MUNI
MED

Computer network user

Daniel Klimeš , Jan Krejčí , Roman Šmíd

MUNI
MED

Safety principles when working with IT

Risks when working in a computer network

Roman Šmíd , Jan Krejčí , Daniel Klimes

Computer security

- is part of information security
- deals with the part of security that is related to ICT
  - Network security
  - Internet security
  - Security of end devices
  - Cryptography (PKI and certification authorities, e-signature, e-archiving)
  - Special means (wiretapping, surveillance)
- the goal is
  - prevent computer attacks
  - ensure safe operation
  - limit the likelihood of risks occurring

MUNI MED

Computer security

- Relates to:
  - end devices, (personal computers, mobile devices)
  - all other parts of the IT infrastructure, especially servers and computer networks.

- includes roughly the following activities:
  - Ensuring protection against unauthorized physical manipulation of IT (physical theft)
  - Data access security (authentication and authorization)
  - Ensuring protection against unauthorized data manipulation (violation of integrity, confidentiality and availability)
  - Ensuring data is backed up (recovery plan)
  - Security of software protection against theft (copyright protection)
  - Security of communication and data transfer (cryptography)

Data security above all else

- data is the most valuable electronic asset we have
- in order to be used correctly, they must be **available and only to authorized persons**
- in order for them to be protected, they must be secured
  - so that we don't lose them somehow
  - so they don't end up in the wrong hands
- but the consequences of the loss are individual, it depends on the nature of the data
  - if we lose them or our key information is acquired by a competitor, it could also mean the end of our business or operations
  - when it comes to personal or sensitive data, it can be used to blackmail or compromise the user

The most common attacks and threats

- **a virus** is a malicious program that can spread and operate without the user's knowledge
- **phishing** is an attack that uses social engineering methods to obtain sensitive or login information
- **spyware** is software that sends data from an infected computer without the user's knowledge
- **DoS and DDoS** is an attack that causes a service to be overwhelmed and shut down
- **spam** is unsolicited commercial communication (most often by e-mail)
- **hoax** is deceptive information
- **ransomware** is a virus that encrypts the end device, for decryption the attackers want a high ransom in an anonymous currency

Network security - home wifi network I.

- The basic thing is not to leave the wireless access point or router in the default settings from the manufacturer.
- It is necessary to set a new administrator password and choose the appropriate Wi-Fi security.
- Existing forms of security for home wifi routers:
  - Open network (do not use even by mistake, communication is not encrypted)
  - WEP encryption (obsolete, long broken)
  - WPA-PSK encryption (can be used in an emergency, but has weaker encryption)
  - WPA2-PSK encryption (if AES or TKIP encryption option is additionally available, use AES encryption)
  - WPA3 encryption (new since 2018) – improved encryption, but not all devices support it

Network security - home wifi network II.

- in domestic conditions, we prefer WPA2-PSK security in combination with AES encryption
  - offers a reasonable level of security
  - It is already supported by all wireless devices
- it is necessary to choose a good PSK (reasonably long and complex password) and also a non-trivial name of the access point (SSID).
  - a password of at least 13 characters, a combination of letters and numbers is recommended
  - do not use known passwords (there are lists of the most used passwords)
- turn off WPS (WiFi Protected Setup)
  - broken in December 2011

Internet security - email threats

Threats:

- SPAM - unsolicited messages sent for the purpose of:
  - Advertising distribution
  - Collection of active email addresses
  - Distribution of malicious code
  - Lure of money

- Phishing - an unsolicited message, sent in bulk for the purpose of:
  - Enticing access data to various services
  - Eliciting private information

- Spear Phishing – an unsolicited message targeted and customized for a specific user
  - The goal is to introduce malicious code into the organization's internal network in order to gain access to sensitive company data
  - It is a very sophisticated attack that even experienced users can fall for

MUNI MED

Internet security - email rules

- Rules:
  - Do not click on links in unknown messages (danger of address forgery, redirection to a page with malicious code)
  - Do not open attachments in unknown and suspicious messages
  - Do not send logins and passwords, credit card numbers anywhere
  - Paying attention to suspicious features in messages (machine-translated text, links leading elsewhere than their description, messages pretending to come from mass-used services (Facebook, banks, etc.), suspicious sender address
  - Do not ignore any warnings from antivirus programs
  - Don't be intimidated (If you don't install XY software, your computer will be at risk...)

Internet security
sample spam containing a virus

Dear Madam, dear Sir,
thank you for your trust in online shops obchody24.cz.

With this email, we confirm that we received your order in good order.

Order number (variable symbol): JCBDF729B439057
Order date and time: 11.01.15 00:45
Contact details: Barbora Záňová, +420 604 920 148

Your order:

SONY DSC-F828 Cyber -Shot 8 million pixels , white: 1 x CZK 23,549.00 = CZK 23,549.00
Transport PPL: 113 CZK

Total purchase price incl. VAT: CZK 23,662.00 Payment method: Payment in advance - payment card
Note: Payment confirmation and invoice can be found in the attached file (ucet111D535.zip)

-

Now please wait for our operator, who will contact you within a maximum of 1 working day and agree on the details of your order.

MUNI MED

Internet Security - Sample Phishing

AirBank

Dear Customer,

your account has been blocked For more details You will be unable to deposit, withdraw or spend while your account remains disabled. Please click the Sign in below and confirm your details for re-enabling your account

Login

Copyright © 1999-2018 AirBank. All rights reserved.

Vážený zákazníku.

Toto je maximální varování pro ochranu vašeho účtu před neoprávněným přístupem.
uvedených pokynů.

Chcete-li svůj účet okamžit uvedený odkaz.

https://www.crestwoodtrust.com/contacts/detailed/verifyaccount/processes/auth/index.htm
Kliknutím přejdete na odkaz.

https://www.fio.cz/login/bank/startup/login-infodata/html

****

Copyright © 2018 Fio banka

MUNI MED

Internet Security - Instant Messaging

- What is IM ? Facebook chat, WhatsApp, Viber, Skype, Telegram ... any real-time communicator
- Threats in instant messages are similar to email threats
- The rules for safe use are the same as the email rules
- Threats stemming from an out-of-date IM client
  - An outdated client can be exploited to install malicious code on a PC without the user's knowledge

  - **Ensure regular updating of the client used to the latest version and have an updated anti-virus program**
  - **Not mindlessly clicking on every link someone sends me**

MUNI MED

Internet security - cloud services

- **MS OneDrive, Goggle Drive (Google Drive) etc ...**
- **The threat is the handing over of your data to a foreign entity.**
- With most cloud services, by using them, you agree that **the company can use the data uploaded there for any purpose** , pass it on to other entities, publish it, analyze it, etc.
- This applies to the vast majority of unencrypted cloud providers and email service providers.
- **These services are unsuitable for any sensitive data** – personal data, scientific publications….
- A possible solution is **encrypted cloud services** , i.e. those where the service provider cannot see your data, because it is stored encrypted on their servers and only the user has the key.
  - Email services – Protonmail , Lavabit ,…
  - Storage Services – SpiderOak , Mega.nz,…
  - If you don't want to hand over your data to a third-party company, use only encrypted cloud services. It is always advisable to read the terms of use of the given service.

MUNI MED

Internet security - social networks

- The basic rule is not to click on anything, think. Even your friends' computers can be attacked by malicious code that sends posts or links to their FB profile or private messages.
- Always remember that what you post about yourself on the Internet usually cannot be taken back.
- When using social media, think about who and what information you make available.
- Beware of mindlessly spreading or sharing/ liking hoaxes (HOAXes).
- **Facebook** - misused to spread spam, hoaxes, malicious code
  - Trusting friends is dangerous: I'll click on anything one of my friends posts
  - Difficult orientation in an environment that changes frequently - traps for uninformed users
  - Clickjacking - a combination of social engineering and Like buttons
    - Example: Click all the Like buttons one by one to view the video, etc.
    - In the end, it's often just a website with malicious code, a page that sucks people's money or artificially increases traffic
- **LinkedIn** - similar rules apply to Facebook, so far less widespread, focusing on the workspace
- **Twitter** - spreading addresses of sites containing malicious code

MUNI MED

Security of end devices

- End devices can be considered:
  - Desktop computers
  - Notebooks
  - Tablets
  - Smart phones
  - Smart watch

- The security of end devices can be increased:
  - Antivirus
  - Antispyware
  - By backing up your data
  - By regularly updating the OS and the programs used

Security of end devices - mobile

- main problems:
  - operating systems and their updates

    Device manufacturers are often slow or non-existent in updating the OS in response to new security vulnerabilities. Especially older phone models are often left without updates by the manufacturer and thus vulnerable to long-known bugs. It is always advisable to check whether the manufacturer guarantees the availability of system security updates for its device, and for how long. (E.g. Android One service , etc.)
  - user inattention

    When installing new applications, the OS always asks the user if he can grant the application permission for certain activities within the system (eg reading/sending SMS, accessing the Internet, etc.). Users should be careful what permissions they grant to an app and what apps they install.

- devices often include:
  - confidential user data
  - access to various services (email, banking, etc.)

- however, they are often not adequately secured in case of device loss.
  - A PIN or gesture unlock is not enough
  - Encrypting the entire device, including the SD card, is sufficient protection.
  - It is also convenient to activate the option of remotely erasing the device in case of loss

- full-fledged work tools - the need to follow the same safety principles as when working with a PC

Security of end devices - mobile

- A smart phone (smartphone) contains an advanced operating system, allows the installation and modification of other programs that further expand the capabilities of the phone.
- OS examples: Android, iOS, Firefox OS, Tizen , MeeGo , HarmonyOS , ChromeOS
- Advantages:
  - a large number of applications and thus the possibilities of what can be done with the phone (office, games, reading books, Internet applications, navigation, etc.)
- Disadvantages:
  - typically shorter battery life
  - often larger dimensions
  - various security risks (viruses, disclosure of private information)
  - Price

Security of end user devices - tablets

- Touch devices, the operating system often the same as on smartphones, can also have telephone functions.
- They form an intermediate link between smartphones and classic personal computers or laptops.
- Some newer tablets are full-fledged computers with a standard OS
- OS used: Android, iOS, Linux, Windows

Security of end devices - connectivity

- the connection is wireless (WiFi or LTE)
- may contain
  - full-featured internet browser
  - email client
  - Communicators
  - VoIP clients
  - VPN
  - terminal clients
  - remote area
- when connected via GSM, the data tariff may be a limiting factor. After the data limit is exhausted, the connection slows down and working with the Internet becomes inconvenient or does not work practically at all. Choosing the right data plan is important.
- A full-fledged work tool - the need to follow the same safety principles as when working with a PC

Ensuring protection

- Principles when working with the Internet, email and social networks
- Regular updates
- Antivirus and antispyware
- Saving access passwords
- Proper home network security
- **Prevention is crucial!**

MUNI MED

Ensuring protection - regular updates

- you need to understand the messages of the operating system and other programs
- be able to respond adequately to events requiring a user response
- update regularly:
  - operating system
  - antivirus database
  - antispyware database
  - all software

MUNI MED

Ensuring protection - regular backups

- The data is often more important than the hardware itself

- It is important to back up:
  - Do I know what is being backed up from my device, where and at what intervals?
  - Can I check if the backup is working?
  - Can I restore the backed up data if needed?
  - Do I have backups in multiple locations?
  - Are my backups secure?

  - We back up at regular intervals, preferably automatically

Ensuring protection - backup options

Backup options:

- Physical medium
  - CD/DVD
  - Another computer
  - USB drive
- NAS
  - (Network Attached Storage - "data storage on the network", for example an external disk connected to the network)
- Cloud storage
  - OneDrive
  - GoogleDrive
- Application backup
  - Windows Backup (in Windows 7 and Windows 10)
  - Duplicates (for both Windows and Linux)
  - Cobian Backup (for Windows)
  - SyncThing - synchronization

Ensuring protection - antivirus

- It is advisable to use some of the commercial solutions, but it is recommended to use at least some freely available antivirus product.

- For domestic non-commercial use, these are for example:
  - Microsoft Antivirus - a product of Microsoft, since Windows 10 part of the system as Protection against viruses and threats. Sufficient, in Czech.
  - Avast Free Antivirus - product of the Czech company AVAST Software, free registration renewal required after 1 year
  - AVG Antivirus FREE – another Czech product, also suitable for normal use
  - Panda Cloud Antivirus FREE – cloud-based antivirus, less PC load

- Anti-viruses usually automatically update their virus databases, you need to leave this function enabled!

Ensuring protection - antispyware

- Antispyware is spyware removal and blocking software.

- There are plenty of free programs for home use:
  - Spybot Search & Destroy - free for commercial purposes, Czech translation
  - Spyware Terminator - free even for commercial purposes, Czech translation
  - Ad Aware SE Personal Edition - free for non-commercial purposes
  - Windows Defender - a standard component of Windows Vista and higher versions

- antispyware is not necessary all the time, but it is advisable to occasionally install one, update it and have your computer scanned .

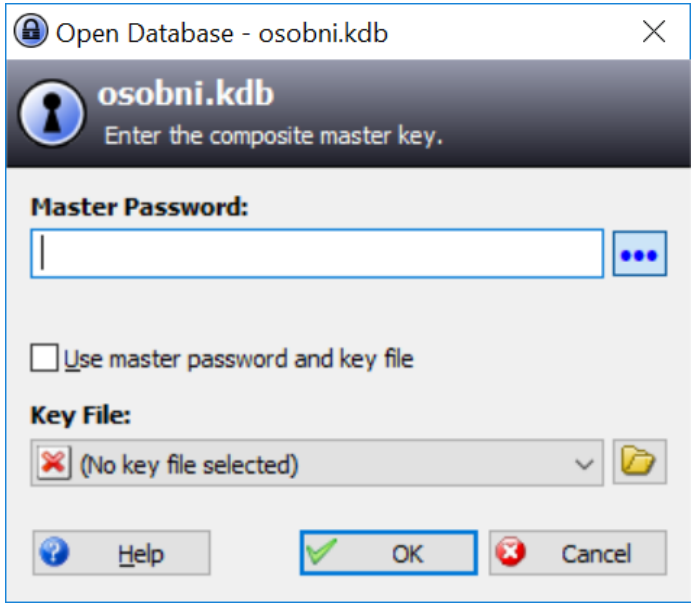
Ensuring protection - access passwords

We normally use many different internet services - we have many access data

- Dangerous tendencies - to use the same and simple password everywhere
- Well-known services face frequent hacker attacks to steal user credentials (often successfully)
- If I have the same login and password everywhere, a hacker will gain access to all my accounts at once !
- Principles:
  - **unique password** for important services (access to the bank, etc.).
  - Email and password are often required as access data. **Never enter the same password as we have in the email !!** If this information is disclosed , hackers will start using your e-mail to spread spam and viruses, and there is a risk of blocking your account.
  - If we have many passwords, consider using **a software password manager**
  - **two-factor authentication for important services (banking, etc.) (e.g. confirmation via SMS code, etc.)**

Access passwords - password manager

- A password manager is a useful helper for safe work with passwords
- You only need to remember one main password, the other passwords are safely and clearly stored in the program.
- Among the most famous software in this category are:
  - **KeePass Password Safe** - clear password manager, free and for commercial use, there is also a version for mobile phones
  - **Bitwarden** - add-on for Internet browsers, prefills Internet forms, generates passwords
  - **Password Agent -** can store passwords and other information, installation option on a USB stick



MUNI MED

Services providing authentication

- Third-party authentication services are also a suitable way to authenticate users.
- We set up an account with the provider and then leave the transmission of authentication information to the provider.
- The advantage is that we only have to remember one name and password, and in all other services that support it, we will use the login through this provider.
- We also have control over what data we pass on and to whom.

- mojeID (www.mojeid.cz) is a widespread and trusted provider , which can also be used to log in to state administration websites, the Citizen Portal, etc.

Breach of protection - what we are at risk of

A breach of protection may result in loss or unavailability of data:

- caused by inattention or carelessness (they can be prevented):
  - loss of information
  - unavailability of information
- caused by a third party (attacker, thief):
  - data theft
  - misuse of data

Problem situations - accidental data leakage

Caused by inattention or carelessness (they can be prevented):

- loss of information
  - occurs in the event of technical failure (for example, disk failure), or deletion or shredding by the user (by mistake)
  - neither you nor anyone else has the information –> they cease to exist
  - the only protection is regular backups
  - the consequences of data loss are individual, depending on the nature of the data.

- unavailability of information
  - we do not have access to the storage location (we are offline), or we have lost access data (password, key)
  - the main protection is regular backups
  - secondary protection in some cases can be a backup access path (or access backup)

Problem situations - data leakage by attack

Caused by a third party (attacker, thief):

- data theft
  - occurs during data theft or a ransomware attack
  - availability protection is regular backups
  - protection against abuse is the security of data carriers (encryption or password - external disk, flash disk, telephone, ...)
  - there is a possibility of data misuse

- misuse of data
  - occurs when data is stolen or actively attacked by an attacker
  - we do not physically lose data as such
  - if the data is misused, its value decreases and the information can be used against us

Problematic situations - what threatens us

- Direct financial loss (theft of money from an account via a credit card)
  - Correct setting of limits on the card
  - Authorization of all operations through the second factor
- Police prosecution (accusation of using a PC for illegal activities)
- Problems at work (blocked email, VPN, ...)
- Blackmail and discrediting (publication of sensitive information, photos, e-mails...)
- Data Loss (RansomWare)
  - WannaCry (May 2017)
  - Benešov Hospital (December 2019)

    In a ransomware attack on a hospital in Benešov at the end of 2019, the network drives of all devices in the network were encrypted and the hospital was out of order for more than 3 weeks.
  - FN Brno – in 2020, FN Brno experienced a similar attack, vital hospital systems were shut down, operations were postponed, and there were large financial losses.