Co-funded by the European Union

FIGHT AGAINST LOVE SCAM

PROJEKTREFERENZ:

2024-1-NL01-KA210-ADU-000253818

01.09.2024 - 31.08.2026

CC BY NC SA

Co-funded by the European Union

SENSIBILISIERUNG FÜR SENIORINNEN UND SENIOREN

- Sicherer Umgang mit Passwörtern
- Digitale Betrugsversuche erkennen
- Betrug mit dem Vier-Augen-Prinzip verhindern
- Zwei-Faktor-Authentifizierung
- E-Mail-Angriffe
- Telefonbetrug
- Hoovering: erneute manipulative Kontaktaufnahme
- Spoofing: Vortäuschung einer falschen Identität

Co-funded by the European Unio

SICHERER UMGANG MIT PASSWÖRTERN

Tipps für sichere Passwörter:

- Verwenden Sie für jedes Konto ein starkes und einzigartiges Passwort.
- Ein starkes Passwort ist lang und enthält mehrere Sonderzeichen oder Symbole.
- Verwenden Sie keine leicht zu erratenden Angaben wie Jahreszahlen, Namen bekannter Personen, Familienmitglieder oder Haustiere.
- Nutzen Sie einen Passwortmanager, um Ihre Passwörter sicher zu speichern und zu verwenden.

Co-funded by the European Unio

WIE ERKENNT MAN DIGITALE BETRUGSVERSUCHE?

- **Am Telefon:** Mitarbeitende eines Helpdesks fragen niemals nach Anmeldedaten oder verlangen die Installation eines Programms.
- **Über WhatsApp oder Telegram:** Prüfen Sie, ob die Nachricht von einer Ihnen bekannten Telefonnummer stammt.
- **Per E-Mail:** Achten Sie auf Phishing-E-Mails.

Co-funded by the European Unio

BETRUG MIT DEM VIER-AUGEN-PRINZIP VERHINDERN

Legen Sie im Voraus fest, wen Sie im Zweifelsfall kontaktieren können:

- Wenn Sie eine Nachricht von einer unbekannten Nummer erhalten, in der nach persönlichen Angaben, Geld oder anderen Informationen gefragt wird.
- Wenn eine unbekannte Person Sie anruft und Sie auffordert:
  - Geld zu überweisen
  - ein Programm zu installieren
  - auf einen Link zu klicken
  - sich auf einer Internetseite oder in einem Konto anzumelden

Co-funded by the European Unio

BETRUG MIT DEM VIER-AUGEN-PRINZIP VERHINDERN

Legen Sie im Voraus fest, wen Sie im Zweifelsfall kontaktieren können:

- Wenn Sie eine dringende E-Mail erhalten, in der Sie aufgefordert werden, für eine Geldüberweisung auf einen Link zu klicken.
- Wenn eine unbekannte Person vor Ihrer Tür steht.
- Wenn Sie das Gefühl haben, dass etwas nicht stimmt.

Co-funded by the European Unio

ZWEI-FAKTOR-AUTHENTIFIZIERUNG

- Mit der Zwei-Faktor-Authentifizierung ergänzen Sie Ihre Apps und Konten um eine zusätzliche Sicherheitsebene.
- Bei der Anmeldung geben Sie nicht nur Ihr Passwort ein, sondern bestätigen Ihre Identität zusätzlich auf einem zweiten Weg:
  - über eine App von Google oder Microsoft auf Ihrem Smartphone
  - per SMS auf Ihrem Smartphone
  - über eine E-Mail-Nachricht
- Dadurch sind Sie besser vor Angriffen auf Ihre Konten geschützt.

Co-funded by the European Unio

E-MAIL-ANGRIFFE (1)

- **Veröffentlichen Sie Ihre E-Mail-Adresse nicht im Internet.**

Tragen Sie Ihre Adresse nicht öffentlich in sozialen Medien, Internetforen oder auf Webseiten ein. Dort kann sie schnell von Unbefugten gefunden werden.

- **Seien Sie beim Abbestellen vorsichtig.**

Newsletter, die Sie selbst bestellt haben, können Sie sicher abbestellen. Bei E-Mails unbekannter Unternehmen sollten Sie dies vermeiden, da Absender dadurch erkennen können, dass Ihre Adresse aktiv ist.

- **Verwenden Sie Webmail.**

Dienste wie Gmail oder Outlook.com verfügen häufig über wirksamere Spamfilter als die E-Mail-Dienste mancher Internetanbieter.

Co-funded by the European Unio

E-MAIL-ANGRIFFE (2)

- **Verwenden Sie eine temporäre E-Mail-Adresse.**
Nutzen Sie diese für Webseiten, denen Sie nicht vollständig vertrauen. Dafür gibt es beispielsweise temporäre E-Mail-Dienste. Beachten Sie, dass bei manchen Diensten keine Antworten empfangen werden können.

- **Erstellen Sie Alias-Adressen.**
Bei vielen Anbietern können zusätzliche E-Mail-Adressen eingerichtet werden. Verwenden Sie diese beispielsweise für Online-Einkäufe.

- **Markieren Sie Spam als Spam.**
Die meisten E-Mail-Dienste lernen dadurch Ihre Einstellungen kennen und können ähnliche Nachrichten künftig besser blockieren.

Co-funded by the European Unio

TELEFONBETRUG

- **Gefälschter Anruf Ihrer Bank:**
Fordert Ihre Bank Sie telefonisch auf, Geld zu überweisen oder Anmeldedaten beziehungsweise Ihre PIN weiterzugeben? Legen Sie sofort auf. Eine Bank verlangt dies nicht telefonisch. Suchen Sie die offizielle Telefonnummer Ihrer Bank selbst heraus und rufen Sie dort an.

- **Gefälschter Anruf mit einer aufgezeichneten Nachricht:**
Sie hören eine Aufnahme, häufig in einer anderen Sprache, und werden anschließend mit einer Person verbunden, die Geld oder persönliche Informationen verlangt oder Sie zum Herunterladen einer Software auffordert. Legen Sie auf und rufen Sie nicht zurück.

- **Gefälschter Anruf aus dem Ausland:**
Eine ausländische Nummer ruft nur einmal kurz an. Ignorieren Sie den Anruf und rufen Sie nicht zurück.

Co-funded by the European Unio

SPOOFING

Kriminelle können eine E-Mail-Adresse imitieren. Dadurch sieht es so aus, als hätten Sie eine Nachricht von einem bekannten Unternehmen erhalten. Tatsächlich stammt sie jedoch von einer betrügerischen Person.

Diese Methode wird häufig genutzt, um jemanden zu einer Überweisung auf ein anderes Bankkonto zu bewegen. Die betrügerische Person weiß möglicherweise bereits, dass regelmäßig größere Beträge an einen bestimmten Lieferanten überwiesen werden.

Sie gibt sich als dieser Lieferant aus und behauptet, die Bankverbindung habe sich geändert. Dadurch wird das Geld auf das Konto der betrügerischen Person überwiesen.

Co-funded by the European Unio

ZUSAMMENFASSUNG

Die wichtigsten Erkenntnisse im Überblick:

- Verwenden Sie für jedes Konto ein langes und einzigartiges Passwort.
- Nutzen Sie einen Passwortmanager.
- Seien Sie bei alarmierenden E-Mails und Anrufen unbekannter Personen vorsichtig.
- Holen Sie im Zweifelsfall eine zweite Meinung ein.
- Überweisen Sie niemals Geld und klicken Sie niemals auf Links in Phishing-E-Mails.



Co-funded by
the European Union

Vielen Dank für Ihre Aufmerksamkeit

CC BY NC SA