**Topic 4**

1. Security basics

To ensure security of personal data, you should follow those guidelines:

Strong password (10+ symbols, mixed case letters, numbers and special symbols)

Two-factor authentication (via SMS or even better, apps like Google authenticator and Twilio Authy)

Backup your data

Have a password manager and use different password for each site

Try biometric login

Don’t leave your password in obvious places like on computer screen

Use strong Wi-Fi passwords

Ensure not to use common words as passwords – they can be cracked by dictionary attack

Watch out and don’t open or download suspicious emails

Click on “show file extensions” to not open files pretending to be PDF files

Adopt anti-virus

Install updates

Download software only from trusted sources

For enterprises: physical security of data centers (and own all the datacenters), employee access control, strict permission scopes

Security in IT is the defense of digital information and IT assets from internal and external, malicious and accidental threats.

Information security, physical security

Application security – protection of applications themselves

Countermeasures – application firewalls, encryption programs, patch management, biometric auth

Password can be cracked either via bruteforce, or via dictionary attack

….

5. Malware, types

Malware is a program designed to cause some damage to the host computer which can replicate itself

Virus – when executed it replicates itself

Trojan horse – acts as a legitimate program, but does something else in the background

Worm – can replicate without human interaction, distributed via emails and software vulnerabilities

Bot – automated program to perform specific tasks

Spyware – program tracking user actions and sending all personal data to use it to e.g. re-sell

Keylogger – detecting all key-strokes to e.g. leak all users’ passwords

Adware – program showing nasty pop-up ads, clicking on which can install more viruses

Ransomware – program encrypting the data and acting for money for data to be decrypted

Rootkit – masks it or other software existence

Bug – error in the source code which cases program to crash or do unexpected behaviour

6. Ways to be infected

Downloading from suspicious sites, inserting random USB flash drives, installing pirated software

7. Ways to avoid infection

Install antivirus and keep it and the system up to date, do backups, enable firewall, use only software from official websites, don’t open suspicious emails

8. Antivirus software, techniques

Antivirus software – type of utility software which looks for and removes malware

Available on all types of computers. Kaskersky, Avast, Avira, etc

Run in background and detect already existing malware

Or identity the malware that is being sent to the computer

2 ways of detection: virus signature (series of unique program instructions) and heuristic analysis

9. Cyberwarfare attacks, cyber weapon

Cyber weapons used to attack critical government or military infrastructure

From DDOS to tailored attacks

Easily ordered

10. Social engineering, state of the issue

Social engineering – manipulation technique that exploits human errors to gain private info or access

Often for financial gain

For individuals: credentials, card info or computer access

Still very popular today

11. Methods of social engineering

Shouldering – looking up some info behind someone’s shoulder for example

Pharming – redirect to other fradulent websites to gain more data, install more malware, sell counterfeit products

Phishing – Deceptive emails to steal information

Baiting – promising some gain to the individual

Spear Phishing – spoofed targeted emails against individuals or organizations

Vishing – physhing over phone

Tailgating – passing into restricted area with someone

Rogue Antivirus – tricking into believing that malware is installed, and will be uninstalled upon payment

12. Protection techniques against phishing, vishing, smishing

Be cautions about phone calls from unknown numbers. Re-check with your contacts book. Displayed name can be spoofed

You can use voicemail. Record conversations with unknown numbers

Don’t press any buttons, it can be used against you in automatic phone systems

Don’t enter personal info in pop-up screens

Install spam filter and adblocker

Don’t open suspicious links

13. Encryption, it’s types, usage, importance

Encryption is the process of converting data into a format which is called cipher text

Asymmetric – secret key cryptography, data is decrypted and encrypted with it

Symmetric – private key cryptography – private key sign, public key verify/recover

14. Protection against ransomware

Install antivirus software, updates

Don’t pay for decryption

Update OS

Backup data to external drives and clouds

Don’t enable macros in emails