Portfolio

Project: Students' Cybersecurity

Group: Materials

Members: Alexander Scott, Anna Kabanets, Ahmad Mohammadi, Crislyn Saviste, Martin Pedak, Karin Toom, Raili Krusta, Ricco-Karol Klemmer, Sadat Awudu

Supervisor: Catlyn Kirna

Project report

1. Description of the terms of reference and goals of the project

Our project is, first of all, related to the notions of cybersecurity and social engineering with a focus on the general population. According to the report by the European Union Agency for Cybersecurity (December 2015), the term 'cybersecurity' is relatively new, multifaceted, and non-universal. In order to make the creation of the project possible, we decided to use the definition provided by the Cambridge Dictionary (n.d.), which states that cybersecurity is the "things that are done to protect a person, organization, or country and their computer information against crime or attacks carried out using the internet". In its turn, social engineering refers to the manipulation of people with intention to get access to data (Webroot page, n.d.).

When we started off with brain-storming ideas about the upcoming project, we got a few insights that determined our work. These include:

- people generally tend to downgrade the importance of security in an online space on the personal level
- younger population is at higher risk because they use internet since early childhood and do not possess the needed knowledge to protect themselves
- people learn better through the experience of others rather than through reading complex theory

Our main goal was to raise awareness and educate the population through the creation and distribution of the age-appropriate user-friendly materials on the topics related to cybersecurity.

The key tasks were:

1) to research the field by ourselves and to transform this knowledge into something accessible by general population
2) to figure out which form of materials to use and create them
3) to disseminate materials and ensure the sustainability of the project by giving them out to the stakeholders

That is the rationale behind the idea to create chat-recorded-videos about the variety of life-like situations related to cybersecurity; and share them through Instagram targeted ads.

With this in mind we started to develop the action plan, which helped us to keep each other accountable and ensured the division of labor. We came up with the strategy of splitting into the three sub-groups called according to the type of the task - “Research”, “Language”, and “Technical”. The beginning of the actual work towards the completion of the project was a bit confusing for all of us, so we decided to split the research part and the script-writing between us equally, in other words, everyone has done it. After the research phase we got more variety in terms of group composition. The “Language” team dealt with the translation of the scripts into Estonian and Russian languages along with their cultural adaptation. The “Technical” team included general group management, video-creation, video-editing, posting on social media, target ad management, gathering statistics, and contacting the stakeholders. As we realized at the end of the project, this strategy helped us to keep track of things and organize the work of each other. In reality, all of us took part in two or even all three teams since this distribution was linear in time (e.g. no one can translate the script without it being written in the first place/there can be no video creation without the translated to the appropriate language script, etc.).

Essentially to mention that in the process of looking for the stakeholders, we got interest from the people working with cybersecurity-awareness-raising among elderly. Thus, in the middle of the project we decided to add tutorial videos that will guide a viewer through the step-by-step process on how to use some of the tools for protection (e.g. two-step verification) aimed at this demographic. This led to further division into chat-sub-group and tutorial-sub-group, which were working on certain types of videos and thus had different tasks.

Even though we struggled with communication as a group, we managed to get things done at the right time and deliver materials that we had created. The project is finished, but the materials will be further in use by our stakeholders.

Used materials:

What is Social Engineering? Examples and Prevention Tips | Webroot

Definition of Cybersecurity - Gaps and overlaps in standardisation — ENISA (europa.eu)

CYBERSECURITY | meaning in the Cambridge English Dictionary

2. The importance of the problem, its description and choice of methods

As more and more people are starting to use technology, the importance of cybersecurity knowledge is also increasing. People are not afraid of the Internet, because they might not think about it as a “real thing” but as something that exists somewhere further away and they might feel that they can not be harmed by people on the Internet. For example, kids are taught not to share their personal information to a stranger on the street but they are willing to do so on the Internet, because the threat doesn’t seem real. Many people don’t know that once something is posted on the Internet, it will always stay there, even if they deleted it and they can’t see it. People feel safe to say and post whatever they want, without acknowledging the consequences of their actions.

It also applies to posting on social media like Facebook and Instagram, which was a big part of our project. The main problem about social media is oversharing (personal) information by the one posting about him-/herself or about someone else. When posting to social media, you should think through - who do you want to share this information with and if the information is worth sharing? Can this information harm yourself or someone else? What to do when someone shares a picture or information about you that you don't want everyone to see/know, etc? Internet privacy was also a part of our project - the main focus was on oversharing information, but we also covered the safety part - creating strong and safe passwords and we told people not to share their passwords with anyone, even with someone they trust, because it can be used against them.

The Internet is full of useful and educational information, but there is also a lot of false and/or harmful information and people can not always make a difference between these two. A good example is fake news - it's misleading or false information that is presented as true and many people will believe it and share it, but they don't check the source. Another example is information about health - we all know that if we Google our illness symptoms, Dr. Google insists that we will die in the next three days, and so on… It is necessary to teach people of all ages how to find reliable and trustworthy information.

Another big problem nowadays since everyone has smartphones and Internet access, is screen addiction, which can affect anyone, despite their age and nature. Screen addiction affects both mental and physical health if it goes too far. And the technology creators are always finding new ways to keep people looking at the screen more and more - like sending notifications about unimportant things (for example, "user X on Instagram is following user Y, go check it out"), analyzing the person's internet usage (for example, what content they watch or search for), show them personalized ads, and so on. Screen addiction is a serious health risk, because it affects relationships, personal life, working, school, etc.

Our idea was to make educational short videos (max 1 minute) and to promote them to our demographic groups on Instagram, because it's a very popular platform and it provides a great analytics of engagement. The videos were posted to "Instagram stories" and they covered many cybersecurity issues like scamming, phishing, oversharing, security issues (passwords) and they also included tips of what to do in different situations. The project is needed to bring awareness to people in different age groups, but especially young people, because there really isn't very much information about cybersecurity on the Internet in Estonian and Russian and it is quite hard to find - if you don't specifically look for it, then you won't find it.

3. Description of activities and reaching the stakeholders

Research

Our project started with a research on topics we thought could be the best ones to cover during our project. Topics that we thought were the most important were: fake news, passwords, personal information, screen addiction, phishing and scamming. After finding out the themes for research we were split into groups and began to conduct our research using academedical sources. Our research can be found as **Extra 1.** below.

Video scripts

After research was conducted each member of the team was responsible for creating at least three video scripts. Scripts had to be short, realistic and carry the main lesson of how to be safer on the given topic. Scripts had to be suitable for different ages and themes had to be interesting.

Translating

All our scripts were first written in English. For our videos we had to translate them into Estonian and Russian as these were the languages we decided to do our videos in. The main reason we decided to do the videos in Russian as well were the fact that there are few or not so good materials in Russian language available. So this part of the population is not covered enough in cyber security information. We thought this could be our special thing as we had Russian speaker in our group who was fine with translating the scripts.

Posting

Videos were posted to Instagram stories from our account in December. Postings were consistent and they were not posted every day as this would have been bothering for the followers.

Reaching the stakeholders

During our project we also reached out to a few stakeholders. In the beginning we were not sure what would happen to our project in future and where it should go after we are finished. At one point the idea was to show the videos more publicly on city outdoor LED-screens or share it on different media platforms but as we contacted different companies we realized this would have been a difficult task and it needed more money than we had. So after all we decided to contact schools we know and want to be evolving and innovative. This also helped us to focus on specific age groups and get feedback for the future. We also had a meeting with a police representative (Maarja Punak) who deals with cyber security on a daily basis and she gave us some good ideas and plans for the future.

We can proudly say that we have three deals for our videos. Two deals are with Estonian high schools, where two of our team members went and the last deal is with Maarja Punak we met during the project. Things can still change and we could have a lot more stakeholders through them. Now we can say that our project will have a positive impact on hundreds of youngsters and elderly people because these materials are going to be used for learning.

4. Sustainability of the project

To ensure the sustainability of the project activities we have contacted a few stakeholders mentioned before. Two schools we contacted were really interested to use our materials in their IT lessons, to teach kids the threats on the internet. These chat-videos are sure to provoke discussion and are good to analyse in the lessons.

We also have an agreement with Maarja Punak we met during the project. Police have different ways to advise people how to behave online. The information provided to us was that the police has a number of resources with a broad demographic, the inclusion of facebook groups, email, phone numbers, and weekly meetings, give a variety of ways for someone that suspects having been affected by some cyber crime or needs information concerning cybersecurity and the likes can contact the appropriate authority through these

channels in order to gain relevant information in a timely manner. What had been offered to our project was a collaboration to see whether our means of communication and information sharing provided a novel outlet for a demographic that was potentially lacking in resources — the elderly. Seeing that the virus has played a bit of a part itself over the past few months has limited our ability to reach out to the elderly groups with our tutorial videos with the help of the police's weekly meetings, though we have been informed that our videos could also be published onto their website once a final copy was to be finished and approval made by Maarja Punak's superior officers.

The websites that had been mentioned and provided that include sundry topics are the following:

https://www.targaltinternetis.ee/, https://kiusamisvaba.ee/, https://cyber.politsei.ee/, https://www.lasteabi.ee/, https://www.facebook.com/politseinik.maarja/, https://www.instagram.com/seepoleokei/,

Our Instagram account will also remain public. Although we will no longer promote it, it will still remain open and discoverable for anyone who wants to spend their free time to get knowledge from our chat-videos in a fun and lively way.

Last but not least we have got ideas from our supervisor Catlyn Kirna, who has different contacts who may be interested in our materials. These plans are not 100 percent sure yet, but these are being developed and need further approval from us and university. We are happy that different organizations can use our materials in the future to provide people with better knowledge.

5. Summary of the results and annexes

The results of our project include the content we created as recorded chat-videos (real-life scenarios) and tutorials (step-by-step guides) for raising awareness on how to protect oneself from the various issues online. We distributed them through a social network (Instagram) and will continue to do so through the stakeholders. On our Instagram page, one can find the videos in the section of Highlights. Of course, the main result is a better understanding of the threats in the online environment by the population. Also, we have tested that it is possible to educate people through Instagram on the topic of cybersecurity, therefore, further exploration of the field, research, and investments will be more successful as they can take into account our project and experience.

https://www.instagram.com/cybersafetips

Research

Our project started with a research on different themes we wanted to include on our videos. All the group members researched information and together we managed to cover topics such as: fake news, passwords, personal information, screen addiction and phishing e-mails/scamming. We gathered more information than we actually needed for the videos and unfortunately we were unable to use it all. Although we really think the research itself is also a good study material and it can be useful for many people in different age groups. Our research is added as **Extra 1.** down below.

Tutorials

While creating the chat videos, it became apparent that there is a demand for some topics that are better approached using a different style of content. As a result, we chose to use tutorial video style short clips to demonstrate how to go through with some of the more important actions to make your online accounts more secure.

After discussing and researching the topics, we started making the tutorials. Several videos were created, which were then run by a small focus group, to get feedback on presentation, accessibility and general usefulness. The focus group was fairly small. As tutorials are more focused on the elderly age group, current covid-19 situation meant in person focus group interviews were out of the question. That made the process a fair bit more difficult, however we still managed to get some useful feedback. Tutorial videos were then re-edited based on that feedback. As a result of this process, we ended up with well researched and reviewed tutorial videos that can be used by people to guide them through various security related actions related to their online accounts.

Chat-videos

Our group decided to create chat type videos where there is conversation between two people. We created scenarios and scripts, what are the themes we want to make the chats about and what should we write so that these would catch an eye and be informative at the same time. We posted our videos to the instagram account as mentioned before. These are reachable for anyone and they will remain there even after the project is over.

Media analyse results

On our media platform account we were able to gain 48 followers. We promoted together 11 stories - both in russian and in estionian language. We think that the promotions were successful as the maximum number of people reached were 7173. Not less than 2000 per promotion as the minimum number was around 3000 - that means with every promoted story over 2000 people saw it. Maximum number of people who visited our profile after seeing our promotion video was 127. We gathered the information that our videos were mostly watched by females among the 13-17 age group. Since one has to be at least 13 y.o. to create an account on Instagram, we couldn't get official statistics on whether/how many people under 13 y.o. were interested in the videos (this population is still present in the social media through faking their date of birth). Videos were surprisingly popular in Russia. From the analytics we see that our videos top locations were Moscow and Harju County.

Project action plan

TASKS	DEADLINE	STUDENT NAME

Research Themes: ● what are the main problems ● Where to find help ● Collect info in one document ● write a short summary abstract for future use in the videos		Everybody
Screen addiction research	9th Oct	Raili Ricco
Oversharing personal information research	09. Oct Review 16th oct	Karin Anna
Phishing emails - Scamming research	16th Oct	Martin Ahmad
Passwords research	16th Oct	Crislyn Ricco
Social Engineering research	9th Oct	Alex
Fake news research	16th Oct	Sadat
Demo video 1st: oversharing personal info:	23 Oct 9th/16th	Raili - video creation Anna - video editing
Scripts for videos		Everyone
Translation		Raili, Karin, Crislyn - Estonian Anna - Russian
All videos done	January 2021	Everyone:

		Tutorials - Alex, Martin, Ahmad Chats - Raili, Anna, Sadat Help with details: Crislyn, Ricco-Karol, Karin
Instagram account management		Karin, Anna
Posting all the chat-videos, instagram promotion	during december	Karin
Searching and contacting stakeholders		Crislyn, Ricco-Karol, Karin
Powerpoint presentation	12th Jan	Alex
Portfolio	17th Jan	Everyone

Media coverage

Our whole project idea was to make real life situation videos to post on social media platforms so these will be easily reachable for youngsters and primary school children. The tutorial videos were planned for distribution through the police and Maarja Punak. The choice of media platform was based on the opinion that this app is commonly used among youngsters. We created an instagram business account where all finished videos are now posted. Our chat-videos are posted as stories that are divided into groups of language - estonian and russian videos. Videos were posted during the month of december and we tried to post consistently. We needed to share our account and promote our posted videos so we could reach as many people as possible. Gathering followers were not so easy as we thought in the beginning of the project. Group members shared our account with their friends so this is where our first followers came. Also we contacted our supervisor and ELU Interdisciplinary Studies Senior Specialist so they could share our account. Unfortunately this also did not help to gather as many followers as we would like.

Big part of our project was the promotions of the postings. The importance of the promotions were to gather analytical data. With the data gathered we now know who were most interested in our videos and who are those most suitable for. The information from promotions showed that we were able to reach a lot of people. As an interesting part we would point out that our videos were seen in Russia even if we first planned to share them only in Estonia and to Russian speakers in Estonia. We were unable to do the promotions as

planned in the beginning because of technical difficulties and incorrectly managed time but we think this was a great place to learn what can be done differently next time.

Self-reflection report

Sadat:

What did you do?

- My task for the ELU project was on the research part to research and write about fake news.

- On the technical part I was in a team with Anna and our task was to edit the videos in Russian concerning password, scamming, oversharing and screen addiction.

What were some difficulties?

- My most difficult task was editing the videos especially adding sounds to the videos because it had to be precise. It took long hours and was very stressful.

Karin:

What did you do?

- I suggested presenting our work on Instagram so I made our gmail and Instagram account.

- I did research about personal information and helped to present our ideas in a midweek presentation.

- I made scripts and translated them to Estonian.

- I have made the Instagram postings and I am the one who is responsible for adding the videos to our Instagram stories. Also I contacted the ELU for a funding request.

- searched for stakeholders and participated in meetings

What were some difficulties?

- The hardest part was to find ideas for the scripts and for the Instagram posts. Also I think we struggled the most with communication as we had such a big group.

Crislyn:

What did you do?

- I did a research on passwords.

- I made scripts about different themes and translated them to Estonian.

- I searched and contacted the stakeholder to ensure the sustainability of the project.

What were some difficulties?

- The most complicated part was probably the start of this project, so many different people with different ideas and different views. At the beginning it was a bit hard for me to understand 100% and follow but as the time has passed, it has been an interesting experience and taught me a lot.

Ricco-Karol:

What did you do?

- I researched information about screen addiction and passwords. I wrote 3 scripts. I also contacted Tamsalu Gymnasium to send our videos to them to show in classes.

What were some difficulties?

- The hardest part was to find ideas for the scripts and for the Instagram posts. Also I think we struggled the most with communication as we had such a big group.

Martin:

What did you do?

- I did research and suggested ideas for the project.

- Worked on tutorial idea formation and video creation process.

-Did focus group research for tutorial videos as well as tutorial video editing based on feedback.

What were some difficulties?

- Video editing for education purposes was something I had never done before.

Ahmad:

What did you do?

My contribution was in research and creating tutorial videos and their edit also with other tutorial members.

What were some difficulties?

- Creating Contents for educational purposes and raising awareness through these contents was something precious and a unique experience.

Alexander:

What did you do?

I came up with the format for the ideas, researched topics, participated in an ELU workshop, participated in a meeting with the Police, worked on and edited tutorial videos with my two other team members, prepared the presentation and presented for the final presentation, and helped Anna in the general project management, involving the creation of our whatsapp group, google drive, and communication with our supervisor and the rest of the group.

What were some difficulties?

Overall group flow, synergy, and communication were difficult to coordinate. It is especially taxing when you cannot meet face to face and while juggling your other courses. Deciding when it is time to take action yourself versus waiting for someone to proactively partake can be unnerving.

Anna:

What did you do?

Since the beginning of the project, I was holding a half-leading position shared with Alex. I also did parts of the research on the topic of oversharing; came up with ideas for three scripts; created demo video with Raili; participated in the ELU workshop, meetings with TTU and Police; did some parts of Instagram management, translated all the scripts from English to Russian; created the videos in Russian language with Sadat, which included:

- typing scripted chats on iMessages
- learning how to use app InShot for video editing
- speeding up the video ~5 times and cutting out the useless parts
- teaching Sadat on how to add sounds to videos, so he was doing the audio tracks
- through Instagram creating clips for the end of our videos (with advice, logos, and music)

What were some difficulties?

I have never done projects of this scale before, so a lot of things were new to me. Communication with the group was an issue, but also self-management, learning new skills in a short time, and balancing the project with other courses. I learned a lot from this experience.

Raili:

What did you do?

- I did a thorough research about screen addiction.
- I translated most of the video (chat) scrips to Estonian and created the texting videos in Estonian - texted myself on two phones, screen recorded it, and then later edited these videos. (like Anna)

What were some difficulties?

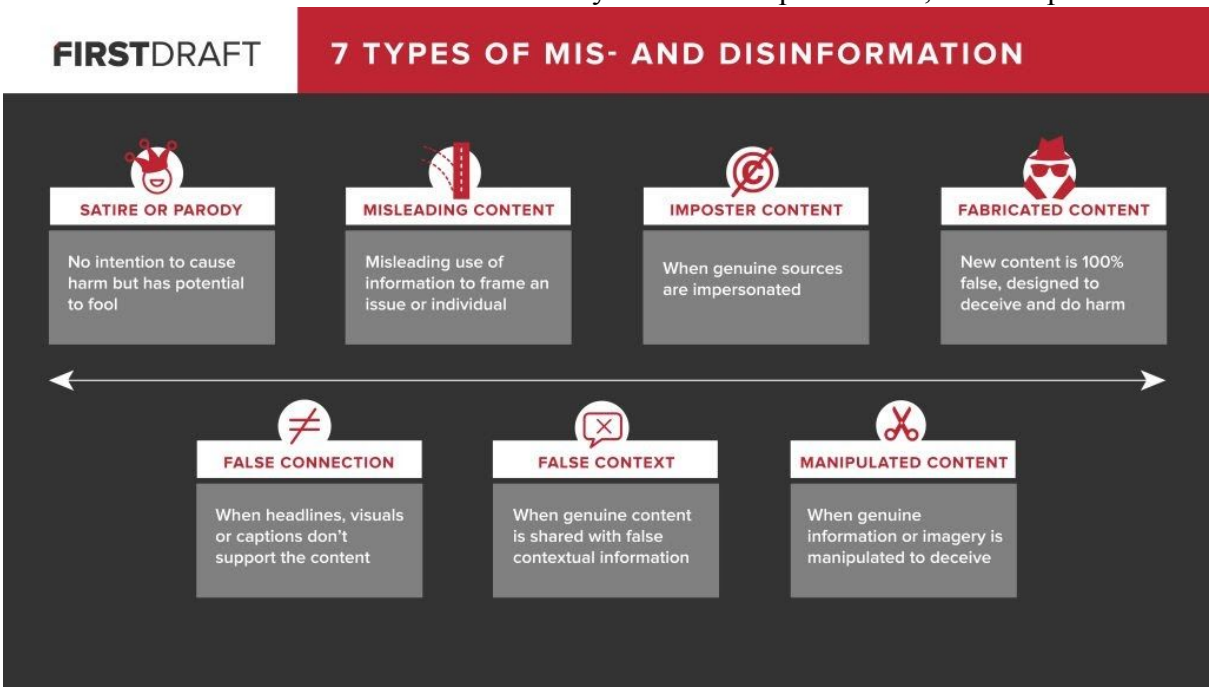
- I was not very happy about how the videos turned out, because I wanted them to be more realistic (sound examples for example), but since the time was running out and I suddenly had a bit too much workload with this project, I did not have the time to create perfect videos with suitable soundtracks, but in the end, I think they turned out just fine.
- Communication!

Extra 1.

Fake News

Fake news means different things to different people. Literally, it means news stories that are false: the story itself is created, with no genuine facts, sources, or quote. In most cases, these stories are propaganda that is purposely designed to mislead the readers or may be designed as "clickbait" written for money making (the author profits on the number of people who click on the story). In recent years, fake news has become rampant through social media because they are easily and quickly accessible.

Ironically, the universe of "fake news" is much bigger than false news stories. Some of these may have a shred of truth but lack any concrete details. They may not include any documented facts. Although some may include essential facts but are deliberately written with provocative language, that leaves out peculiar details or only presents only one viewpoint. Fake news exists within the larger ecosystem of misinformation and disinformation. According to the Merriam-webster dictionary, misinformation is incorrect or misleading information that is mistakenly created or spread; the intent is not to deceive whereas disinformation is false information that is deliberately created and covertly spread "in order to influence public opinion or obscure the truth".
Claire Waddle of FirstDraftNews.com provides a visual image of the seven types of misinformation and disinformation in the ecosystem. As she pointed out, "its complicated"



Where does it come from?
How misinformation and disinformation is produced can directly be attributed to who the author(s) is and the different aims of creating them.

Who are these authors? They may include:

- Partisans who want to influence political beliefs and policymakers
- states using it as a foreign policy tool to influence other states
- Entertainers using it as their content to entertain their audience

- Poor or untrained journalists - who want to create internet traffic on their websites
-
- Someone wanting to make money, regardless of the content of the article

The ease with technology in copying, pasting, clicking, and sharing information online has helped these types of articles to proliferate. In most cases, these articles are designed to provoke an emotional response and placed on certain websites in order to entice readers into sharing them widely. Also, fake news articles may be generated and spread by "bots".

What can one do about Fake news?

- Think critically. Ascertain the accuracy of the information before sharing them
- Think twice. If you any doubt, do NOT share the information

Passively accepting information without double-checking, or sharing a post, image, or video before we have verified and this adds to the noise and pollution in the ecosystem. We have to take responsibility for independently checking what we see online before posting or spreading them.

SOURCES
https://guides.lib.umich.edu/fakenews
https://firstdraftnews.org/latest/fake-news-complicated/
https://www.merriam-webster.com/dictionary/disinformation

Passwords

Two thirds of people use no more than two passwords for all their online accounts. It might seem easy to use one easy password on multiple sites, but there are some threats we might not think about in the first place. Using the same password for multiple accounts is basically a hackers delight because they are able to basically double dip into your several accounts.

Tips:

- If the site has enhanced security, enable it. Have them send you alerts or prompts for additional information if you log into a site from a new computer or location.
- If available, enable two-factor authentication.
- Identify where else you may have used your password and change the password at all the other sites. This may be a painful process but think of the ramifications and impact if someone else can logon to or take ownership of these accounts.
- Do not use easily predictable passwords like your phone number, name, birthdate or something like that.
- Determine your password length.
- Frame a password pattern which contains Alphabets, symbols and characters.
- The minimum password length experts now recommend to avoid being compromised by brute-force cracking is 13
- For extra safety - use a password manager (there are different opportunities on the internet). You'll be relieved when the next data breach happens and you know you're safe.

- This is a list of the 10,000 most frequently used passwords. If any of yours are on it, your account will be compromised in second by any of the most common dictionary-based cracking tools. https://www.passwordrandom.com/most-popular-passwords

How/Where to find help:

- Whether your personal data gets compromised or your password is exposed you must contact the police immediately. Time is critical in the field of cyber security. The sooner the police get the information about cybercrime, the more likely they are to catch the criminal.
- Also, notify the website's management - they might have the tools to help.

Research materials:

https://www.keepersecurity.com/blog/2016/10/07/20-fascinating-facts-about-passwords/

http://www.passwordrandom.com/most-popular-passwords

https://www.youtube.com/watch?v=yzGzB-yYKcc&ab_channel=LastWeekTonight

https://www2.politsei.ee/et/nouanded/it-kuriteod/

Personal information

Personal information is any kind of information that helps to identify a person. That includes name, picture, fingerprints, family information, home address, work place, etc. (Eesti.ee, 2019)

It might seem normal to share personal information with our friends in social media but there are some threats we might not see or think about in the first place.

Some tips how to be wise social media user:

- Share only appropriate pictures - every picture you share can be used by hackers/ web pedofiles etc. It is really important to understand that every picture we share can be found and used for criminal purposes.
- Do not share intimate/naked pictures and share them via messenger, instagram etc! If someone asks for nude pictures please say "NO". These pictures can be spread around the internet - and even often by the people we know.
- Please do not share pictures of any kind of tickets (airplane, concert, etc) as the information from the tickets can be used for different kinds of crimes. As example one: the picture you made from your concert ticket can be used to enter the concert; secondly: tickets often have your personal information on them so even if you do not mean to share any it can be read out of the picture.
- Posting pictures online can have consequences, even if it's your parents who are doing the posting. It's okay to ask your parents to take down/not post pictures that you think might cause you humiliation down the road. Not all funny family photos should be shared with everyone.

As per Estonian Data Protection Inspection law, sharing pictures where other persons are in the background need their permission. Any kind of permission is fine, even verbal. If a picture is shared online on social media without their permission it is against the law and illegal. (aki.ee, 2020)

- Keep your personal information to yourself. Do not share your home address, phone number, personal ID, etc.

Personal identification code is part of usual person information and it is not counted as delicate information. Although it is best to share only your date of birth when needed. (aki.ee, 2020)

We are living in an era of bloggers, and it is promoted as a great job. Many children get inspired by young bloggers on social media and start to behave in a similar manner. They post selfies, their daily routine, things they buy and use, etc. Youngsters get more comfortable in the online environment while exposing themselves to various risks. Children open up their emotions to the general public (usually, their accounts are not private). If the child does not have a support system through family and friends, he or she can become an easy target for pedophiles and other criminals.

What to do?

If you have experienced a traumatic episode, if you need to share emotions or feelings - contact 24/7 Child Helpline 116 111 instead of posting about it on social media.

Everything you post online can be used against you, including any mental struggle.

Lewis, A. (May 7, 2007). Blogs and Teenagers: Teenage Blogging. Counselling Connection Website. Retrieved from https://www.counsellingconnection.com/index.php/2007/05/07/it-is-all-about-me-blogs-and-teenagers-3/

A MOTHER far from home. (November 14, 2019). 7 Questions To Ask When Posting Kid Photos On Social Media. Retrieved from https://amotherfarfromhome.com/oversharing-our-childrens-lives/?utm_source=pinterest&utm_medium=social

Goldstein, K. (May 29, 2019). I'm a Mom and a Children's Privacy Lawyer: Here's What I Do and Don't Post About My Kid Online. Parents Website. Retrieved from

https://www.parents.com/kids/safety/internet/im-a-mom-and-childrens-privacy-lawyer-what-i-do-and-dont-post-online/?utm_medium=social&utm_source=pinterest&utm_campaign=pinshare&utm_content=e80da6fe-39aa-4261-9e3d-59b7933e1f69

- Sharing information about your parents (job positions, surnames, salaries) can endanger yours and your family's safety. People can use this information for data theft and for abduction of a child for monetary gain
- With the same reasoning in mind, don't share the location of your home, pictures of the house/apartment from inside and outside. Remember about inserted features of location tagging in the social media (Instagram, Facebook, etc.). Never put precise locations, especially of the places you visit often (home, school, favorite cafe, playground, etc.)

Information about personal information sharing on social media and what are the criteriums when Data Protection Inspectorate can interfere can be found on webpage https://www.aki.ee/sites/default/files/dokumendid/meediavaidlusse_sekkumise_kriteeriumid_11.03.19.pdf. (aki.ee, 2019)

Sources:

Data Protection Inspectorate. *Question-Answer.* (29.07.2020) Webpage: https://www.aki.ee/et/eraelu-kaitse/kusimus-vastus (13.10.2020)

Data Protection Inspectorate. Disclosure of Personal Data in the Media: Data Protection Inspectorate Intervention Criteria. (19.03.2019) Webpage: https://www.aki.ee/sites/default/files/dokumendid/meediavaidlusse_sekkumise_kriteeriumid_11.03.19.pdf (13.10.2020)

Eesti.ee. Protection of personal data and privacy. (04.11.2019). Webpage: https://www.eesti.ee/et/turvalisus-ja-riigikaitse/turvalisus/isikuandmete-ja-eraelu-kaitse/ (13.10.2020)

Screen addiction

1) What is screen addiction?

It's when screen use becomes so compulsive that it leads to impaired daily functioning in terms of productivity, social relationships, physical health, or emotional well-being - screen use is interfering with work or school, having a negative impact on relationships, encouraging inactivity or less sleep. Problematic screen use may reach a point where problematic screen use does become a recognised behavioural addiction.

There are three main behaviours that help identify addiction - 1) cravings, 2) tolerance and 3) withdrawal. We all have cravings from time to time - for example, a crave for certain food. Early signs of cravings is that a person/child wants to spend more time on the screen, often at the expense of other activities, even ones they used to enjoy. Tolerance is when the amount of something you need to achieve a "high" starts to get bigger. For example, when a person/child used to be happy about using social media an hour a day, when the tolerance has gotten bigger, the person/child wants to spend more and more time on social media to achieve satisfaction. Withdrawal is often associated with feelings such as anger, agitation, depression - in kids, you may notice a stark change in mood and behaviour when devices are taken away or switched off. This cycle is very hard to break.

2) Screen Dependency Disorder (explained)

Adult brains are more developed and are not so much affected, but children's brains are susceptible to significant changes in structure and connectivity which can stunt neural development and lead to a screen dependency disorder, which consists of: internet addiction disorders, internet gaming disorders, problematic internet use, compulsive internet use, pathological internet use, video game addiction, pathological technology use, online game addiction, mobile phone dependence, social network site addiction, Facebook addiction.

Screen dependency disorder can have devastating effects - a child's screen dependency may lead to insomnia, back pain, weight gain or loss, vision problems, headaches, anxiety, dishonesty, feelings of guilt and loneliness. The long-term effects of these symptoms can be as severe as brain damage - many studies have found that screen dependency disorder results in children's brains losing tissue in frontal lobe, striatum and insula, which are the areas that help to govern planning and organization, suppression of socially unacceptable impulses and the capacity to develop compassion and empathy.

3) How much screen time is okay?

- Younger than 18 months - avoid screen use completely.
- Age 18-24 months - choose high-quality programming and watch it with their children to help them understand what they're seeing.
- Age 2-5 years - 1 hour per day of high-quality programs. Parents should co-view media with children to help them understand what they are seeing and apply it to the world around them.

- Age 6+ - place consistent limits on the time spent using media and the types of media, and make sure media does not take place of adequate sleep, physical activity and other behaviours essential to health.

4) Screen addiction among teens - is there such a thing?

Regardless of the problem, "We feel the issue is best conceptualized as a "habit" over an "addiction". "When teens think about their behaviour as a habit, they are more empowered to change." Labeling someone an addict, essentially saying he or she has a chronic disease, is a powerful move. And it may be especially dangerous for teens, who are in the process of forming their identities.

Tech industry is turning toward something "less and less about actually trying to benefit people and more and more about how we keep people hooked." In other words, as long as these companies make their money from advertising, they will have incentive to try to design products that maximise the time you spend using them, regardless of whether it makes your life better.

5) Signs of screen addiction -

- Losing interest in other activities like sports and playing.
- Using screens as a mood-booster - if your child is turning to a screen when they need a "boost" of happiness or need to use it as a comfort when they are bummed out, this could be a sign of over-dependency.
- They are sneaky about their usage - have you caught them on their phones or devices after lights out? Or when they should be doing homework or chores? This could be a sign of an unhealthy relationship with screens.
- Screens are interfering with relationships - whether it's with family, friends or even romantic if they're older, relationships of any kind should not be built around a screen. At home, a fight or argument could stem from screen usage, while cell phone usage could be interfering with quality friend time.
- They experience withdrawal - if taking the phone, video game, iPad, etc away from your child is a constant and frustrating battle, they could be experiencing symptoms of withdrawal.
- Screen time interferes with daily activities - child's device use is interfering with bedtime, meal time, everyday communications and school work. That's a good checklist for adults too.
- You are spending more time with virtual friends than real people - catching up on Facebook or Instagram can make you feel socially connected to others, but it cannot replace the emotional and physical benefits of being with people face-to-face.
- Screen time is the main activity that brings you happiness - if you find you are happiest when watching videos, playing a game or scrolling through social media, that's a warning sign.
- You find yourself spending more and more time online - screens are everywhere - at home, at work, at play, at restaurants.
- The quality of your work has suffered - you may begin a work project on a computer but before too long, you're checking personal emails, looking at sports scores, and buying something you personally need on Amazon.
- You feel agitated if you leave your phone at home.
- Family and friends complain about the amount of time you spend online.
- You've tried to cut back on your screen use without success - although you want to decrease your TV watching, video game playing, or email checking, you haven't been

able to. It's been really hard to create new habits to limit your scream time. You've tried to impose screen limits without much long-term success.

6) Reducing screen time

With more time spent on devices, there is less time for physical activities. Prolonged screen time could also lead to worse eyesight, higher levels of anxiety and stress as well as issues with attention and focus.

How to reduce screen time:

- Track screen time

Monitoring how much screen time is clocked and what it's being spent on could be helpful as many people tend to underestimate the amount of time they spend on electronic devices.

- "Technology- free zones"

Establish zones where electronics are simply not allowed (kitchen, dining room)

- Make your phone go grayscale

Without all those colors, apps like Instagram, Facebook, Snapchat and even new apps, are much less interesting.

- Disable 'raise to wake'

All it takes is a little nudge and your phone's screen will light up and these wake-ups will launch into long unplanned phone sessions.

- Turn off almost all notifications
- Delete social media apps

Delete apps that you just use to "scroll through".

- Don't use your phone as your alarm clock

One minute you're setting the morning's alarm and the next 30 minutes you're in other apps

- Implement a routine

Implementing a routine helps you control your screen time

Research:

https://www.familyeducation.com/kids/5-warning-signs-of-screen-addiction

https://www.crosswalk.com/faith/spiritual-life/10-signs-of-screen-addiction.html

https://choice.npr.org/index.html?origin=https://www.npr.org/sections/ed/2018/02/05/579554273/screen-addiction-among-teens-is-there-such-a-thing

https://www.blackscreens.com.au/what-is-screen-addiction

https://nhahealth.com/screen-dependency-disorder-the-effects-of-screen-time-addiction/

https://nhahealth.com/screen-dependency-disorder-the-effects-of-screen-time-addiction/

Phishing e-mails/scamming

Phishing is a cyber-attack that uses disguised email as a weapon.
The goal is to trick the email recipient into believing that the message is something they want or need a request from their bank, for instance, or a note from someone in their company and to click a link or download in order to steal sensitive information.

Here's How Phishing Works

In a typical case, you'll receive an email that appears to come from a reputable company that you recognize and do business with, such as your financial institution. In some cases, the email may appear to come from a government agency, including one of the federal financial institution regulatory agencies.

The email will probably warn you of a serious problem that requires your immediate attention. It may use phrases, such as "Immediate attention required," or "Please contact us immediately about your account." The email will then encourage you to click on a button to go to the institution's Website.

In a phishing scam, you could be redirected to a phony Website that may look exactly like the real thing. Sometimes, in fact, it may be the company's actual Website. In those cases, a pop-up window will quickly appear for the purpose of harvesting your financial information.

In either case, you may be asked to update your account information or to provide information for verification purposes: your Social Security number, your account number, your password, or the information you use to verify your identity when speaking to a real financial institution, such as your mother's maiden name or your place of birth.

*If you provide the requested information, you may find yourself the victim of identity theft***.**

How to Recognize Phishing

Scammers use email or text messages to trick you into giving them your personal information. They may try to steal your passwords, account numbers, or Social Security numbers. If they get that information, they could gain access to your email, bank, or other accounts. Scammers launch thousands of phishing attacks like every day and they are often successful.

Scammers often update their tactics, but there are some signs that will help you recognize a phishing email or text message.

Phishing emails and text messages may look like they're from a company you know or trust. They may look like they're from a bank, a credit card company, a social networking site, an online payment website or app, or an online store.

Phishing emails and text messages often tell a story to trick you into clicking on a link or opening an attachment. They may

- say they've noticed some suspicious activity or log-in attempts
- claim there's a problem with your account or your payment information
- say you must confirm some personal information
- include a fake invoice
- want you to click on a link to make a payment
- say you're eligible to register for a government refund
- offer a coupon for free stuff

How to Protect Yourself from Phishing Attacks

Your email spam filters may keep many phishing emails out of your inbox. But scammers are always trying to outsmart spam filters, so it's a good idea to add extra layers of protection. Here are some steps you can take today to protect yourself from phishing attacks.

1. Protect your computer by using security software

Set the software update automatically so it can deal with any new security threats.

2. Protect your mobile phone by setting software to update automatically

These updates could give you critical protection against security threats.

3. Protect your accounts by using multi-factor authentication

Some accounts offer extra security by requiring two or more credentials to log in to your account. This is called multi factor authentication. The additional credentials you need to log in to your account fall into two categories:

- Something you have — like a passcode you get via text message or an authentication app.
- Something you are — like a scan of your fingerprint, your retina, or your face.

Multi-factor authentication makes it harder for scammers to log in to your accounts if they do get your username and password.

4. Protect your data by backing it up

Back up your data and make sure those backups aren't connected to your home network. You can copy your computer files to an external hard drive or cloud storage.

Research:

https://www.imperva.com/learn/application-security/phishing-attack-scam/

https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-phishing

https://www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams#report