V/ALET

Stay safe from scams:

Your Fraud Prevention Handbook

VALET

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

Social network scammers create convincing fake profiles to build trust using psychological tactics like feigning sympathy or affection. They invest time in building relationships through genuine interest and conversation. As relationships progress, they request money due to supposed financial setbacks, often with inconsistent or limited personal details in their profiles.

Protect yourself by:

- Avoiding sharing personal or financial details or sending money to strangers.
- Refraining from sharing compromising photos or videos to prevent potential blackmail.
- Researching new acquaintances online to verify their identity and intentions.
- Staying vigilant on social networks, dating platforms, and apps where scammers operate.
- Insisting on video calls to confirm identities and be cautious of excuses like "camera issues."

Phishing

VIALET

Phishing is a cyber attack using fake emails, messages, or websites to trick people into revealing sensitive information like passwords or credit card details. These messages appear legitimate, often from trusted sources like banks or social media platforms, aiming to deceive recipients into clicking malicious links or sharing confidential data.

Protect yourself by:

- Verifying information and avoid rushing decisions.
- Never sharing payment credentials or click suspicious links in emails, SMS, or messages.
- Ignoring alarming messages about blocked accounts or services; financial institutions don't request sensitive details over the phone.
- Logging in directly to financial institution websites and shop at trusted online stores.
- Checking "Smart-ID" notifications for authorized operations.
- Being cautious of unexpected lottery wins or inheritances.
- Considering if suspicious messages match recent transactions.
- Watching for typos or unfamiliar links in emails.

Vhishing

VIALET

Vishing (voice phishing) uses phone calls or voice messages to trick victims into sharing sensitive information. Scammers impersonate banks, government agencies, or tech support, creating urgency about account issues or security threats to obtain personal details over the phone.

Protect yourself by:

- Being cautious with unexpected calls from banks, government agencies, or tech support.
- Verifying the caller's details independently by calling the official organization number.
- Enabling two-factor authentication for added account security.
- Taking time to assess and verify the legitimacy of the caller before sharing information or taking action.

Identity Theft

VIALET

Identity theft is when scammers fraudulently use someone else's personal data for economic gain. It can happen through lost wallets, use of public Wi-Fi, data breaches, phishing attacks, or skimming.

Protect yourself by:

- Using strong, unique passwords and a password manager.
- Avoiding sharing sensitive information online.
- Keeping social media pages private and not accepting requests from strangers.
- Installing reputable antivirus software and using a VPN on public Wi-Fi.
- Shredding documents with personal or financial information.
- Regularly checking bank statements and credit reports for suspicious activity.
- Verifying identities before sharing personal information.

Money Mules

VIALET

Money mules are individuals who allow others to use their bank accounts for a fee, often opening accounts in their name to facilitate illicit transactions.

To recognize potential involvement as a money mule:

- Watch out for job ads on portals or social networks that promise easy money transfer tasks.
- Be wary of emails or messages offering lucrative job opportunities involving money transfers.

Protect yourself by:

- Never sharing payment credentials like PIN codes or card numbers.
- Avoiding unclear or suspicious job ads; research publicly available information about companies and job opportunities thoroughly.

Investment Fraud

VIALET

"Illegal provision of investment services" refers to offering investment services without the required license from the Bank of Lithuania or another EU supervisory institution. This often involves foreign companies promoting investment opportunities in Lithuania through websites or phone calls.

Protect yourself by:

- Verify licenses and research companies before engaging with any service provider. Legitimate EU investment firms should be licensed by the Bank of Lithuania or another EU supervisory institution.
- Be skeptical of high returns with low risk.
- Avoid offshore companies based in places like Vanuatu, Belize, or Seychelles.
- Use official resources like the Bank of Lithuania's website or ESMA to check for warnings about unauthorized investment firms.
- Seek professional advice if you're new to investments.
- Report fraud to regulatory bodies like 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.