VALET

Stay safe from scams:

Your Fraud Prevention Handbook

V/ALET

In today's digital age, financial fraud poses a significant threat to individuals and businesses alike. Scammers are becoming increasingly sophisticated, making it essential for everyone to be vigilant and informed about potential risks.

This booklet is designed to equip you with practical knowledge and actionable tips to safeguard your money and identity. Whether you're managing personal finances or overseeing business transactions, understanding the common tactics used by fraudsters is crucial for maintaining financial security.

Remember, knowledge is your best defence against fraud. Let's work together to ensure that your finances remain secure and your peace of mind intact.

Romance Fraud

VIALET

Scammers on social networks create fake profiles, often posing as others in coordinated groups with convincing covers. They engage victims using psychological tactics, faking sympathy or even love to build trust gradually. Unlike quick phishing attempts, romantic scammers take their time, starting with genuine interest and normal conversation to gain trust through manipulation.

As relationships deepen, they plan meetings, but encounter supposed financial setbacks, making in-person meetings impossible and prompting requests for additional funds. Scammer profiles often contain inconsistent details or limited personal information.

How to protect yourself?

- Be wary of strangers asking for personal or financial details or requesting money.
- Avoid sharing compromising photos or videos, as they can be used for blackmail.
- Before trusting someone new, research them online, including their job and photos, to verify their identity and intentions.
- Stay vigilant and cautious. Scammers lurk on popular social networks, dating platforms, and apps.
- Don't hesitate to ask questions and insist on video calls to verify identities. Be wary of excuses like "camera issues."

Phishing

VALET

Phishing is a type of cyber attack where attackers use fraudulent emails, messages, or websites to trick individuals into revealing sensitive information such as passwords, credit card numbers, or other personal data. Typically, phishing messages appear to be from a legitimate source, such as a bank, social media platform, or trusted organization. The goal is to deceive recipients into clicking on malicious links or providing confidential information.

How to protect yourself?

- Always verify information and avoid rushing into decisions. Never share your payment credentials (PIN codes, CVV, card numbers) or click on suspicious links in emails, SMS, or messages. Ignore alarming messages or calls about blocked accounts or services. Financial institution employees never request sensitive details over the phone. If in doubt, hang up and call the bank using the official number on their website—never call back a suspicious number.
- Log in directly to financial institution websites and shop at trusted online stores.
- Check "Smart-ID" notifications for authorized operations.
- Be cautious of unexpected lottery wins or inheritances.
- When receiving suspicious messages, consider if it matches your recent transactions or orders.
- Look out for typos or non familiar links in emails.

Vhishing

VIALET

Vishing (voice phishing) is like phishing but involves the use of phone calls or voice messages to trick victims into divulging sensitive information. In vishing attacks, scammers often impersonate legitimate entities like banks, government agencies, or tech support services. They use tactics such as urgent messages about account issues or security threats to manipulate individuals into revealing personal information over the phone.

How to protect yourself?

- If you receive a call from someone claiming to be from a bank, government agency, or tech support service, be cautious, especially if you weren't expecting the call. Fraudsters often use urgency or threats to pressure victims into providing sensitive information.
- Ask for the caller's details, then independently verify their identity by calling the official number of the organization they claim to represent (not the number they provide).
- Enable two-factor authentication on your accounts whenever possible. This adds an extra layer of security by requiring a second form of verification (e.g., a code sent to your phone) in addition to your password.
- Scammers often create a sense of urgency to pressure victims into immediate action. Take your time to assess the situation and verify the legitimacy of the caller before providing any information or taking action.

Identity theft

VIALET

Identity theft is a type of crime where scammers obtain and use another person's personal data in a fraudulent or deceptive manner, typically for economic gain. Identity theft could occur through various means: losing your wallet, using public Wi-Fi, experiencing data breaches, falling victim to phishing or spoofing attacks, or through skimming.

How to protect yourself?

- Use strong, unique passwords for your online accounts and consider using a password manager.
- Do not disclose sensitive information online
- Keep your social media pages in private mode, do not accept invitations from people you do not know
- Install reputable antivirus software on your devices and use a virtual private network (VPN) when accessing public Wi-Fi networks.
- Destroy documents containing personal or financial information before discarding them to prevent dumpster diving.
- Regularly review bank statements and credit reports for unauthorized transactions or suspicious activity.
- Verify the identity of individuals or organizations requesting personal information before sharing any details.

Money Mules

VIALET

Those are individuals who, for a fee, "lend" their bank account to withdraw or transfer money, opening an account in their name and allowing others to use it.

The origin of illegally obtained funds is often related to data theft, the use of malware, internet fraud, fake online stores, impersonation of company executives, simulated romantic relationships, and so on.

How to recognize that you could become a money mule?

- It is common to find supposedly legitimate job advertisements on job portals ("Money transfer agent jobs"). Such advertisements are also available on social networks (Facebook posts in closed groups), and personal offers (enquiries) can be received by email or through correspondence apps (Whatsapp, Viber).
- Money mule ads mimic real company websites with similar web addresses to appear authentic. They claim to seek "local/national representatives" or "agents" to act temporarily on behalf of a foreign company, suggesting tasks involving money or goods transfer while avoiding fees and taxes.
- Victims are assured of a risk-free opportunity and offered higher pay for involving friends in the scheme.

How to protect yourself?

- Never share your payment credentials (PIN codes, CVV, card numbers)
- Avoid unclear or suspicious job advertisements, always check publicly available information for Companies and job opportunities.

Investment Fraud

VIALET

“Illegal provision of investment services” is the activity of offering investment services without having a license issued by the Bank of Lithuania or another supervisory institution in an EU member state. An example commonly encountered is services promoted in Lithuania by companies established in foreign countries like Vanuatu, Belize, Seychelles, etc., offering investment in the Forex market, commodity markets, or virtual assets via websites or phone.

How to protect yourself?

- Verify licenses and registration, research companies before engaging with any service provider. In the EU, legitimate investment firms should be licensed by the Bank of Lithuania, or another recognized supervisory institution in an EU member state.
- Be skeptical of unusually high returns with little to no risk.
- Avoid offshore companies based in jurisdictions such as Vanuatu, Belize, Seychelles, etc.
- Utilize official resources such as the Bank of Lithuania's website or the European Securities and Markets Authority (ESMA) to check for warnings or alerts regarding unauthorized investment firms.
- Seek professional advice if you have little to no experience with investments.
- Report fraudsters to the regulatory bodies. In Lithuania you should reports it to the Bank of Lithuania (prieziura@lb.lt) and Lithuanian Police.

VIALET

If you suspect fraud or encounter suspicious activity, don't hesitate to report it. Safeguarding against fraud is crucial for protecting yourself and others. Whether it's identity theft, financial scams, or any form of deceptive behavior, reporting it promptly can prevent further harm. Your vigilance can make a difference.

When encountered fraud – please reach out to support@vialet.eu or complaints@vialet.eu