# *Social engineering*

## Wat is het?

- Social engineering is een techniek waarbij een cybercrimineel mensen manipuleert om vertrouwelijke informatie te verkrijgen die toegang verleent tot systemen.
- Social engineering stuurt menselijk gedrag om handelingen uit te voeren die een aanvaller verlangt, de mens is vaak de zwakste schakel in de computerbeveiliging.
- In social engineering werken criminelen met bepaalde psychologische principes die gedrag van mensen sturen.
- 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.
- Social engineering-aanvallen kunnen op grote schaal plaatsvinden zonder een specifiek doelwit (denk aan email). Ze kunnen zich ook richten op goedgelovige mensen en hun kwetsbaarheden of op hoge functionarissen in (zeer) gevoelige functies zoals CIO's.

## Belang voor Nederland

- Het vertrouwen van mensen om digitale middelen te gebruiken is essentieel voor de moderne economie en samenleving.
- Mensen moeten digitaal vertrouwen kunnen hebben in mensen en organisaties waarmee ze online interactie hebben.

## Gevolgen bij misbruik

Verlies van vertrouwen om digitale diensten te gebruiken door:

- *Schade aan personele data*
  Bijvoorbeeld identiteitsdiefstal nadat een crimineel je wachtwoorden kent.
- *Financiële schade*
  Bijvoorbeeld valse online offerte (spookfacturen) of geld overmaken met valse Whatsapp.
- *Fysieke schade*
  Bijvoorbeeld Loverboys op social media of dating apps, ze laten slachtoffers verliefd worden en daarna exploiteren ze hen.
- *Schade aan vertrouwelijke informatie*
  Bijvoorbeeld criminelen manipuleren slachtoffers met chantage of verleiding om bedrijfsinformatie te verwerven.
- *Schade aan het vertrouwen*
  Bijvoorbeeld online social engineering in het kader van desinformatie, om groepen mensen te beïnvloeden op specifieke onderwerpen (5G, COVID-19 vaccinaties, etc.).

## Is misbruik al eens voorgekomen?

- Buiten EU: US 2016 verkiezingen: hackers kregen via een spearphishing-aanval toegang tot e-mails van de Democratische Partij met gevoelige informatie. Bovendien werd social media voor desinformatie gebruikt.
- Europa: In 2018 werd onthuld dat een hacker het account van een Britse RAF-vlieger had overgenomen en een match had met een ander RAF-personeelslid om informatie over F35s te krijgen.
- Nederland: Maastricht University 2019, De gestolen data werd gebruikt om de organisatie af te persen, om het losgeld te betalen.

**Cybersecurity specifieke relevante nationale wetgeving of andere richtlijnen**

- Computercriminaliteit III (amendement 08/12/2016);
- Richtlijnen van de Digital Trust Center;

**What is social engineering?**
**https://www.youtube.com/watch?v=Vo1urF6S4u0**

**Social Engineering: phishing example**
https://www.youtube.com/watch?v=xuYoMs6CLEw