Co-funded by the European Union

FIGHT AGAINST LOVE SCAM



PROJECT REFERENCE:

2024-1-NL01-KA210-ADU-000253818

01-09-2024 - 31-08-2026

ECREC
European Center for Researching, Education and Consulting

EUTH
WONDERS E.V

IGOR VITALE
INTERNATIONAL

Co-funded by the European Union

Awareness for seniors

- Staying safe with passwords
- How to recognize digital scams
- Preventing scams with the four-eyes principle
- Two-Factor Authentication
- Email attacks
- Phone scams
- Hoovering
- Spoofing

Co-funded by the European Union

Staying safe with passwords

Tips for secure passwords:

- Use a strong and unique password for every account.
- A strong password is a long password with several special characters or symbols.
- Don't use information hackers can guess, such as years, idols, or the names of family members or pets.
- Use a password manager to store and use your passwords securely.

Co-funded by the European Union

How to recognize digital scams?

- By phone: helpdesk staff never ask for login details or to install a program
- Via WhatsApp or Telegram: check whether the person messaging you is doing so from a known number
- Via email: through phishing emails

Co-funded by the European Union

Preventing scams with the four-eyes principle

Agree in advance who you can contact if in doubt:

- When you receive a message from an unknown number asking for details, money, or other information.
- When you are called by someone you don't know and are asked to:
  - Transfer money
  - Install a program
  - Click on a link
  - Log in somewhere

Co-funded by the European Union

Preventing scams with the four-eyes principle

Agree in advance who you can contact if in doubt:

- When you receive an urgent email asking you to click a link to transfer money.
- When someone you don't know is standing at your door, and
- Or when you have a gut feeling that something isn't right.

Co-funded by the European Union

Two-Factor Authentication

- When you set up two-step verification, you add an extra layer of security to your apps and accounts.
- When you log in, you not only have to enter your password, but also confirm in another way that you are who you claim to be:
  - An app from Google or Microsoft on your phone
  - SMS on your phone
  - Email message
- This gives you better protection against hacking.

Co-funded by the European Union

Email attacks (1)

- **Don't post your email address online**
  Never put your address on social media, internet forums, or websites. It's quickly found there by the wrong people.

- **Be careful when unsubscribing**
  You can safely unsubscribe from newsletters and mailings you signed up for. Don't do this for emails from unknown companies. If you do, spammers will see that your email address is active, and you may receive even more spam.

- **Use webmail**
  Use Gmail or Outlook.com for your email, because these services have much better spam filters than the email services of internet providers (such as KPN and Ziggo).

Co-funded by the European Union

Email attacks (2)

- **Use a temporary email address**
  Do this for websites you don't fully trust. This can be done, for example, with 10minutemail. Note that you can't receive a reply with all of these kinds of services.

- **Create aliases**
  With many internet providers, you can create additional email addresses (aliases). Use these for things like online shopping. Check how to create aliases.

- **Mark spam as spam**
  You can do this with most email services. By doing so, they learn your preferences and will (hopefully) block similar messages in the future.

Co-funded by the European Union

Phone scams

- Fake call from your bank:
  Does your bank ask you by phone to transfer money or to give your login details or PIN code? **Hang up immediately**. A bank never calls you for this. If you think the call might be important, look up your bank's correct phone number yourself, call that number, and explain that you were called.
- Fake call with a recorded message:
  You hear a recording (often in another language) followed by a menu. You are then connected to someone who asks you for money or personal information. Or the person asks you to download software. **Hang up and do not call back**.
- Fake call from abroad:
  You are called from a foreign number, but the phone only rings once. **Ignore the call and do not call back.**

Co-funded by the European Union

Spoofing

Hackers can imitate an email address. It then looks like you're receiving an email from a company you know, but in reality it's a hacker.

This method is often used to persuade someone to transfer money to a different bank account. The hacker often already knows that this person transfers large amounts to a supplier every month.

By posing as this supplier and stating that the bank account number has changed, you end up depositing money into the hacker's account.

Co-funded by the European Union

Summary

The key lessons at a glance:

- Use long, unique passwords for every account.
- Use a password manager.
- Be wary of alarming emails and calls from strangers.
- Bring in a second pair of eyes when in doubt.
- Never transfer money and never click links in phishing emails.



Co-funded by
the European Union

Thank you for your attention