TECHNICAL UNIVERSITY IN ZVOLEN
UNIVERSITY OF THE THIRD AGE

Funded by the European Union

TECHNICAL UNIVERSITY UNIVERSITY OF THE THIRD AGE IN ZVOLEN EST. 1996
MOBILITY PROGRAM 2024-2027
2024-1-SK01-KA121-ADU-000204079

Internet security ABC- protect your self online

KA121 - Accredited projects for mobility of learners and staff

2024-1-SK01-KA121-ADU-000204079

Arturs Ievins, NGO Project Net, Latvia

www.ProjectFUND.net

Introduction

What is Internet Safety?

- Protecting Your data and privacy online
- Avoiding threats (viruses, scams, phishing)
- Using the internet responsibly

Why is it Important?

- Increased digital presence leads to greater risks
- Prevent identity theft, fraud, and data breaches

Common Online Threats

Phishing Scams

- Emails or websites pretending to be legitimate
- Often ask for personal information like passwords or credit card details

Malware and Viruses

- Harmful software that can damage your computer or steal personal information

Ransomware

- Blocks access to your data and demand payment

Identity Theft

- Criminals steal personal information to impersonate someone

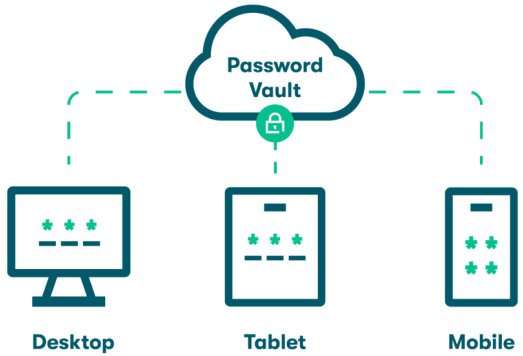
Password Security

Best Practices for Passwords

- Use complex passwords: at least 12 characters, including letters, numbers, and symbols. Its better to use longer sentence than simple words
- Avoid common words and personal information (don use Your kids name)
- Use unique passwords for each online account

Password Managers

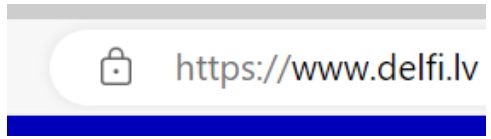
- Store and manage all your passwords in one place
- Create strong, random passwords easily



Safe Browsing Tips

Use Secure Websites

- Always check for “HTTPS” and a padlock icon in the address bar
- Avoid entering personal information on unsecured sites



Avoid Suspicious Links

- Don’t click on pop-ups or unknown email links
- Check the URL before entering sensitive information

Clear Browser History and Cache

- Reduces the risk of saved passwords and personal data being compromised

Social Media

Limit Your personal information

- Avoid sharing to much- your location, address, phone number- to public space
- Be careful about what you post; it can be used against you, or your friends and relatives

Privacy Settings

- Review and adjust privacy settings regularly
- Limit the audience for your posts

Be Wary of Friend Requests

- Only accept requests from people you know
- Scammers can use fake profiles to look as someone You know

Securing Devices

Keep Software Updated

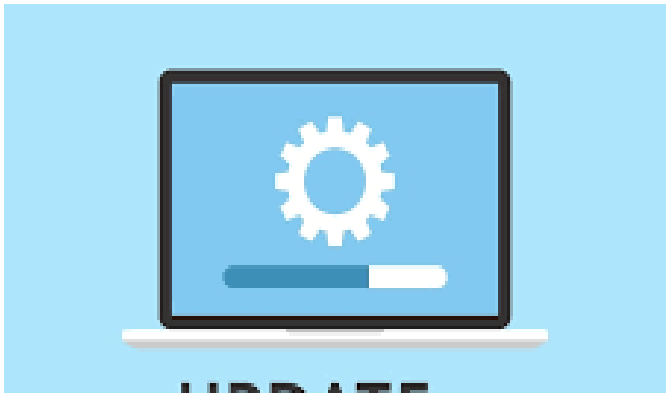
- Regularly update your operating system, apps, and antivirus software (yes, do not ignore that auto update prompt)
- Updates often contain critical security patches

Use Antivirus and Anti-Malware Software

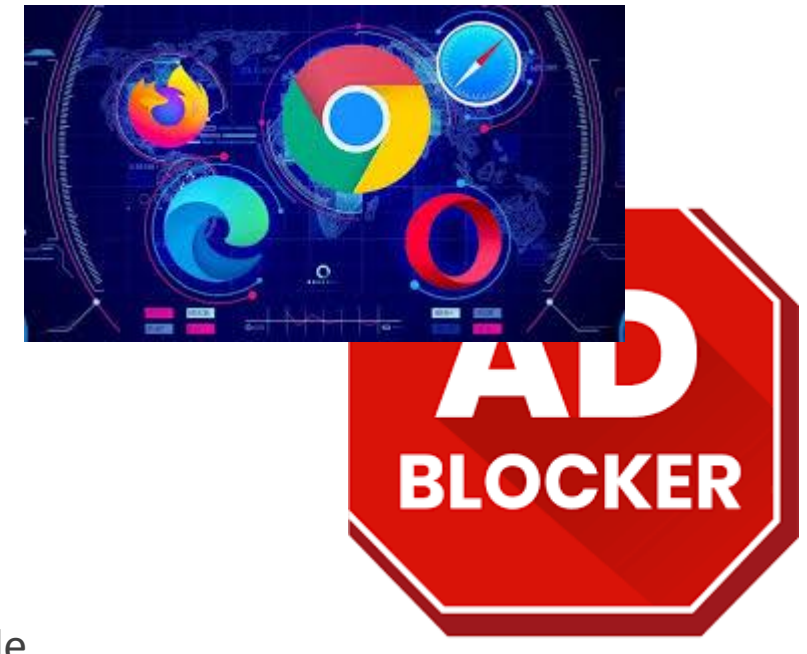
- Protect against malicious attacks
- Perform regular scans to detect any threats

Enable Two-Factor Authentication where possible

- Adds an extra layer of security by requiring a second form of identification
- Useful for email, social media, and financial accounts



Some practical tips



- Use reliable web browsers
- Clear history and cookies often
- Install pop-up blocker extensions like uBlock Origin or Adblock Plus
- Use privacy mode in browser
- Inventory and remove unused apps from mobile devices (each year Third Saturday of March is worldwide digital cleanup day)
- Think twice before installing new app – is it useful- and necessary

Conclusion and Takeaways

Key Takeaways

- Stay vigilant: Always think before clicking or sharing
- Protect personal data: Use strong passwords and privacy settings
- Secure your devices: Regular updates and antivirus software

Additional Resources

- National Cyber Security Alliance: staysafeonline.org
- Internet Safety 101: internetsafety101.org
- Digital cleanup day digitalcleanupday.org

Thank You