



Funded by the European Union



Financial security

KA121 - Accredited projects for mobility of learners and staff

2024-1-SK01-KA121-ADU-000204079

Artūrs Ieviņš, NGO Project Net, Latvia



Introduction

What is Financial Safety?

- ▶ The practice of safeguarding your financial information, accounts, and assets
- Protecting yourself from fraud, theft, and mismanagement of funds

Why is Financial Safety Important?

- Prevents loss of money, identity theft, and credit damage
- Helps secure your financial future and peace of mind
- Seniors are often targeted by fraudsters, mostly because of savings accumulated true years of work

Common Financial Threats

Identity Theft

Criminals steal personal and financial information to open credit lines or commit fraud

Phishing Scams

Fraudulent messages that trick individuals into providing personal information

Credit Card Fraud

Unauthorized use of your credit card to make purchases or transfer funds

Investment Fraud

Scams offering fake or misleading investment opportunities- if it looks to good it most probably is not legit

Protecting Personal Financial Information

Don't share sensitive financial information (e.g., bank details, credit/ debit card numbers etc.) unnecessarily, even inside family or with close friends

- Destroy sensitive documents before disposing of them
- Use Strong Passwords and Two-Factor Authentication (2FA) wherever possible
- Passwords should be complex, unique, and not reused across multiple accounts. It's better to use longer passwords and full sentences if problematic to remember random codes
- Check your Bank and Card Statements often for unusual activity
- Report any suspicious activity to your bank immediately, do not wait for next day

Safe Online Banking and Shopping

Use Secure Websites

- Look for "HTTPS" and a padlock icon before entering any financial details
- Use well known online shops, check reviews before ordering
- Avoid using public Wi-Fi for online banking or shopping- do not

Beware of Phishing Emails and calls

- Banks will never ask for your password or PIN via email or by phone.
- Always verify the source before clicking on any links or providing details
- Call your bank if something seems suspicious. Use only official customer service center numbers or chat systems in i-bank applications

Set Up Alerts

Enable transaction alerts/ messages for your accounts to see if there is any unexpected payments

Protecting Yourself from Financial Scams

Red Flags

- If an offer seems too good to be true, it probably is scam
- Be wary of unsolicited calls, emails, or messages promising easy money or prizes
- Push to react quickly, treats to involve authorities or lose of money

Verify Before You Act

- Never provide financial information over the phone or email unless you initiated the contact
- Always research a company or investment opportunity before committing funds. Avoid if not 100% sure

Common Scams to Watch For

- Ponzi schemes
- Fake charities
- Lottery scams
- Fake investment opportunities
- Romance scams

Protecting Against Online Financial Theft

- Protecting Against Online Financial Theft
- Use Multi-Factor Authentication (MFA), in addition to strong passwords
- Avoid public WI-FI networks if possible- public networks are vulnerable to attacks and can be used to collect your personal information
- Use separate accounts and credit cards for online shopping or daily purchases and savings.
- Only use secure apps for transactions
- Keep Your Devices Updated, install latest security patches when offered by manufacturer
- ▶ Do not react on urgent requests if not 100% sure about person making request. Verify emails and messages thru other channels

Conclusion and Takeaways

- Stay vigilant: Monitor your accounts and credit regularly
- Protect your financial information: Use strong passwords, 2FA, and secure websites
- Be cautious with investments and offers: Research before committing money
- Act quickly if you detect fraud: Report it and take action to secure your accounts

Thank You