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 voor senioren

- Veilig omgaan met wachtwoorden
- Hoe herken je digitale oplichting
- Oplichting voorkomen met het vier-ogen principe
- 2Factor Authenticatie
- E-mail aanvallen
- Telefoon scams
- Hooveren
- Spoofing

Co-funded by the European Union

Veilig omgaan met wachtwoorden

Tips voor veilige wachtwoorden:

- Gebruik voor ieder account een sterk en uniek wachtwoord.
- Een sterk wachtwoord is een lang wachtwoord met een aantal speciale tekens of symbolen.
- Gebruik geen informatie die hackers kunnen raden zoals jaartallen, idolen, namen van familieleden of huisdieren.
- Gebruik een wachtwoordmanager om uw wachtwoorden veilig te bewaren en gebruiken.

Co-funded by the European Union

Hoe herken je digitale oplichting?

- Via telefoon, helpdesk medewerkers vragen nooit om inlog gegevens of om een programma te installeren
- Via whatsapp of Telegram, let op of persoon die u een bericht stuurt vanaf een bekende nummer
- Via e-mail, doormiddel van phishingmail

Co-funded by the European Union

Oplichting voorkomen met het vier-ogen principe

Spreek af wie u kunt benaderen bij twijfel:

- Wanneer u een appje krijgt van onbekende nummer en gevraagd om gegevens, geld of andere informatie.
- Wanneer u gebeld wordt door een onbekende en er gevraagd wordt:
  - Geld over te maken
  - Een programma te installeren
  - Op een link te klikken
  - Ergens in te loggen

Co-funded by the European Union

Oplichting voorkomen met het vier-ogen principe

Spreek af wie u kunt benaderen bij twijfel:

- Wanneer u een dringende mail krijgt waar u op een link moet klikken om geld over te maken.
- Wanneer er iemand voor de deur staat die u niet kent en
- Of wanneer u het onderbuikgevoel heeft dat er iets niet klopt.

Co-funded by the European Union

2Factor Authenticatie

- Als je twee stap verificatie instelt, voeg je een extra beveiliging laag toe aan je apps en je accounts.
- Als je inlogt, moet je niet alleen je wachtwoord invullen, maar ook nog op een andere manier aangeven dat je bent wie je beweert te zijn:
  - app van Google of Microsoft op je telefoon
  - SMS op je telefoon
  - E-mail bericht
- Hiermee ben je beter beveiligd tegen hacken.

Co-funded by the European Union

E-mail aanvallen (1)

- **Plaats je mailadres niet online**
  Zet je adres nooit op sociale media, internetfora en websites. Daar worden ze snel gevonden door de verkeerde mensen.

- **Pas op met afmelden**
  Je kunt je veilig afmelden voor nieuwsbrieven en mailings waar je je voor hebt aangemeld. Doe dat niet voor mails van onbekende bedrijven. Doe je dat wel, dan zien spammer dat je mailadres actief is en kun je nog meer spam ontvangen.

- **Gebruik webmail**
  Gebruik Gmail of Outlook.com voor je mail, want die diensten hebben veel betere spamfilters dan de maildiensten van de internetproviders (zoals KPN en Ziggo).

Co-funded by the European Union

E-mail aanvallen (2)

- **Gebruik een tijdelijk mailadres**
  Doe dat voor websites die je niet helemaal vertrouwt. Dat kan bijvoorbeeld met 10minutemail. Let op dat je niet bij al dit soort diensten een antwoord kunt ontvangen.

- **Maak aliassen aan**
  Bij veel internetproviders kun je extra mailadressen (aliassen) aanmaken. Gebruik die voor bijvoorbeeld online winkelen. Bekijk hoe je aliassen aanmaakt.

- **Markeer spam als spam**
  Dit kan bij de meeste e-maildiensten. Door dit te doen, leren die je voorkeuren kennen en blokkeren ze in de toekomst (hopelijk) soortgelijke berichten.

Co-funded by the European Union

Telefoon scam

- <u>Neptelefoontje van uw bank</u>:
  Vraagt uw bank u via de telefoon om geld over te boeken of uw inloggegevens of pincode door te geven? **Verbreek dan meteen de verbinding**. Een bank belt u hier namelijk nooit voor. Als u denkt dat het telefoontje belangrijk is, zoek dan zelf het juiste telefoonnummer van uw bank op, bel dit nummer en leg uit dat u bent gebeld.
- <u>Neptelefoontje met een bandje</u>:
  U hoort een bandje (vaak in een andere taal) gevolgd door een keuzemenu. Daarna krijgt u iemand aan de lijn die u om geld of persoonlijke gegevens vraagt. Of de persoon vraagt u om software te downloaden. **Verbreek de verbinding en bel niet terug**.
- <u>Neptelefoontje vanuit het buitenland:</u>
  U wordt gebeld door een buitenlands nummer, maar de telefoon gaat maar 1 keer over. **Negeer het telefoontje dan en bel niet terug.**

Co-funded by the European Union

Spoofing

Hackers kunnen een mail adres nabootsen. Het lijkt dan alsof je een mail ontvangt van een bedrijf waar je bekend mee bent, maar in werkelijkheid is het een hacker.

Vaak wordt deze methode gebruikt om iemand te overwegen geld op een andere bankrekening te storten. De hacker weet vaak al dat deze persoon maandelijks grote bedragen overmaakt naar leverancier.

Door zich voor te doe als deze leverancier en aan te geven dat het banrekeningnummer is veranderd, stort je geld op de rekening van de hacker.

Co-funded by the European Union

Samenvatting

De belangrijkste lessen op een rij:

- Gebruik lange, unieke wachtwoorden voor ieder account.
- Gebruik een wachtwoord manager.
- Wantrouw alarmerende mails en belletjes van onbekenden.
- Schakel uw extra paar ogen in bij twijfel.
- Maak nooit geld over en klik niet op links in phishingmails.



Co-funded by
the European Union

Bedankt voor uw aandacht