CLASS **Digital Security and Safety ABC for High School Students**

Duration – 45 min

Digital Security and Safety ABC (Skaitmeninio saugumo ABC)

Objectives	**Teaching Material**	**Time/duration - 45 min**
- to increase awareness of the importance of the digital security; - to introduce the key principles of the digital security; - to know and be able to apply basic digital security and safety measures individually.	Computer, mobile phone, pad; Internet; Projector Pen, pencil, paper sheets	

SLIDE 1. Introduction - 5 min

It is always good to start a class with an icebreaker to energize the attendees and to get their focus on the subject of the class.

Start with one or two questions. If it is an online class the teacher could use the polling form – in MSTeams Forms or Slido.com or some other, or simply ask attendees to say or write in the chat, or raise hands.

- Ask the question. In your opinion what percentage of the entire internet is visible to us?

Students will say (write) figures/percentage. (Answer is in SLIDE 11 – only 4 % of the total internet). It is advised not to give an answer to students now but tell them that the concrete data (answer) students will learn later during this class.

Another question.

- Do you cover your computer camera? Please raise your hand (or write in the chat, or do a polling on slido.com or Forms, etc.) Why? Ask students to comment.

or

- Please raise your hand who uses the Wi Fi in public places? Why Yes, why No? Are you sure that you are safe? Ask students to comment.

or

- Please raise your hand whose mobile phone WiFi function is turned on all the time, when when in town? Ask students to comment, why. After students answer, the teacher can explain that to keep your mobile phone WiFi turned on when in the street or public places it is the same as to shake hands with every person you meet in the street, i.e. mobile phone WIFI connects with every internet provider in the street. The turned on WIFI function allows to trace down the person, i.e. get more information about the person.

SLIDE 2. The Objective of the Class:

Today we will speak about how Internet functions and how to navigate safely and ensure the personal digital security. We will talk about the digital literacy which is not only about the computer or mobile phone hacking. We will discuss how the internet, the digital environment and the social media affect our personal life.

SLIDE 3. These we show you a few cases when the direct harm/damage was done by steeling the digital identity, by steeling private data and then blackmailing, i.e. attempting to profit from that data. Further the cases (examples) are presented. It is adviced to offer the local and current examples.
Case 1. Mission SIBERIA (Misija Siberia) Lithuania https://misijasibiras.lt/apie/. Every year the Lithuanian youth visits places in Siberia where Lithuanian citizens were deported during the Soviet regime. Participants of Mission Siberia meet with local Lithuanians and tidy up and put in order Lithuanian cemeteries in the places of deportation.
A malign person (or organization) created a twitter account under the name "Mission Siberia" and started to tweet that the project was nonsense, that it was fake, etc. The identity was hijacked and the malign communication harmed/diminished the reputation of Mission Siberia.
Case 2. Last year in October a cyberattack on a Finnish psychotherapy group at a therapy clinic left the treatment records of tens of thousands of patients at risk. Patients were blackmailed, they were emailed with demands for bitcoins worth €200-500 (£180-450) in return for having their data deleted.
Around 10GB of information on 300 patients, including diagnoses, contact information and patient diaries, were leaked on a Tor site, offers on selling the data were speculated on the Dark Web.
This happened in Finland, the country which is extremely strong in cyber/digital security.
Case 3. There was a similar case in Lithuania, when the Beauty Clinique was hacked and clients data was stolen, demanding payments for the data not be made public.
Case 4. In December 2020 google stopped function for an hour which caused a very serious chaos, the daily routine was disrupted.
Case 5. This case as a solution example. Scotland runs the program for young people who are trained in digital security and safety and after finishing the course they are contracted/get jobs in organizations, companies to ensure digital solutions. https://www.scottishtecharmy.org/our-projects

Ask students to share their experience.

SLIDE 4. Holistic Security Pyramid . It is important to develop a holistic understanding of elements making the digital security. The basis of the security pyramid is our mindfulness about the digital security, then we have to take care of our equipment, protect it physically, keep locked, close, do not expose them to strangers, do not lose them, keep in safe places. On the very top of the pyramid is the technological security: our passwords, authentication protocols, personal settings, etc.
Slide 5. Arguing that you don't care about privacy because you have nothing to hide is no different than saying you don't care about free speech because you have nothing to say.
Or and additional argument of being security mindful - You lock your apartment, house, bicycle or your car when you leave them, although you also might say that there is nothing very valuable in your house, why should bother to lock it. Neither you share the key of your house with everyone..

SLIDE 6. Digital literacy. We talk about the security because we want you to understand (not to scare). The key principles that we would like you to follow when functioning in the digital space and in social media are following.

- If the service or product in the social media is free, then we are the product or the game.
- Our security is strong as much as the weakest point in the chain;

The Cambridge Analytica case is a straightforward example what and how personal data could be used and abused. Moreover, the Cambridge Analytica case, the process of how they collected loads of very detail information about individuals (87 mln persons). People provided w this information themselves. The company designed the quiz on the Facebook and the app harvested as much data as it could about the user and the users group of friends, etc. and turned the Facebook data into a political messaging weapon. The Trump Presidential election campaign used this data to make their messages very persuasive, tailored according to the psychological characteristic of individual American voter (Psychographics method was used).
More information https://www.theguardian.com/news/2018/may/06/cambridge-analytica-how-turn-clicks-into-votes-christopher-wylie for those who want to learn more about the case.
It raises many questions, but it is important to note that people on FB filled in those quiz voluntarily - did not question why they are giving away so much of private information even not knowing whom to.

Another issue is our biometrics: face, finger prints, etc.. There so many apps and games (for instance an app of how a person will look his/her older age) that collect biometrics and people even do not know in what servers their biometrics is stored, what countries' get hold of their data, what laws protect personal data.
Cambridge Analytica Ltd (CA) was a British political consulting firm

- Digital security is a journey we plan ourselves;
- During it, we must always be ready to be hacked.

We have to know that we can be hacked any time, there will always be new virus, new technologies which might be instruments for malign actions. For instance, the most recent a huge scope espionage case - Russia IT companies hacked many major American private companies and state agencies and manage to collect lot of sensitive information about security technologies, etc.
One more point. Please note that the normative framework of the internet world is still reactive, is still under formation. The core of the digital security should be the mindset of an individual.

SLIDE 7-9. Task to students. In their opinion which of the two passwords (Slide 7) is stronger. The answer is - the second one (Slide 8), it will take centuries to break it. And it is easier to remember, because such password is a meaningful phrase.
Another advice is to apply the multi-factor authentication; do not use the same password for many accounts have a habit to change passwords and write down passwords and keep in one place (a book, block note).

SLIDE 10. How does the internet work? Pose question to students if they know how internet works, whether the selected song in Spotify directly travels to the mobile phone or computer. Let students watch the video explaining the principle of internet https://youtu.be/AYdF7b3nMto (6 min)

SLIDE 11. Come back to the question asked at the very beginning of the class – how much of internet is visible to us, people. Answer – only 4 %; Read the slide. 90 % of internet is Deep Web which is accessible for the search engines. Another 6% is a Dark internet.

SLIDE 12. Practical task for students to test personal resilience to phishing and scams. It will take 10 min. Share the link to the test on chat and ask students to answer 10 questions. Ask students to say what score they got, what questions were easy and what were more difficult. Note, the test is in Lithuanian.
https://www.sukciupinkles.lt

Or ask students to check if their emails are safe, have not been compromised (pwned):
https://haveibeenpwned.com
and/or in https://www.f-secure.com/en/home/free-tools/identity-theft-checker

SLIDE 12—15. Show that WIFI in public places is not secure and safe. It should be noted that, firstly, the internet providers ask many personal data before granting the permit to log in. Another thing, that your device reacts to the nearest internet source (router) which might be a malign equipment, placed for the purpose to get an access into your computer, mobile phone, etc.
The secure way is to use the VPN (Virtual Private Network), i.e. browse the internet via VPN which establishes a protected network connection when using public networks. VPNs encrypt your internet traffic and disguise your online identity. For those who are more interested, worth suggesting and show how VPN functions, for instance, NordVPN (Tesonet product) https://whoer.net;

SLIDE 16. Closing remarks. Remind students that they themselves are responsible for their digital security. It is worth repeating again that:

- If the service or product in the social media is free, then we are the product or the game.
- Our security is strong as much as the weakest point in the chain;
- Digital security is a journey we plan ourselves;
- During it, we must always be ready to be hacked.

May offer/suggest students to watch video on social engineering. The link.
https://www.youtube.com/watch?v=fHhNWAKw0bY