



Funded by the  
Erasmus+ Programme  
of the European Union

Overview of Understanding and Handling Cyber-Attacks

# Proactive Actions

**Safeguarding against Phishing in the age of 4<sup>th</sup> Industrial Revolution**

**[www.cyberphish.eu](http://www.cyberphish.eu)**

*This project has been funded with support from the European Commission.*

*This publication [communication] reflects the views only of the author, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*



# *Learning Goals*



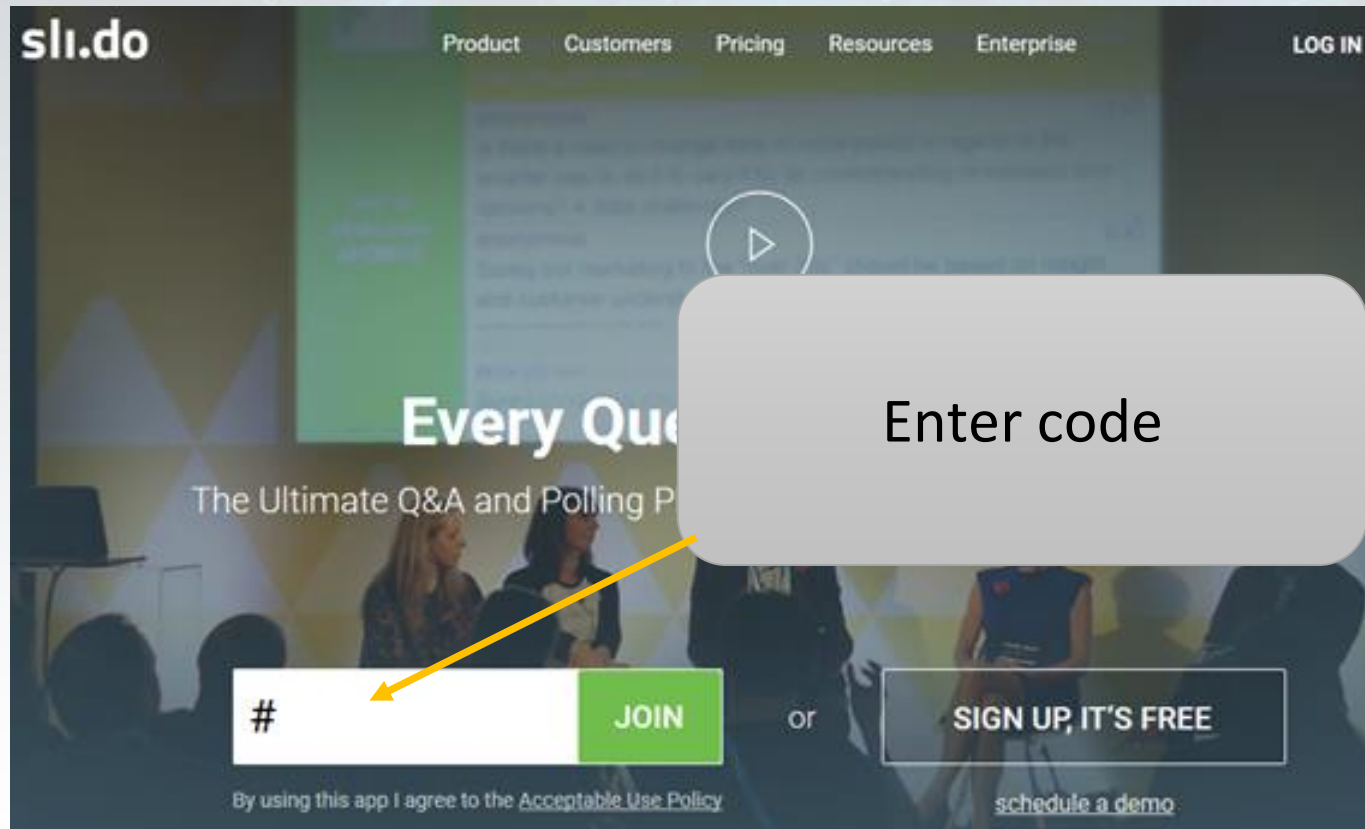
Cyber hygiene on the Internet  
Cyber hygiene on the workplace  
Technological tools and measures

# Student Workload



Lecture	2 h
Audio and video material	1 h
Case studies	0,5 h
Further reading	1,5 h
Preparation for exam	1 h

*Practical exercise: please provide as many adjectives as possible in the sli.do environment related to the security of the internet and digital devices*



Enter code

# *Internet Cyber Hygiene*

**USERNAME:**

Administrator

**PASSWORD:**

•••••

**LOGIN**



# Personal Information

Personal information is information that defines the relationship between a specific piece of information and a person.\*



\* Malinauskaitė-van de Castel, Inga. *Data subjects' rights in virtual social networks: doctoral thesis.* – Vilnius, 2017.

# *What are Personal Data?*

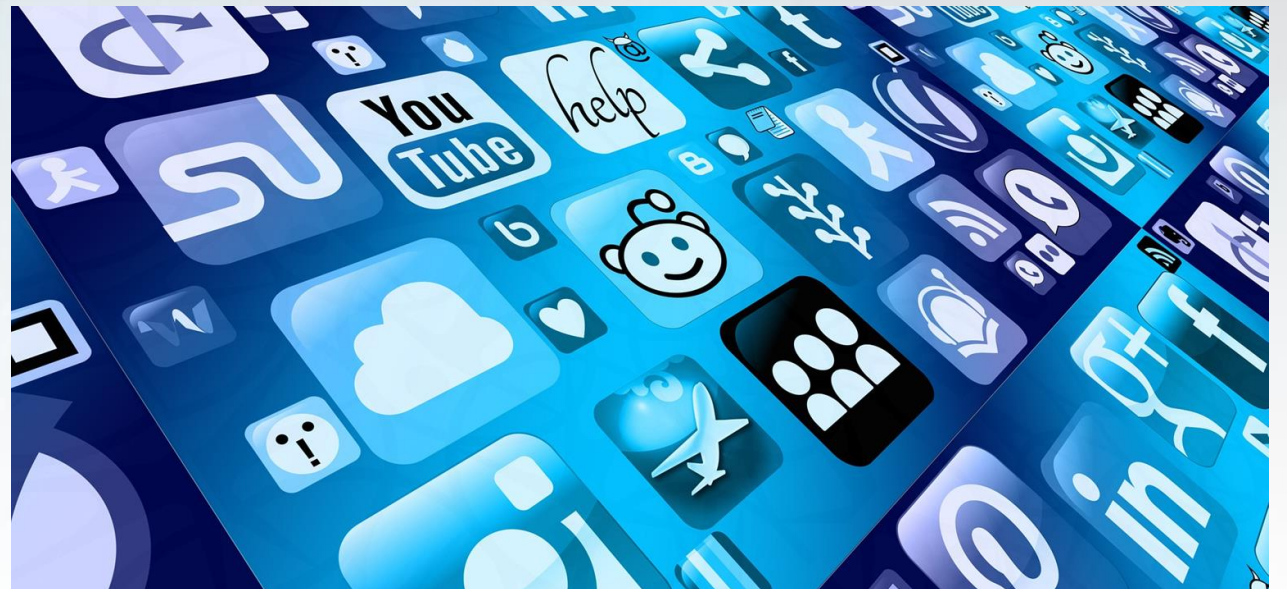
- Person's contact data (i.e., name, surname, home address, mobile number)
- Biometric data
- Personal code
- Persons' ID or passport code
- Person's income
- Passwords
- Financial data
- Customers data
- Intellectual data without owners' permission





# What are Public Data?

- Public data may be:
  - Company code
  - Company email, like [info@company.com](mailto:info@company.com)
  - Depersonalized data
  - Nickname
  - Hobbies
  - Nature photos
  - Blogs
  - ...



# Why it is Important do not Publish Personal Data

- Identity theft
- Cyber crimes (theft, blackmail, harassment)
- Possible damage to reputation:
  - Anyone on the Internet could access freely available data
  - Published data will be used against the person
- The more information is published on the Internet, scammers easier could steal persons identity, use data for attacks etc.



# Check What Info are Available About You

- Use a search engine to search for yourself online and see what information you can find
- Check information about yourself by using different search engines
  - Google
  - Bing
  - DuckDuckGo
- Use quotations and other symbols performing search, examples:
  - “Name Surname” – you will get information about this person
  - “Name Surname@” – you will emails associated with this person
  - “Name Surname” filetype: PDF – you PDF document where this person is mentioned

# *Publishing Photos*

- Have you thought about:
  - Who has access to your photos?
  - Are there other people in the photo?
  - Is there GPS information of the location stored in the photo?
- Using search engine you can try find photos with you



# *Photos and Videos Sharing*

- Respect other people's privacy
- If you want to share a photo or a video with people you know, it is good manners to ask permission
- Do not distribute photos of other people's children without their parents' permission
- Do not use photographs of people in your promotional material unless they have given their permission
- Photograph strangers only in a public place. If the person has expressly stated that they do not want to be photographed, you cannot take photographs of them
- Do not share photos and videos as a tool for revenge or ridicule
- Do not share violent, hateful or offensive photos and videos. Even if you want to condemn violence or hatred
- Do not share photos and videos where you or your friends or relatives are caught breaking the rules, behaving inappropriately or even breaking the law

# *Photos and Videos Sharing*

- If you find a photo of yourself or your relatives and you do not want it to be shared, you could take the following measures
  - Contact the publisher and request removal
  - Contact the administrator of the social network and ask for the photo to be removed, explaining the situation
  - If the above steps have not helped, contact the Personal Data Protection Inspectorate

# *Friends in Social Networks*

Be smart and selective when who you accept users as a friend on a social networks



# *Beware of Publishing Any Identifying Information About Yourself*

- Everything you put on the Internet could be permanent
- Information could be available on archives, i.e. <https://web.archive.org>
- Other people could
  - save information on their devices
  - print or
  - re-publish information on the Internet













# Monitor What Information is Published on the Internet About You

- You can monitor if new information about the user is published on the webpages, blogs, scientific research, forums, YouTube by using change detection and notification services, like [Google Alerts](#)
- On the Google Alert system it is possible to provide keywords
- When new results is found, user will get notification email or user can view results at [www.google.com/alerts](http://www.google.com/alerts) at any time



# *Request for Removal of Personal Information from Google Services*

- You could report providing complete information that content about you would be removed from Google services
- You could request to remove content from such Google services

-  Google Search
-  Blogger/Blogspot
-  Google Maps and related products
-  Google Play: Apps
-  YouTube
-  Google Images
-  A Google Ad
-  Drive and Docs
-  Google Photos and Picasa Web Albums
-  Google Shopping
- See more products

# Check if Your Data Was Breached

- You can check if your email or phone is in a data breach by using online tools, like [Have I Been Pwned?](#)
- You can also check if your password was breached <https://haveibeenpwned.com/Passwords>. Breached passwords are searchable online and anyone could download them

';--have i been pwned?

# Monitor Data Breaches

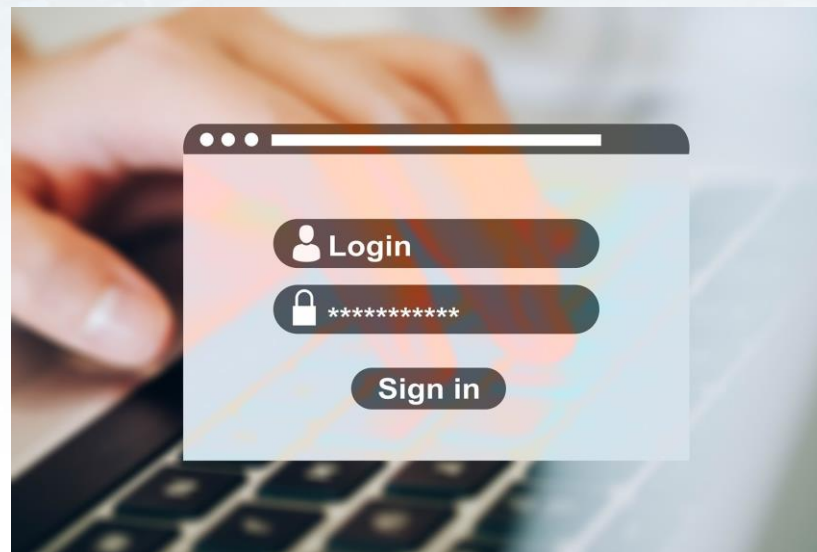
- You can register on special portals, which informs if user account was breached i.e. <https://monitor.firefox.com>



More information: [www.cnet.com/tech/services-and-software/firefox-monitor-shows-if-your-personal-information-was-lost-in-a-hack](http://www.cnet.com/tech/services-and-software/firefox-monitor-shows-if-your-personal-information-was-lost-in-a-hack)  
<https://www.online-tech-tips.com/computer-tips/what-is-firefox-monitor-and-how-it-protects-your-login-details/>

# *Actions if Your Account Was Breached*

- If your data was breached, it means that your email and password could be in cyber criminals hands. In such case you should
  - change your password of breached account immediately
  - change other accounts password if you used the same password
  - enable two-factors authentication, if vendor supports it



# *Avoid Sharing Personal Details*

- Users should be cautious about how much information provide, because usually people tend to share more information on social networks
- Do not publish own plans, home addresses, financial information
- Customize your account security settings and manage who can see your posts and other information



# *Use Different Email Box for Different Purposes*

- Email for personal life, like [name.surname@gmail.com](mailto:name.surname@gmail.com)
- Email for business purposes, like [name.surname@company-name.com](mailto:name.surname@company-name.com)
- Email for registrations
  - you could create account for registrations in free email services portals
  - you could use temporary email service, like [Guerrilla Mail](#), [Mailinator](#)

# *Don't Trust, Just Verify*

- Be caution when you click links that you receive in messages from your friends
- Don't trust that a message really is from whom it says it's from
- *READ before clicking* anything to download or to install free programs





The image features a hand holding a smartphone in the center. The background is a complex digital network of white lines and dots on a dark blue gradient. Two large, glowing spheres made of interconnected nodes are positioned on the left and right sides. A semi-transparent dark blue horizontal bar is overlaid across the middle of the image, containing the text.

# *Digital Devices Hygiene*

# Digital Device Security

- Users must behave responsibly when using both computers and smart devices, and use appropriate security measures, because smart devices have similar functions to desktop or laptop computers
- Using these devices can lead to the same security problems as computers, loss of data, etc..
- Smart devices can also be protected against viruses and other potential online threats just like computers

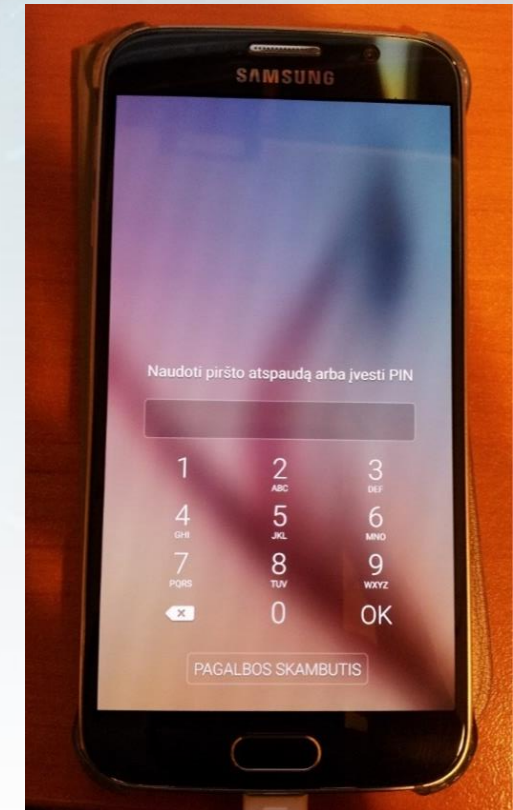
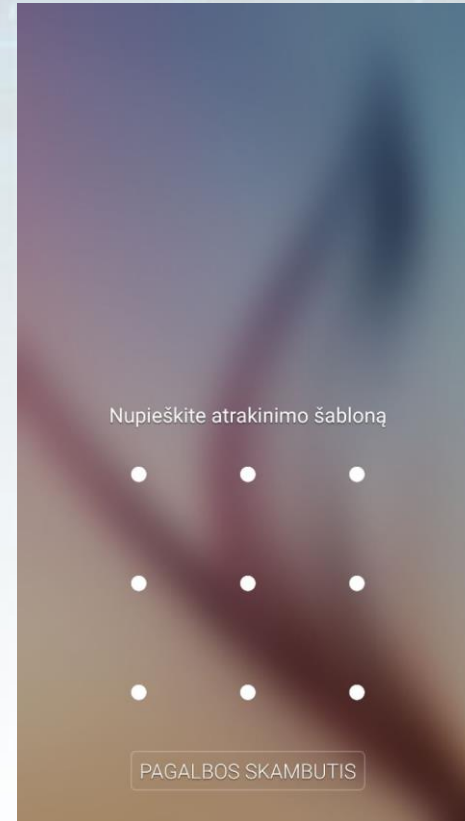


# *Use Logins and Passwords Connecting to Digital Devices*



# Activate Use of a PIN or Other Secure Login Function

- For mobile devices, it is recommended that you activate your PIN each time before using your device to prevent unauthorized persons from browsing your device, viewing your personal data, photos, etc.
- Some devices have other secure login features such as fingerprint scanning, eye scanning
- Enable auto lock function after you finish work with device



# *Private Browsing*

- Disable third party cookies
- Use private browsing mode
- Use browser plug-ins such as [HTTPS Everywhere](#)
- Use Virtual Private Network VPN solutions if you need to hide traffic
- Check what Google knows about you  
<https://myactivity.google.com/myactivity>

# *Password Management Guidelines*

- Do not share your usernames and passwords to other persons, even to your colleagues
- Never store your passwords in a note, memo or file on your computer or mobile device
- Do not use passwords made up of names, addresses, phone numbers and other easily guessed words
- Use different passwords for different accounts
- Change your passwords periodically for better security
- Use password managers to protect your passwords, like [Firefox Lockwise](#), [NordPass](#), [KeePass](#)



# *Advices Leaving Your Workplace*

- Disconnect from information systems when finish work
- Closing the browser does not necessarily log you out
- Lock your digital device when you are away from your device even for a while. If you leave unlocked device other persons could
  - Access your information without your permission
  - Access confidential data
  - Send emails from your account
  - Delete your files
  - Do another malicious activity



# *If You Use Someone Else's Device*

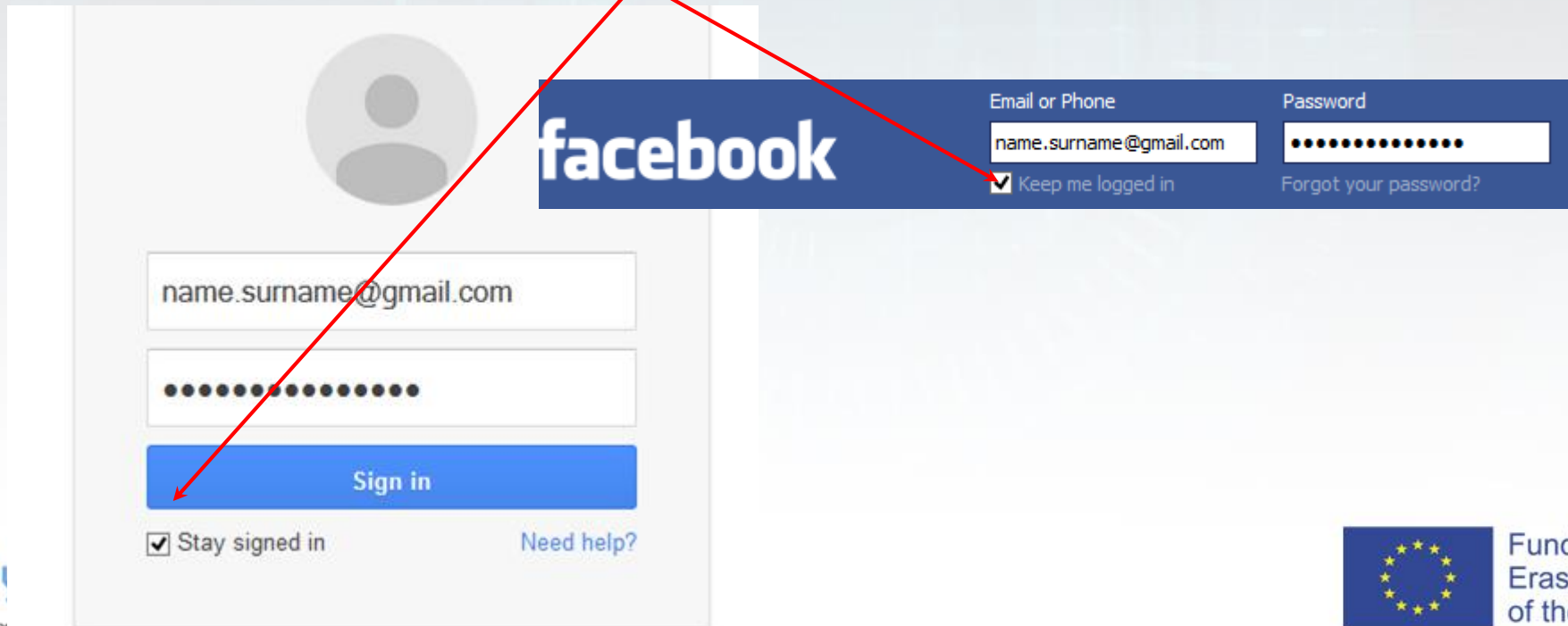
- Change the password of the service you used from a trusted computer and network, if you used someone else's device and you suspect unusual activities
- Use a "virtual" keyboard to enter passwords
- Log out of websites that require authorization
- Do not save your login information
- Delete your internet "history" and files you downloaded

# *Defend Yourself Against Shoulder Surfing*

- When you are working with digital device, like PC, laptop, smart phone, someone could observe looking over someone's shoulder what user is doing on the screen, what information or passwords is inputting, in order to get information and use it for malicious actions.
- In order to protect from yourself from shoulder surfing:
  - locate an area where you can sit or stand with your back to the wall
  - Be aware of your surroundings at all times, not just people but also video cameras that might be taking video of your actions

# Login and Logout

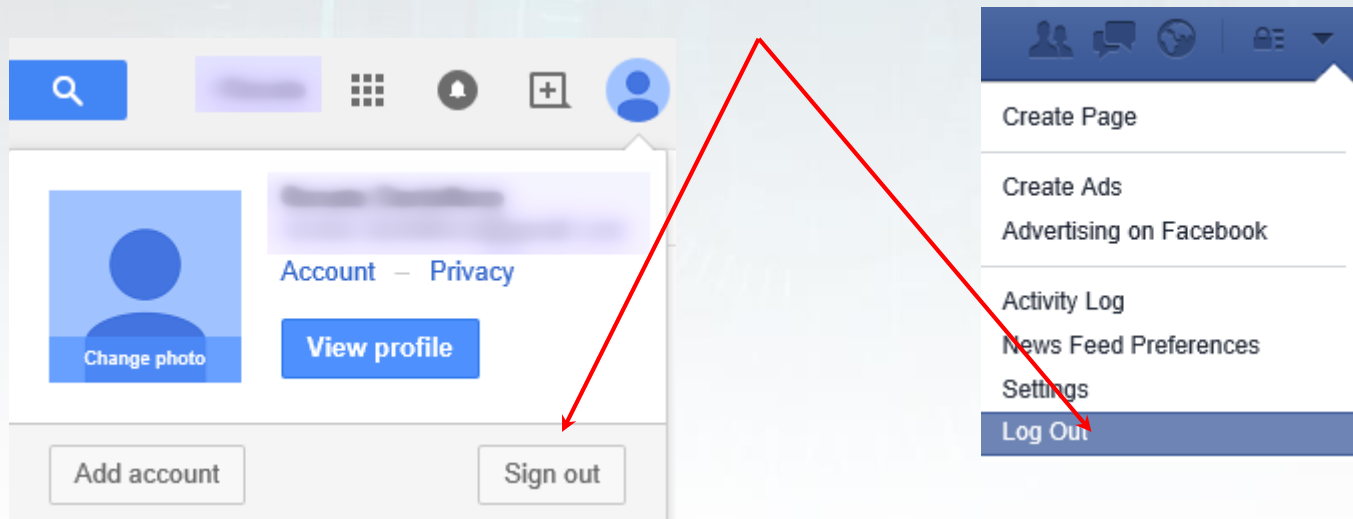
- Using public computer (or someone else's device) uncheck box "Keep me logged in" or "Stay signed in"
- Don't allow the web browser to remember your password to automatically log you in



The image shows a screenshot of the Facebook login interface. A red arrow points from the text "Don't allow the web browser to remember your password to automatically log you in" to the "Keep me logged in" checkbox, which is currently checked. The login form includes fields for "Email or Phone" (containing "name.surname@gmail.com") and "Password" (masked with dots). Below the "Keep me logged in" checkbox is a link for "Forgot your password?". The main login form has a "Sign in" button and a "Stay signed in" checkbox (checked) with a "Need help?" link.

# Login and Logout

- Using public computer (or someone else's device) log out of accounts and apps



# *Disconnect from Systems Remotely*

- You can sign-out remotely, if you forgot to sign-out from your accounts working with public or someone else's computer or if you lost your digital device
- You need to check, if service provides remote sign out function, like it has Google, Facebook, Dropbox, Netflix, Microsoft, Instagram, Amazon etc.

**For example:**

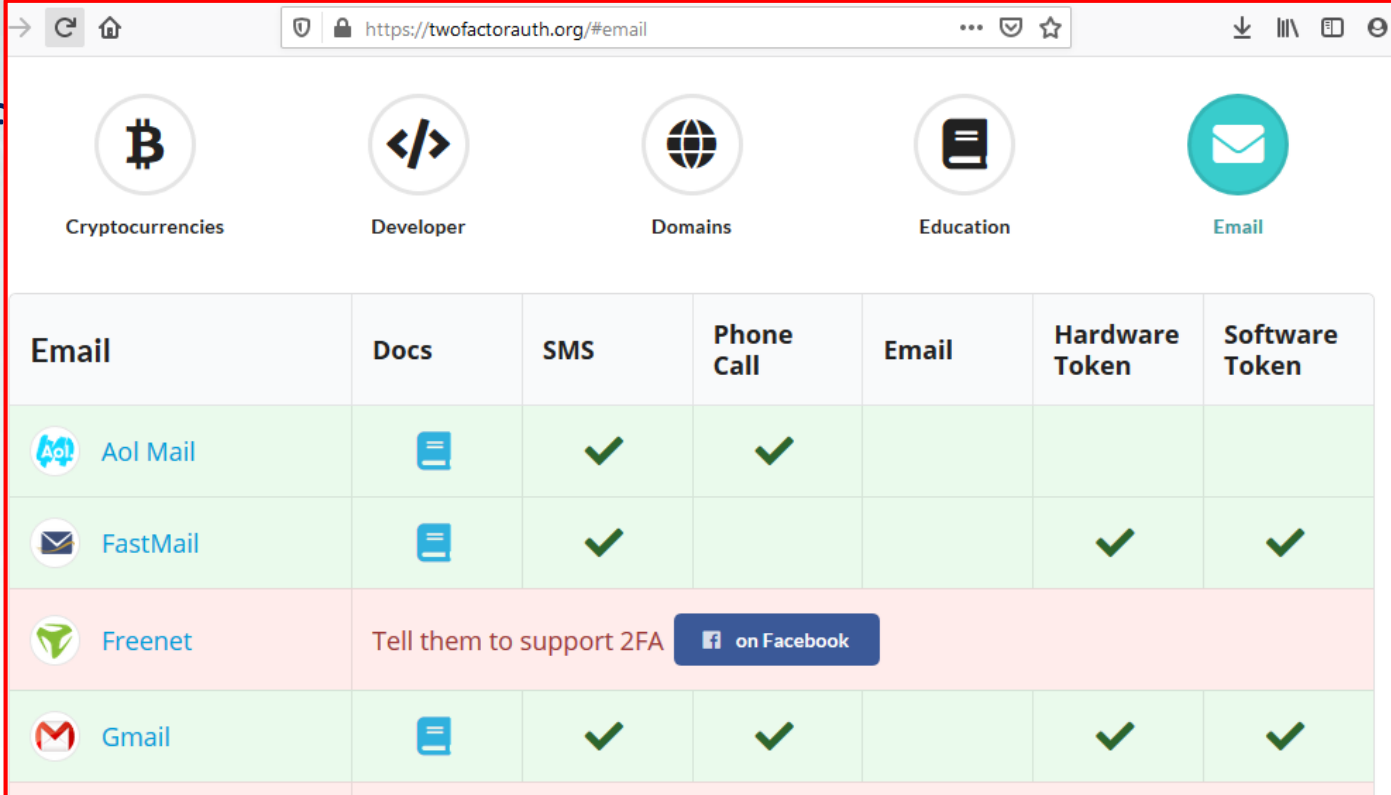
**Sign-out from Google** <https://support.google.com/mail/answer/8154?hl=en&co=GENIE.Platform%3DDesktop>

**Sign-out from Netflix** <https://help.netflix.com/en/node/18>

**Sign-out from Dropbox** <https://help.dropbox.com/accounts-billing/settings-sign-in/device-list-remote-sign-out>

# Two Factors Authentication

- It is recommended to enable two factors authentication, if your service provider support it
- Check which websites support two-factor authentication, i.e. <https://twofactorauth.org>



The screenshot shows the website <https://twofactorauth.org/#email>. The page features a navigation bar with icons for Cryptocurrencies, Developer, Domains, Education, and Email. Below this is a table with columns for 'Email', 'Docs', 'SMS', 'Phone Call', 'Email', 'Hardware Token', and 'Software Token'. The table lists several email providers: AOL Mail, FastMail, Freenet, and Gmail. AOL Mail, FastMail, and Gmail are marked with green checkmarks in the 'SMS' and 'Phone Call' columns. FastMail and Gmail also have green checkmarks in the 'Hardware Token' and 'Software Token' columns. Freenet is highlighted in red and has a message: 'Tell them to support 2FA' with a 'on Facebook' button.

Email	Docs	SMS	Phone Call	Email	Hardware Token	Software Token
AOL Mail		✓	✓			
FastMail		✓			✓	✓
Freenet	Tell them to support 2FA <a href="#">on Facebook</a>					
Gmail		✓	✓		✓	✓



# *Technological Issues*

# *Install Legal Software and Apps Only from Trusted Sources*

- Install only legal software and apps
- Do not install untrusted software
- Install apps only from trusted sources, like:
  - Google Play
  - Apple App Store
  - Microsoft Store
  - ....

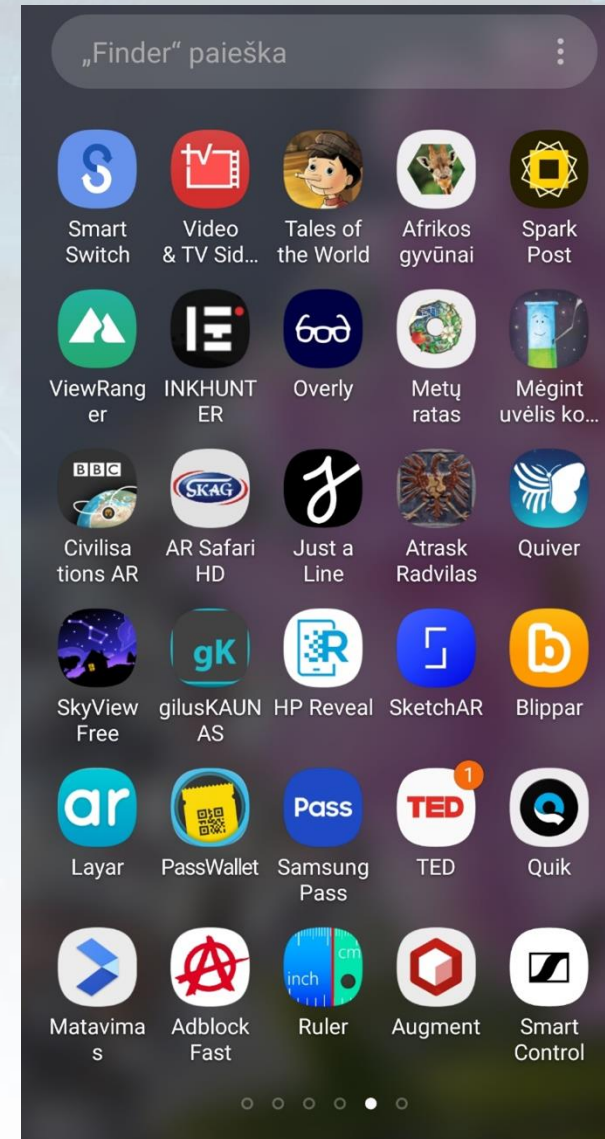


Google Play



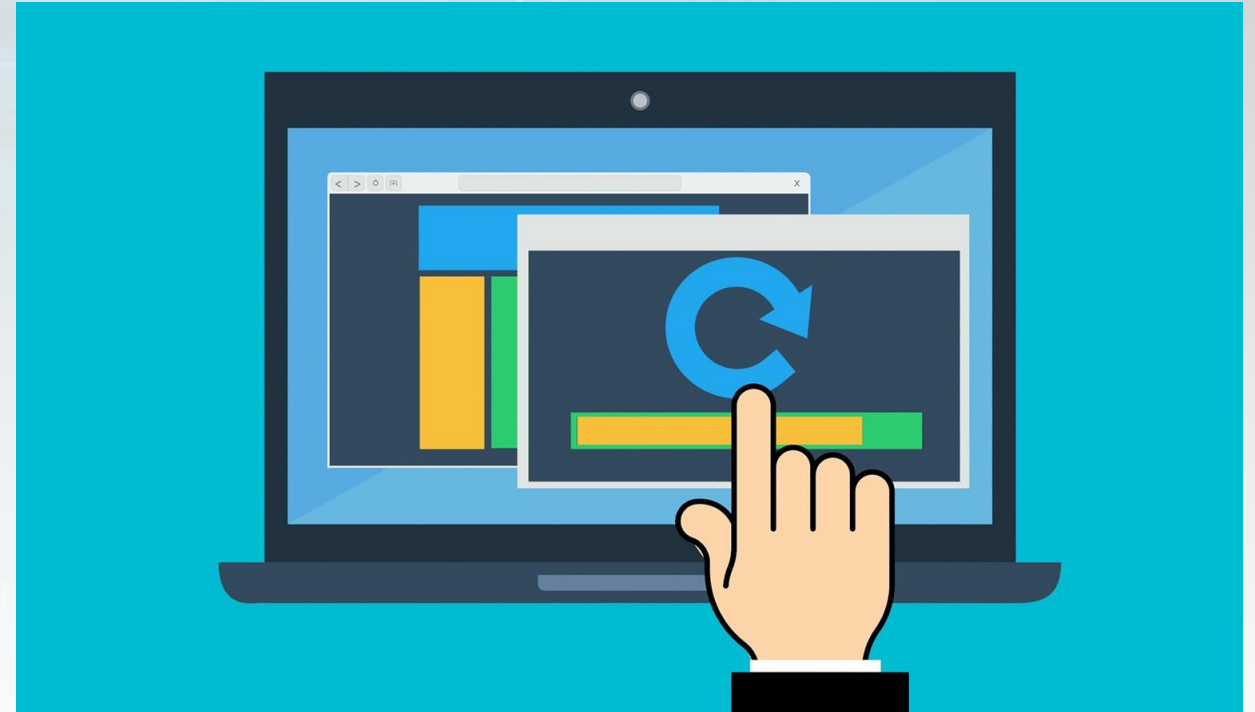
# Question

- Do you know the purpose of all the apps on your device?



# Keep Updates Software

- Ensure that all necessary updates and patches are regularly installed on devices, applications and information systems
- Enable automatic operating system and software updates



# *Use Antivirus and Internet Protection Tools*

- Most antivirus software are commercial and are charged
- For personal use there are a number of free antivirus programs available. Examples:
  - Avira Free Antivirus
  - AVG
  - Avast
  - Bitdefender Antivirus Free Edition
  - Windows Defender

# *Use Spam and Email Filters*

- Spam filters analyse, detect and stop unwanted or dangerous emails. Spam filters could analyse emails for different criteria
  - Header filter
  - Content filter
  - Blocklist filter
  - Rules-based filter
- Spam filter prevent servers from being overloaded and prevent employees from reaching spam to their emails
- You should be aware that the spam filter does not completely prevent unwanted and fraudulent emails

# *Use System Encryption Feature*

- System encryption feature encrypts all data – including application data, downloaded files, and everything else – on your phone or tablet
- You'll have to enter your PIN or password each time you turn on your phone



# Backup Your Data

- Backing up your data protects you in the event of a computer crash or electrical outage or surge, like a lightning storm might produce
- Use an external hard disk or other storage medium for your backup copies
- Back-ups could be stored on:
  - External storage devices
  - Online drives, like Dropbox, Apple iCloud, Google Drive etc.



# Identity Protection Tool

- Use warning signs that your data has been compromised or your account has been hacked, like [Canary tokens](#)
- *Canarytokens* is a free tool that helps you discover you've been breached by having attackers announce themselves
- Canary token is a file, URL, API key, or other resource that is monitored for access. Once the resource has been accessed, an alert is triggered notifying the object owner of said access



More information:

<https://canarytokens.org/generate> [www.lacework.com/blog/canarytokensandransomwareoperations](http://www.lacework.com/blog/canarytokensandransomwareoperations)

# Identity Protection Tool

- Canary token could be
  - Web bug, URL token (alert when a URL is visited)
  - DNS token (alert when a hostname is requested)
  - Unique email address (alert when email is sent to unique address)
  - Tokens for MS Word, MS Excel, PDF files (alert when document is opened)
  - Windows folder (alert when folder is opened)
  - Etc.



More information about tokens generation:  
<https://canarytokens.org/generate>



# *Smart Devices Security*

- Check and configure the permissions and privacy settings for all apps
- Enable remote control and data destruction
- Backup your mobile device data
- Turn off Bluetooth when not in use
- Be careful when viewing information on your phone in public places
- Reset your device to factory settings before selling it

# *Device and Network Protection*

- Destroy devices or memory sticks that are no longer in use.
- It is recommended to connect only to trusted wireless networks that are protected by passwords
- Encrypt USB and other media
- Properly delete documents containing personal information

# *Other Recommendations*

- Avoid P2P and distributed file sharing
- Download files legally
- Avoid surfing websites that you don't already know
- Avoid Deals That Are Too Good to Be True

**The most important counterbalance  
to cyber criminals:  
consumer awareness and vigilance!**

# Useful Topic-Related Links

## **What is personal information? | Personal data**

<https://www.cloudflare.com/en-gb/learning/privacy/what-is-personal-information/>

Video about how it is easy to get hacked: [https://youtu.be/1hpU\\_Neg1KA](https://youtu.be/1hpU_Neg1KA)

## **What is Cyber Hygiene? A Definition of Cyber Hygiene, Benefits, Best Practices, and More**

<https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more>

**What is a digital footprint? And how to protect it from hackers** <https://www.kaspersky.com/resource-center/definitions/what-is-a-digital-footprint>

## **How to Protect Your Digital Privacy**

<https://www.nytimes.com/guides/privacy-project/how-to-protect-your-digital-privacy>

## **How to Remove Personal Information From the Internet**

<https://www.lifelock.com/learn-identity-theft-resources-remove-personal-information-from-the-internet.html>

# Summary

## Proactive actions

- Cyber hygiene on the Internet
- Digital device hygiene
- Technological issues



# Assignment

## Fill in the form:

- Name, surname,
- e-mail address,
- the name of the school you graduated from,
- names of your animals

*TIP: You can use Google Form, but make sure the task is precise, for example, <https://forms.gle/uckbLqBmY2mkFs93A>*

# Assignment



Discuss:

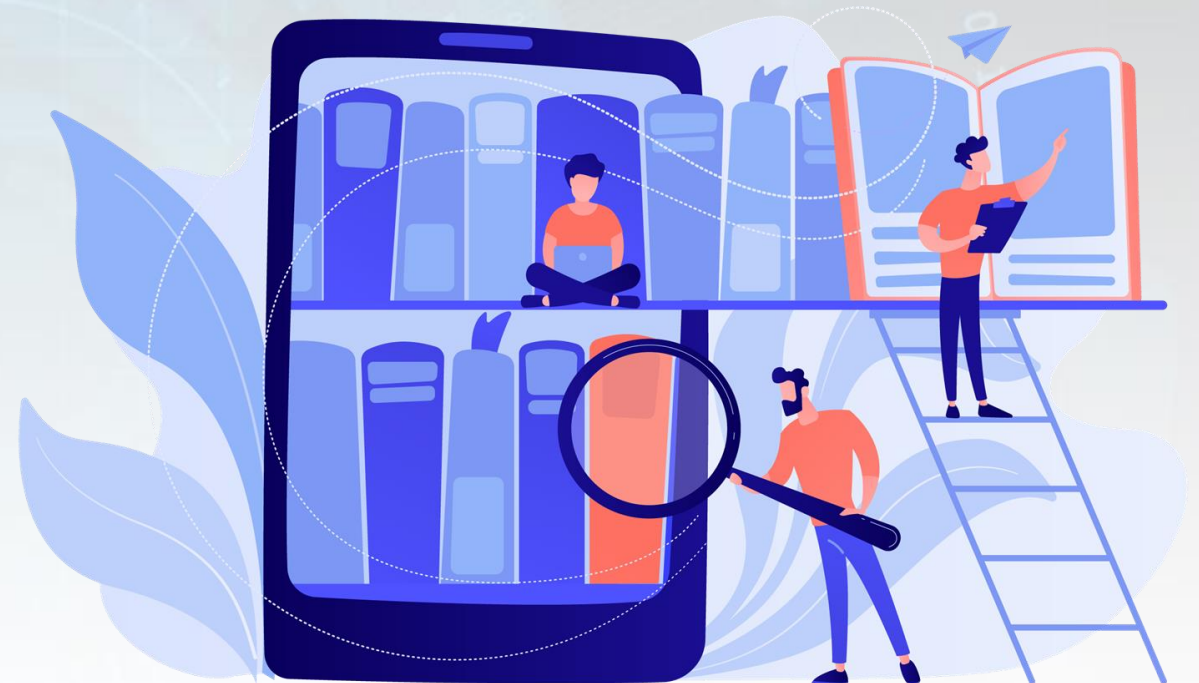
- What kind of footprint you leave on the internet?
- How do you protect your personal data?
- How do you protect your digital devices?
- What is Two factors Authentication and where do you use it?

Make Google search about yourself.  
What did you find?



# Further Reading

- **European Union. Agency for Network and Information Security** Review of Cyber Hygiene Practices, 2016
- **Gerardus Blokdyk**, Cyber Hygiene Third Edition, 2018
- **Gerardus Blokdyk**, Cyber Hygiene a Complete Guide - 2020 Edition



# Short Videos

- How is it easy to be hacked?
  - [https://youtu.be/1hpU\\_Neg1KA](https://youtu.be/1hpU_Neg1KA)
- What is a Digital Footprint?
  - <https://youtu.be/CfICOt2ul80>
- How to protect your data online
  - <https://youtu.be/XjJZoHOlgu4>
- What is Two-Factor Authentication (2FA)?
  - <https://youtu.be/mMKo-fG89jQ>
- A Data Breach Has My Data, What Do I Do?
  - <https://youtu.be/k5rIMr-u0Jw>
- Mobile Security Awareness
  - <https://youtu.be/ahNb6kA0Lms>



# Thank you!



Resources of pictures used in the presentation from:

- [www.pixabay.com](http://www.pixabay.com)
- Personal archives

Screenshots made from websites