STATE DATA PROTECTION INSPECTORATE

FAQ: How to reduce the risk of identity theft?

17 December 2025

The State Data Protection Inspectorate, like other Lithuanian institutions, receives inquiries from individuals regarding identity theft and how to mitigate the associated risks and threats. Personal identity is one of a person's most valuable assets. If your identity is stolen, you may lose money, face difficulties obtaining loans, credit cards, or traveling abroad and etc.

Providing just your name, address, and date of birth is often sufficient for someone to create a "version" of you. The more personal data is acquired, the more severe the consequences that malicious actors can inflict. Identity thieves employ a wide range of methods—from the simplest to the most sophisticated—to obtain an individual's personal information and subsequently use it to open bank accounts, obtain credit cards, apply for loans, benefits, and so forth in another person's name.

Several indicators should be monitored, as they may suggest that an individual is or may become a victim of identity theft:

- You have lost or had important documents stolen, such as a passport, driver's license, etc.;
- You have applied for loans or benefits but were informed that you had already applied for them, even though you had not;
- You receive invoices or receipts for goods or services you did not order;
- Despite having a good credit rating, you are denied financial services, credit cards, or loans;
- You receive letters or notifications regarding debt repayment, even though you are not indebted;
- You notice unfamiliar bank transactions, payments, or transfers;
- You receive notifications about password changes or login attempts to your social media account or email, which you did not initiate.

How to reduce the risk of identity theft?

- Ensure protection of all documents containing personal information, such as driver's licenses, passports, bank account statements, utility bills, and similar items;
- Destroy old or unnecessary documents that reveal your name, surname, address, or other personal information;
- Monitor your credit history report and regularly review statements from your credit cards and bank accounts for completed transactions;
- When changing your place of residence, inform your bank, credit card providers, mobile operators, television, and other service providers of the address change to prevent personal correspondence from reaching unauthorized individuals;
- Bear in mind that the less information you disclose about yourself, the lower the risk of it falling into the wrong hands—for example, review privacy settings on social networks, restrict the audience who can view your profile and posted information;
- When purchasing goods online, exercise caution: select secure websites that display the company's contact information, a clear privacy policy, product/service warranties and return policies; choose sites that use data encryption (valid SSL certificate), and verify that the website address begins with https;
- Use unique passwords for different accounts and enable two-factor authentication (2FA) to enhance account security, if possible;
- Do not open attachments in suspicious emails, avoid clicking links in such messages, and verify the sender's address;
- If you receive an SMS with a suspicious link, do not click it and check the sender's information;
- Keep your operating system and antivirus software continuously updated;
- Protect your devices by using a screen lock (PIN, password, facial recognition), avoid public Wi-Fi networks, and if unavoidable, use a VPN (Virtual Private Network).

What to do if you become a victim of identity theft?

If you suspect that you have become a victim of identity theft, act promptly to prevent or minimize potential negative consequences. Recommended actions include:

- Notify the police and other relevant authorities about lost or stolen documents, such as passports, driver's licenses, credit cards, etc.;
- Inform your bank and financial institutions about unusual transactions and operations related to your personal accounts;
- Change all passwords;

- If you discover that an account has been created in your name on an online store or similar platform, immediately notify the relevant entity and request the removal of the fraudulent account.

Additionally, we recommend familiarizing yourself with information available on the Lithuanian Police website regarding how individuals may become victims of fraud upon disclosure or loss of personal data. We also recommend reviewing guidelines issued by the National Cyber Security Centre on staying safe online, as well as recommendations of the Lithuanian Banks Association on preventing online fraud.