Co-funded by the
Erasmus+ Programme
of the European Union

Security Plan for General Public

Lithuania

The goal of the security plan

To provide the most important cyber security tips for users.

1. Disable public access

1. Turn public sharing off. Prevent your team from allowing public access to filters and dashboards from now on.
2. Set default sharing for filters and dashboards to private. Prevent accidental granting of public access to filters and dashboards.
3. Find and update shared filters. Remove public access to filters, if it's been granted.
4. Find and update shared dashboards. Remove public access to dashboards, if it's been granted.
5. Remove public access to users and groups. Revoke the *Browse users and groups* permission from the *Anyone* group, if it's been granted.

2. Use VPN

The safest way to use public Wi-Fi network is tu use VPN (virtual private network).

If you connect to public Wi-Fi network using a VPN you can rest assured that no one on that network will be able to intercept your data.

3. Do not connect to Wi-Fi automatically

One of the biggest threats with free WiFi is the ability for hackers to position themselves between you and the connection point.

The hacker also has access to every piece of information you send out—emails, phone numbers, credit card information, business data, the list goes on.

If you use a public Wi-Fi network, do not touch any of your personally identifiable information.

4. Use SSL (Secure Sockets Layer)

When browsing the internet, be sure to enable the "Always Use HTTPS" option on websites that you visit frequently, including any and all sites that require you to enter any type of credentials.

5. Use double authorization

Two-factor authentication works as an extra step in the process, a second security layer, that will reconfirm your identity. Its purpose is to make attackers' life harder and reduce fraud risks.

6. Connect only to reliable Wi-Fi networks

To avoid risks, it’s better to connect to those Wi-Fi networks, that are owned by familiar and reliable owners.

7. Save your personal data

Protecting your personal information can help reduce your risk of identity theft. There are four main ways to do it:

1) know who you share information with;

2) store and dispose of your personal information securely, especially your Social Security number;

3) ask questions before deciding to share your personal information;

4) and maintain appropriate security on your computers and other electronic devices.

8. Switch on firewall

Most operating systems have a firewall that checks all incoming and outgoing connection requests and protects your computer from unauthorized remote access.

Firewalls can block messages linking to unwanted content.

9. Use antivirus

A system without an antivirus is just like a house with an open door.

An open and unprotected door will attract all the intruders and burglars into your home. Similarly, an unprotected computer will end up inviting all the viruses to the system. An antivirus will act as a closed door with a security guard for your computer fending off all the malicious intruding viruses.