more about this in Lesson 4 of this module) is enabled at an unprecedented level. You might be using software for teaching, that requires your students to create accounts, or your school might be using various platforms to track or report students’ progress to relevant stakeholders, such as local administration or parents. Furthermore, you might be disseminating various surveys among your students, or you might be sharing photos of your students and their work in conferences, to your colleagues and online. Put yourself in your students’ shoes and think about your work or personal data being shared without consent, for instance. This might give an idea on why ethical and consensual data collection, analysis and processing, as well as their secure storage and treatment is important form an ethical standpoint.

Most probably, this is nothing new for you – probably your school’s ethical committee or legal department are actively engaging you in various practices to ensure you are abiding by the law and ethics, related to data collection. And ethical data collection is not a new topic, especially in the academic world of research, where this issue has been discussed for a really long time.

[4] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en

However, cybersecurity, as a domain of the ethical data treatment is relatively new and sometimes brushed under the carpet out of ignorance. It is important to understand that everything, that is digitally stored, processed, or shared is probably vulnerable, susceptible to risk and might need further protection, as the implications and impact of data leaks are tremendous, dangerous and punishable by law. And we store digitally almost everything – and so does the software we use at schools. This means that the more digital systems are being incorporated in your teaching practice and your students' academic lives, the more the complexity of the associated ethical issues and challenges are being increased (Slade, 2013).

Another topic that should be discussed when considering the cybersecurity issues, related to the ethical treatment of personal data is that while on the whole, privacy concerns any data which, either alone or when linked to other, relate to an identifiable individual or individuals, but there is also other data, which might be interesting to third parties. It is very clear now how personal data might be abused by malicious parties for various purposes. However, data, collected by various software products might provide qualitative data, which would uncover behavioral information about your students, which could be further sold, leaked or legally shared as per the agreed upon privacy policy of the software used, for instance to target and personalize advertisements for, ultimately, financial profit of somebody else. This is a cybersecurity aspect of the ethical treatment of data, you should be aware of and know that if such information is collected, then the data is subject to the relevant EU data protection standards (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2016).

As a teacher, the student data that you, or the software you use for learning purposes in the classroom, collect, analyze, use or share should be understood as a moral practice. It concerns your students' identity, safety and well-being – both physical and emotional. Furthermore, it is your obligation to commit and ensure transparency when it comes to students' personal data and how it is being collected, shared, processed, analyzed and stored. Including by you, when at a conference and sharing pictures or works, created by your students.

For the ethical treatment of data, from a cybersecurity perspective, we recommend that you engage in conversation with your ethical committee, legal department and Data Protection Officer (DPO) of your school. Re-examine with them the privacy policies of the software you use or plan to use for educational purposes and converse about the ethical and legal implications from the use of this software. Inform the students and their parents about what data is collected from the software you are using for educational purposes, how it is collected, analyzed, protected and for what purposes and for how long is it stored.

Take highest measures applicable and abide by the cybersecurity policies of your school related to your students' data protection. Encrypt everything you can, be mindful on how your devices are protected both physically and software-wise. Be mindful on what you share, where, with whom and whether it is necessary, as well as how – avoid sharing unencrypted personal data. In lessons 2 and 3 of this module, we will go into further detail about some of the tools you can use to protect personal data both online and offline.

Insist on structured cybersecurity policies in your school if such are not already established. Regardless of whether you are an IT teacher, a music teacher or a member of the school administration, you are likely to be working with data and understanding the ethical implications of insecure treatment of data, you should speak up for a unified policy that will ensure a common cybersecurity baseline which you and your colleagues could lean onto. Encourage the school administration to organize teacher workshops, where you could learn more about how to protect information or where you could ask questions. Seek further training and learning opportunities for you and your colleagues and speak up for their importance.

Last but not least, engage your students and their parents, if possible in a dialogue about the ethical aspects of personal data. Encourage your students to never share unnecessary information about themselves or their families and friends. Help them get familiar with tools to protect their information or get them in contact with a colleague that could do this, if you are not IT confident yourself. Encourage them to seek further information and work for providing them with opportunities to learn more – organize extracurricular activities for students, invite guest lecturers, get in touch with cybersecurity professionals your students can speak to.

Ethical principles are a broad, complex and highly contextual dilemmas which should be a primary concern when it comes to data and privacy protection in schools. As teachers, it is of utmost importance that we protect our students and ourselves to maintain the good reputation of the teaching profession and to ensure the safety of the vulnerable parties, that could be harmed the most by privacy breaches and data leaks.

MENTAL HEALTH

Cybercrime has great impact on us as human beings and in this aspect, cybercrime is not much different than other crimes. Humiliation is more powerfully felt emotion than either happiness or anger (Otten, 2013) and cybercrime way too often feeds on shame and humiliation. We would like to invite you, at the beginning of this chapter of the lesson, to view three videos that we think might help us bring our point across. The first video is the powerful TED Talk by Monica Lewinsky titled “The price of shame[5]”, which deals with the subject of cyberbullying and public humiliation. The next video is called “Amazing mind reader reveals his 'gift'[6]” and with it, we aim to convey how much information we share online on a day-to-day basis. The third video is the TED Talk of Adam Anderson, called “Cyber Crime Isn't About Computers: It's About Behavior[7]” which deals with the fact that cybersecurity not only affects our psychology, but it uses psychology to affect us.

[5] https://youtu.be/H_8y0WLm78U
[6] https://youtu.be/F7pYHN9iC9I
[7] https://youtu.be/c_2Ja-OTmGc

Simply put, when we think of cybersecurity and data protection and the implications from the lack thereof, we often consider primarily the technological aspects of software and hardware protection. However, what quite often happens is that we forget to think about emotional consequences of data protection. We forget that we adopt technology as extension of our humanity and the impact technology has on our mental state and how it makes us feel.

Think about the fact that technology has direct implications on our social lives, on our cognition, on the way we organize and establish order in our lives. When we talk about psychology, we should also consider the fact that psychology is one of the most commonly used instrument to conduct a cyber-attack by itself. How it makes us feel, besides that, is only one aspect of cybercrime. How it is used against us, is another.

Cybercrime, however, not only affects our mental health, but also exploits our psychology. Think of all the tactics used by cyber-criminals, such as phishing, scamming, ransomware and social engineering – cyber criminals often consider our psychological vulnerabilities as tools to manipulate us and gain profit out of our lack of precaution or preparedness. Cybercrime is as dangerous and multi-faceted as it is, because of the skillset an attacker possesses – for a successful attack, the attacker should understand not only how technology works, but how people work, why they use this technology and for what purposes, what are the stakes for us if we are being compromised and how we as people function among other people and exploit that.

We as people are different and the same goes for our students and is something we need to recognize as a society. Some are more prone to risk taking, for instance, and this could reflect in their online behavior, which could result in them being targeted, whether they have taken actions to protect their data or not. Such actions could be buying from online shops without trusted SSL certificates, for instance. This is why it is important to practice good cybersecurity habits, both yourself by yourself and in your classroom.

When it comes to cybersecurity, as you know from Adam Anderson’s TED talk, which you watched in the beginning of this chapter of the lesson, good habits are fundamental for your safety – just as locking your front door is when it comes to not wanting someone to break into your house. Locking your front door doesn’t mean you are full proof, but at you are not welcoming the criminal home by leaving your door open. Likewise, **regardless how good your cyber defense infrastructure might be, if you are reckless, you will be at a higher risk**.

A very important habit, you as teacher need to adopt is constant vigilance when it comes to your students’ cybersecurity habits as well as taking any opportunity there is to talk to your pupils about digital citizenship and the freedoms and responsibilities that come along with it. While we may think that students will not be interested in listening to all we have to say about this topic, you have to remember that they are listening and retaining more than we think – especially the victims of cybercrime or those with risky behavior. Speak out about those topics every now and then, hold class discussions about that, ask students to share experiences, share your knowledge on the topic with them. This way you become a figure of trust by making students realize you are interested in them beyond the school curriculum and that you are invested in their well-being and safety.

You have to remember that cyberbullying, for instance, is not something that many parents have the knowledge how to deal with. Converse with parents as well, if you have this opportunity, and encourage them to be as active in their children's online life, as they are in their offline life. Ultimately, parents will raise their children as they see fit, however \ sharing what you know and what you see, might result in a sustainable impact on preventing cybercrime or supporting a child's mental health if they happen to be a victim.

Important habit is to address crime if you see a crime. You may overhear students talking about being harassed online, or a student might confide with you about being a victim of cybercrime. Especially with crimes, such as cyberbullying and other forms of cyber humiliation, every support counts and every support might just make the difference. If someone is being cyberbullied, advise them to keep all evidence of cyberbullying, keep a log with the dates and times of the instances, and report the instances (Hinduja, 2015). Show your students you have their back – talk to them when they come to you, refer them to the school counselor, if you see signs of distress, talk to their parents and the school administration and never take the issue of online abuse or cybercrime lightly.

Last but not least, take care of yourself. A survey[8] carried out in long ago, in April 2009 by the Association of Teachers and Lecturers[9] and the Teacher Support Network[10] suggests that teachers, as well as students, are increasingly at risk of being the victims of cyberbullying – we can imagine how those numbers have changed since 10 years ago. It found that one in seven teachers have been cyber bullied and of those, 68% had received unpleasant emails, 26% had been the subject of abuse on websites and 28% had received abusive text messages. Protect yourself and your mental health – reach out to authorities, speak to the school administration, put your cyber defenses up and always stay mindful on what you share online. Don't hesitate to speak to a therapist – cyber abuse and cybercrime are as impactful and real to a person's life and mental health as is any other type of crime and abuse.

COSTS OF DATA AND IDENTITY THEFT

According to 2018 Identity Fraud: Fraud Enters a New Era of Complexity[11] from Javelin Strategy & Research, in 2017, there were 16.7 million victims of identity fraud. Data breach cases and identity theft reports are increasing and on the rise. More and more complex schemes are being introduced by cybersecurity criminals, but quite often, the targets become those, who just don't take the precautions

[8] https://www.atl.org.uk/Images/Joint%20ATL%20TSN%20cyberbullying%20survey%202009.pdf

[9] https://www.atl.org.uk/

[10] https://nyc.teacherssupportnetwork.com

[11] https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

necessary to protect themselves at least by following some basic cybersecurity principles.

And even when following the basics of cybersecurity hygiene, most unfortunately, identity theft can happen to anyone and has far-reaching consequences for its victims. According to a study, conducted by the US Department of Justice (DOJ)[12] in 2014, revised in 2017, 17.6 million people in the US experience some form of identity theft each year. This includes activities such as personal information being used to open unauthorized accounts, but doesn't take into account issues such as ransomware, where the victim is bullied into paying in order to retrieve stolen information with no guarantee whether this information could be leaked somewhere else anyway and potentially used by other malicious parties for various purposes.

As per the report of the US Department of Justice, "The economic impact of identity theft is made up of direct and indirect financial loss. Direct financial loss, the majority of the total loss associated with identity theft, refers to the monetary amount the offender obtained from misusing the victim's account or personal information, including the estimated value of goods, services, or cash obtained. Indirect loss includes any other costs caused by the identity theft, such as legal fees, bounced checks, and other miscellaneous expenses (e.g., postage, phone calls, or notary fees). Direct and indirect losses do not necessarily reflect personal losses to victims, as victims may be reimbursed for some or all of the direct and indirect losses."

Apart from the financial aspects, the price of being a victim of a data leak could be continuous humiliation, job loss, family break-up, and so much more. A survey from the Identity Theft Research Center[13] found that 69 percent of the interviewed victims of identity theft felt fear for their personal and financial security. Another 65 percent felt rage, anger or humiliation. Sleep disruption and insomnia was reported by 40 percent. These feelings reportedly increased over time when victims were unable to settle the issue on their own, according to the report.

Even more frighteningly, Javelin Strategy[14] found that children are increasingly the victims of identity fraud. While children in the US have long been a target for Social Security Number misuse and credit card fraud, it appears the impact is growing. The security firm found that over 1 million children were ID theft victims in 2017.

On the other hand, you may not be a victim, but you or your school's failure to comply with the security regulations, that potentially cause a data breach may leave your school open to substantial fines. Article 83(5)(a) of the GDPR states that infringements of the basic principles for processing personal data are subject to the highest tier of administrative fines. This could mean a fine of up to €20 million, or

[12] https://www.bjs.gov/content/pub/pdf/vit14.pdf

[13] https://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf

[14] https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity

4% of your total worldwide annual turnover, whichever is higher. This again means job loss, loss of reputation, financial loss, community crises.

The Data Protection Act is a key law within the UK. Failure to comply can have serious consequences. Violating data protection law can see you and your business prosecuted, resulting in harsh punishments. These can include fines of anything up to £500,000 or action being taken that could result in a prison sentence.

Following proper data protection procedures is crucial to help prevent financial, material, psychological, physical and moral damages. Having control over our personal data is our own right, but it comes with responsibilities as well – we are responsible for taking at least the basic measures to protect ourselves and our identity, and save ourselves the tragedy of data loss.

SUMMARY

As our society and educational system increasingly depend on electronic data and computer networks to conduct our daily lives, growing pools of personal data are being transferred and stored online. This can leave individuals exposed to privacy violations, and for our schools this might mean being exposed to potentially enormous liability, if and when a data security breach occurs.

Cyberattacks and breaches have grown in frequency, and losses are on the rise. Against this backdrop, we are ever than before interested in cybersecurity and protecting our digital data as in 2018 the ITRC[15] reported that hacking was the most used method of breaching data, with 482 data breaches resulting in almost 17 million records exposed.

We from Be@CyberPro recognize the need for more cybersecurity professionals and the need for better awareness and knowledge about cybersecurity in general, but especially related to schools. We recommend you make yourself familiar with the Be@CyberPro educational resources for teachers, students and parents, as well as to check out the resources and newsletters available on our project website.

Talking about the issues of data protection and cybersecurity is of highest importance to ensure a safer future for all of us. Please check out the resources in this lesson as well, so as to find more information about the issue and importance of data and privacy protection.

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

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

REFERENCES AND FURTHER INFORMATION

Hinduja, S. &. (2015). Bullying beyond the schoolyard: Preventing and responding to cyberbullying (2nd edition). *Thousand Oaks, CA: Sage*. Retrieved from http://cyberbullying.org/bullying-beyond-schoolyard-preventing-responding-cyberbullying-2nd-edition

Otten, M. &. (2013). Humiliation as an Intense Emotional Experience: Evidence from the Electro–Encephalogram. *Social neuroscience. 9*.

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.

Slade, S. &. (2013). Learning Analytics: Ethical Issues and Dilemmas. *American Behavioral Scientist, 57(10)*, 1510–1529. doi:https://doi.org/10.1177/0002764213479366

1. https://www.ofcom.org.uk/research-and-data/multi-sector-research/cmr/cmr-2018
2. https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

3. https://en.wikipedia.org/wiki/European_Convention_on_Human_Rights
4. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en
5. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/public-administrations-and-data-protection/what-are-main-aspects-general-data-protection-regulation-gdpr-public-administration-should-be-aware_en
6. https://www.youtube.com/watch?v=H_8y0WLm78U
7. https://www.youtube.com/watch?v=F7pYHN9iC9I
8. https://www.youtube.com/watch?v=c_2Ja-OTmGc
9. https://www.atl.org.uk/Images/Joint%20ATL%20TSN%20cyberbullying%20survey%202009.pdf
10. https://www.atl.org.uk/
11. https://nyc.teacherssupportnetwork.com
12. https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity
13. https://www.bjs.gov/content/pub/pdf/vit14.pdf
14. https://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf
15. https://www.javelinstrategy.com/coverage-area/2018-identity-fraud-fraud-enters-new-era-complexity
16. https://www.idtheftcenter.org/2018-data-breaches/
17. https://www.babble.com/parenting/cyberbullying-prevention-young-children/
18. https://www.babble.com/parenting/protecting-kids-cyberbullying/
19. https://ptaourchildren.org/understand-cyberbullying/
20. https://www.pacer.org/publications/bullypdf/BP-23.pdf
21. https://www.pacer.org/publications/bullypdf/BP-27.pdf
22. https://www.pacer.org/bullying/resources/parents/mobile-and-online-safety.asp
23. https://pacerteensagainstbullying.org/advocacy-for-others/cyber-bullying/
24. https://yourteenmag.com/social-life/teen-bullying-tips/how-to-prevent-cyberbullying
25. http://www.privacyandcybersecuritylaw.com/
26. https://staysafeonline.org/wp-content/uploads/2017/09/What-To-Do-If-You-Are-a-Victim-of-Cybercrime.pdf
27. https://techcommunity.microsoft.com/t5/System-Center-Blog/bg-p/SystemCenterBlog

28. https://youtu.be/cLory3qLoY8
29. https://www.dpnetwork.org.uk/resources/

LESSON 2.2 - 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 the everyday life has resulted in 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 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 cyberespionage 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, as you know from Module 1, 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 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, to fight cybercriminals and to safeguard entire network infrastructures. This is why, the Be@CyberPro Project Consortium developed this lesson with the goal of providing you with the 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 personal 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 to compliment what we already know from Module 1. We will go over 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.

Photo1by TheDigitalWay from Pixabay (www.pixabay.com)

PASSWORDS

As a society, we are really bad with passwords. You can read some of the more famous showcases of that statement here[16] 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. You already know a lot about password protection from Module 1, so without further ado, we will offer you some useful tips related to your password habits that can potentially spare you from headaches.

1. Basic principles

We know that creating simple passwords is plain suicide. Using your child’s name for your e-mail password is something that no one does anymore, however, 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, passwords that were long were considered more secure than passwords that were short. However, what password would you consider more

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

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 child’s name or your favorite 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 increasing 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 firstly that you will be putting the required symbols, capital letters and numbers at the beginning or 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 and in Module 1.

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 on whether you have created a profile with the same e-mail on 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 from 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”.

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 by all information, or set of claims, that you have made online for yourself or is made by somebody else in reference to you. Such claims might be that you work in a certain place – your school might have managed your name as an employee on the school website, or you may have mentioned your affiliation to the school yourself through your LinkedIn 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 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 university diploma as credentials 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 extent 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 the pseudonym which 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 in 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 professional digital identity, a personal digital identity, a classroom digital identity, a sports digital identity and much 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 boss in another way.

Unlike the analogue world, however, digital connections are very quick to be established and are characteristic with 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 less 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. However, we recommend that you do not use your personal computer for work. Vulnerabilities in your personal computer may result in leakage of information, related to your work identity and information and vice versa. Using your work device 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 work e-mail for personal communication, which is a big no. Or using personal e-mail account for work. 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 password protect 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 spouse, your child, etc., such as where they work, where they go to school, etc. They can share this themselves, if they want but really, unless you deem 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 students, you must ask for explicit consent both from the students and their parents – this is the law.

6. Stay vigilant and educate yourself

Keep track of your credit card records, 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 risk involved with identity theft and identity-based harassment and even the simplest measures could help you out significantly.

E-MAIL COMMUNICATION

A lot has been said in Module 1 about 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 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 security 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 downside (check out this article[17]). End-to-end encryption is a far more secure method of communication, but it's also difficult to

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

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 firstly 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 for work and personal life

As mentioned above, avoid using the same address for personal and formal or work-related communication. Most probably, your school’s system administrator has made the effort to secure your work e-mails well enough, so do not use your personal e-mail to exchange sensitive or work-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 work 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 in 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.

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 contents. 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 basic knowledge to assess if a network is too unsecured to connect to and what we should never do on an unknown network.

In lesson 3 of this Module, we discuss a bit how you can secure your own network, so here we will not go into that. Most of this contents will be an overview on what consists of an unsecure 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 in 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 unsecure 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 intents 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 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 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. 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 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[18] 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

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

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[19] 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 which 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—include 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 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.

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

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 are a lot of dispute against buying VPN services, as using payed 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[20] 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.

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

If you are interested in learning how to set up your own VPN server, check out those five tutorials and find the one that answers to your technical background and fits your context.

1. Build Your Own VPN. Browse Securely from Anywhere –

   https://youtu.be/mmsIC_JEk7s

2. How to setup a VPN - Build your own VPN server on windows 10 for free –

   https://youtu.be/5GWIHv94KPM

3. How to Setup a VPN in Windows 10 –

   https://youtu.be/6ZCiXx6KYtA

4. Create Your Own VPN Server On AWS - AWS Casts –

   https://youtu.be/nENfIjvb5P4

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.

SUMMARY

Cybersecurity often is understood to refer to the Internet and the online space. However, not only is the notion of what cybersecurity is complex, but it also is 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 the digital cyber space and the physical space come closer, risks and threats in the cyber space 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. Most of this material has already been expanded upon in Module 1, so here 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. Within the next lesson in this Module, we continue with securing your personal data and privacy offline and the basic principles related to protecting ourselves and our families as much as possible.

As teachers, we have some responsibility in instilling the good practices, related to cybersecurity and online behavior with our students. We well know that students spend a lot of time online, so we encourage you to start a discussion about safe online behavior and good practices. Share what you know and learn from your students, as discussing cybersecurity and viewing potential vulnerabilities and threats from different angles is what makes the ultimate difference on a larger scale.

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

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=mmsIC_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

LESSON 2.3 - TOOLS AND METHODS TO PROTECT INFORMATION AND PERSONAL DATA OFFLINE

INTRODUCTION

Protecting your personal information, privacy, financial information or passwords from malicious parties has been a recognized priority by many, with for obvious reasons and many benefits. However, many of us, due to ignorance or skepticism, still fail to comply with basic cybersecurity hygiene practices.

It is true that your school's system administrators might be the people who secure your school data, come up with security procedures or provide you with the maintenance and support you need to feel safe with relation to your work. Nevertheless, we believe that everyone should be familiar with at least the basic principles, so that you can protect your privacy and personal data of your personal devices, networks and software products. The reason behind the importance of protecting your personal devices more often than not, goes beyond just protecting your own privacy. We might have sensitive data or information, related to our work, on our home computer – we might be checking homework or student projects, we might be keeping participant lists for the school trip next month, we might be keeping back-ups of our work documents. Failure to protect your personal devices in cases such as this, might result in sensitive data exposure, vulnerabilities and much more.

It is true that you might never get hacked and your cybersecurity habits or the lack thereof, might never result in information leakage, however why take the chance? In this lesson, we will introduce some of the basic hygiene principles related to keeping your personal information and data safer. Those are habits, that you can implement in your personal life and in your work, as well – the system administrators can secure the school infrastructure and take relative care of the school devices, but it is your actions, as an employee, that will ensure that their precautions have the anticipated results.

Cybersecurity is a shared responsibility. It is not only the job of a small department in your school to keep you and your students safe. Cultivating good cybersecurity habits will improve the overall cybersecurity posture of yourself, your family and your work environment, and following those guidelines, you will likely increase the awareness of the people around you. Not securing your devices is like not locking the door to your apartment – sure, it is true that no one might come in, but you most likely have built the habit of locking your door anyways, right? The same goes for cybersecurity.

This lesson will discuss the security of your computer(s) and smart devices such as smartphones or tablets. This lesson, however, will not provide information on how to secure other smart devices that you might have, such as IoT devices in your home, etc., although some of the guidelines for securing your other devices, might prove useful for this case also. If you have IoT devices in your home, we suggest that you take your time and research by yourself, depending on your device and its functions, what steps you can take to ensure its security and the security of the other devices, connected to the same network.

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

BASIC PRINCIPLES

There are a lot of general cyber hygiene practices when it comes to protecting your personal data and privacy while offline. Most of those practices are pretty generic and will not depend on your device, the software you install or the operating system you use. However, some of them might and you will have to find a way to customize, according to context. This is usually something, you can pretty easily find information on how to do online, however, if in doubt, contact the IT department of your school and ask them.

Without further ado, let us start with the basics of offline protection.

A very important principle of cyber hygiene is to take good care of **the software you install on your computer**. Install licensed software only and avoid installing software from unknown sources. Run the privacy policies along to your legal department, ethical committee and Data Protection Officer, to make sure the software you use or plan to use, both for administrative and educational purposes, complies with the data protection regulations of the school (more about this in Lesson 4 of this module). Keeping your software up to date is also very important, as you know from Module 1. Updating your software keeps you safe from known vulnerabilities, that are being fixed throughout the course of the software maintenance. If possible, automate and schedule your software updates. Same goes for **installing operating system updates**.

It you want a word of honesty we all find operating system updates a tedious chore. However, the reason why these updates exist and are so important is that they contain crucial security patches that will protect you against most recent known vulnerabilities. Skipping these updates leaves your device at risk. The same goes for updates on your smartphone, as well as other smart devices you might be using.

Another step we recommend you take from a software point of view is to uninstall software you no longer use and no longer plan to use. Not using a piece of software will mean you will likely not think much about it and maintaining it up to date. **If not using it, consider removing it**.

When it comes to information and software that you are not using, we strongly recommend to **take good care of the devices you are not using**. Much information could be taken from old computing devices you are not using anymore. Such devices are old hard drives. After securely backing up the data from your old device, you should sanitize and shred, magnetically clean the disk or if you are planning on reselling an old phone or laptop for instance, look for appropriate software tools to wipe the device clean. WikiHow has a wonderful step-by-step tutorial[21], teaching you how to do so. By the same token, we recommend that you **disable file and media sharing** when not needing them. This means turning off Bluetooth or not making files or media publically available, especially if they contain private data or information, to other machines in your network.

You should consider, installing **antivirus software** on your computer, if your school has not taken care of that already. There are plenty of free software tools you could use and although they are not a full proof defense against new or advanced malware, there can save you a lot of trouble. Research free antivirus software and install one. Most of the antivirus software will have browser extensions and will be useful for your online security as well. Make sure your Firewall is up and revisit Module 1 if you don’t remember much about Firewalls and how to set them up.

If you happen for some reason to need to use someone else’s computer, first, try to avoid it. Secondly, be mindful if you want to use a USB stick to export some information, as malware is easily transferred through external memory devices. Thirdly, use incognito browsers (tutorial here[22]) and log out of all your profiles, if you visited such. Never save passwords on somebody else’s device and never upload (or download) personal data and private information to a device that is not yours. Incognito browsing or private browsing is a common practice for leaving fewer traces while browsing the web.It is a privacy which is common for most contemporary web browsers and how it works is it disables all browsing history, storage of data in cookies and web cache. This will allow you a person to browse the web by leaving almost no trace of what you did online. Browsing incognito could, however leave traces on the hard drive and memory of the device, so be

[21] https://www.wikihow.com/Destroy-a-Hard-Drive

[22] https://www.digitalcitizen.life/keyboard-shortcuts-incognito-private-browsing-inprivate

mindful of that as well. Check out this great Wikipedia article[23] for more information about private browsing.

However, in this module, we discuss the basics of offline hygiene, so let us get back on track with some recommendations. Another recommendation we have for you is to **keep your desktop clean**. Don't keep private files or files containing personal data on your desktop. This will not protect you from hacking or malware but it is just common sense to protect you from snooping. Keep only what you really need on your desktop and make sure it is as little as possible.

While on the topic of snooping, be mindful of the so-called **shoulder surfing**[24]. Shoulder surfing is basically the practice of someone looking over your shoulder at your desktop screen while you are working or doing something on your computer, on a phone or an ATM machine. If you share an office with a colleague, for example, and a parent comes in to talk to your colleague, be mindful about what you are doing in this moment and whether they can see. Avoid working with personal data while external people are around.

Another general cyber hygiene practice, we spoke about already in this module and in previous modules is **backing up your information**. As you know from Module 1, there are some basic principles which you need to follow when backing up your data. Without trying to repeat the information you already have, we will just briefly mention that backing up your information on a regular basis is a must. How often you need to back up your information depends on many factors, such as what information you work with, how much information you have, how much have you modified or added, etc. Basically, if there is no school policy, defining a minimal back-up schedule, you should back-up as often as you can, as long as it is meaningful (if nothing has changed since your previous back-up, a new one might not be as necessary). If you could schedule automatic back up mechanisms, depending on your schools' security policy, we recommend you do so.

Security professionals recommend you keep at least 3 copies of important data – 1 on your device, 1 on a secure cloud storage and 1 on a secured offline external drive. A common anecdote among security professionals is that only 1 back-up means no back-up. You should verify the integrity and the availability of the backed-up data regularly and your back-ups should be encrypted – use strong passwords and reliable tools for them. Last but not least, when it comes to back-ups we recommend that you do not keep all your eggs in the same basket – don't have all your back-ups in the same backpack or in the same location (obviously, this applies to your offline back-up on an external drive).

When it comes to mobile devices, as we recommended above for your computer, you must be careful when installing applications. We recommend installing applications from trusted sources only (such as Google Play Store for Android). Usually, by default, you will not be able to do so, however, by mistake or not, you might have enabled the option to install applications from unknown sources – we call this **sideloading**. There's nothing wrong in installing software from other

[23] https://en.wikipedia.org/wiki/Private_browsing

[24] https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)

sources if you trust the source and you are sure what you are doing. However, we recommend that you keep this option off and enable it only if you most definitely need to use it.

If you are sharing your device with somebody else, for instance if your child is playing on your phone or tablet, we suggest enabling **parental mode** which will allow access only to certain applications and websites and will ensure that your child will be less likely to delete, buy or see something by accident.

Another important issue, concerning your privacy and the privacy of your students is **geotagging**. Now, with social network apps you can easily upload photos to your social networks from your phone right when you make them. This is an issue because many phones embed geotags (basically reveal your location) within the picture file and anyone with a basic skillset could look up where you were when this photo was taken. Some social media strip geotags when a photo is uploaded, but this is not a guarantee enough. Turn off the geotagging settings on your smart devices to ensure yours and your students' privacy.

Photos, images and video saved on your computer may also contain personal data. A facial image is considered personal data. Additionally, other data such as location or date and time of capture and others (known as EXIF metadata) might be stored in the case of digital images. Even more frighteningly, high-resolution recordings might as well enable biometric recognition of the persons depicted. Tutorials that can help you and we recommend are this one[25], provided by Norton and this one[26], provided by MakeUseOf.

Last but not least, as a general recommendation, we very much advise you to l**earn how to use virtual machines and actually use them**. Now, if you are not very tech savvy, the concept of virtualization and virtual machines might seem scary or too abstract. If you are reading this and you are getting scared do not give up yet, we promise it is not as hard as it sounds.

Firstly, it is not a route that everyone needs to take, but we think it is generally very useful and as cybersecurity professionals, we use it a lot. Virtualization simply means running one operating system on another – so, if you have your regular Windows, you can install a "guest" operating system on it – for instance Linux, or Windows again. This comes in very handy, as you could configure your guest operating system, to have no permission to interact with your host system, meaning what you can see from your virtual machine cannot harm your regular operating system. So, for instance, you want to open a sketchy website – you could do it from your virtual machine. Your virtual machine will sidestep your operating system and will keep it safe, so if any malware attacks your virtual machine, you can just get rid of the virtual machine and create another one and your computer is remaining safe. The same goes for using USB sticks that are not yours. You could

[25] https://us.norton.com/internetsecurity-how-to-how-to-remove-gps-and-other-metadata-locations-from-photos.html

[26] https://www.makeuseof.com/tag/3-ways-to-remove-exif-metadata-from-photos-and-why-you-might-want-to/

open them with your virtual machine and if some malicious code comes lurking out of the external device there is no need to panic.

This video[27] is great to start with – it offers a beginner guide to installing VirtualBox (a commonly used free software to create virtual machines) on a Windows Machine and configuring and running an Ubuntu virtual machine. This video[28], on the other hand, provides a more in-depth introduction to VirtualBox and how to install, set up and use it. If you prefer written explanation and instruction, this is a great guide[29] that will get you through the process of setting up and running a virtual machine.

PROTECTING THE ACCESS TO YOUR DEVICES

In no particular order of importance, we would like to point your attention first to **where you keep your computer**. We understand, of course, that when it comes to your work computer or laptop, you most probably would keep it in your office or in the case of a laptop – you might bring it along with you to a classroom. With PCs, you cannot really bring them around or move them much, but we really encourage you to take all precautions to securing your PC with other means – for instance, a general rule of thumb will be locking your computer anytime you are away from your computer, even for 2 minutes, and shut it down when you leave the office, apart from when there is scheduled maintenance or something like this. For laptops, however, we recommend that you are more careful.

If you are bringing your laptop around or to home, make sure you are confident that if someone steals your computer, the data on it will be safe. This means that everything is encrypted, you are logged out of all accounts, and all information you carry is backed-up somewhere else as well and your only concern will be finding a new machine and spending 2-3 hours to configure and personalize it as you like.

If you are leaving your laptop in your office at school, shut it down and close the lid anytime you are away from the keyboard for more than 20 minutes (otherwise you could just lock it). This is generally a protection against snooping and spilling drinks on it. If you will not be around it for more than 4-5 hours, we recommend that you shut it down, close it and put it away (in a cupboard, or somewhere not on top of a desk). As cybersecurity professionals, we tend to go a bit overboard with the security measures we recommend and apply ourselves. However, this is not a measure against theft, but more so against, snooping and having someone mess with your computer. If your room is under video surveillance or is being locked when you are away, most likely, this will not be needed, however it is a good practice in general to protect your device and keep it safe.

[27] https://youtu.be/sB_5fqiysi4
[28] https://youtu.be/D1dVhDYAv9E
[29] https://lifehacker.com/the-beginners-guide-to-creating-virtual-machines-with-v-5204434

We already mentioned **locking your computer while away**. This is very easy, and saves a ton of trouble – this is, of course, if your computer is password protected, which it should be. This stepreduces the chance that your account will be used by someone else should you ever walk away from your computer while logged in. In order for a lock to be effective, you will have to make sure that your computer is configured to prompt for a password when waking. If you are not sure how to lock your computer or set a password, do not worry we will guide you to tutorials that will get you covered along this lesson. To learn how to lock your computer, check out this step-by-step guide[30] for Windows and Mac users. If you are a Linux user, look up in Google how to lock your computer depending on your Linux distribution (Ubunto, CentOS, etc.). Generally, Windows users could use the Windows Key + L to lock their device, Mac users would use the Control + Shift + Eject shortkey combination (or Control + Shift + Power for newer Mac devices that do not have an optical drive), some Linux distributions would lock with Ctrl + Alt + L.

It is a very good idea to introduce automatic inactivity logout to your device if you haven't already. Basically the automatic logout will have your back if you need to urgently go somewhere and you forget to lock your computer. Windows 10, as well as all other operating systems, can automatically lock your screen if your system has been idle for a while. You can choose how long the idle period is for. It can be as short as one minute or as long as an hour or more. This video[31] will teach you how to configure this setting if you are not familiar with it for Windows.

If you forget to lock your screen, or you feel your password has been compromised, you can change your password and then remotely log out of Windows 10. This video[32] goes into more detail about it. However, logging out will be no help at all if your device is not password protected.

This brings us to the next point – at least **password protect your device**. Choose a non-trivial password, or passphrase, as we discussed in Lesson 2 of this module and configure it. This tutorial[33] by the Windows Central will show you how to do so for Windows if you are not already familiar with. If in doubt, speak to the IT support of your school.

There is a saying about passwords, which is a bit cynical, but it is true – that passwords are like underwear – you should not share them with other people and you should change them often. Furthermore, we can add to that, that you should not use one password for multiple purposes and you should not use "easy" passwords. We know you have a lot of accounts, and we do too. There are free password managers that are easy to use and safer than writing down your passwords on a sheet of paper (which you should never do) or using one password for multiple websites. The reason why you should not use one password for multiple websites is that sometimes, data from some websites gets compromised. Passwords might be poorly protected and non-encrypted or salted (not sure what

[30] https://www.wikihow.com/Lock-a-Computer

[31] https://www.youtube.com/watch?v=JuRQ55_G-eU – **PRIVATE VIDEO!**

[32] https://youtu.be/cvZVHbBTPp4

[33] https://www.windowscentral.com/how-manage-user-accounts-settings-windows-10

we mean by salted – learn here[34]) and might leak. If hackers have your username (very often your e-mail) and password, they can try and break into some other accounts you might have. This is a very unpleasant situation for you as you might get locked out of accounts, might suffer financial and emotional loss, might suffer other sorts of damage – don't risk it. Password managers often offer functions and features such as generating a secure password or reminders to change passwords you haven't changed for a long time.

Sometimes, our work forces us to share a device with somebody else. This is really a not recommended situation, but if you cannot change it, take at least the basic precautions of creating **different accounts for all users and assign them user roles**. Those two tutorials[35][36] should help you do this if you have not configured different accounts already. In situations like this, we recommend you encrypt and back-up everything you have and store as little as possible – use this device as a work terminal basically and export everything immediately. Teach the person you share this device with some principles about protecting your device and the Be@CyberPro materials as in this case, security becomes a shared responsibility.

In general, we recommend you practice the **Principle of Least Privilege (PoLP)**. The PoLP stipulates that if you could do your job without needing to use administrator or root privileges, you should not log in as administrator. Logging in as a user with highest privileges leaves your system vulnerable to exploitation that could possibly result in your whole system or device being compromised, your entire hard drive being formatted, or having a new user account with administrative access created. When performing maintenance on your device or installing new software, getting rid of old one or installing updates, log in as administrator but be very cautious and whatever you can, do offline.

Here, we would like to also point your attention to your smartphone or other mobile devices you might have. Securing the access to your smart mobile devices is important for protecting your personal data and privacy, but will most likely keep personal data with relation to your job at a higher level of security as well. You might be logging in to check your work e-mail or keep some documents on your phone, or you might be logged in to a cloud service you use to store your back-ups or work information. As we did in the previous lesson of this module, we do recommend that you avoid keeping work-related information on personal devices, however, sometimes it might be important for you in order to be able to perform your work duties while away from keyboard, or while on the go.

In this chapter, we will speak in more detail about securing the access to your devices, with a focus on your personal smart devices.

To begin with, if you are not using a **secure lock screen** already, you should start doing so. From security reasons, to simply not being able to unlock your screen while your device is in your pocket, or to prevent a child deleting information by

[34] https://en.wikipedia.org/wiki/Salt_(cryptography)

[35] https://support.microsoft.com/en-us/help/4026923/windows-10-create-a-local-user-or-administrator-account

[36] https://www.lifewire.com/create-user-account-in-windows-7-3506832

mistake, setting up a lock screen is a must. There are various options to secure the access to your smart device available, depending on your device. Most commonly, you would at least have the option of a pattern or password unlock. Some smart devices have fingerprint scanners as well, which is a good option if you really don’t want anyone else being on your phone or tablet.

We recommend passphrase rather than a pattern for several reasons. Firstly, we come up with relevantly simple patterns for unlocking our devices, so it would be easier for someone to guess your pattern. Secondly, when using a pattern, quite often your finger will a leave a smudgy trace on the screen, showing what the pattern is – cleaning your phone screen often will most likely not do the trick of covering up the revealing smudges as you most likely will unlock your phone. Those traces are easily visible if you look at the device screen at a certain angle and lighting. To avoid this, we recommend setting up some sort of non-trivial passphrase.

As for your laptop or PC, your smart devices need to be configured to **automatically lock the screen** when idle. This will ensure that if you leave your device on your desk or in the classroom, most users will not be able to browse through your phone.

We also suggest that you lock your SIM card. If your phone gets stolen, simply removing the SIM card and using it on another device might cause quite a lot of trouble. This is why, we suggest you set up a SIM card lock (PIN number, which should be harder than four zeros) that will need to be entered before the SIM card could be used. This doesn’t have too much to do with protecting personal data and privacy, however it is a tip that might save you some trouble.

An option which we hope you don’t need to use, but is good to have configured is the **“Find my Device” setting**. Google offers such service for Android devices, but there are similar options in store for other smart device operating systems out there – for instance the “Find my iPhone” for Apple users. With this option you are able to track down your device, call it, send a message to it to show on the screen or remotely reset your device if there is no chance of getting it back.

You can use this option even if you have not previously configured it, however, if keeping work-related information or personal data on your phone, we encourage that you get familiar with the options that this setting provides you as soon as possible.

If you realize that you have lost your device, you might be able to quickly locate it through this app, make sure your personal data is safe by locking your phone, setting up a recovery message or remotely purging your data. If your phone has been stolen, and you have not set a lock-screen method, a thief might be able to reset your phone before you attempt to locate it, which will make you unable to use this option to retrieve your device.

Photo 2 BiljaST from pixabay (www.pixabay.com)

If you have set up **Two-Factor Authentication** on your Google account (which is a good thing in general) you might run into the problem of having to input a six-digit code before getting access to your account to use the “Find my Device” app. Two-Factor Authentication usually relies on sending you this six-digit code to your phone, which would be an obvious issue. Enabling Two-Factor Authentication is the first step to having a secure mobile device, so this is a good thing, however in situations, such as this one, it is good to have backup codes saved somewhere safe, preferably in a password manager, for situations such as this one. Most services that offer two-factor authentication provide several back-up codes anyway, upon enabling the Two-Factor Authentication option. Keep them somewhere safe for situations, such as this one, and don’t give up on using multi-factor authentication.

Check out this wonderful article by How-to-Geek[37] for more information about Find my Device.

Last but not least, sensitive data which is saved to internal storage or SD card should be secured. As with data on computers, we recommend **encryption**. You can encrypt your folders and files with various software available and free to use and this will save you a lot of worries, if your phone gets stolen and you are worried that you have some files, containing personal data of your students on your SD card, for instance.

[37] https://www.howtogeek.com/170276/how-to-locate-your-lost-or-stolen-android-phone-and-wipe-if-necessary/

ENCRYPTION

We cannot talk about protecting information and personal data without mentioning encryption. Encryption is a topic, which is discussed in details in Lesson 3 (Protecting digital content) of Module 1 (Protecting devices and digital content), so here we will just recap some basic principles about encryption and mention it as one of the tools we recommend for protecting personal data and privacy.

Even if you are not mindfully using encryption, you are most likely using it anyway. Most banking and financial management applications, for instance use it, as well as some chatting apps like Viber and WhatsApp. You open websites with https, which we hope most of the websites you regularly visit are. In HTTPS, the communication protocol is encrypted using Transport Layer Security (TLS), or, formerly, its predecessor, Secure Sockets Layer (SSL).

What encryption does is it reformats regular data into secure code using mathematical equations and cryptographic tools to encrypt and decrypt messages. This makes it very hard for someone else to read your messages or eavesdrop on your conversations or transactions.

There is a saying in the IT sphere that you should dance like nobody's watching and encrypt like everyone is. We do recommend that everything that you don't want an unauthorized person looking into, that you encrypt.

Basically, what encryption does is it protects two types of data – data at rest and data in transit. Data at rest refers to data on your hard drive, for instance and ensures that if your laptop is stolen, the data will be unreadable. Data in transit may refer to data transferred to a cloud service, or through e-mail or between browsers – encryption helps that if the traffic is being intercepted, that your information is cannot be read.

Photo 3 TheDigitalArtist from pixabay (www.pixabay.com)

There are free and reliable tools you can use to encrypt your information both on your computer and on your smart devices, for instance the excellent open-source tool VeraCrypt[38].

Depending on the use case, there might be various options:

- The most basic way to protect computer hard drives and the data on them is full disk encryption (FDE). This means that all data which is on your computer or an external hard drive or memory device is automatically encrypted.
- You can also encrypt individual folders, disk partitions and files. This is more time consuming, but it is a good option if a folder you are encrypting, for instance, will not stay in its place of origin – like when you are uploading this data to a cloud server. It is very useful for backing-up information and keeping it safe somewhere besides on your hard drive.
- You can pre-encrypt data that is syncing with a cloud service, which will make it unreadable by the cloud or anyone who hacks into it. Any unencrypted files that are stored in your computer in this case are considered vulnerable.

There are also other types of encryption concerning e-mail encryption such as end-to-end (E2E) encryption which obscures the messages so only senders and receivers can read it, encrypted web connections (HTTPS as discussed above) or encrypted mail servers (Secure/Multipurpose Internet Mail Extensions - S/MIME).

You can have e very secure infrastructure overall in your school, however while good infrastructures and strategies could be very effective to protect you in your local network, encryption is what saves you in the long run. If you have been putting off adopting encryption as a part of your security policy, there is no need for further delay.

SECURELY DELETING DATA

This might not be new information to you, but generally when you delete information from your computer it is not always really being deleted. Most times, when you delete files, you are getting rid of the reference to those files from the file system table, however this file will still continue to exist on your disk. If you are using a hard disk drive (HDD) deleting a file, the master file index simply tags it as belonging in the recycle bin, not the folder. The actual data remains intact until we overwrite that spot on the drive. Since the storage space is random, this can take a while. If using a Solid State Drive (SSD), which are known to constantly reorganize files to optimize storage, the information may eventually be overwritten, but again it may not.

[38] https://www.veracrypt.fr/en/Home.html

This is especially valid for Windows and as any of you advanced Windows users know, files that are nominally “deleted” by Windows usually remain recoverable on your hard drive. This leaves your deleted data very vulnerable to being recovered, which is especially traumatic if it comes to sensitive or personal data, that you do not want being retrieved – for instance if you are going to be giving away a device to be used by somebody else or if you downloaded something personal on a public computer.

The good news is that there are many free software tools that help you to make sure you securely delete files, so that they cannot be recovered like Eraser[39], Blank and Secure[40] and many others. Be careful if using an SSD as some cleaning utilities like CCleaner or DBAN are made for magnetic disk drives and won't work on SSDs. Also, cleaning information from SSDs might be harder.

SSDs are different from regular HDDs, primarily because they use different technologies to record data. An HDD is a spinning platter that writes with a moving mechanical arm. An SSD is more akin to a flash memory stick, storing information in cells. To write new data to a cell, the drive must first erase existing data. When you delete a file, a TRIM command immediately removes all reference to that file. However, TRIM only works on internal solid state drives, not on external devices.

A group of engineers at the University of California[41] studied data purging from an SSD. Trying to securely erase a single file left behind anywhere from 4 to 75% of the information. And it’s tough on the drive and might actually damage it. This is why disk encryption for SSD users is even more crucial. A helpful article for SSD users is this one[42] by MakeUseOf.

Most of the applications for securely deleting files from your computer will be useful if you want to wipe a USB clean (you might also choose to format it, which we recommend). Yes, the same issue does apply to external memory devices. Simply clicking the delete button on the files in your USB. Windows and MacOS operating systems come with an in-built format option that can erase everything from an external storage device, usually accessed by right-clicking on the memory device and choosing the “format” option. Just make sure you do not format your internal hard drive by mistake when formatting a USB device or an SD card - it is an easy mistake to make and there is no going back. This tutorial by comparitech.com[43] will help you learn more about the process of formatting your external memory devices and will suggest some software tools for secure removal of files.

[39] http://eraser.heidi.ie/

[40] http://www.pendriveapps.com/freeraser-portable-file-shredder/

[41] https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf

[42] https://www.makeuseof.com/tag/7-terms-need-know-buying-new-ssd/

[43] https://www.comparitech.com/blog/information-security/securely-erase-hard-drive-sd-card-flash-drive/

SHREDDING

Shredding is the act of destroying physical documents, containing sensitive or personal information in a way that makes it hard or impossible to be retrieved by other parties. It is a secure and economical way to keep no longer needed documents read by the wrong people. We have all heard of cases of sensitive documents being thrown away by companies and further retrieved by somebody else. This might result in very bad lawsuits, financial loss and sensitive data exposure.

This is undoubtedly a very unpleasant situation for everyone involved. The simple act of throwing away old documents is not likely to provide you with the security level needed for the adequate protection of your students' privacy or the confidential records of your school.

We all know how much documentation a school produces, and we need to make sure that it is securely disposed of if and when no longer needed. Furthermore, secure disposal of physical documents is no longer optional – it is the law. If your school does not have a shredder (the actual device that you put the paper in and it curs it into strips or other fine particles) consider raising the topic with your school administration, legal department or Data Protection Officer (DPO).

Taking the time to shred unnecessary documents is a bit of a painful process, however the benefits are immense. If your school does not have a shredder or is not ready to purchase one yet, there are services such as on-site shredding, which allow you to rent a shredder for a limited time and some will shredding vendors will also offer to do the shredding for you, after signing a non-disclosure agreement.

A positive side of outsourcing this service, should you chose this path of getting rid of documents, is that the school employees will not be taken away from the specific job they were hired to do when shredding documents. Shredding documents might be a distraction and might put your school at risk if it is not properly executed.

There is another plus side to partnering with a vendor that possess expertise and infrastructure creates a defensible document destruction program. It exhibits due diligence of your school by implementing disposal practices that meet your legal obligations and ensure compliance with pertinent regulations and industry standards. This might be of importance if applying for certain projects or funding programs.

If considering buying a shredder, we encourage you for one that will also shred other documents, such as CDs. This way, you ensure that even digital copies of obsolete information are properly disposed of and cannot be retrieved. Such shredders will likely save more time for you in the long run as well, as many of them have the capacity to destroy documents that are paper-clipped or otherwise bound together, which will result in less time for preparing your documents for destruction.

Another and a more cost-effective, but more time-consuming way to get rid of paper documents is purchasing a multi-cut pair of scissors. This might be a solution if your school is not willing to commit to purchasing a shredder machine or subscribing for a shredding service, but you want to ensure that at least the documentation you are producing and wanting to destroy, is being destroyed properly.

Photo 4 by stux from pixabay (www.pixabay.com)

Shredding documents is not a 100% guarantee for securely getting rid of unneeded documentation. There have been instances of reconstruction of shredded documents or the so-called practice of “unshredding”. The reconstruction of a shredded document is a very resource consuming practice, and the chances of happening are not as high. Getting rid of documents by just throwing them away will very likely result in them being at least read by someone else. Shredding them minimizes the risk for that and makes it very hard for them to be reconstructed and used against you by malicious parties.

If getting rid of your personal documents at home, a pair of multi-cut scissors is likely to do a good job for you, assuming that you don’t produce a lot of documentation in your home on a regular basis. People have been known to recycle shredded documents by using them for animal bedding (hamsters, Guiney pigs and other rodents), use them for the fireplace if such, or if documents are not too sensitive as package insulation. Otherwise, if well shredded, they could be recycled in the paper bin.

SECURING WI-FI NETWORKS

There have been quite a few instances where innocent Internet users have been arrested for uploading child pornography or sending harassing e-mails when in reality, their email accounts or wireless connection where hacked though the unsecured Wi-Fi networks that they had at home. At your school, your system administrator would be the one taking care of that, however, if working from home, you need to know that external parties might be able to access your private information through a poorly secured Wi-Fi network.

This may sound very scary, and it is, however there are simple steps you can follow in order to make your home network a bit more secure, so as to prevent neighbors stealing your Wi-Fi or even worse, cybercriminals benefitting from your lack of security to take over your devices, steal your personal data or conduct criminal acts on your behalf. The first thing you have to know is that you are not powerless and that even basic security measures can make a tremendous difference when it comes to your protection.

This is **not entirely an offline protection issue**, however the measures you take to protect yourself are the measures that will protect you also while you are offline and someone else might be willing to take over your network while you are away.

The first thing you have to do is to **change the default password** of your home router, if you haven't already. Don't put trivial passwords that are easy to break. Change your passwords from time to time, especially if you feel a change in the quality of the connection or if the data LED of your wireless router is constantly blinking and none of the family members are using the Internet at home. The password, you can change from your router settings panel, below we discuss you find out how. Meanwhile, you can entertain yourself by browsing through this list[44] of default usernames and passwords of various network equipment. If you find anything you recognize there, you need to change it immediately. And never run an open (not password-protected) connection.

Make sure, when setting up your password, to choose the **WPA2** option as discussed in the previous lesson in this module. You can refresh your knowledge about the difference between WPA2, WPA and WEP with this great article from How-To Geek[45]. Passwords protected with the WEP encryption are a lot easier to brute-force attack than those encrypted with WPA2. Chances are that hackers are not checking out your home Wi-Fi networks for vulnerabilities, although – you never know, however, there is no reason to not use the stronger WPA2 protocol unless and unlikely you have a very old device that does not support WPA2.

Same goes with setting WPS (Wi-Fi Protected Setup). WPS offers you to type a small PIN number instead of a more complicated password. PIN numbers are easy to brute-force and while a number of routers will time out an attacker after they a

[44] http://www.cirt.net/passwords

[45] https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/

certain number of brute-force attempts, that hasn't stopped more ingenious WPS attacks. It is easier to just disable it entirely and rely on a password.

If the **SSID** (or your Wireless Network Name) is still set to default, it may reveal immediately the brand of the equipment you are using or at least show carelessness as to maintaining your wireless settings. Don't change it to something which might reveal your identity to your neighbors or some random person on the street, of course.

Another thing you need to know is how to access your **wireless routing settings**. Usually, by typing in 192.168.1.1 in your web browser and entering your SSID and password, you will be able to access your router settings. Check in with your router's user manual (should be available online in case you are not keeping your paper manual or the box for the router) if this is not working. Here are some links to some of the more popular router brands, where you can download or view your user manual - Cisco[46], Linksys[47], Netgear[48], Apple AirPort[49], D-Link[50], TP-LINK[51].

Nextly, while still in your settings panel, you need to know that your laptop computer, mobile phone, tablet and all other gadgets have a unique MAC address. You can find the MAC addresses of your devices in several ways, however, the easiest way to find your mobile devices' MAC address is if you check their Settings page. On your laptop you can open a command prompt and type ipconfig/all to find the MAC address of your computer's network card (should be listed under Physical Address). Look for the MAC addresses in your router's DHCP Client Table under the **Wireless Mac Filter** section. There, you can add or remove the MAC addresses of all your known devices so that only whitelisted devices can access your wireless Internet. This is a bit inconvenient when you introduce a new device to your home network, however it is a problem, which is solved in less than 5 minutes and is worth the trouble.

A further topic when it comes to your home Wi-Fi network is firmware. Some home routers have **firmware update** options in their settings menus and some might even notify you about a new firmware update the moment you log into their apps or web-based user interfaces. You want to make sure that your router is running the most up-to-date firmware. It is the same as updating your software – obsolete, unmaintained software is likely more vulnerable and has known vulnerabilities. Most people who maintain the software of their computers will tend to rarely check about the firmware of their routers.

Unfortunately, while some routers will download the firmware automatically, when you access the settings page, it is also possible that your router will require you to upload new firmware yourself. If so, you'll have to download the right firmware from the router's manufacturer and manually update the router by browsing for

[46] http://www.cisco.com/cisco/web/support/index.html

[47] http://www.linksysbycisco.com/US/en/support

[48] http://www.netgear.com/support.aspx

[49] http://www.apple.com/support/airport/

[50] http://www.dlink.com/support/

[51] http://www.tp-link.com/support/download.asp

this firmware file and starting the update process yourself. You'll have to do this each time you want to update your router with new firmware, which means you'll have to check for new firmware fairly regularly, perhaps a few times a year. It is a pain, but it saves you from a lot of threats. You could also consider upgrading your router.

Photo 5 by Fotocitizen from pixabay (www.pixabay.com)

A few other tips you might find useful for securing your home network:

1. **Anything you don't need – disable**. If your router has remote management or **remote administration** options, you probably would not use them, so make sure they are disabled. If you are not running **FTP** servers from home – disable the option. You can enable it later if needed. If you are not **SSH**-ing into home or you are not needing to access your router through **Telnet**, consider turning them off. You can always undo that if needed.
2. Consider disabling **UPnP** if you are not gaming or using torrent services. Check out this website[52], dedicated exclusively to UPnP attacks. Even if you are gaming or using torrent trackers, you still can disable UPnP and manually forward ports. More information on manually forwarding ports is available here[53].
3. If you are having smart devices or if you are giving access to your network to guests coming into your home, consider putting up a **separate network** for them. It is a feature to implement, security-wise. This means that your router will set up a second SSID for your guests or IoT devices and any device connecting to your guest network will be separated from the devices on your primary network. You can further adjust what your guests will see in terms of your primary network and what they will not. You can connect your less

[52] http://www.upnp-hacks.org/upnp.html

[53] https://www.lifewire.com/how-to-port-forward-4163829

secure devices on this network as well. If you are curious and would not mind going a little bit overboard security wise, you can also segment off your network with separate **SSIDs and VLANs** – more information is available here[54] and here (aczlan's comment)[55].

4. While you are on vacation or away from home for a longer period of time, **switch off your router**. You will not be using it to connect to the internet while away, so do not leave it on when you wouldn't be needing it.

MONITORING AND CONTROL

Security monitoring and control is highly specific, yet broad topic in cybersecurity. We will not go into detail about it or about industry-level practices here. With this topic, we would like to point your attention at the fact that maintaining a good level of security is a process which takes mindfulness, habit-forming, vigilance and continuous improvement and attention.

We recommend that you schedule time every week to review your security practices, take time for back-ups, cleaning up outdated software and data and maintaining your devices. All of those practices that are recommended for protecting your information and personal data, both on and offline, require continuous maintenance, and while some of them are a one-click task, most of them will require that you revisit and maintain them.

This time investment will, however, insure that you have a good grip on your cybersecurity habits. This will transfer to your work, your personal life, your family and your students and this way. Just by showing care and attention to those aspects of your digital culture, will enable you to lead by example and showcase the importance of this to the people around you. Moreover, it will give you a certain level of security in your own practice and will leave you better equipped and more confident in your safety.

We all have days at work, when we have less to do. Take this time to ensure the safety of you and your students. Updating software should not take you more than 15 minutes if done on a regular basis. Cleaning up your desktop or maintaining it clean is a few minute effort as well. Shredding documents and securely deleting information from your PC will require less and less time after the initial time investment and effort and will take less out of you with time. Encrypting your information is a legal obligation – take your time to ensure your compliance with it.

Securing your mobile device will save you a lot of nerves and worries, should something happen. Consider spreading those practices in your family as well and raise your children with cybersecurity mindfulness and digital responsibility practices to not have to face easily avoided issues and having to ask yourself the question "why didn't I do that". We promise, it is worth it.

[54] https://www.routersecurity.org/vlan.php

[55] https://forum.openwrt.org/t/multi-ssid-wifi-on-different-vlans/23359/4

Photo 6 geralt from pixabay (www.pixabay.com)

SUMMARY

The technology, which we use every day and somewhat take for granted, has changed our lives and our work in many positive ways. The impact technology has on our social, work and personal lives is tremendous, but with all the positive impacts, we remain responsible for how we maintain and ensure our safety using it.

Securing your personal information and data, as well as the personal data of your students is a step you legally, morally and emotionally need to take, in order to feel secure at your day to day live. We cannot ensure the 100% safety on any device, but having good cybersecurity habits might ultimately be the thing that makes the difference and ensures our peace of mind.

In this lesson, we looked into some of the basics of protecting your data offline and securing your home network. Things, such as some basic tips and cybersecurity practices will undoubtedly come in handy when you start applying them, if you haven’t already. Encryption will provide you with security with relation to the data you store and protect. Disposing of physical and digital files with some security aspects in mind will change the way you think about information and will indefinitely help you organize your physical and digital space. Learning to secure your own home network will help you appreciate the data you and your family generate and protect, and will showcase the meaning behind why personal data and protecting our privacy is important to us.

Adopting those security habits will help your overall cybersecurity awareness, will make you more confident and will help you understand the technology you use every day a little bit better. Most importantly, those habits will enable you to lead by example, transfer your knowledge to the people around you, help your students with advice and showcase the importance of taking care of your digital identity and your privacy.

Photo 7 by JanBaby from pixabay (www.pixabay.com)

LINKS, REFERENCES AND FURTHER INFORMATION

1. https://www.wikihow.com/Destroy-a-Hard-Drive
2. https://www.digitalcitizen.life/keyboard-shortcuts-incognito-private-browsing-inprivate
3. https://en.wikipedia.org/wiki/Private_browsing
4. https://en.wikipedia.org/wiki/Shoulder_surfing_(computer_security)
5. https://us.norton.com/internetsecurity-how-to-how-to-remove-gps-and-other-metadata-locations-from-photos.html
6. https://www.makeuseof.com/tag/3-ways-to-remove-exif-metadata-from-photos-and-why-you-might-want-to/
7. https://youtu.be/sB_5fqiysi4
8. https://youtu.be/D1dVhDYAv9E
9. https://lifehacker.com/the-beginners-guide-to-creating-virtual-machines-with-v-5204434
10. https://www.wikihow.com/Lock-a-Computer
11. https://www.youtube.com/watch?v=JuRQ55_G-eU **- PRIVATE VIDEO!**
12. https://youtu.be/cvZVHbBTPp4
13. https://www.windowscentral.com/how-manage-user-accounts-settings-windows-10
14. https://en.wikipedia.org/wiki/Salt_(cryptography)

15. https://support.microsoft.com/en-us/help/4026923/windows-10-create-a-local-user-or-administrator-account
16. https://www.lifewire.com/create-user-account-in-windows-7-3506832
17. https://www.howtogeek.com/170276/how-to-locate-your-lost-or-stolen-android-phone-and-wipe-if-necessary/
18. https://www.veracrypt.fr/en/Home.html
19. http://eraser.heidi.ie/
20. http://www.pendriveapps.com/freeraser-portable-file-shredder/
21. https://www.usenix.org/legacy/events/fast11/tech/full_papers/Wei.pdf
22. https://www.makeuseof.com/tag/7-terms-need-know-buying-new-ssd/
23. https://www.comparitech.com/blog/information-security/securely-erase-hard-drive-sd-card-flash-drive/
24. http://www.cirt.net/passwords
25. https://www.howtogeek.com/167783/htg-explains-the-difference-between-wep-wpa-and-wpa2-wireless-encryption-and-why-it-matters/
26. http://www.cisco.com/cisco/web/support/index.html
27. http://www.linksysbycisco.com/US/en/support
28. http://www.netgear.com/support.aspx
29. http://www.apple.com/support/airport/
30. http://www.dlink.com/support/
31. http://www.tp-link.com/support/download.asp
32. http://www.upnp-hacks.org/upnp.html
33. https://www.lifewire.com/how-to-port-forward-4163829
34. https://www.routersecurity.org/vlan.php
35. https://forum.openwrt.org/t/multi-ssid-wifi-on-different-vlans/23359/4

LESSON 2.4 - PRIVACY POLICIES AND DIGITAL FAIR PLAY

INTRODUCTION

The topic of copyright, authorship and GDPR compliance is a subject of continuous discussion but is, nevertheless, still an issue with lots of pitfalls and intricate details. Remember back in 2011 when a monkey took a few selfies[56] with the camera of the famous photographer David Slater and the copyright lawsuit, which followed, claiming that the monkey owned the rights to the photos it took with the stolen camera and that David couldn't use those images for profit? Might sound ridiculous, after all – we are teachers, using materials to help our students learn, however all of this matters when you developed your own lesson materials using photos taken by somebody else and distribute them among your students or make a presentation at a conference, containing pictures, showing the faces of your students.

The goal of this lesson is to provide you with a strong foundation on which you could build up your knowledge and uphold to the types of licenses, copyright, authorship and provide you with some common criteria for GDPR compliance with regards to teaching, as well as to encourage you to enter a dialogue with your school's data protection officer.

Along the lines of this lesson, you'll discover some general tips related to managing your digital identity and protecting it within documents and data produced by you for your teaching practice. Furthermore, you'll get familiar with common license types as well as some aspects and basic facts related to privacy policies and how you could apply this knowledge to help enhance your teaching resources and use it as a competitive advantage to suit your interests, needs and teaching purposes.

Last but not least, this lesson will provide you with some useful resources to deepen your knowledge on the subject, as well as helpful lists and cheat-sheets to support you find good content online, which you could ethically use to enhance your teaching practice.

Please note that **Be@CyberPro is NOT giving you legal advice** nor best practices in the field. This lesson provides you only with a fundamental baseline of educational materials to familiarize you with the above-mentioned and to guide you towards knowing what to ask about and knowing the right question. Those resources should be viewed critically and only as educational information of a generic nature and you should seek consultancy from your legal department, ethical committee and your school's data protection officer to help resolve doubts, issues or determine on the level of local legislation, best practices, approaches and advice.

[56] https://petapixel.com/2017/09/12/photographer-settles-monkey-selfie-copyright-lawsuit/

Photo 1 by Fernando Arcos from Pexels (www.pexels.com)

AUTHORING CONTENT AND COPYRIGHT

Creating educational resources for your students or sharing with them images, videos and text, sharing multi-media is part of every educator's not only academic life, but also personal life. Having a vast majority of sources and having a quick online access to many resources enables us to create unique and engaging learning content. However, now that we're able to create many more artifacts to engage our students in the classroom, it is essential that educators and students alike have a solid foundation of understanding about their rights and responsibilities, as well as the rights and responsibilities of content creators and owners, whose materials they use in their day-to-day life.

Teaching ourselves and our students responsibilities about the fair creation and use of online materials is not only a legal concern. It is a subject of the moral environment of the technological boom we are witnessing and concerns not only school materials and projects but also sharing materials and content online and is fully valid for the professional world our students will soon be entering into. In this context, educators should be able to serve as role models and serve as an example why and how **copyright and plagiarism** is part of their lives and lesson design.

Check out these YouTube videos for a more in-depth introduction:

- Copyright & Fair Use Guidelines for Teachers[57]

[57] https://youtu.be/kNBoBw39hAs

- Understanding plagiarism & copyright[58]

Before we begin with the topic of what copyright is and what does copyright cover, we should briefly discuss the difference between the terms plagiarism and copyright infringement.

Plagiarism, as defined by Wikipedia[59], is the "wrongful appropriation" and "stealing and publication" of another author's "language, thoughts, ideas, or expressions" and the representation of them as one's own original work.

Copyright infringement, on the other hand is, again by Wikipedia's definition[60], is the "use of works protected by copyright law without permission, infringing certain exclusive rights granted to the copyright holder, such as the right to reproduce, distribute, display or perform the protected work, or to make derivative works". Basically, copyright is here to ensure that a content creator has a control over the dissemination of their original work and may require some form of compensation or attribution for the viewing or the use of their work.

The two concepts are similar but legally, they differ and both the actions of plagiarism and copyright infringement are a subject of legal consequences, which makes it necessary in this world of shared information, to be able to recognize what and under which conditions could be used or shared.

So, **what does copyright mean and what does it cover**.

As per the definition of the Copyright Alliance[61], copyright is the collection of rights that automatically vest to someone who creates an original work of authorship – like a literary work, song, movie or software. These rights include the right to reproduce the work, to prepare derivative works, to distribute copies, and to perform and display the work publicly. The purpose of copyright is basically to provide content creators, regardless of the medium of their expression with the legal encouragement to continue to create. This encouragement means provision of property rights over their content, as well as some form of legal protection and economic compensation for their efforts in the case of a copyright infringement.

The copyright law protects any original product that is set in a tangible or digital form, be it an image, a sound, a video, a text or other media or mixed-media artifact.

There is no legal requirement that a copyright owner should register their work as copyright, or place a copyright notice on the work, to obtain copyright protection, according to the Copyright Alliance. This means that your original and creative lesson plan or educational infographic that is fixed in a tangible medium is

[58] https://www.youtube.com/watch?v=AOAZQjqcygw - **THIS VIDEO DOES NOT EXIST!**

[59] https://en.wikipedia.org/wiki/Plagiarism

[60] https://en.wikipedia.org/wiki/Copyright_infringement

[61] https://copyrightalliance.org/ca_faq_post/what-is-copyright/

automatically protected by copyright, and so is the original video that a student created or their graphic design project.

This means that, for example, a teacher’s original video lesson or a student’s original graphics or music compositions are protected by copyright. So are the most recent images, videos, and writing that others have created and shared both online and offline.

Ideas and facts are not protected by the copyright law as they are not creative works in the case of facts, or are not a tangible artifact, in the case of ideas. Some old works are also not copyright covered, due to copyright rights expiry (the duration of copyright protection can vary but it lasts until at least 50 years after the author's death). Check out this fact sheet[62] on copyright from the European Intellectual Property Rights Helpdesk (EHD)[63] for more useful information.

LICENSE TYPES

The good news is that there are **plenty of materials, sources and media you and your students can use for educational purposes** and we are going to talk about just this right now.

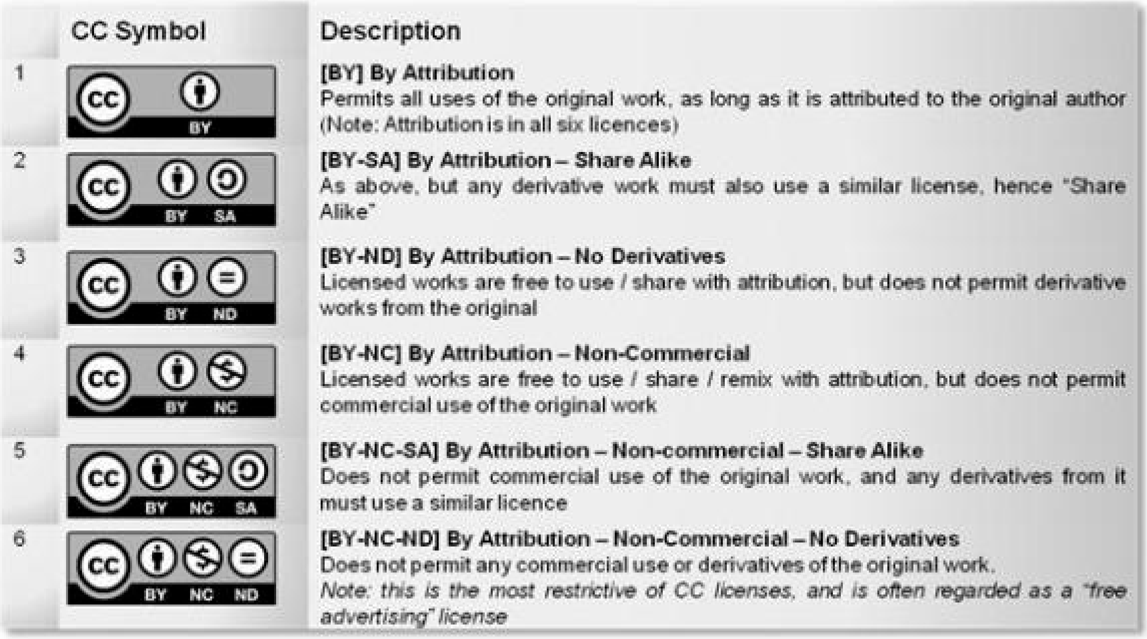
The first important term for you is **public domain**. This is a category of tangible artifacts that you could use for educational purposes without having to pay commissions for their use and without having to obtain permission for their dissemination. If a work falls into the public domain category, this means that the work is not covered by copyright or the authors’ rights over the content have expired. This includes any content such as many classical works of art, which are created before the second decade of the last century.

Another important term for you as an educator is the term **Creative Commons License (CC License).** The Creative Commons License is a type of open copyright license, which implies that the content creator grants users with the rights to use this content free of charge, upon fitting into certain criteria. More about the Creative Commons License is available in the Creative Commons Website[64] including information about the different types of Creative Commons licenses, as well as image searches, resources with free of charge content available for remix and reuse as well as information about proper attribution and much more. This website is an absolute staple for every educator, offering a library of free media resources and links to free content.

Free content, however, does not mean unrestricted use of content. For you, as an educator, who is using this information for educational purposes, this might not always apply, however it is important to know the different types of Creative Commons Licenses and their icons, so that you could choose the most suitable

[62] https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-copyright_essentials.pdf
[63] https://www.iprhelpdesk.eu/
[64] https://creativecommons.org/

content for your work. Below, you'll find a picture containing the six, most widespread Creative Commons License Types.

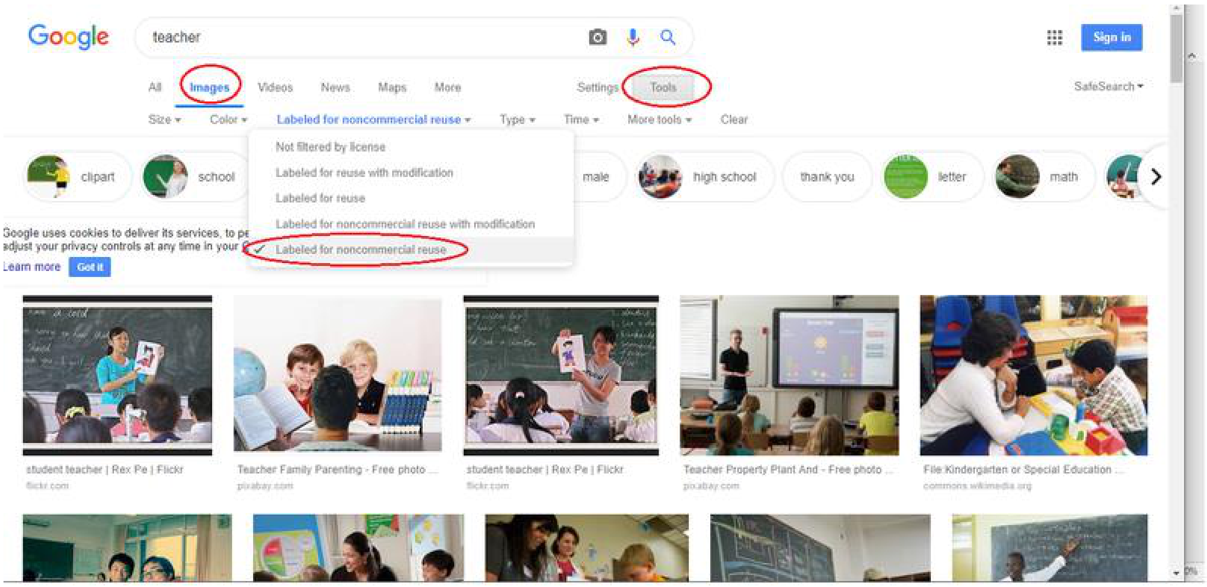


	CC Symbol	Description
1	cc BY	**[BY] By Attribution** Permits all uses of the original work, as long as it is attributed to the original author (Note: Attribution is in all six licences)
2	cc BY SA	**[BY-SA] By Attribution – Share Alike** As above, but any derivative work must also use a similar license, hence "Share Alike"
3	cc BY ND	**[BY-ND] By Attribution – No Derivatives** Licensed works are free to use / share with attribution, but does not permit derivative works from the original
4	cc BY NC	**[BY-NC] By Attribution – Non-Commercial** Licensed works are free to use / share / remix with attribution, but does not permit commercial use of the original work
5	cc BY NC SA	**[BY-NC-SA] By Attribution – Non-commercial – Share Alike** Does not permit commercial use of the original work, and any derivatives from it must use a similar licence
6	cc BY NC ND	**[BY-NC-ND] By Attribution – Non-Commercial – No Derivatives** Does not permit any commercial use or derivatives of the original work. *Note: this is the most restrictive of CC licenses, and is often regarded as a "free advertising" license*

Photo 2 Source of CC License Symbol / Images3: http://creativecommons.org/about/licenses/

As you can see from the above-mentioned image, the Creative Commons License permits free use, upon attribution and with certain restrictions.

A helpful tool for educators is the option, provided by many platforms, to search for resources labeled for free for non-commercial use. A screenshot below shows enabling this option for the Google Image search to find images, under the Creative Commons License for non-commercial use.



teacher

Labeled for noncommercial reuse

✓ Labeled for noncommercial reuse

Google uses cookies to deliver its services, to pe
adjust your privacy controls at any time in your

Google
Sign in
All
Images
Videos
News
Maps
More
Settings
Tools
SafeSearch
Size
Color
Type
Time
More tools
Clear
Not filtered by license
Labeled for reuse with modification
Labeled for reuse
Labeled for noncommercial reuse with modification
clipart
school
male
high school
thank you
letter
math
Learn more
Got it
student teacher | Rex Pe | Flickr
flickr.com
Teacher Family Parenting - Free photo ...
pixabay.com
student teacher | Rex Pe | Flickr
flickr.com
Teacher Property Plant And - Free photo ...
pixabay.com
File Kindergarten or Special Education ...
commons.wikimedia.org

Photo 3 Screenshot from a Google Search (www.google.com)

Another example is YouTube, where you can view and even download works under the Creative Commons License.

Photo 4 Screenshot from a YouTube Search (www.youtube.com)

Those are only two examples, however a lot of web platforms offer this search options. Don't forget, when browsing for content, to look through the filters and the advanced search settings of the platform you're using to see if there is the option to look for such content. If there is not an option like this, depending on the type of platform you're using to search for media content, you might consider to ask the platform's customer support if they have any plans for integrating such a search tool. This way, as a customer to this platform, you are proactively raising the topic of the importance of transparency, regarding the options for use and reuse of content and you are raising your voice.

Along with the lines of the content licensing, there are other types of licensing, especially targeted towards video clips, images, vector art and clipart known as stock contents. Those are commonly subscription-based services, which provide you the option to buy content for small monthly subscription fee or per image. Some websites, like vectorstock[65] or canva[66] offer free content as well under some restrictions and upon attribution.

A list of many free or low-cost content sources is available on the hubspot.com[67] blog for free and we encourage you to browse through the resources mentioned there and share them with your students.

[65] https://www.vectorstock.com/

[66] https://www.canva.com/

[67] https://blog.hubspot.com/marketing/free-content-marketing-tools-list

GDPR COMPLIANCE

We hope that thus far, we managed to convince you that protecting your students' privacy, as well as your own, is essential. Personal data protection means respecting one's privacy and their freedom to exercise their rights over their own data and identity – both online and offline.

GDPR, the General Data Protection Regulation aims at **protecting the fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data**. GDPR entered in force as of May 25th, 2018 in all member states of the European Union with the general goal to harmonize data privacy laws across Europe(REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL, 2016). Since the enforcement of the GDPR, there has been a lot of anxiety across Europe about the storage and processing of personal data – and not without a reason. However, there are a few things to know, as a teacher, that would significantly improve your awareness and experience on the topic of compliance with the GDPR and in this lesson, we intend to go over a few of them in brief.

Firstly and very importantly, there is **the concept of data protection officer** or DPO for short. With the GDPR now in force, most institutions within the European Union, including academic ones, are required to appoint a single Data Protection Officer. Make sure you **know who is the DPO of your school**, get in touch with them and converse about specific aspects of your practice, so that you make sure your work complies with the regulations of the European Union regarding the protection of yours and your students' data. Among the core duties of the data protection officer of your school is ensuring that employees are aware of data protection issues and requirements and their work complies with the national and European policies regarding data protection.

Your DPO should be able to clarify the concept of **what personal and sensitive (or special data) is** and under what conditions and how you can collect, store, process and destroy those types of data. There is generally a common understanding established for those two terms, which every organization expands upon based on their specific context. **Personal data** is any information that can help identify a person, such as name, contact details, as well as grades or other forms of school assessment. **Sensitive or special category of data** concerns data such as a person's religious beliefs, sexual orientation, dietary restrictions (which might reveal a person's religion), health conditions, etc. This data could be obtained only with the informed consent of the parents and the students and could be processed only under certain conditions. Read more about the special category of data here[68].

Photos, images and video may also contain personal data. A facial image is considered personal data. Additionally, other data such as location or date and time of capture and others (known as EXIF metadata) might be stored in the case of digital images. Even more frighteningly, high-resolution recordings might as well

[68] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

enable biometric recognition of the persons depicted. These cases are considered sensitive personal data by the GDPR. Ask your DPO in cases where you want to include images of your students in a presentation or share them in any other way with third parties.

There are two other roles, besides the data protection officer, the importance of which is highlighted by the GDPR, namely **a data controller** and **a data processor**. Both parties have different legal responsibilities and those roles can be performed by natural or legal person, public authority, agency or other body. As per the GDPR, the data controller determines the purposes and means of the processing of personal data – most probably, this will be the school itself. The data processor processes personal data on behalf of the controller and has to have a contract with the controller. A data processor could be a software product, an online environment you might use for tutoring or interacting with parents, as well as a single person, such as a photographer coming in your school to take yearbook photos – anyone who performs operations such as collecting, storying and disposing of data. If you process students' data, be personal or sensitive data, as most teachers do, you enter the role of a data processor.

As a data processor, you enter in a very delicate role in protecting your students' rights over their personal data. A few important tips that could help secure your students' data:

1. Use only **legal software** and get yourself familiar with this **software's privacy policy**. If in doubt about the compliance of a certain piece of software with the GDPR, report to your DPO immediately. Know **what personal or sensitive data your students reveal** using this software. Encourage them to use only legally obtained software on their home computers as well by informing them on the risks arising from the use of illegitimate software.
2. If you are using educational software, which requires your students to create user accounts, **promote protecting their data** by pseudonymising their real names and encouraging them to critically assess what information shared by them might be considered personal or possibly revealing their identity.
3. If you are considering **to introduce a new software product in your school, you will need to inform your school's DPO in order to make sure that it is done compliantly**.
4. Discuss with your DPO what **a data breach** is. Understanding what constitutes a data breach is of paramount importance and a legal obligation for you and if you suspect one has occurred, you are obliged to report it to your DPO.
5. **Encrypt** documents and files containing personal and/or sensitive data. Encrypt your work computer or the folders containing personal and/or sensitive information, store personal data on school equipment only, use strong passwords, and set your devices to auto-lock after five minutes of no activity.
6. Be **cautious with mobile storage devices** – encrypt them or the data you transport using a USB stick and know that a lot of malware could be transported through USB sticks.
7. Update your **anti-virus software** regularly.

8. Be mindful of your **online communication**. Do not include personal data within e-mails or if you must, send it as an encrypted container. Always use your work devices and profiles for work-related communication. Be careful when opening and replying to e-mails.
9. **Inform yourself** – learn more about cyber hygiene and protection and strive to learn more about GDPR compliance. Make sure to browse the GDPR-related resources in the end of this lesson.
10. **Make sure to obtain informed consent from the students and their parents** for out-of-the-ordinary collection of data, such as surveys, projects, interviews, etc. Check with your DPO what data collection that you plan to perform requires that you obtain informed consent from the parents and the students themselves.
11. **Learn how to hide EXIF metadata from pictures** – tutorials that can help you and we recommend are this one[69], provided by Norton and this one[70], provided by MakeUseOf.

Last but not least, encourage and promote responsible data handling and data protection among your students. Explain and work with them to understand the importance of identity respect and the value of data. An engaging way to involve your students in a discussion and reflection on the topic of data protection is the Cyber Chronix[71] mobile game developed by the Joint Research Centre[72]. The game is designed to introduce young people to concepts including the notion of personal data, the right to be forgotten, personal data breaches, the right to data portability and informed consent. Players are taken to a futuristic planet several light years from Earth. The aim is to help their character to make it to a party, while they encounter several data protection-related obstacles along the way.

If you would like to learn more about GDPR and GDPR compliance, contact the DPO of your school, the legal department and the ethical committee of your school, as well as consider.

PRIVACY POLICIES

Privacy and the right over one's own data are among the core principles that lay in the foundations the European Union. We, as teachers in the European Union are required to abide by the laws of the Union to protect and respect our students' rights over their own data and identity. This is among the European Convention on Human Rights'[73] core statements and is part of the EU legislation that member countries have to respect.

[69] https://us.norton.com/internetsecurity-how-to-how-to-remove-gps-and-other-metadata-locations-from-photos.html

[70] https://www.makeuseof.com/tag/3-ways-to-remove-exif-metadata-from-photos-and-why-you-might-want-to/

[71] https://play.google.com/store/apps/details?id=ec.europa.publications.cyberchronix&hl=bg

[72] https://ec.europa.eu/jrc/en

[73] https://en.wikipedia.org/wiki/European_Convention_on_Human_Rights

In this part of the lesson, we discuss privacy policies mainly in relation with web-platforms, digital tools, programs, instruments and applications and we discuss some of the most crucial aspects of them with relation to practicing the teaching profession.

We would like to highlight the importance of taking the **issue of introducing new software for educational purposes** in your school. If you would like to introduce new software for your learning environment, the most crucial step is to **familiarize yourself with the privacy policy** of the software and **get in contact with your school's legal department, ethical committee and your DPO** of your school to make the decision on whether this software is appropriate for school use or not.

Firstly, a few words of introduction on what a privacy policy is and what you as a teacher have to know about privacy policies, before event talking to your legal department about introducing a new software tool in your classroom.

A **privacy policy is a legal statement that discloses how and what the issuer of the software and potentially (and most probably) third parties manage, gather and disclose in terms of user data**. As we already know from the GDPR compliance chapter of this lesson, **personal data** is any information that can help identify a person, such as name, contact details, as well as grades or other forms of school assessment. **Sensitive or special category of data** concerns data such as a person's religious beliefs, sexual orientation, dietary restrictions (which might reveal a person's religion), health conditions, etc. A privacy policy in other words, should provide sufficient information about what data is collected, kept confidential, shared or even used for profit.

A privacy policy could be accompanied by **data use statement**, which would indefinitely provide more detailed information about the issue of what, how and for which purposes is collected. **Make yourself familiar with a software's privacy policy and data use statement (if applicable) and bring them along with you for the discussion with the legal department, ethical committee and DPO of your school.**

What to look for in a privacy policy?

A privacy policy, as per the "Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data"[74] of the Organisation for Economic Co-operation and Development (OECD)[75] recommends with regards to privacy policies that they should provide 1) notice should and when someone's data is being collected and for what 2) purposes this data is collected. Privacy policies should ask for 3) consent for this data being collected and processed and inform on the 4) security measures applied to protect the stored data. Every privacy policy should further inform on any 5) data disclosure and should be granted 6) access and control over their data at all times.

[74] https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

[75] https://www.oecd.org/

Last but not least, the software issuer should be able to disclose within a privacy policy a clear 7) accountability mechanism, where they state how they will inform in a timely manner all users in case of a security breach concerning their privacy and provide them with a mechanism through which users could hold the data collectors accountable for privacy mistreatment.

After making sure that all of these points are present in the data policies and data use statements of the software of choice, get yourself familiar with **your school's policy on selecting new educational software**. Follow this policy's guidelines and contact the people responsible for making this decision.

There is a chance that the software you would want to use is **already approved by your school** and is being currently used by a colleague. In this case, ask for anything that you should know about the use of this software in an educational context to ensure the ethical and legal treatment of your students' privacy.

All of this so far takes under consideration both online and offline software products that you suggest being used for your classroom purposes. However, it is not uncommon that we as teachers, are often confronted by our students or parents regarding the choice of software used in the classroom. Be prepared for such dialogue and have your reasons behind the choice of this software, including **knowledge about software tools that are already used in the classroom and their privacy policies**. Examine the software that is already used in your classroom critically. Some software products might have been used in your school for years, but that doesn't necessarily mean that they are compliant or that you could ignore making yourself familiar with their privacy policies and statements regarding the treatment of your students' data.

When browsing through privacy policies, be careful and **look for terms such as FERPA (Family Educational Rights and Privacy Act), COPPA (Children's Online Privacy Protection Act), GDPR (General Data Protection Regulation) or PPRA (Protection of Pupil Rights Amendment)**. Converse with your legal department about potential non-compliance with your school's data protection policies.

There is also a possibility that a **student of yours wants to use a new software product for an assignment** or school project. It is important that you do not discourage your students to expand beyond the tools in the school curriculum and that they explore other educational opportunities besides the one in the classroom, however this holds certain dangers and responsibilities on your side.

As an educator, you cannot officially endorse the use of unapproved by the school software tools. If the use of such product is not compatible with the purposes of the assignment, this is rather clear as situation. But if it is, this is a great opportunity to teach your students about the considerations that need to be taken into account when using a new piece of software.

Firstly, we recommend that you ask that your student inform their parents about this and that together with the parents, they install or go through the process of initiating the use of a new software. It is a great opportunity to involve your students in a discussion about data privacy and ensuring their data's safety. Ask your student if they have to create a profile to use the software or platform they want to use for their assignment. What information do they have to provide, in order to be able to use this software and are they OK giving away this information. Data could be anything from names and e-mail address to financial information, age or address – would your student's parents consent to this information being provided and does the software you plan to use require your parents' permission?

Engage your student in dialogue on whether the information they share through using this app is shared with anyone else – who can view their name, for instance? Tell them to check in the privacy policy or the data use statement? Does this app collect further data? Further data could be obtained through imagery – do you share your personal photo somewhere? It could also represent location information – do you share your location or your country? Does this app collect GPS data for some reason?

Those are questions you yourself have to consider if planning to introduce a new piece of software to your classroom, so you apply the same principles of precaution you would otherwise, when advising your students. Remember that it is not a problem if a student can't give you an answer to all of those questions right away. If possible, ask him to write these questions down and research them for a day or two and have them talk to their parents about any doubts they might have. It is a great learning opportunity for them about their own rights and their own stance on providing personal data to use software products. Make sure you let your students know that this is their data and they have right over it.

TEACHING RESPECT AND RESPONSIBILITY

It is fairly common for teachers to be scared to bring out the topic of digital responsibility if they lack the tools and knowledge on how to keep students safe and educated about the digital world. This makes the most important step towards teaching your students responsibility and digital culture **to expand your own knowledge and practice what you preach**.

The Be@CyberPro teachers' materials are a great place to start, however we recommend that you dive deeper, looking into the resources recommended at least. The more you delve into the subject, the more you will increase your recognition of knowledge gaps, generational gaps and places where you lack understanding in a global context. Filling in those gaps by researching on your own, by signing in to dedicated trainings or by finding and talking to knowledgeable people in the field will give you the confidence to talk about those subjects and know your own reasoning behind the importance of a good digital culture.

Practicing the best practices yourself, on the other hand, will **cultivate your own digital hygiene habits and teach by example**. Seeing that you adhere to the principles you speak about, will convey them the sense of value, which is more powerfully manifested by example, rather than with words.

We know that it is not all that easy to incorporate new material in the already tight-knitted school curriculum. Although we recognize a need for dedicated lessons on cybersecurity literacy and issues, we recommend that you start **incorporating those topics seamlessly, on an everyday basis, within your regular lessons**.

The best way to ensure that your students are familiar with the rights and responsibilities of digital citizenship is to make digital citizenship a part of their regular lessons. As your classes would likely involve on some level working with technology anyway, you could create the habit of practicing good digital culture. For instance, if your students have to make a presentation on a given topic, demand that they include all copyright and intellectual rights as footers in their slides and ask that they highlight them with a certain color. If they have to work with a given software, you might ask them to make themselves familiar with the privacy policy of the software or ask them to make a summary of what personal data they have shared with a software used for school purposes. Anytime your students give you a written assignment, demand that they include the sources of the photos they have used and provide them with information about online places, where they can obtain copyright-free images.

You can engage younger students to reflect on how would they feel if someone would make profit from their hard work, if it was done without their consent.

We also recommend using interactive websites and applications, such as Respect for Copyright[76], which provide age appropriate and engaging content to help teachers teach their students about their freedoms, rights and responsibilities within the digital world.

Teachers need to be able to understand and teach students about copyright, public domain, fair use, and Creative Commons. To the aid of teachers in this mission come numerous great resources, lesson plans and applications to help young adults build the stable foundation needed to make wise choices online.

- Common Sense Education[77] – fantastic lessons and animated videos on copyright and fair use.
- Teaching Copyright[78] – information on public domain
- Creative Commons[79] – here you will find high-quality, engaging videos about copyright and Creative Commons licenses

It is important that you share with your students lists and resources with content which is free to use for educational purposes. One such list is the hubspot.com blog[80] which was mentioned above. Other useful lists you could disseminate among

[76] http://respectforcopyright.org/
[77] https://www.commonsense.org/education/lesson/copyrights-and-wrongs-9-12
[78] https://creativecommons.org/about/
[79] https://www.teachingcopyright.org/
[80] https://blog.hubspot.com/marketing/free-content-marketing-tools-list

your students are mediacommons website[81], techsavvyed.net[82], buffer.com[83], blogtyrant.com[84], resignal.com[85], sitepoint.com[86] to name a few. Make sure your students have the resources they need to fairly use content for their assignments and academic life.

As mentioned previously in this lesson, everyone who creates an original and tangible artifact, regardless of the media form it is in, is creating a copyright work. This means that your students' original work is copyrighted. Make sure, if you want to share your students' work, show it to colleagues or reuse it, to ask for their permission. This will give them the sense of value for their work and will showcase the importance of copyright. Many students don't really care about their own copyrights or don't know about them and it is important for them to know that copyright laws protect them as well and aim to encourage them to create further and explore their creativity through various mediums of expression.

Some students might already be familiar with that, as it is not uncommon for teenagers nowadays to post creative content on different platforms and even earn money from their work. If you have a YouTuber as a student, or know about someone, who is already selling their content online, it might be a good idea to involve them into the process of ducation their peers about their own copyrights. Make a short seminar with them where the teenager who is fluent with these concepts could share their expertise with their peers and with you as well. Students are likely to show more interest to the words of a peer who already understands the importance of copyright, rather than yours.

Educate your students about the GDPR and about their rights over their own personal data. Make them familiar with their right to retract their data and help them realize the importance of their data. Talk about them with the different types of software you use for educational purposes and summarize the privacy policies for them, so that they know it is something that is worth mentioning and worth talking about.

Last but not least, do not forget that teaching students about digital fair play is not only a teacher's job. It is a common responsibility that we as a society share. Talking to parents to talk to their children about the digital responsibilities is also an important step you could take to help your students advance their knowledge on the topic and recognize its importance.

[81] https://mediacommons.psu.edu/free-media-library/
[82] http://www.techsavvyed.net/archives/1997
[83] https://buffer.com/library/free-images
[84] https://www.blogtyrant.com/376-super-useful-royalty-free-creative-commons-and-public-domain-websites/
[85] https://resignal.com/blog/30-free-image-websites-creative-commons-royalty-free/
[86] https://www.sitepoint.com/creative-commons-sources/

Photo 5 by Startup Stock Photos from Pexels (www.pexels.com)

SUMMARY

Within this lesson, we provided an overview of some of the most crucial topics related to copyright, authorship, licensing of content and general tools related to GDPR compliance for your teaching profession. We further provided you with some general tips related to managing your digital identity and protecting it within documents and data produced by you for your teaching practice.

We expect that you are now familiar with common license types as well as some aspects and basic facts related to privacy policies and have a level of confidence that allows you to apply this knowledge to help enhance your teaching resources and use it as a competitive advantage to suit your interests, needs and teaching purposes.

We strongly encourage you to dig deeper and seek further understanding of those topics as the importance of upholding to those standards of fair use could give you, apart from all the obvious ethical and legal advantages, the sense of confidence and security that you can go about exercising your profession with the law on your side.

Last but not least, we hope that we convinced you that instilling in your students a sense of responsibility, related to their use of digital content and distribution of tangible artifacts of their own, is of paramount importance to their future careers, academic practice and basic digital hygiene habits. In a world, the progress of which, is dependent on hard work, creativity and intellectual outputs, cultivating a culture of mutual respect will allow your students to grow up as responsible users and producers of content and will be an important factor for the development of our community.

Please note that **Be@CyberPro is NOT giving you legal advice** nor best practices in the field. This lesson provides you only with a fundamental baseline of educational materials to familiarize you with the above-mentioned and to guide you towards knowing what to ask about and knowing the right question. Those resources should be viewed critically and only as educational information of a generic nature and you should seek consultancy from your legal department, ethical committee and your school's data protection officer to help resolve doubts, issues or determine on the level of local legislation, best practices, approaches and advice.

For further details, apart from turning to the resources provided within this lesson, we encourage you to do your own research and reach out the legal department, ethical committee and the data protection officer of your school.

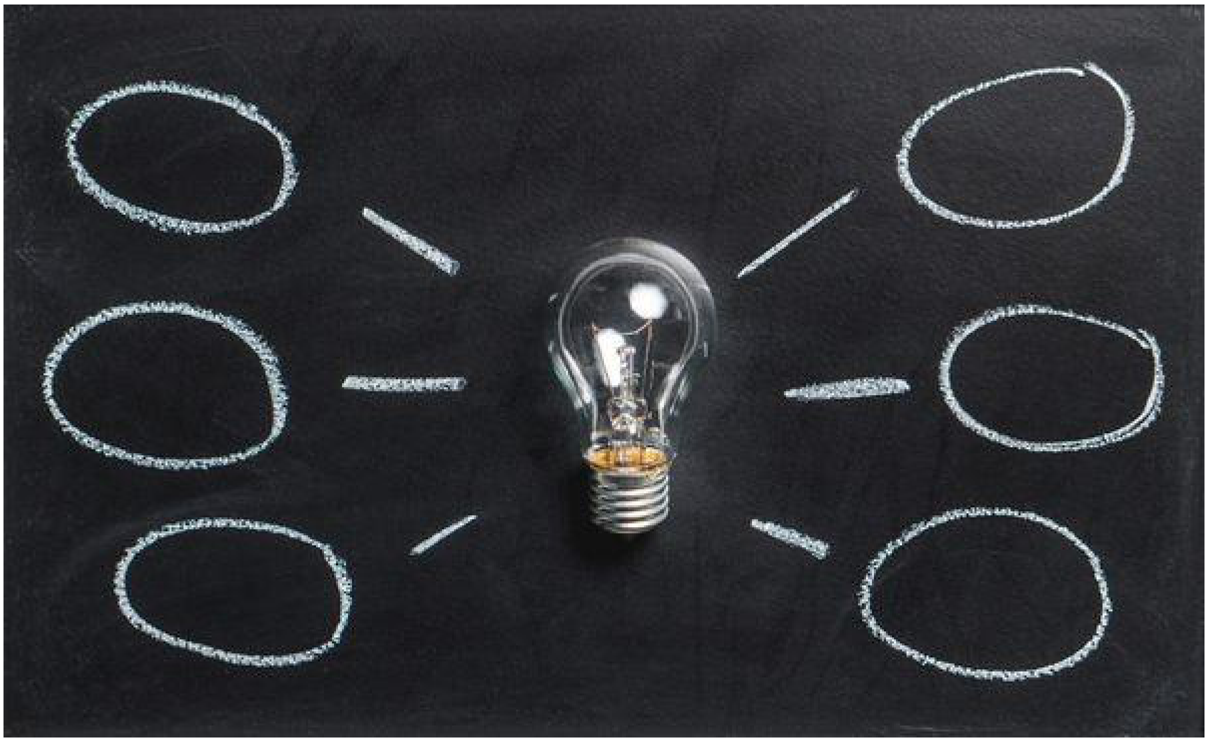


Photo 6 by Pixabay from Pexels (www.pexels.com)

LINKS, REFERENCES AND FURTHER INFORMATION

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://petapixel.com/2017/09/12/photographer-settles-monkey-selfie-copyright-lawsuit/

2. https://www.youtube.com/watch?v=kNBoBw39hAs

3. https://www.youtube.com/watch?v=AOAZQjqcygw

4. https://en.wikipedia.org/wiki/Plagiarism

5. https://en.wikipedia.org/wiki/Copyright_infringement

6. https://copyrightalliance.org/ca_faq_post/what-is-copyright/

7. https://www.iprhelpdesk.eu/sites/default/files/newsdocuments/Fact-Sheet-copyright_essentials.pdf

8. https://www.iprhelpdesk.eu/

9. https://creativecommons.org/

10. https://www.vectorstock.com/

11. https://www.canva.com/

12. https://blog.hubspot.com/marketing/free-content-marketing-tools-list

13. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/special-category-data/

14. https://us.norton.com/internetsecurity-how-to-how-to-remove-gps-and-other-metadata-locations-from-photos.html

15. https://www.makeuseof.com/tag/3-ways-to-remove-exif-metadata-from-photos-and-why-you-might-want-to/

16. https://play.google.com/store/apps/details?id=ec.europa.publications.cyberchronix&hl=bg

17. https://ec.europa.eu/jrc/en

18. https://en.wikipedia.org/wiki/European_Convention_on_Human_Rights

19. https://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm

20. https://www.oecd.org/

21. http://respectforcopyright.org/

22. https://www.commonsense.org/education/lesson/copyrights-and-wrongs-9-12

23. https://creativecommons.org/about/

24. https://www.teachingcopyright.org/

25. https://blog.hubspot.com/marketing/free-content-marketing-tools-list

26. https://mediacommons.psu.edu/free-media-library/

27. http://www.techsavvyed.net/archives/1997

28. https://buffer.com/library/free-images

29. https://www.blogtyrant.com/376-super-useful-royalty-free-creative-commons-and-public-domain-websites/

30. https://resignal.com/blog/30-free-image-websites-creative-commons-royalty-free/

31. https://www.sitepoint.com/creative-commons-sources/

32. https://www.youtube.com/watch?v=-9H6Ksp36q0

33. https://ferpasherpa.org/

34. https://studentprivacypledge.org/