

# Furtul de identitate



**Furtul de identitate** sau fraudă de identitate reprezintă utilizarea ilicită a informațiilor personale de identitate (PII) a victimei de către infractor, pentru a obține un avantaj financiar și alte beneficii.

## Tipuri de tehnici:



- **Business Email Compromise (BEC):** atacatorii fac uz de identitatea unei persoane de încredere, de obicei în cadrul companiei, iar victima este păcălită să facă o tranzacție financiară sau să divulge informații sensibile, personale sau corporative.
- **Doppelgangers digitali:** tehnică antifraudă "măști digitale" a fost expusă atunci când identitățile digitale furate au apărut ca un produs de tranzacționare pe piețele darknet.
- **Identități SIM-Swapping:** această tehnică vizează deținătorii de criptomonede și persoanele sau conturile cu profil înalt, cu intenția de a fura identitatea victimei.

## RECOMANDĂRI privind prevenirea furtului de identitate:

- **Utilizați autentificarea cu 2 factori (2FA)** - aceasta reprezintă o măsură de siguranță pentru a preveni furtul sau pierderea parolei și pentru a asigura succesul procesului de autentificare cu mai mulți factori.
- **Autentificați orice expeditor al unei cereri** - pentru a transfera bani personal sau prin telefon.
- **Protejați toate documentele și copiile actelor de identitate** - (fizic sau digital) împotriva accesului neautorizat.
- **Nu divulgați informația privind identitatea** - cererile nesolicitate prin telefon, e-mail sau care nu ar trebui să primească răspuns.
- **Utilizați dispozitive protejate cu parolă** - astfel asigurând o bună calitate a credențialelor și metode sigure pentru stocarea acestora.
- **Acordați atenție sporită la utilizarea rețelelor publice Wi-Fi** - dacă utilizați una, evitați accesul la aplicații și date sensibile. Folosiți un serviciu VPN de încredere pentru a vă conecta la rețelele Wi-Fi publice.
- **Verificați tranzacțiile** - documentate prin extrase bancare au studiați regulat chitanțele pentru nereguli.
- **Instalați filtre de conținut** - pentru a filtra fișierele nedorite, e-mail-urile cu conținut rău intenționat, spamul și traficul de rețea nedorit.

