Co-funded by the European Union

FIGHT AGAINST LOVE SCAM



RIFERIMENTO DEL PROGETTO:
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

Sensibilizzazione per gli anziani

- Proteggere le password
- Come riconoscere le truffe digitali
- Prevenire le truffe con il principio dei quattro occhi
- Autenticazione a due fattori
- Attacchi via email
- Truffe telefoniche
- Passare l'aspirapolvere
- Spoofing

Co-funded by
the European Union

Proteggere le password

Consigli per password sicure:

- Utilizza una password complessa e univoca per ogni account.
- Una password sicura è una password lunga che contiene diversi caratteri speciali o simboli.
- Non utilizzare informazioni che gli hacker possono indovinare, come anni, idoli o nomi di familiari o animali domestici.
- Utilizza un gestore di password per archiviare e utilizzare le tue password in modo sicuro.

Co-funded by the European Union

Come riconoscere le truffe digitali?

- Per telefono: il personale dell'assistenza non chiede mai le credenziali di accesso né di installare un programma.
- Tramite WhatsApp o Telegram: verifica se la persona che ti sta inviando il messaggio proviene da un numero conosciuto.
- Tramite e-mail: attraverso e-mail di phishing

Co-funded by the European Union

Prevenire le truffe con il principio dei quattro occhi

Mettetevi d'accordo in anticipo su chi contattare in caso di dubbi:

- Quando ricevi un messaggio da un numero sconosciuto che ti chiede dettagli, denaro o altre informazioni.
- Quando ricevi una chiamata da uno sconosciuto che ti chiede di:
  - Trasferire denaro
  - Installa un programma
  - Fai clic su un link
  - Accedi da qualche parte

Co-funded by the European Union

Prevenire le truffe con il principio dei quattro occhi

Mettetevi d'accordo in anticipo su chi contattare in caso di dubbi:

- Quando ricevi un'email urgente che ti chiede di cliccare su un link per trasferire denaro.
- Quando qualcuno che non conosci è in piedi alla tua porta, e
- Oppure quando si ha la sensazione che qualcosa non vada.

Co-funded by
the European Union

Autenticazione a due fattori

- Attivando la verifica in due passaggi, aggiungi un ulteriore livello di sicurezza alle tue app e ai tuoi account.
- Quando effettui l'accesso, non solo devi inserire la password, ma anche confermare in un altro modo la tua identità:
  - Un'app di Google o Microsoft sul tuo telefono
  - SMS sul tuo telefono
  - Messaggio di posta elettronica
- Questo ti offre una maggiore protezione contro gli attacchi informatici.

Co-funded by the European Union

Attacchi via e-mail (1)

- **Non pubblicare il tuo indirizzo email online.**
  Non inserire mai il tuo indirizzo sui social media, sui forum internet o sui siti web. Verrà trovato rapidamente dalle persone sbagliate.

- **Fai attenzione quando ti disiscrivi.**
  Puoi disiscriverti in tutta sicurezza dalle newsletter e dalle comunicazioni a cui ti sei iscritto. Non farlo per le email provenienti da aziende sconosciute. In caso contrario, gli spammer vedranno che il tuo indirizzo email è attivo e potresti ricevere ancora più spam.

- **Utilizza la webmail.**
  Usa Gmail o Outlook.com per la tua posta elettronica, perché questi servizi hanno filtri antispam molto più efficaci rispetto ai servizi di posta elettronica dei provider internet (come KPN e Ziggo).

Co-funded by the European Union

Attacchi via e-mail (2)

- **Utilizza un indirizzo email temporaneo.**
  Fallo per i siti web di cui non ti fidi completamente. Puoi farlo, ad esempio, con 10minutemail . Tieni presente che non tutti questi servizi garantiscono una risposta.

- **Crea alias.**
  Con molti provider Internet, puoi creare indirizzi email aggiuntivi (alias). Usali per attività come gli acquisti online. Scopri come creare alias .

- **Segnala lo spam come spam.**
  Puoi farlo con la maggior parte dei servizi di posta elettronica. In questo modo, impareranno le tue preferenze e (si spera) bloccheranno messaggi simili in futuro.

Co-funded by the European Union

Truffe telefoniche

- Chiamata falsa dalla tua banca :
  la tua banca ti chiede telefonicamente di trasferire denaro o di fornire le tue credenziali di accesso o il codice PIN? **Riaggancia immediatamente** . Una banca non ti chiamerà mai per questo motivo. Se pensi che la chiamata possa essere importante, cerca tu stesso il numero di telefono corretto della tua banca, chiama quel numero e spiega di aver ricevuto una chiamata.
- Chiamata truffa con messaggio registrato :
  senti una registrazione (spesso in un'altra lingua) seguita da un menu. Vieni quindi messo in contatto con qualcuno che ti chiede denaro o informazioni personali. Oppure ti chiede di scaricare un software. **Riaggancia e non richiamare** .
- Chiamata falsa dall'estero:
  ricevi una chiamata da un numero straniero, ma il telefono squilla solo una volta. **Ignora la chiamata e non richiamare.**

Co-funded by
the European Union

Spoofing

Gli hacker possono falsificare un indirizzo email. In questo modo, sembrerà che tu stia ricevendo un'email da un'azienda che conosci, ma in realtà si tratta di un hacker.

Questo metodo viene spesso utilizzato per convincere qualcuno a trasferire denaro su un conto bancario diverso. L'hacker, di solito, sa già che questa persona trasferisce ingenti somme di denaro a un fornitore ogni mese.

Fingendosi questo fornitore e affermando che il numero di conto bancario è cambiato, si finisce per depositare denaro sul conto dell'hacker.

Co-funded by the European Union

Riepilogo

Le lezioni chiave in sintesi:

- Utilizza password lunghe e univoche per ogni account.
- Utilizza un gestore di password.
- Fate attenzione alle email e alle telefonate allarmanti provenienti da sconosciuti.
- In caso di dubbio, chiedete sempre un secondo parere.
- Non trasferite mai denaro e non cliccate mai sui link contenuti nelle email di phishing.



Co-funded by
the European Union

Grazie per la tua attenzione