

# Digitale criminaliteit

## Begrippen en uitleg



### AAN- EN VERKOOPFRAUDE



Aan- en verkoopfraude is een vorm van internetoplichting, waarbij malafide verkopers en aankopers slachtoffers oplichten op webwinkels, online handelsplaatsen en sociale media.

### ACCOUNT TAKEOVERS



De dader hackt de webshopaccount van een slachtoffer en bestelt hier vervolgens diensten of goederen mee. Om te betalen, gebruikt de dader de betaalopties die gekoppeld zijn aan het account, zoals achteraf betalen, creditcards of kredietverstrekkers, zoals Klarna.

### BEC-FRAUDE



Medewerkers van een organisatie worden door de dader via e-mailberichten misleid om een valse factuur te betalen of via de bedrijfsrekening een geldbedrag over te schrijven naar de oplichter. De oplichter creëert een mate van urgentie of noodzaak om de medewerker onder druk te zetten.



#### CEO-fraude

De dader stuurt een mail naar een medewerker namens een hooggeplaatst persoon in de organisatie met de vraag om een geldbedrag over te schrijven naar een rekeningnummer of met het verzoek om giftcards aan te kopen.



#### Digitale factuurfraude

De dader stuurt een gepersonaliseerde e-mail met valse betaalgegevens naar een medewerker van een organisatie die betrokken is bij een betalingsafdeling. De dader kan ook een factuur van het bedrijf onderscheppen, en het rekeningnummer aanpassen.



# Digitale criminaliteit

## Begrippen en uitleg



### BOILERROOMFRAUDE



Daders laten slachtoffers geld of cryptovaluta beleggen voor niet bestaande, hoge rendementen. Slachtoffers worden online benaderd en onder druk gezet om snel een beslissing te nemen voordat deze 'unieke kans' aan ze voorbijgaat.

### DATINGFRAUDE



Datingfraudeurs maken, vaak via datingsites en sociale media, contact met mensen die op zoek zijn naar een relatie. Eenmaal in contact wordt een "relatie" tot stand gebracht. De fraudeur vraagt na enige tijd met een smoes om een geldbedrag van het verliefde slachtoffer. Dit kan lange tijd doorgaan.

### DOXING



Het met kwade bedoelingen verzamelen of (verder) verspreiden van persoonlijke, gevoelige of privéinformatie zoals een woonadres, telefoonnummer, een foto, paspoort, naam van een werkgever en gegevens van familie of vrienden.

### HULPVRAAGFRAUDE



De dader doet zich voor als een bekende van het slachtoffer, en vraagt onder het mom van urgentie een geldbedrag aan het slachtoffer via een berichtendienst. Oplichting via WhatsApp komt het meest voor. Hulpvraagfraude is te beschouwen als de digitale variant van de klassieke babbeltruc.



# Digitale criminaliteit

## Begrippen en uitleg



### ONLINE SEKSUEEL MISBRUIK



Online seksueel misbruik betreft het ontvangen van ongewenste, beledigende, seksueel getinte e-mails of berichten of het meemaken van ongepaste seksuele toenaderingen via sociale media, datingsites of online chatrooms.



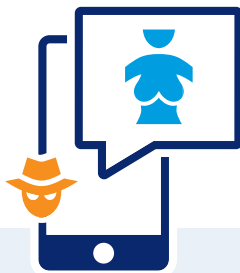
#### Grooming

Grooming is digitaal kinderlokken. Een volwassene legt online contact met een minderjarige met het doel om seksueel misbruik te plegen of om kinderpornografische afbeeldingen te produceren.



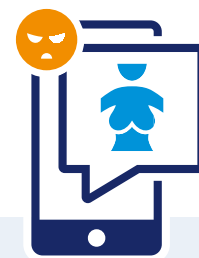
#### Sexting

Bij sexting is er sprake van het uitwisselen van seksueel getint (beeld)materiaal. Dit kan vrijwillig, maar ook onvrijwillig zijn.



#### Sextortion

De dader verkrijgt seksueel getint (beeld) materiaal en dreigt vervolgens met de verspreiding van dit materiaal. De dader probeert het slachtoffer te dwingen tot (financiële) vervolgacties of jaagt het slachtoffer vrees aan.



#### Wraakporno

De dader verspreidt zonder toestemming seksueel getint (beeld)materiaal. Het slachtoffer hoeft hier niet van op de hoogte te zijn. De dader is enkel uit op persoonlijke genoegdoening, aanzien en/of een (seksuele) kick.



# Digitale criminaliteit

## Begrippen en uitleg



### PHISHING



Een verzamelnaam voor alle activiteiten waarmee een dader door middel van deceptie persoonlijke gegevens van slachtoffers verkrijgt of binnendringt op een account of apparaat. Slachtoffers klikken bijvoorbeeld op een link en vullen persoonlijke gegevens in die een dader kan inzien. De meest voorkomende vormen zijn bankphishing en betaalverzoekfraude.



#### Bankphishing

De dader probeert bank- of cryptogegevens van een slachtoffer te bemachtigen. Het slachtoffer vult bankgegevens in op een website die lijkt op de website van een bedrijf of instantie, maar wordt beheerd door de dader. De gegevens komen terecht bij de dader, die toegang krijgt tot de bankgegevens van het slachtoffer.



#### Betaalverzoekfraude

Een vorm van bankphishing waarbij het slachtoffer wordt benaderd via een online handelsplaats. De phishing-link kan o.a. verwerkt zijn in een vals betaalverzoek of verzendlabel.

### TELEFONISCHE HELPDESKFRAUDE



Vorm van phishing waarbij de dader het slachtoffer benadert via telefoon en zich voordoeft als helpdeskmedewerker van bijvoorbeeld een bank, een technologisch bedrijf of overheidsinstelling.



#### Bankhelpdeskfraude

Het slachtoffer wordt gebeld door een zogenaamde bankmedewerker die hem geld probeert afhandig te maken. De dader probeert het slachtoffer te overtuigen om zo snel mogelijk geld of andere waardevolle spullen bij hem veilig te stellen, omdat er iets niet in de haak zou zijn met de bankrekening.

