Social engineering

Wat is het?

- Social engineering is een techniek waarbij internetcriminelen mensen manipuleren. Zo verleiden oplichters je bijvoorbeeld om persoonlijke of bedrijfsgevoelige gegevens te delen voor het zogenaamd deblokkeren van een account.
- Social engineering is het beïnvloeden van mensen waardoor ze dingen doen die in het voordeel van een internetcrimineel zijn.
- In de context van cybercrime kan social engineering zowel in de fysieke als in de digitale wereld plaatsvinden. Denk aan het verleiden om op een foute link te klikken.

Welke gevolgen heeft het voor jouw bedrijf?

- Financiële schade, bijvoorbeeld door ransomware of spookfacturen.
- Schade aan vertrouwelijke informatie.
- Schade aan het vertrouwen binnen een bedrijf, ook onder werknemers.

Hoe kun je het voorkomen?

- Bouw aan een positieve bedrijfscultuur, waar schaamte plaats maakt voor een meldcultuur.
- Investeer in trainingen en workshops.
- Wees kritisch hoe en op welke wijze informatie wordt weggegooid.
- Vergrendel je computer als je even wegloopt.
- Overweeg de aanschaf van privacy screenprotectors voor laptop/telefoon.
- Kijk voor meer tips en informatie op de website van het **Digital Trust Center (DTC)**.

Alert Online richt zich op het creëren van bewustwording rondom online veiligheid, op het vergroten van kennis over online veiligheid en op het stimuleren van cybersecure gedrag.
De Alert Online spiekbriefjes zijn gebaseerd op de **cyberspiekbriefjes voor Tweede Kamerleden**.
Kijk voor meer tips en informatie op veiliginternetten.nl