Project IDCAP: Improve Digital Competence in Adult People

Project Number: 2018-1-PL01-KA204-051003

How to protect my device?

Competence area: Protecting devices

Introduction

This module covers the most important topics worth attention when working with digital devices on a daily basis: your smartphone, tablet, laptop, and desktop computer.

The aims of the module is:

- to explain methods for protecting devices from being physically accessed by others - PINs, password entry, fingerprinting, face recognition;
- to teach how to protect digital devices from being accessed remotely by other users – installation and use of antivirus programs and applications. Safe downloading of applications and documents to device;
- to explain benefits of backing up the information on digital device and offer tehnical possibilities.

1. Physical security of devices

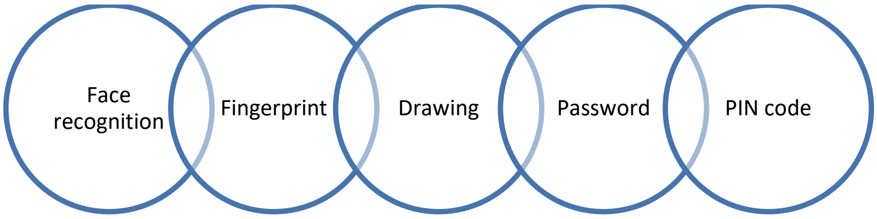
Many people today have a computer, a mobile phone, and some other device they want to protect from harm. The threats are: human physical activity (recklessness, carelessness, failure, malfunction), malware (viruses), hackers, natural phenomena / catastrophes, technical failures, etc. Like any important thing, we want to keep data safe. There are many ways to protect your device: by encrypting your device, using pin a code, using fingerprint locks, facial recognition, the function “find my device”, locking, and deleting your data.

Factors that can increase the physical security of your devices:

- passwords / PINs;
- special devices and software;
- security of premises;
- proper use of the equipment (in accordance with the instruction manuals);
- protection against fire or wet.

When using passwords / PINs and / or special software/ fingerprints, the device cannot be used in the case of theft. There are programs available to track a stolen device.

Examples to unlock your phone:



Protecting information by using an external data storage:

- Only copy files to / from an external data storage (such as CDs, DVDs, or USB flash drives) for specific tasks,

- When connecting external data storage to your computer, scan it with an antivirus program,
- Use extreme caution when using external data storage provided by friends and acquaintances,
- Do not store important and sensitive information on your devices unnecessarily.

2. Encryption

Encryption is the process of encrypting readable information so that it can only be read by someone who has a secret code or a decryption key. This is a way to hide/ lock the information until the code is entered and the information is converted back into readable text. Many people use data encryption for the security of sensitive data.

You have the ability to encrypt both the data you store on your devices and the data you send. There are several encryption methods. For example, FDE is a full disk encryption used to encrypt the entire disk in your system. This means that all information, not just some, is hidden.

HTTPS online encryption is used to protect the data being sent. This means that the information is encrypted on the way from the browser to the home page. Emails and other communication programs also offer encryption methods that you must set yourself. The key to successful encryption is to keep your key / password secure and make it very complex - as long as possible and otherwise secure. You can use the password manager to remember passwords.

Encryption can work if your device is secure. The primary consideration is to make sure that the device is uncompromised, free of viruses, or not compromised in any other way. Regularly make sure that the device is not accessible to unwanted persons. Remember, if the application / program you want to use does not offer encryption, then consider other options. It is important to use secure applications / software that do not endanger you.

3. PIN code/ drawing

A pin code is a special security mechanism that is applied to authorize your bank account, device or any sensitive information. The pin code must not be revealed to anyone. It is recommended to change it in the same way as changing your password. You must remember your Pin code. To protect yourself, do not make payments from public computers or from unfamiliar devices. There are programs that can read everything the user enters using the keyboard - including pin codes. Therefore, use the pin code only on your private devices. **Drawing-type pin codes** are also available, so be careful, as people tend to create them too simple, standard, and the screen of the device needs to be cleaned regularly to prevent it from being tracked by drag lines. When entering a pin or drawing, it is advisable to cover one hand with the other as you type, and make sure that the screen of the device is not too bright and clearly visible from other angles.

4. Fingerprint

Fingerprint sensor is available for several devices. It is a biometric device that helps to quickly identify a person. It can be set on almost all smart devices that have a built-in fingerprint sensor. Fingerprinting can be less secure than a complex pin code, combination, or password. There are several ways to physically remove your fingerprint from your device. Be aware that removing your fingerprint can also be done from other everyday things. If your device is not secure, your fingerprint can be read as any information from your device.

A two-factor authorization process is used for the type of fingerprint authentication. This means that usually the pin code is also used. If the devices cannot recognize / read the fingerprint, then the pin code is used. Also, after updates or power-on, the pin code is used for security purposes.

If you choose to use your fingerprint as a method to unlock your device, go to your device's settings and follow the appropriate steps. The first setup is very important - your fingers are scanned. It is advisable to keep the phone in a natural position and make sure that you follow all the steps required of you.

There may be problems with its use if the sensor is damaged, dirty, or the required device update has not been performed. Several companies prefer to replace their fingerprint with a face recognition tool.

5. Facial recognition

Facial recognition is a type of authentication that requires a camera. It is an option to unlock your device or to connect to specific apps by showing your face on the camera. Experts working on artificial intelligence for many years now recognize that facial recognition is one of the safest ways to connect to the system.

To set up facial recognition, you need an appropriate device, camera, and face setup - you'll need to scan your face from all sides to be recognized by your device.

In most cases, a cheap phone's facial recognition system uses only a forward-facing camera and some not-so-sophisticated algorithms - and maybe even a flash to take a better photo. However, a conventional 2D camera without an infrared sensor and a spot projector can be easily fooled by displaying a photograph.

If you choose facial recognition as a safety mechanism, it is recommended to use a high-quality device. Make sure it works. Experts are still working on improving this system. They acknowledge that facial recognition will be used in the future to access specific websites, shop items, and other activities.

6. Finding Your Phone

Programs are designed to locate and manage your phone at any time. This feature is used if your phone is lost or stolen. You can locate, delete data, view the battery charge, and connect to a Wi-Fi network. Although note that features may vary depending on the operating system. There are both built-in programs that help you keep track of your phone activity and there are ones that can be separately downloaded and are available for purchase.

To use this feature, you need to turn it on (on your device) and explore the capabilities of the device. Use the internet search to find out all about your device or consult the person who can help you to do so.

Google, too, is a service that lets you remotely lock, call, log out, and more. Your device can be found via the Internet. Practice shows that this feature is mainly used to lock the device and log out of certain profiles, but it is not always possible to physically find the device. There are several programs that charge for this feature. Apple's program is called "Find My iPhone", Microsoft's program is "My Windows Phone" and Google offers "Find My Device". These are just a few of the many programs.

7. Safe use of mobile apps

It is important to get mobile apps from a secure and reliable source. Criminals have learned to create and distribute infected mobile apps that look like the real ones. If you install such an infected app, criminals can take control of your device.

For Apple devices, you only download iPad and iPhone applications from the Apple App Store. In this store, Apple has conducted security screenings on all mobile applications prior to their release. Apple cannot "catch" all infected applications, but such a managed environment dramatically reduces the risk of infection. If Apple finds an infected app in its store, it will be immediately removed from the store. Windows Phone takes a similar approach for managing applications.

Android gives you the choice to download the app from anywhere on the Internet. You need to be more cautious about the apps you are installing as not all of them are tested. Google maintains an app store - Google Play and its apps have at least a basic security check. It is recommended to use apps only from Google Play. Avoid apps from other websites as it is relatively easy to distribute malicious apps that infect your mobile device. For more protection install antivirus software on your mobile device.

Permissions. Once you have installed the app from a trusted source, configure it according to your privacy preferences and needs. Always consider before giving permission to an app - do you want to give it permission and do you really need the app. If you let the app to always know your location, you can enable the app developer to track your movement, or even sell that information to others.

Updates. Mobile apps need to be updated regularly. Criminals always look for vulnerabilities in apps. Most devices allow you to update apps automatically. If this is not possible, check for app updates at least once every two weeks. Finally, when an app is updated, always review what changes are made to the app permissions.

8. Lock and wipe

Locking your device is a very simple way to protect yourself from damage or disclosure of information. Also, physically connecting the device to the desk, the workplace tends to discourage thieves from obtaining the device. Only a special key can unlock it.

There are various ways that can protect our device not only physically. A user must not leave his workplace with an unsecured workstation: for temporary absence - **Lock Computer; (Windows + L), longer off - Log off or Shut down**. For phones and tablets, you can set your device to lock automatically after a certain number of seconds. Most devices have a single, easy-to-access shut-off button that facilitates the process.

Not switching off your device can cause other people to interfere with your device. When you're done with your work, it's safer to turn off device completely. Losing your internet connection prevents the device from being accessed by hackers. Keeping the device turned on always increases the risk.

Wipe is the action of making hard disk information unreadable. This means that the data is as deleted, but it is possible to recover it with the help of a suitable program. When replacing a device, the hard drive, it is advisable to clean it as much as possible. However, the safest way is to physically destroy your hard drive to make sure your files are not restored.

9. Viruses and antivirus

Cybercrime gains control by installing malware on computers or devices. This allows the criminal to monitor your online activity, steal passwords or files, and use your system to attack others.

Malware is basically computer software used for illegal purposes. The term comes from the combination of the word’s "software" and "malicious". Cyber criminals install malware on computers or devices to gain control over them. Once installed, the malware allows the criminal to monitor your online activity, steal passwords or files, and use your system to attack others. Malware can infect any device, from Apple computers to security cameras.

Encryption viruses are a special type of malware that is now actively spreading on the Internet, threatening victims' documents and other files.

Protect Yourself - Stop the Malware!

Unfortunately, antivirus programs cannot stop all malicious software. Cyber-criminals are constantly developing new and sophisticated software that can evade anti-viruses. Of course, antivirus developers are constantly improving their solutions as well. Cyber criminals exploit vulnerabilities in your software. The newer / current software version you have, the less vulnerability it has. It is therefore recommended:

- Keep your operating systems, apps, browsers, extensions, and other applications up to date. The simplest solution is usually to have automatic updates installed.

A common way in which cybercriminals infect computers and mobile devices is through the development of fake software or mobile applications, making them available on the Internet, and deceiving people to voluntarily install them.

- Download and install programs only from trusted online stores, and study program reviews and avoid those that are little used or have only a few positive reviews.
- Delete an app that you no longer need.
- Cyber criminals often manipulate people to set up their own malware, for example, they can send you an email that contains an attachment or link in the text and may look like it came from a friend or your bank. Unfortunately, when you click a link or download an attachment, malware is installed on your system.
- Regularly back up your systems and files, either in the cloud or offline, such as on an external hard drive.

10. Licensed and Unlicensed Programs

If the program has a price, it must be purchased and downloaded legally. You also need to pay attention to where you download your programs. Do not do this on suspicious websites - it may endanger your device and other software on your computer. Computer users must consider the copyright laws that apply to books, video and music discs and cassettes, and software. Copying, distributing, or using computer programs without the permission of the copyright owner is called piracy.

Illegal use of computer programs is, for example:

- Installing one legally purchased software CD on multiple computers, if the license or agreement states that it may be installed on only one computer;
- Copy the program for installation and distribution without the author's permission;
- Installing software from an illegally purchased disk.
- Downloading illegal copies of computer programs from the Internet.

Software and other types of files (texts, images, etc.) are offered to be downloaded free-of-charge over the Internet. Their publishers do not always have the rights to distribute them for use by others. Therefore, you need to make sure that you are legally allowed to make copies before downloading.

11. Downloads

Download is the process of storing files from a network server to a storage device. Downloading files is required if the user wants to obtain files offered on the website, such as documents, pictures, music, videos and software.

To save a file or image to your computer or device, download it. The file will be saved to the default download location.

You can download different file types:

Type	**Format**	**Example**
Text	Docx, txt	Kopsavilkums.docx
Picture	Jpg. Gif, png.	IMG0034.jpg
Audio	Mp3, wma	Voice.mp3
Video	Avi, mpg, mpeg	Ceplis.avi

Type	Format	Example
Programs	Exe	Skype.exe
Archive	Zip, rar	Arhivs.zip

The file download option can be specified in different ways but is usually characterized by a link or the Download button (Download).

12. Browsers

A browser is an app for viewing web pages. To view a web page, it is first downloaded or transmitted from the global web server to the user's computer before it is opened.

In order to use the Internet services, you need:

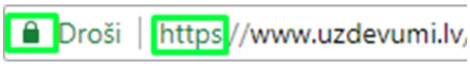
- Programmable device with network connection capability;
- An Internet Service Provider (ISP) that ensures that the device can be connected to the Internet (additional hardware may be required);
- Internet browser.

Some examples of browsers include:

It is not safe to open any page because there are risks that the page contains viruses, which can also open fraudulent pages that spoof information.

There are signs by which you can assume that a web page is secure. The two simplest features that indicate the security of a page are displayed in the address bar:

- **https** before address (indicates that information is transmitted to the computer in an encrypted form);
- The normally locked "lock" symbol (the lock symbol may vary in different Internet browsers).



🔒 Droši | https://www.uzdevumi.lv/

Downloading a page stops if:

- Download is delayed;
- detects during the download, the information required for the page is missing.

The page needs refreshed if:

- The page failed to load. For example, some images have squares with red crosses on the page or not all information is available;
- The page has not been viewed by the user for some time and the information on the page has changed during this time (the page does not update automatically).

13. Copies of data

It is important to store data not only on a computer but also in some other place. In this case, it is always possible to restore important data in case of any problems with the computer.

Data usually stored on computer:

- photos;
- working papers;
- important programs, software;
- video, audio projects;
- e-mail archive and friends' emails.

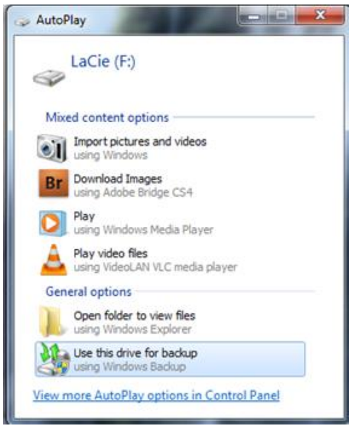
If you think you don't need copies of data, remember that there are many ways you can lose important documents.

- The simplest way to lose all your data is to lose your computer or if it gets stolen (this applies more to laptops).
- There is a possibility to accidentally delete data or copy over something else in important documents.
- Your computer can be infected, and malware can corrupt certain data or even damage your hard drive.
- There may be some technical issues (including hard drive breakage - nothing is everlasting) that can result in the loss of some data.

Making copies of data.

To a Windows computer:

- **Purchase an external storage device**. It can be any USB flash drive or external hard drive. It is desirable to purchase a device that has at least twice as much space as your computer's memory.
- The first time you connect an external storage device to your computer, it offers you the option of using it as a place to store data. If this option does not appear, simply type the name of the program in the "Backup" search window.


AutoPlay
LaCie (F:)
Mixed content options
Import pictures and videos
using Windows
Download Images
using Adobe Bridge CS4
Play
using Windows Media Player
Play video files
using VideoLAN VLC media player
General options
Open folder to view files
using Windows Explorer
Use this drive for backup
using Windows Backup
View more AutoPlay options in Control Panel

- The following window will open, where you will have to click on "Set Up Backup". Next, you will need to select which external disk you want to back up your data to. In the end, you will have to click "Save Settings and Run Backup".

- After you complete these steps, Windows will make the first backup copy of your data (the key is to not remove the external storage disk!). You can select "Change schedule" below and the following image will appear. The figure shows that you are given the option of choosing the schedule when the data copies will be restored. You are offered the opportunity to do this once a day, weekly and monthly. The main thing to remember is that the device you are backing up to must be connected to a computer at the selected time and day.

Making copies of data to a Mac OS computer.

This is very much the same as with a Windows computer. When you insert an external storage disk, you will be able to use it as a backup location. You must choose it or go through System Preferences -> Time Machine. Then select the required external storage disk and make a copy of the data on it.

Making copies of data on a mobile phone.

A very convenient way to back up your contacts and calendar is with your Google Account (Gmail email). With the Account & Sync Setting, you can turn on the backup function at any time. A Google Account should appear next to your accounts if you have accessed it from your phone. The advantage of using such copying of contacts is that when you change phones, the data will be automatically copied to the new device. On the Internet, you can view information about your contacts on the left by clicking on Gmail. Aside from the capabilities Google offers, there are other types of software that offer backup options. One option is to simply copy important data by connecting your phone to a computer. You can also find individual programs on the Internet that provide backups. If you are looking for one that is right for you, it is important to make sure that it is suitable for your computer's operating system.

Making copies of data on the Internet.

For free, this service is usually available with memory limitations (approximately 5GB-7GB). Using this service allows you to store your most important data on the Internet, which means you can access it from anywhere and from your computer. The service provider ensures that this data is stored in an encrypted form. Examples of such service providers are www.mimedia.com and www.backup.comodo.com Of course, this type of data storage is convenient in terms of access, but various security issues are not excluded.

If there is a loss of data, it is easy to restore from a backup. In Windows, type "Backup" in the Start Menu search, and then click "Restore My Files". On Mac computers, press "Time Machine" and then "Enter Time Machine". Or, simply take your external storage device, where you have backed up your data, connect it to your computer and copy the files you need.

Benefits of making data copies.

- **Moral benefit** - you don't have to worry about anything happening to your computer; you can rest assured that your important data will not be lost anywhere!
- **Financial benefit** - If you have problems with your hard drive, it can be quite expensive to have the services of a professional to restore this data. If you have a backup of your important data, you will not need such services.

14. Rooted device

Rooting is a process that allows users of smartphones, tablets and other devices running Android mobile operating systems to gain privileged control (known as root access) across various Android subsystems. The purpose of this process is to overcome the restrictions imposed by manufacturers on certain devices. Thus, rooting allows you to change or replace system applications and settings, run specialized apps that require administrator-level permissions, or perform other actions that are not available to another regular Android user. On Android, rooting can also make it easier to completely remove and replace your device's operating system, usually with a newer version of its current operating system.

Summary

By learning the topics covered in the module, learners know how to provide physical security of devices and they also understand principles of encryption. Learners can recognize and use digital device protection techniques - facial recognition, password entry, figure drawing on a digital device screen and fingerprinting.

By using described techniques in the module, it is possible to locate lost phone. Learners are informed about different kind of viruses threatening devices and possibilities to avoid them. To maintain security of devices, users should also pay attention to downloads and use only legal and licenced programs. After provided information learners can master the principles of using antivirus programs and applications, tell the difference between web browsers and use of them.

Finally, learners are aware of how to back up the information on their digital device and they also understand purpose of rooted device.

Bibliography

- Pieslēdzies, Latvija! (n.d.). *Esiet sveicināti datorskolā! Mācies pats*. [Online Course]. Tet.lv. https://www.tet.lv/piesledzies-latvija/materiali/start/
- Swedbank. (n.d.). *Swedbank privātpersonām*. Swedbank.lv. https://www.swedbank.lv/private
- Valsts reģionālās attīstības aģentūra. (n.d.). *Valsts pārvaldes pakalpojumu portāls.* Latvija.lv. https://www.latvija.lv/
- *Mana Latvija.lv. Dari digitāli!* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/
- *Drošība internetā.* (n.d.). Mana.latvija.lv. https://mana.latvija.lv/drosiba/
- *E-rīki jeb ceļvedis e-pakalpojumu lietošanā*. (n.d.). Mana.latvija.lv. https://mana.latvija.lv/e-riki/
- *Esiet sveicināti Mācību e-vidē!* (n.d.). [e-learning environment]. Macibas.mana.latvija.lv. https://macibas.mana.latvija.lv/
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Cert.lv. https://www.cert.lv/lv
- Informācijas tehnoloģiju drošības incidentu novēršanas institūcija. (n.d.). Esidross.lv. https://www.esidross.lv/
- Uzdevumi.lv. (n.d.). Uzdevumi.lv. https://www.uzdevumi.lv/
- Baltijas Biroju Tehnoloģijas. (n.d.). *Astoņas digitālās prasmes, kas jāmāca bērniem*. Smartboard.lv. https://smartboard.lv/zinas/astonas-digitalas-prasmes-kas-jamaca-berniem/
- Brečko, B., Ferrari, A. (2016) *Patērētāju digitālo kompetenču sistēma*. https://publications.jrc.ec.europa.eu/repository/bitstream/JRC103155/lfna28133lvn.pdf