Digital Citizenship

Privacy and Security Course

Readings | Exercises | Case studies | Quizzes

Erasmus+

ATHENS LIFELONG LEARNING INSTITUTE

TEAM 4 excellence

SEAL CYPRUS

Strategic partnership to develop open educational resources for teaching digital citizenship

2019-3-RO01-KA205-078053

DIGCIT

D15 – Digital Citizenship "Privacy and Security" Course

Revision: v.1.1

Intellectual output	IO2 - Educational Materials for digital citizenship
Activity	Course Curriculum Development
Deliverable lead	Arbeitskreis Ostviertel e. V., Germany
Due date	15 March 2021
Authors	Jan LEYE
Abstract	The course "Privacy and Security" covers the risks and benefits to the personal information and data of digital citizens. While the societal benefits of carrying out rights and duties, hobbies and social interactions online are immense, more and more threats to every citizens' privacy keep on emerging. This course teaches the most important aspects of acting secure and the importance of protecting one's privacy.
Keywords	Model course; digital citizenship; course plan; privacy; security; digital environments; social networks; internet security risks; hardware; software; education; reflection; reflective thinking

Acknowledgement

This paper has received funding from the European Commission under Grant Agreement—2019-3-RO01-KA205-078053, ERASMUS+ Strategic Partnership project "Strategic partnership to develop open educational resources for teaching digital citizenship".

Disclaimer

„The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."

Copyright notice

Contents

Introduction

Privacy and security are old terms, but their importance only grew in recent years. The module "Privacy and Security" explains the modern interpretation of privacy as a human right in a digitalized era.

The Digital Citizenship Educational Handbook of the Council of Europe defines privacy as a right that *"concerns mainly the personal protection of one's own and others' online information, while security is related more to one's own awareness of online actions and behaviour."*

Privacy and security are dependent on each other, more so in a digital environment. Facing threats relating to hardware, software, and the user themselves, protecting one's own privacy is a continuous challenge and responsibility for any digital citizen.

This module aims at raising awareness on the importance of privacy in relation to living a fulfilling life and the necessary steps that need to be taken to protect this privacy. It will present knowledge and practical advice on the fundamentals of modern security in the face of modern risks. The modules will cover the following topics et al:

- What is privacy?
- What is security?
- What are digital environments?
- How does privacy affect our lives?
- How does a digital device work?
- How to behave secure and responsible?

1. Module 1 – Introducing privacy

Source: Unsplash

Course overview

Summary: This module covers the fundamentals of privacy, its definition, and its role in today's digital environment. It also showcases the importance of privacy as a human right.

Structure:

- Course overview
- The definition of privacy
- Digital privacy
- The importance of privacy
- Case study
- Supplemental reading
- Exercise
- Feedback
- E-Quiz

Learning objectives:

- Understand the definition of privacy
- Recognize the importance of privacy
- Explain the importance of privacy

The definition of privacy

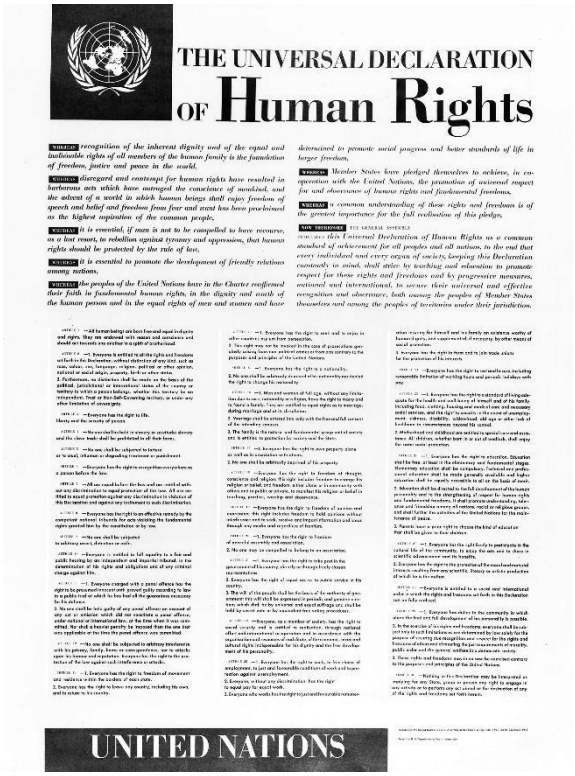
There is no globally acknowledged definition of privacy because the term can have different meanings depending on culture, history, or personal experience. During this course, we will use a definition that should sufficiently apply to most Western democracies:

Privacy is someone's ability to be in a state of no company and no observation, or in short: it is the right to be let alone. Being in privacy means keeping personal information and matters secret and only sharing personal information and matters at one's own will. The protection of privacy, therefore, means the freedom from unauthorized intrusion into one's personal space, information, and matters.

Confusion often stems from the issue that the terms "privacy" and "data protection" are used as synonyms. They are both connected to each other, but while privacy refers directly to the personal space or sphere of an individual, data protection specifically refers to the protection of "any information relating to an identified or identifiable natural (living) person".[1] Privacy covers all aspects of the personal sphere, like the physical protection of your home. For example, if you fall victim to unwanted physical contact, your right to privacy was harmed, but not your right to data protection.

The right to privacy is a human right as stated in Article 12 of the 1948 Universal Declaration of Human Rights (UDHR):

> *"No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."*[2]


THE UNIVERSAL DECLARATION OF Human Rights

UNITED NATIONS

Source: Public domain

[1] https://edps.europa.eu/data-protection_en

[2] https://www.un.org/en/about-us/universal-declaration-of-human-rights

The protection of privacy was specifically recognized by the Council of Europe when the European Convention on Human Rights (ECHR) was signed in 1950 and became effective in September 1953. Article 8 of the ECHR is titled "Right to respect for private and family life" and states:

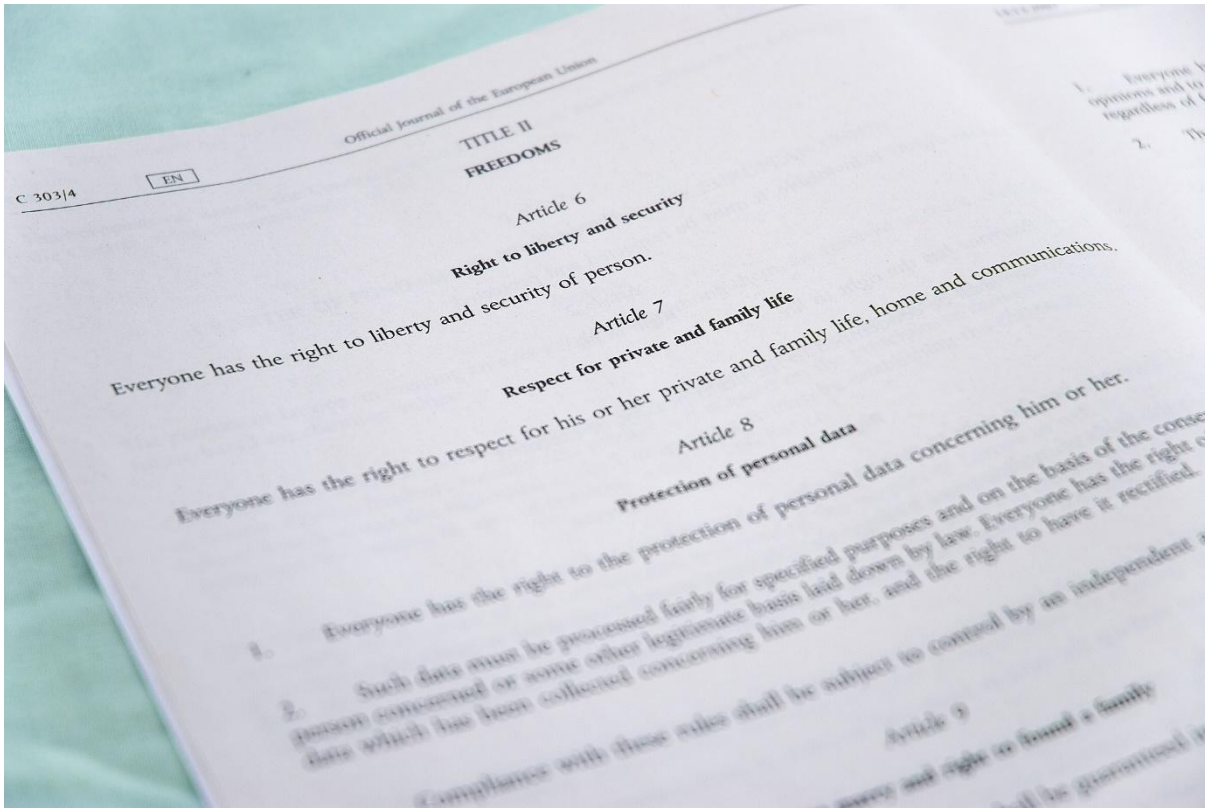
> *"1. Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or the protection of the rights and freedoms of others."*[3]

Furthermore, the European Union recognizes the right to privacy in the Articles 7 and 8 of the Charter of Fundamental Rights of the European Union (CFR) which was drafted in 2000 and became legally effective in December 2009:

> *"Article 7*
>
> *Respect for private and family life*
>
> *Everyone has the right to respect for his or her private and family life, home and communications.*
>
> *Article 8*
>
> *Protection of personal data*
>
> 1. *Everyone has the right to the protection of personal data concerning him or her.*
> 2. *Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.*
> 3. *Compliance with these rules shall be subject to control by an independent authority."*[4]

[3] https://www.echr.coe.int/Pages/home.aspx?p=basictexts&c

[4] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:12012P/TXT&from=DE



Source: Wikimedia

Digital privacy

The digital era brought new opportunities and challenges alike. When talking about privacy in a digital environment we usually use the term "digital privacy". Digital privacy includes the right to privacy and all its applicable definitions from the analogue world as well as data protection.

Digital privacy might be a confusing term because privacy as a legal term already covers all areas of application: It does not matter whether privacy is endangered in the real world or a digital environment because its protection is applied independently of technology, place, or time. When talking about "digital" or "electronic" privacy we basically want to emphasize specific risks and dangers to privacy which originate in new(er) technologies like the internet, social networks, or new devices.

The European Union established two main rulesets which specifically protect privacy and data protection rights in digital or electronic environments: the ePrivacy Directive[5] (full title: Directive on Privacy and Electronic communications) and the General Data Protection Regulation[6] (GDPR). Both try to deal with internet-related privacy and data protection concerns, for example by demanding more transparency in the context of marketing or the tracking of personal data.

The importance of privacy

The right to privacy is a prerequisite to the free development of personality, as stated in Article 22 of the UDHR:

[5] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058
[6] https://eur-lex.europa.eu/eli/reg/2016/679/oj

> *"Everyone, as a member of society, has the right to social security and is entitled to realization, through national effort and international co-operation and in accordance with the organization and resources of each State, of the economic, social and cultural rights indispensable for his dignity and the free development of his personality."*[7]

Some member states of the European Union such as Germany or the Netherlands specifically recognize a right to personality in their respective constitutions, for example Article 2 of the German constitution which states:

> *"(1) Every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law."*[8]

Other states such as France chose different means in their jurisdiction to protect the development of personality.

However, they all share a general conception of the importance of personality, its protection, and its intrinsic connection to privacy. Without the protection of privacy, a human being cannot develop and live freely.

Case study - Privacy by design

Privacy by Design: Collecting data in a socially responsible manner without privacy side effects

In this video from the Privacy Week 2017 in Vienna, Konark Modi explains the dangerous "side effects" of the current industry standard applied by tech giants which collect as much data as possible.

https://media.ccc.de/v/pw17-158-privacy_by_design#t=74

[7] https://www.un.org/en/about-us/universal-declaration-of-human-rights
[8] https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html#p0023

Modi demonstrates that privacy can be respected while designing online services and presents an alternative, privacy-respecting version of "Google Analytics".

Self-reflection question: What is a side-effect in context of data collection?

Exercise 1: Private meeting in the World Café

Objectives:

- Understanding your habits of posting personal data
- Recognizing potential risks and dangers to your privacy

Duration: 30 minutes

Tools: pen and paper

Methods: plenum, group work

Description of the exercise: The students are split up into four groups. Each group is assigned to a table with permanent markers/paper or to a breakout session with a virtual whiteboard. Each table/room has one of the following privacy issues assigned to it: (1) Identity theft. (2) Right to be forgotten. (3) Personality. (4) Spyware. Each group is given 5 minutes to reflect on these topics (What do they mean? What is their connection to privacy? Do we know examples? Are they dangerous or beneficial to me?) and write down ideas on the paper/virtual whiteboard. After 5 minutes, the groups start to rotate. The café is closed once each group discussed each topic. Each group determines a speaker who presents the respective results for their group.

Tasks:

- Split up into groups.
- Discuss each topic for five minutes.
- Share your results with the class (please keep in mind that you do not have to share any information that might make you feel uncomfortable).

Debriefing: The trainer should emphasize the universal importance of privacy and that it affects many parts of our life and our well-being.

Lessons learned: Privacy is a complex topic and requires active reflection.

Supplementary reading

- **The Data Protection Day (every year on January 28th)**: "This year, 28 January is a very special day, not only for the Council of Europe, but for the entire global Data Protection community, and above all, for each and every individual protected by this essential right." https://www.coe.int/en/web/data-protection/data-protection-day

E-Quiz

Online quiz			
Course title:	Privacy and Security		
Module Title:	Introducing privacy		
True or False	Indicate if the following statements are True (T) or False (F)		
Statements		T	F
1	According to the United Nations, privacy is a human right		
2	Privacy is the right to keep all information about yourself secret, even to the government		
3	The European Union does not specifically recognize privacy as a right		
4	"Privacy" and "Data Protection" are more or less synonyms		
5	GDPR stands for "General Directive on Privacy Rights"		
6	Some jurisdictions recognize privacy as a prerequisite for the free development of personality		
7	Respecting privacy laws and the design of modern software are mutually exclusive		
8	Data protection refers to the protection of any information relating to an identified or identifiable natural (living) person		

2. Module 2 – Introducing security

Source: Pixabay

Course overview

Summary: This module covers the fundamentals of security. It explains its basic definition, its relation to privacy and showcases the importance of security in digital environments.

Structure:

- Course overview
- The definition of security
- The importance of security
- Case study
- Supplemental reading
- Exercise
- Feedback
- E-Quiz

Learning objectives:

- Understand the definition of security
- Recognize the importance of security
- Explain the importance of security in the context of privacy

The definition of security

Security means freedom from danger caused by external threats or from fear or anxiety regarding harm or danger. Human rights are partly based on the principle that human beings long for a state of being secure.

In the context of digital citizenship, security means the freedom from the danger which can be caused by one's own actions, inactions, and behaviour in a digital or online environment. It is deeply connected to privacy because without applying proper security measures your privacy is endangered. The Council of Europe states on its website:

> *"To become a digital citizen, one is expected to develop a critical and ethical approach to navigate the digital environment with confidence and clarity and act accordingly."*[9]

Therefore, to be secure, the digital citizen must be aware of potential risks and threats which can not only harm herself, but also other people. To better understand the potential harm caused by a lack of security, we can look at an example list of personal data:

- Name and surname
- Home address
- Telephone number
- E-mail address
- Geolocation data
- IP addresses
- Cookie IDs

The leak of any of this data can lead to minor and/or severe harm.

The importance of security

Digital environments pose new and often enough invisible dangers to individuals. To explain the importance of digital security, we can look at the Corona pandemic: The more people are infected with the virus, the higher the chance that other people will be infected. Imagine your device is compromised by malware. Depending on the type of malware, it might not only pose a danger to your privacy but also other people's privacy and could negatively affect their lives.

Security should not be viewed as a privilege, option, or voluntary offer. In contrast, a responsible digital citizen must understand security as a civic responsibility for oneself and other citizens. Following the basic principles of digital safety (see module 4) is an active contribution to a fairer and more positive digital environment.

Security is never only about protecting yourself. It is about protecting all of us, including your friends and families.

[9] https://www.coe.int/en/web/digital-citizenship-education/privacy-and-security

Case study - STOP.THINK.CONNECT

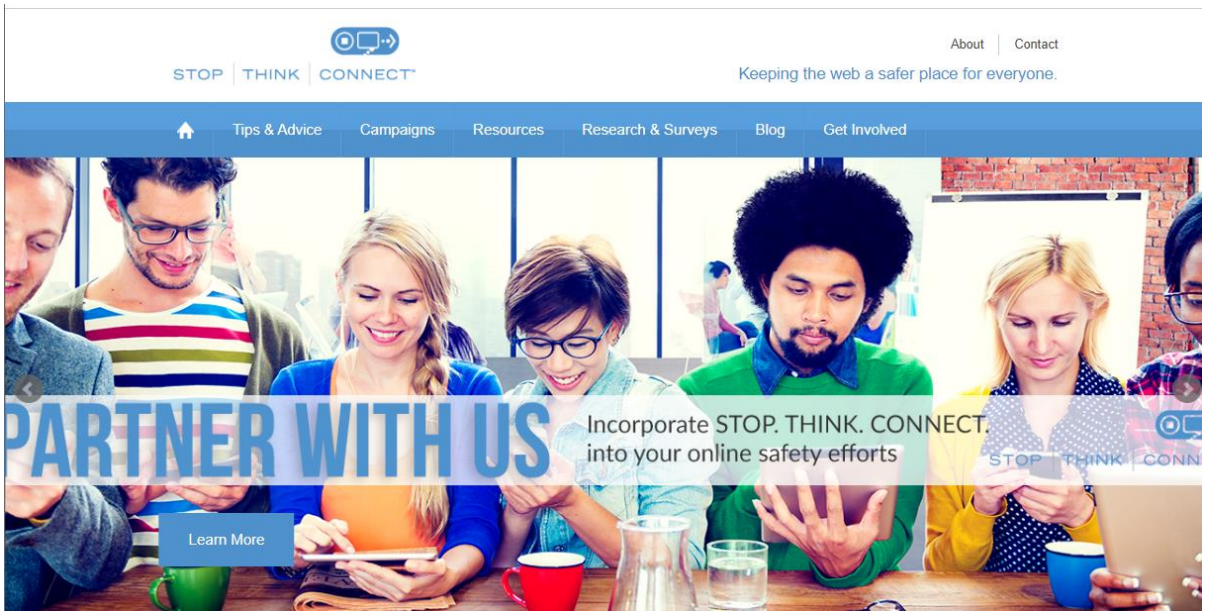
The STOP.THINK.CONNECT. is the first-ever global public awareness campaign developed to help all Internet users keep their personal information, communications, and transactions more secure online.

The US-based organization "National Cybersecurity Alliance" and the "APWG Public Education Initiative" organized this global online safety awareness campaign called "STOP. THINK. CONNECT.". They recommend three basic principles related to digital security:

"**STOP:** Before you use the Internet, take time to understand the risks and learn how to spot potential problems.

THINK: Take a moment to be certain the path ahead is clear. Watch for warning signs and consider how your actions online could impact your safety, or your family's.

CONNECT: Enjoy the Internet with greater confidence, knowing you've taken the right steps to safeguard yourself and your computer (and other devices)."



https://www.stopthinkconnect.org/

More than 800 commercial enterprises, educational institutions, government agencies and NGOs have adopted the STOP. THINK. CONNECT. ™ campaign. Thirteen national government ministries and national-scope NGOs have deployed national campaigns.

Read the Fact sheet https://education.apwg.org/safety-messaging-convention/ and reflect on how organizations can join the campaign.

Exercise 2: Drawing the line

Objectives:

- Understand the difference between personal data and public data
- Recognize your own needs relating to data protection
- Justify the usage of your personal data

Duration: 20 minutes

Tools: pen and paper

Methods: plenum, creative application, writing

Description of the exercise: Think about the following examples for personal data: Your name, age, shoe size, weight, hobbies, wage, shampoo brand, the name of your first pet, the colour of your underwear, the grading of your last exam/job review, your wage, the time when you leave your house. Assign each of these data to one of the following four categories: (1) This data is private; I won't share it. (2) This data may only be shared with my friends. (3) This data can be made public. (4) I don't know where to assign this data.

Tasks:

- Create a table on your paper, each row represents one of the four categories
- Assign all examples to one of the four categories within 5 minutes
- Share your results with the class (please keep in mind that you do not have to share any information that might make you feel uncomfortable)

Debriefing: The trainer should emphasize the reasons why certain examples of personal data are preferably not shared with the public by most of the participants. The plenum should draw conclusions and common grounds about personal data and privacy.

Lessons learned: Personal data needs protection. I should take my time and reflect before I share personal data.

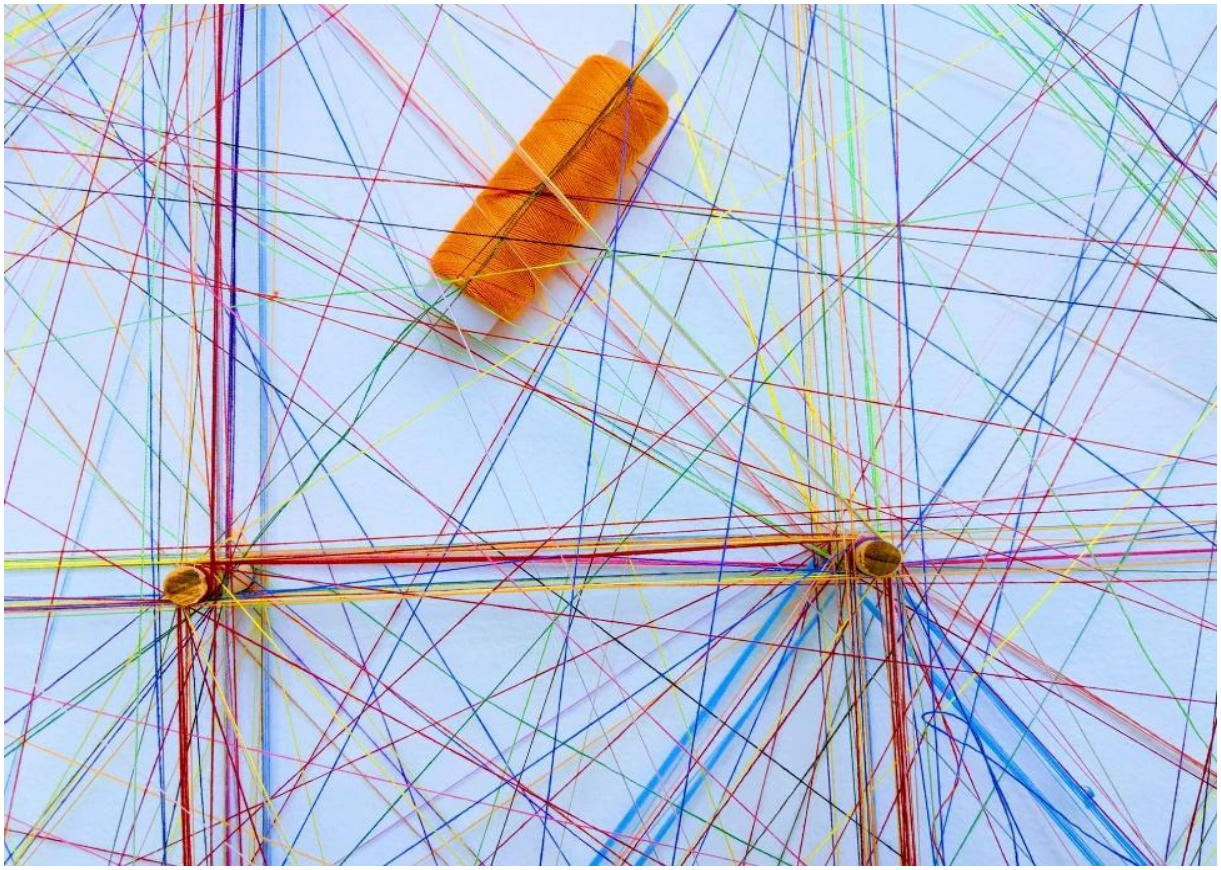
Supplementary reading

- **Facebook Data Leak**: A Twitter thread discussing the consequences and the underreporting of Facebook's data leak, affecting around 533 million Facebook users from all over the world. https://twitter.com/UnderTheBreach/status/1349671294808285184

E-Quiz

Online quiz			
Course title:	Privacy and Security		
Module Title:	Introducing security		
True or False	Indicate if the following statements are True (T) or False (F)		
Statements		T	F
1	A lack of security may endanger your privacy		
2	Your smartphone's IP address is part of your personal data		
3	Security refers to your freedom to gain access to other people's private spheres		
4	If you apply proper awareness of security, you also protect other people		
5	Security is a civic responsibility for digital citizens		
6	A critical and ethical behaviour in a digital environment is part of security		

3. Module 3 – Privacy in a digital environment



Source: Unsplash

Course overview

Summary: This module explains the concept behind digital environments. It focuses on social and communication environments and their respective risks to the user's privacy. In relation to privacy, it critically reflects on the importance and issues of the biggest social network sites.

Structure:

- Course overview
- The premise of digital environments
- Risks of social networks and messengers in a digital environment
- Case study
- Supplemental reading
- Exercise
- Feedback
- E-Quiz

Learning objectives:

- Understand the definition of digital environments
- Recognize the influence of social network sites
- Identify the multi-layered threats to privacy in digital environments

The premise of digital environments

Nowadays, the technical definition of a digital environment usually refers to digital and electronic systems that are integrated, connected, and accessible via the world wide web or other online accesses. For digital citizens, however, digital environments are often defined by contexts and are experienced as connected online spaces, enabled by technology and digital devices.[10]

Digital environments can be used to raise awareness for human rights or issues concerning civil society by connecting each other and expressing your opinion. Digital citizens access digital environments with the help of digital devices such as smartphones or laptops. They gain access to different elements of digital environments which serve different functions.

However, the secure participation of all digital citizens in social and communication environments is connected to a necessary degree of media literacy.

To experience digital citizenship, communication and social services within the digital environments are most important, for example websites, social network platforms or messengers. The United Nations Educational, Scientific and Cultural Organization states in its report on "Culture in the Digital Environment":

> *"This includes the ability to critically analyse the variety of information we are subject to (that is, audio-visual content), to form autonomous opinions, to be actively involved in community issues and to master new forms of social interaction."*[11]

Since digital environments tend to rapidly change their interfaces, accesses, functions, and behaviours, it is important to actively include them in formal and non-formal educational processes for people of all ages.

Risks of social networks and messengers in a digital environment

The digital environment poses risks to digital citizens of all ages and with the rise of social network sites and instant messengers, privacy issues seemingly appear more often than ever.

> *"In 2020, over 3.6 billion people were using social media worldwide, a number projected to increase to almost 4.41 billion in 2025."*[12]

If these services are used in an inconsiderate way, the user can suffer from social, financial, emotional, professional, or legal consequences. The following list provides the most relevant privacy concerns in relation to social network sites:

- **Loss of Data Sovereignty**: The loss of your ability to control the processing of your personal data
- **Lack of Transparency**: The lack of your ability to be informed about the handling of your personal data

[10] "Handbook of Research on Educational Design and Cloud Computing in Modern Classroom Settings", p. 79, 2017, Yannis Kotsanis (Doukas School, Greece), ISBN13: 9781522530534
[11] https://en.unesco.org/creativity/sites/creativity/files/dce-policyresearch-book2-en-web.pdf
[12] https://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/

- **Wrong Perception of Benefits**: A situation in which the perceived benefit of revealing bits of your personal data seems to be larger than the perceived risk of sharing information on an online platform
- **Relaxed behaviour**: The underestimation of the consequences that sharing personal data might cause
- **Permanency of information:** The fact that your personal information is likely to be permanently available online (related to the "right to be forgotten" in the European Union)
- **Profiling**: The threat of a profile being created about you by using available personal information and/or meta-data, for example in the framework of targeted advertisement

Nowadays, one of the biggest threats is the relaxed behaviour on social network sites like Facebook, Twitter, Instagram or TikTok. Each of these sites offers a varying degree of privacy. Sites like Facebook oftentimes force their users to use their real name or else their accounts could be closed, while other social network sites encourage the usage of pseudonyms. However, every social network site can potentially provide enough personal information to make you or others identifiable, for example by using the same profile pictures in different networks, by posting pictures with recognizable environments or by sharing location information with your profile.

In 2020, the US-American satellite internet retailer "Viasat Savings" surveyed 1000 adult US-American citizens, asking how many people on social network sites kept their profiles private:

> *"Turns out, it's evenly split: nearly 50% of the people we surveyed keep their accounts in private mode, while the remaining half chose to be public. According to Kyrsten Holland, internet expert with Viasatsavings.com, "The young and the old have one thing in common: people 18–24 and 54+ are the age groups most likely to make their social media accounts public."*[13]

But even when keeping your profile private, the most important social network sites are owned by private companies with the intention to realize profits. Therefore, they usually reserve the right to use, combine (especially valuable if they own multiple services, for example Facebook, Instagram, and WhatsApp) and/or sell your personal information – that you willingly provided – to other companies which then can aim their advertisement (including political campaigns) towards your interests.

At the same time, experience teaches us that no company can be trusted with keeping your private data stored safely all the time. All major social network sites fell victim to data leaks in the past:

- **Instagram, TikTok, YouTube**: "The security research team at Comparitech today disclosed how an unsecured database left almost 235 million Instagram, TikTok and YouTube user-profiles exposed online in what can only be described as a massive data leak."[14]
- **Facebook:** "The UpGuard Cyber Risk Team can now report that two more third-party-developed Facebook app datasets have been found exposed to the public internet. One, originating from the Mexico-based media company Cultura Colectiva, weighs in at 146 gigabytes and contains over 540 million records detailing comments, likes, reactions, account names, FB IDs and more."[15]

[13] https://www.viasatsavings.com/news/blog/are-more-people-public-or-private-on-social-media/

[14] https://www.forbes.com/sites/daveywinder/2020/08/19/massive-data-leak235-million-instagram-tiktok-and-youtube-user-profiles-exposed/?sh=e35b1371111e

[15] https://www.upguard.com/breaches/facebook-user-data-leak

- **Twitter**: "A quarter of a million Twitter users have had their accounts hacked in the latest in a string of high-profile security breaches at internet firms. Anonymous hackers may have been able to gain access to around 250,000 accounts on the social networking site, including usernames, email addresses and passwords."[16]

The following advice should be followed when dealing with privacy issues in a digital social or communication environment:

- Always follow the principles of data avoidance and data minimization: Never provide personal data and if you must, provide as little as possible (related: always activate as many privacy protection settings as possible)
- Never upload content (for example photos or videos) that you do not own the rights for
- Never share other people's personal information or data (for example private photos, videos or messages) without their explicit consent
- Always verify friend or family requests offline
- Always report suspicious users that try to convince you to share your personal information – others might not be as smart!

A 2012 German study on digital privacy[17] shows that especially young users take a very individual approach to their digital privacy. They often participate in digital social and communication environments in a tug of war between their need for social participation and their fear for their privacy. The study identifies three user types with different privacy strategies:

- **The revealing persons**: This is the smallest group among the study subjects. They are characterized by having open privacy settings in their online accounts while sharing a lot of personal information at the same time. There are relatively more revealing persons among younger people and people with a lower standard of formal education. The study suggests that this group either voluntarily shares their data, or that they lack the competence and awareness for secure privacy settings.
- **The cautious persons**: This group of people has comparatively restrictive privacy settings and are shying away from sharing personal information. They are the antipole to the revealing persons. Although they frequently visit their preferred social network, they probably do not want to miss out on important social information.
- **The privacy managers:** This group of people is continually active in terms of posting status updates and comments on social networks. They possess a vast network of contacts and know many of them in real life as well. They seem to be experts of privacy in a digital environment and can weigh up their sharing habits against the protection of their privacy.

The study concludes that potential privacy threats barely affect the user's behaviour. Interestingly, the principles of digital citizenship itself are not actively sought out.

[16] https://www.theguardian.com/technology/2013/feb/02/twitter-hacked-accounts-reset-security
[17] https://www.medienanstalt-nrw.de/fileadmin/lfm-nrw/Forschung/LfM-Band-71.pdf

Case Study - Social media and identity theft

An article that discusses the modern application of Identity theft by making use of social network sites. It presents four cases of identity theft and provides tips on how to protect yourself from this kind of fraud.

Jessica Velasco for socialnomics.net, 13/01/2016: https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/

> *"Case Study: The Many Sarah Palins*
>
> *Former Alaska governor Sarah Palin is no stranger to controversy, nor to impostor Twitter accounts. Back in 2011, Palin's official Twitter account at the time, AKGovSarahPalin (now@SarahPalinUSA), found itself increasingly lost in a sea of fake accounts.*
>
> *In one particularly notable incident, a Palin impersonator tweeted out an open invite to Sarah Palin's family home for a barbecue. As a result, Palin's security staff had to be dispatched to her Alaska residence to deter would-be partygoers.*
>
> *This phenomenon is not limited only to Sarah Palin. Many public figures and politicians, particularly controversial ones like the 2016 presidential candidate Donald Trump, have a host of fake accounts assuming their identity."*

Self-reflection question: Does over-sharing leave you open to the risk of identity theft?

Exercise 3: Community

Objective:

- Understanding and applying ways to protect your privacy in online communities

Duration: 25 minutes

Tools: digital devices with active internet connections, pen and paper

Methods: plenum, research, group work

Description of the exercise: Students are working together in small groups (maximum of 4 persons). The group chooses a social network site with a high volume of communication (e. g. Facebook, Twitter, Instagram, Twitch, TikTok). Ideally, all students are already active on the chosen site. Afterwards, they try to find a solution for each of the following challenges: (1) How can I activate the most restrictive privacy settings on my profile? (2) How can I remove an embarrassing picture of me that other people shared on the platform? (3) How can I report or block other users? (4) Where do I find the terms of service and what do they state about my privacy? (5) How do I delete my profile and is it really gone?

Tasks:

- Within 3 minutes, choose a social network site
- Visit the sites for fifteen minutes and answer the 5 questions with the help of the site or research
- Share your results with the class (please keep in mind that you do not have to share any information that might make you feel uncomfortable).

Debriefing: The trainer should focus on the obstacles that social network sites create to keep access to their user's personal data. The trainer should also incorporate real-life experiences that some of the students might have already made concerning some of the challenges.

Lessons learned: Once information is public, it is hard to get it back. Be careful when being part of big social networks, they are not your friend.

Supplementary reading

- **Why We Are Addicted to Social Media: The Psychology of Likes**: "Likes on social media are addictive because they affect your brain, similar to taking chemical substances. Likes symbolize a gain in reputation, causing you to constantly compare yourself to your peers." https://steverosephd.com/why-we-are-addicted-to-likes/

E-Quiz

Online quiz			
Course title:	Privacy and Security		
Module Title:	Privacy in a digital environment		
True or False	Indicate if the following statements are True (T) or False (F)		
Statements		T	F
1	There is no societal benefit to digital environments		
2	More than 3 billion people use social network sites now		
3	Facebook automatically deletes my personal data after a certain amount of time		
4	Big tech companies can generally be trusted to carefully handle my personal data		
5	Applying data avoidance is the safest way to keep my personal data secure		
6	Facebook may use my data to personalize my experience according to its terms of service		
7	Profiling is a danger to my privacy		
8	Identity theft is a major threat to inexperienced social media users		

4. Module 4 – Security risks in a digital environment

Source: Unsplash

Course overview

Summary: This module introduces the fundamentals of and different threats to hardware and software. It focuses on everyday life risks and the role of the user as a critical part of typical security vulnerabilities.

Structure:

- Course overview
- Introduction to hardware
- Introduction to software
- Threats to hardware and software
- Case study
- Supplemental reading
- Exercise
- Feedback
- E-Quiz

Learning objectives:

- Understand the role of hardware and software in digital environments
- Identify the individual risks of using hardware and software
- Recognize user-related risks relating to the usage of hardware and software

Introduction to hardware

We are dealing with different devices to take part in a digital environment every day, for example, smartphones, desktop PCs, or ATMs. Hardware is the term used to describe the physical components of these devices. While the hardware itself can be a critical vulnerability, security measures were primarily taken for software and user issues (s. next topic).

The combination of multiple hardware components makes our devices function:

- The CPU (Central Processing Unit) is responsible for carrying out the various commands and calculations necessary for the proper function of our devices. You will find a CPU in your smartphone, your laptop, desktop PC or tablet, for example.
- The GPU (Graphics Processing Unit) is responsible for any graphically demanding processes, such as video streaming or video games. High-workload GPUs require a high amount of power and can process even complex and lengthy calculations in a short amount of time.
- The HDD (Hard Disk Drive) and the SSD (Solid State Drive) are storage devices. They are used to save data or software. Their difference lies in their architecture: HDDs are using magnetic storage technology, while SSDs and all mobile devices are using flash memory technology.
- The Motherboard or mainboard is the core piece of every computer or mobile device. It connects all electronic components of the device.
- The RAM card (Random Access Memory) is a form of computer memory. The device stores the currently executed programs, program parts and data in the RAM. The RAM's access speed and the size of its storage capacities can drastically improve a device's speed.

Introduction to software

Software refers to all kinds of programs or apps that we can install on our devices, like LibreOffice Writer, the VLC player, or your personal banking app. While the hardware is responsible for performing the work, we can use software to determine the task that our devices should do.

There are different types of software for different purposes:

- System software refers to all programs and data that are used to control the processes that make a computer work. System software is intricately connected to the hardware of the respective device and controls the usage of resources; therefore, they provide the infrastructure in the computer. Examples for system software are:
  - operating systems, like Linux, Windows, Android, or iOS
  - device drivers for external hardware such as printers or speakers.
- Application software refers to all programs that perform specific tasks for the users which are not related to system or utility software. All modern devices can execute a range of different application software:
  - Media players, for example the VLC player
  - Word processors, for example LibreOffice Writer
  - Editing software, for example Adobe Premiere Pro
  - Email clients, for example Mozilla Thunderbird
  - Web browsers, for example Mozilla Firefox.

  Application software can either be installed by the user which in most cases works by downloading the program data from an online source or are pre-installed and bundled with certain devices such as smartphones.

- Utility software refers to software that supports the infrastructure, operating systems or application software with additional functions. Utility software is often integrated into operating systems with some of them working in the background, therefore the distinction between system software and utility software is always not clear. Typical examples for known utility software are:
    - Anti-virus programs
    - Data recovery programs
    - File managers

Threats to hardware and software

As we determined in the previous modules, we must pay special attention to our personal data and information. The benefits and reliefs of carrying out many tasks or everyday life routines online may threaten our privacy, for example:

- You might be sick and want to visit a doctor. You search for a specialized doctor using Google on your smartphone. You then proceed to call the doctor, using your smartphone and making an appointment, which you save in the calendar app of your smartphone. On the day of the appointment, you use your smartphone to buy a tram ticket and Google maps to reach your destination. After the appointment, you visit the nearest pharmacy and buy prescribed medicine by using Google Pay with your smartphone.
- You search for interesting people on the dating app Tinder. After chatting for a while with an interesting person, using your smartphone, you exchange your e-mail addresses. You use an e-mail client app on your smartphone and after a while, you exchange your phone numbers. You proceed to use WhatsApp and call each other from time to time. Finally, you meet for your first real-life date. The calendar app on your smartphone reminds you of your date and you use PayPal on your smartphone to pay for the movie tickets. Later at night, you use your smartphone payment options to pay for drinks at the bar, before saying goodbye to each other and calling an Uber to go home.

As the examples show, we often enough use one and the same device for different purposes, while sharing and storing sensitive, personal information. If somebody gains access to this device, they easily get to know or at least reconstruct the most intimate details of your private life.

1. **Hardware risks**

   As technology advances, designing hardware components becomes more and more complex. A recent example from 2018 showcases two examples of critical hardware vulnerabilities: “Meltdown” and “Spectre” both exploit vulnerabilities in modern CPU chips and can be used to access data in programs and operating systems. The vulnerabilities can be exploited in smartphones, desktop PCs and basically every device that uses one of these CPU chips. There are other examples of attacks on hardware components, e. g. “RAMbleed”, but they are usually difficult to execute and require specific prerequisites.

   While there are ways to protect yourself from these kinds of vulnerabilities (see next section), the greatest threat to your hardware is direct access. While it is not likely that your desktop PC at home will be accessed by an attacker, it is easy to lose a USB stick or your smartphone (not always dependent on negligence by the user – expensive smartphones attract thieves, for example).

2. **Software and network risks**

Software and network risks can be a threat to the security of your whole device. They often result either from software bugs (e. g. the programmers made a mistake while creating the software), from online attacks and/or from different types of malware (software that intentionally acts against the interest of the user by harming the computer), including viruses, worms, trojans, spyware or adware.

3. **User-related risks**

Users can pose the biggest threat by executing careless, naive, or uninformed behaviour while using their devices, often related to mishandled password management or usage of personal financial data. User-related risks include cybercrime concepts such as digital social engineering, for example via phishing. In this case, the attacker poses as a trustful communication partner to gain access to personal data or to manipulate their victim to perform a malicious act.

Case Study - My grandmother's favourite scammer

An 88-year-old Chinese grandmother is convinced by a scammer that an elite government task force needs her help to expose an international crime ring. By only using phone calls, one "secret meeting" in a remote hotel and an elaborate story that addresses the needs of "Laolao", the scammer manages to empty her bank accounts and take away her life savings.

An opinion piece by Frankie Huang in the New York Times, 07/12/2019:
https://www.nytimes.com/2019/12/07/opinion/sunday/china-bank-scam-grandmother.html

Self-reflection question: Who are the most target victims of financial scammers?

Exercise 4: The invasion

Objectives

- Understand why security is important
- Identify the consequences of weak security
- Analyse the security issues

Duration: 20 minutes

Tools: smartphones or computers with active internet connections, pen and paper

Methods: role-play, plenum, creative application, practical application

Description of the exercise: Log into your device and imagine that someone else has complete access to it. Work your way through your apps, media files and messenger contents while answering the following three questions: (1) What kind of private, professional, or financial information could the attacker learn about you? (2) What kind of private, professional, or financial information could the attacker learn about your family and friends? (3) Which information would be the most embarrassing to share with a stranger?

Tasks:

- Answer all three questions as far as you can within fifteen minutes.
    - Write down the answers in bullet points.

- Share your results with the class (please keep in mind that you do not have to share any information that might make you feel uncomfortable).

Debriefing: The trainer should find a balance between the newly gained knowledge and the affective nature of the task. The trainer should draw concrete conclusions to improve the security of everyone's devices.

Lessons learned: Device Security is important on multiple levels and protects us from harm.

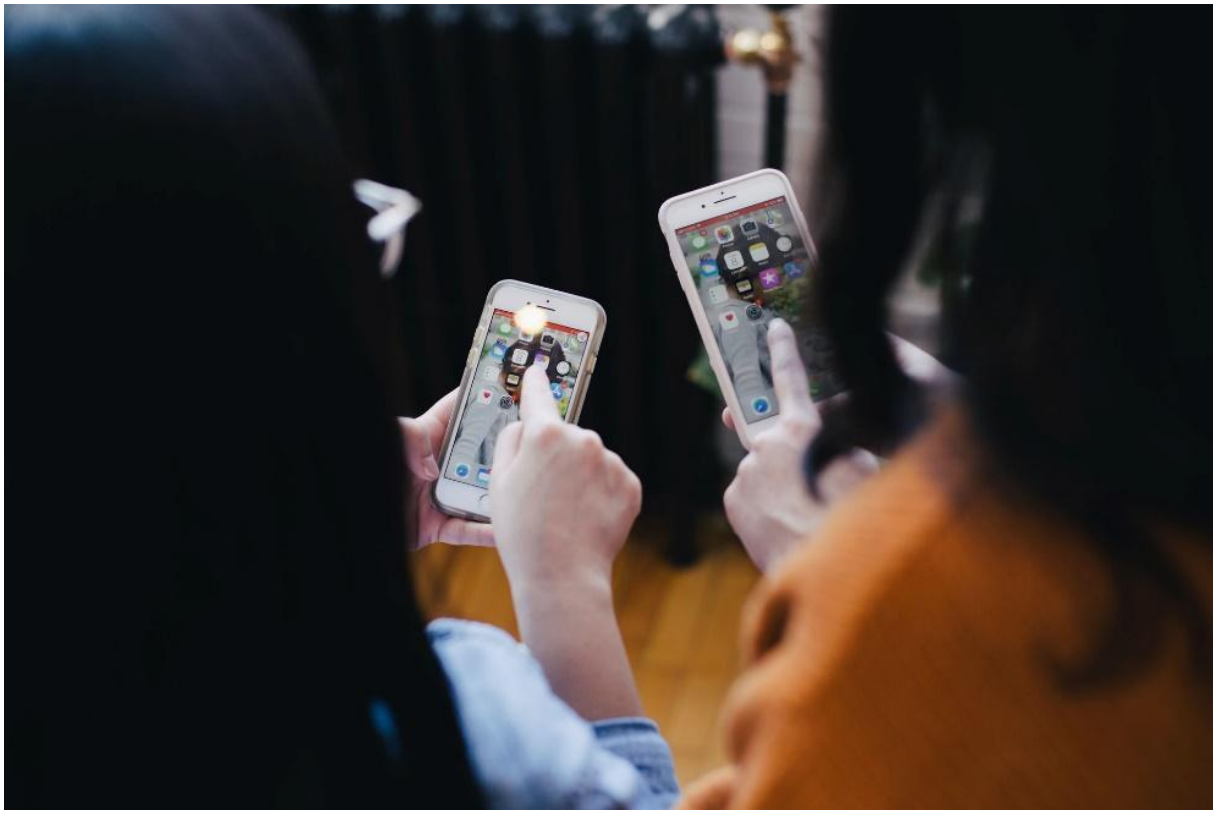
Supplementary reading

- **Project Zero**: "Formed in 2014, Project Zero is a team of security researchers at Google who study zero-day vulnerabilities in the hardware and software systems that are depended upon by users around the world." https://googleprojectzero.blogspot.com/
- **Firefox Monitor**: The Mozilla foundation collects data leaks. By entering an e-mail address, the Firefox Monitor checks if this address was included in past data leaks. This information might help you to better protect yourself or others from, for example, social engineering attacks. https://monitor.firefox.com/

E-Quiz

Online quiz			
Course title:	Privacy and Security		
Module Title:	Security risks in a digital environment		
True or False	Indicate if the following statements are True (T) or False (F)		
Statements		T	F
1	My operating system is an application software		
2	Security vulnerabilities on my digital device are always software-related		
3	I can open a bill that my internet service provider sent me in a .zip file without hesitation		
4	Sharing my geolocation data puts my privacy in danger		
5	Users themselves are often responsible for security leaks		
6	Adware protects my device from unsolicited advertisement		

5. Module 5 – Security tips for the digital environment



Source: Unsplash

Course overview

Summary: This module provides accessible tips on hardware, software, and user-related security issues, focusing on practical advice as an important part of the protection of privacy.

Structure:

- Course overview
- Tips on hardware security
- Tips on software security
- Tips on user-related security
- Case study
- Supplemental reading
- Exercise
- Feedback
- E-Quiz

Learning objectives:

- Recall the basic means of security in digital environments
- Develop a basic security strategy to protect one's and other persons' privacy
- Develop an attitude that promotes conscious and responsible online behaviours and interactions
- Apply security measures to one's devices, accounts, and digital interactions

Keeping your personal information and data safe is not an easy task, but it is worth the effort to protect yourself and others from different types of harm, negatively affecting your professional and/or private life. This list contains general rules that you should always follow:

Tips on hardware security

- **Buy hardware from trustful manufacturers**: It is near to impossible for the average user to find out about vulnerabilities in consumer devices such as smartphones, laptops, or routers. A good starting point is the location and respective jurisdiction of the hardware manufacturer which might require them to respect laws on privacy and security.
- **Do not leave devices unattended**: Do not carry around sensitive information on mobile devices such as smartphones or USB drives. If you must, make sure that your devices are at least password or PIN protected, or even better encrypted by using encryption software, for example VeraCrypt. If you use a desktop computer, always lock your screen, or shut it down when not in use.
- **Turn off geolocation and Bluetooth settings**: As long as you do not need them, there is no reason to keep them activated, since they potentially provide a lot of meta information about yourself.
- **Do not insert devices of unknown origin**: This rule is especially important in a professional work environment. Never insert USB drives or other mobile storage media in your desktop computer, if it was not checked for potential security risks beforehand.
- **Buy backup devices**: Losing important data can cause a lot of damage to your professional or private life (for example by losing your dissertation). Always take your time to back-up important data regularly and find a safe physical space to store this back-up.

Tips on software security

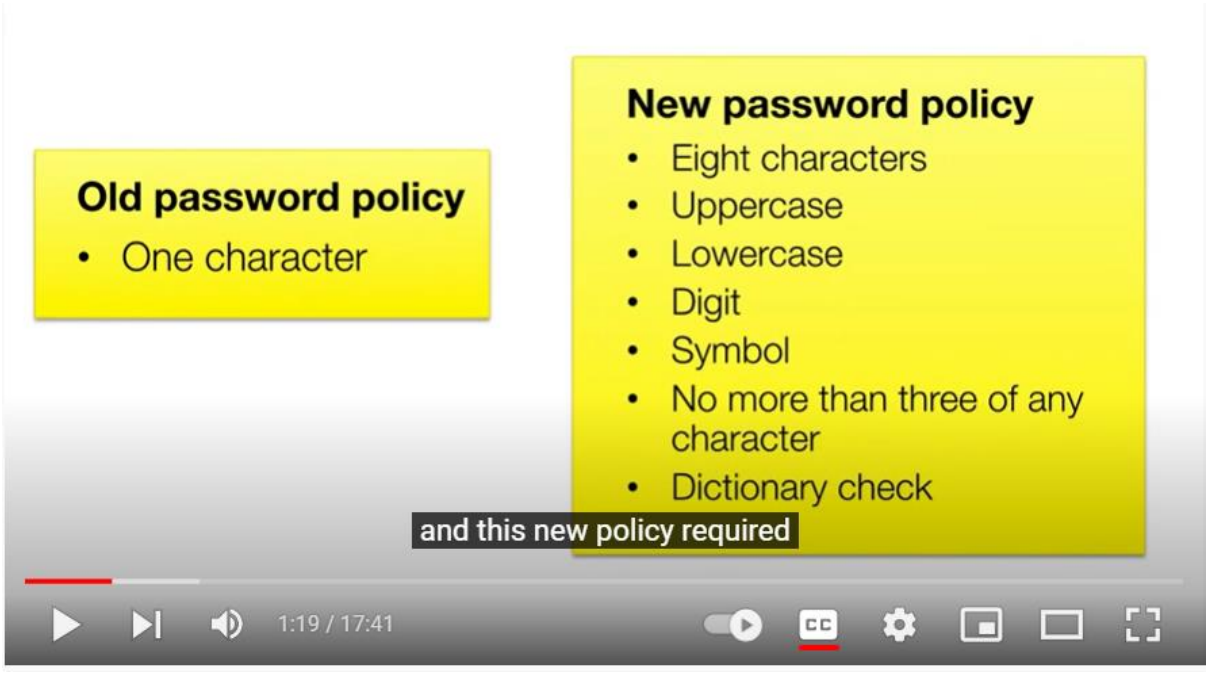
- **Keep your software up to date**: This includes system, utility, and application software. Turn on automatic updates for your programs, apps, and operating system, independent of the device you are using.
- **Use software from trustful sources**: Big Open-Source projects are usually a good resource for capable and secure software, for example Firefox as web browser or LibreOffice for office applications. Take special care when downloading apps to your mobile device that are not vetted by the PlayStore or AppStore.
- **Protect your browser**: Since usually a browser is used to access the WWW, it is extremely important to always keep it as safe as possible. Most browsers support the installation of extensions, such as adblockers (for example uBlock Origin), tracking blockers (for example Facebook Container), firewalls (for example uMatrix) or automatic redirects to https pages (for example HTTPS everywhere).
- **Install anti-malware software (optional)**: The benefits of anti-malware software are disputed since the programs themselves pose potential and real security risks. To protect your system, antivirus software usually requires deep access to your system – but if the antivirus software itself becomes compromised, your system is suddenly open to attacks that would not have taken place without the antivirus software in the first place. Additionally, if you are a responsible user, you should never get into contact with malware software anyways. Antivirus software can still be of benefit for inexperienced users who might be more susceptible to malware traps such as email attachments.

Tips on user-related security

- **Be careful with unknown sources:** Never click on links or attachments from unsolicited e-mails or other messages on any device.
- **Have a good password management:** Use a password manager (for example KeyPass) to create safe passwords and to securely store these passwords. Never use the same password twice.
- **Reduce the usage of personal information to a minimum:** You should always reconsider if unsolicited sharing of personal information and data in a digital environment is necessary, for example on Social Networks. There is usually no benefit in doing so, but it can harm you later, for example by being a victim to social engineering attempts.
- **Avoid scams:** Learn not to trust strangers on the internet or on a phone call. Social engineering in a digital environment is especially dangerous to older people, for example the infamous grandparent scam. Inform yourself and others and make sure that you **never** share personal data and information over insecure digital channels, such as unencrypted emails, messenger chats or telephone calls.

Case Study - Lorrie Faith Cranor: What's wrong with your pa$$w0rd?

"Lorrie Faith Cranor studied thousands of real passwords to figure out the surprising, very common mistakes that users — and secured sites — make to compromise security. And how, you may ask, did she study thousands of real passwords without compromising the security of any users? That's a story in itself. It's secret data worth knowing, especially if your password is 123456 ..."



Released by the TED organization on 24/06/2014: https://www.youtube.com/watch?v=0SkdP36wiAU

Self-reflection question: How strong are your passwords?

Exercise 5: Safe together

Objectives:

- Understand why security is important
- Present the most important security measures

Duration: 20 minutes

Tools: pen and paper

Methods: plenum, creative application, presentation

Description of the exercise: Each student imagines an old family member who bought their first laptop to finally take advantage of modern-day technology. This family member knows how to start their new laptop and asks the student for help with (1) setting up an e-mail address, (2) starting online banking, (3) setting up a profile on Facebook, (4) installing the WhatsApp desktop app, (5) working in a café every morning and getting online over there. Each student prepares a small presentation and focuses on the most important security aspects they want to show their family member.

Tasks:

- Write down at least three bullet points of the most important security aspects for each of the 5 scenarios in 15 minutes.
- Share your results with the class (please keep in mind that you do not have to share any information that might make you feel uncomfortable).

Debriefing: The trainer should emphasize which conclusions the students can draw from the exercise for their own security habits. They should also appeal to the community feeling of helping each other to stay secure.

Lessons learned: Security is important to protect us from harm and we should support each other to stay secure.

Supplementary reading

- **Will Styler**: "So, remember the dissertation I was working on? […] Well, a big chunk of the work I did is gone, because I made some bad decisions, and had some very bad luck. I'd like to share what I did wrong, and how to not be me."
  https://wstyler.ucsd.edu/posts/lost_dissertation_files.html

E-Quiz

Online quiz			
Course title:	Privacy and Security		
Module Title:	Security tips for the digital environment		
True or False	Indicate if the following statements are True (T) or False (F)		
Statements		T	F
1	Using the same password everywhere is secure enough if you do never share it		
2	Automatic security updates can protect my operating system		
3	Anti-malware programs always make my device more secure		
4	Security vulnerabilities on my digital device are always software-related		
5	My smartphone is safe if it is PIN protected		
6	I can safely execute an APK file on my smartphone that I downloaded from a website		

6. Assessment quizzes

Module 1

1) Which of the sentences below fits rather to a description of security online and not privacy online?
   a) The personal protection of one's own
   b) The protection of others' online information
   c) Own awareness of online actions and behaviour

2) Which of the following rulesets protect privacy in digital or electronic environments?
   a) The ePrivacy Directive
   b) The eSecurity Directive
   c) The Privacy and Security Directive

3) What is the full title of the ePrivacy Directive ruleset?
   a) Directive on Electronic Privacy and Online Behaviours
   b) Directive on Privacy and Security online
   c) Directive on Privacy and Electronic Communications

4) What GDPR means?
   a) General Data Privacy Regulation
   b) General Data Protection Regulation
   c) General Data Protection Rules

Module 2

1) When is the Data Protection Day?
   a) 28th of January
   b) 28th of June
   c) 28th of December

2) What is the name of the global online safety awareness campaign organised by the National Cybersecurity Alliance and the APWG Public Education Initiative?
   a) STOP. THINK. CONNECT
   b) STOP. ReTHINK. CONTACT
   c) START. THINK. COMMENT

3) Which content are you allowed to publish online?
   a) Any photos taken from google
   b) Photos taken by my friends
   c) My own photos

4) Which of the following user types is caring about their privacy settings the less?
   a) The cautious persons
   b) The revealing persons
   c) The privacy managers

Module 3

1) Which of the following is responsible for carrying out the various commands and calculations necessary for the proper function of devices?
   a) CPU (Central Processing Unit)
   b) GPU (Graphics Processing Unit)
   c) HDD (Hard Disk Drive)

2) What RAM means?
   a) Remote Additional Memory
   b) Random Access Memory
   c) Range Amount Measures

3) Which of the following refer to utility software?
   a) Linux
   b) VLC Player
   c) Anti-virus programme

4) What is a “Meltdown”?
   a) A hardware vulnerability
   b) An application software
   c) A system software

Module 4

1) What kind of risks are connected to malware, spyware and adware?
   a) Hardware risks
   b) Software and network risks
   c) User-related risks

2) Using a password manager is related to what kind of security?
   a) Hardware security
   b) Software security
   c) User-related security

3) What adware does?
   a) Automatically generates online advertisements
   b) Block automatic advertisements
   c) Helps to format your hardware

4) Which of the following refer to application software?
   a) Web browsers
   b) Operating systems
   c) Data recovery programs

Module 5

1) Which of the following are NOT used as storage devices?
   a) HDD (Hard Disk Drive)
   b) SSD (Solid State Drive)
   c) GPU (Graphics Processing Unit)

2) Which of the following sentences is correct?
   a) Social media settings are giving me full protection of my data
   b) I need to adjust privacy settings on social media to protect my data
   c) My data on social media are fully protected as soon as I only post my own photos

3) With what risks is cybercrime-related?
   a) User-related risks

b) Software risks

c) Hardware risks

4) Where can scam occur?

a) Only offline

b) Only online

c) Offline and online

7. References

Council of Europe (2014). Guide to human rights for internet users

Netter, M., Herbst, S., Pernul, G. (2013). Interdisciplinary Impact Analysis of Privacy in Social Networks

Ladan, M. I. (2015). Social Networks: Privacy Issues and Precautions

Schenk, M., Niemann, J., Reinmann, G., Roßnagel, A. (2012). Digitale Privatsphäre: Heranwachsende und Datenschutz auf Sozialen Netzwerkplattformen

Gross, R., Acquisti, A. (2005). Information Revelation and Privacy in Online Social Networks (The Facebook case)

Cranor, L.F. (2014). What's wrong with your pa$$w0rd? https://www.youtube.com/watch?v=0SkdP36wiAU

Velasco, J. (2016). for socialnomics.net, 4 Case Studies in Fraud: Social Media and Identity Theft, https://socialnomics.net/2016/01/13/4-case-studies-in-fraud-social-media-and-identity-theft/

The New York Times (2019). My Grandmother's Favorite Scammer. https://www.nytimes.com/2019/12/07/opinion/sunday/china-bank-scam-grandmother.html

APWG (2010). STOP. THINK. CONNECT.™ public-awarenress campaign. https://education.apwg.org/safety-messaging-convention/

Media.ccc.de (2017). Privacy by Design: Collecting data in a socially responsible manner without privacy side effects. https://media.ccc.de/v/pw17-158-privacy_by_design#t=74

Appendix

Assessment quiz check sheets

Evaluation quiz Module 1 check sheet – correct answers

1c

2a

3c

4b

Evaluation quiz Module 2 check sheet – correct answers

1a

2a

3c

4b

Evaluation quiz Module 3 check sheet – correct answers

1a

2b

3c

4a

Evaluation quiz Module 4 check sheet – correct answers

1b

2c

3a

4a

Evaluation quiz Module 5 check sheet – correct answers

1c

2b

3a

4c

Instructional design review checklist for youth workers

No	Criteria	Yes	No
1.	**Objectives**		
1.1	Are objectives stated clearly for the learner?		
1.2	Are the course requirements consistent with the objectives?		
1.3	Do chapters/topics thoroughly cover the course's objectives?		
1.4	Do the learning objectives match the learning outcomes?		
1.5	Does the overall content and structure of the course meet its instructional objectives?		
2.	**Structure**		
2.1	Does the course have a concise and comprehensive overview or syllabus?		
2.2	Does the course include examples, analogies, case studies, simulations, graphical representations, and interactive questions?		
2.3	Does the course structure use appropriate methods and procedures to measure student mastery?		
3.	**Content**		
3.1	Does the content flow seamlessly, without grammatical, syntactical and typing errors?		
3.2	Is the content up-to-date?		
3.3	Is the content aligned with the curriculum?		
3.4	Are the desirable outcomes incorporated in the content?		
3.5	Is the content in compliance with copyright laws and all its quoted material cited correctly?		
3.6	Does the course engage students in critical and abstract thinking?		
3.7	Does the course have prerequisites or require a technical background?		
4.	**Assessment**		
4.1	Are the assignments relevant, efficient and engage students in a variety of performance types and activities?		
4.2	Are practice and assessment questions interactive?		
4.3	Do the practice and assessment tasks focus on the course's objectives?		
5.	**Technology - Design**		
5.1	Is the design clear and consistent, with appropriate directions?		
5.2	Are the images and graphics of high quality and suitable for the course?		
5.3	Is the course easy to navigate and offers assistance with technical and course management?		
5.4	Is the course navigation structure consistent and reliable?		
5.5	Are the course hardware and software-defined?		
5.6	Is the audio and on-screen text in sync?		
5.7	Does the architecture of the course allow instructors to add content, activities and extra assessments?		

Feedback on topic for students

Assessment of Module						
Course title:						
Module Title:						
Part A:	On a scale of 1-5 where 1 is the lowest and 5 the highest level of agreement indicate how you feel on the following					
Observations		1	2	3	4	5
1	The subject was interesting					
2	I believe the topics covered were important					
3	I would like to know more about the area					
4	I have learned new things which I am likely to apply in the future					
5	I would like to improve my skills in the area					
6	I am likely to recommend this course					
Part B:	In the space provided please feel free to include any comments and recommendations you wish to make					
Part C:	In the space provided please feel free to include your email address if you would like to be kept informed about this project					