SIM-SWAPPING

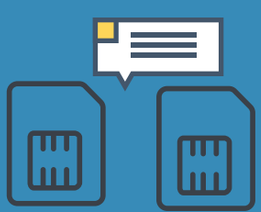
OPLICHTING MET MOBIELE TELEFOONNUMMERS

Sim-swapping gebeurt wanneer een fraudeur, met gebruik van social engineering technieken, controle neemt over de simkaart van uw mobiele telefoon met gebruikmaking van gestolen persoonlijke gegevens.

HOE WERKT HET?

Een fraudeur krijgt toegang tot de persoonlijke gegevens van het slachtoffer via een datalek, phishing, zoekopdrachten op social media, schadelijke apps, online winkelen, malware, etc.

Met deze informatie misleidt de fraudeur de telecomprovider om het telefoonnummer van het slachtoffer over te zetten op een simkaart die hij in zijn bezit heeft. Een fraudeleuze medewerker bij een telecomprovider behoort ook tot de mogelijkheden.



De fraudeur kan nu inkomende gesprekken en sms'jes ontvangen, inclusief toegang tot sms'jes met bijvoorbeeld verificatiecodes van diverse applicaties.

Het slachtoffer zal merken dat de mobiele telefoon niet meer functioneert, en zal uiteindelijk ontdekken dat hij niet kan inloggen op bijvoorbeeld e-mail.

WAT KUNT U DOEN?

- Houd uw software up-to-date, inclusief uw browser, antivirus en het besturingssysteem.
- Beperk informatie en wees voorzichtig met informatie delen op social media.
- Open nooit verdachte links of bijlagen die u via de email of sms ontvangt.
- Beantwoord geen verdachte e-mails of ga geen gesprek aan over de telefoon met bellers die uw persoonlijke informatie vragen
- Update regelmatig uw wachtwoorden.
- Download alleen apps van officiële aanbieders en lees altijd de machtigingen van de apps.
- Koppel, indien mogelijk, uw telefoonnummer niet aan gevoelige online accounts.
- Gebruik speciale authenticatie-apps die als alternatief voor verificatiecodes per sms kunnen dienen.
- Spreek, indien mogelijk, een wachtwoord af met uw telecomprovider om mutaties aan uw abonnement te voorkomen. Deel dit wachtwoord met niemand.
- Controleer regelmatig uw bankafschriften.

BENT U EEN SLACHTOFFER?

- Als uw mobiele telefoon zonder enige reden de ontvangst verliest, meld dit dan onmiddellijk aan uw serviceprovider.
- Als uw serviceprovider bevestigt dat uw SIM is verwisseld, doe dan aangifte bij de politie en verander direct uw wachtwoorden.

#TelecomFraud

EUROPOL EC3 European Cybercrime Centre

POLITIE