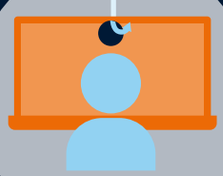
OPENBAAR MINISTERIE

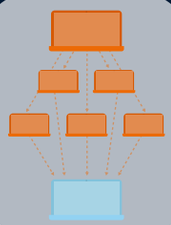
# Cybercrime en digitale criminaliteit

*Cybercrime en digitale criminaliteit ontwikkelen razendsnel. Daders blijven vaak onzichtbaar en brengen mensen en bedrijven grote schade toe. Maar wat is het nu eigenlijk? Welke delicten zijn er, welke straffen staan daar op en wat kun je er tegen doen?*

## Phishing



## DDoS-aanval



## Account Take Over (ATO)

## Ransomware

## Tech Support Scam (TSS)

## Criminele RAT's

## BEC/CEO-fraude

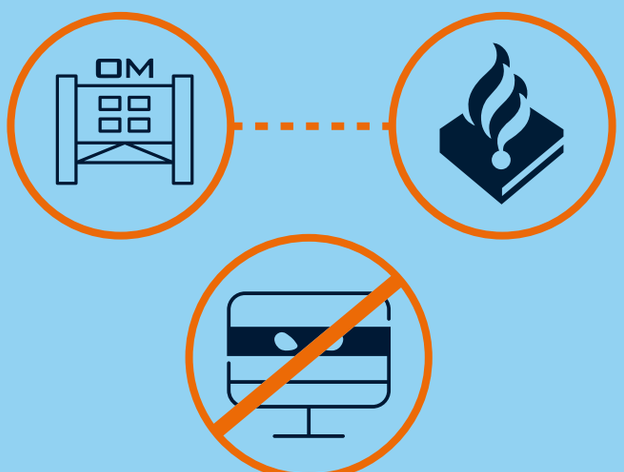
## VIN/WhatsApp fraude

## Betaalverzoekfraude

## Sextortion

## Bulletproof Hosting

OM en politie zetten zich in om deze criminaliteit te bestrijden, met gespecialiseerde cybercrimeteams, cybercrime-officieren en experts




**Wat kun je doen?**
Maak het de cybercriminelen zo moeilijk mogelijk en kijk op:

- OM.nl
- veiliginternetten.nl
- veiliginternetbankieren.nl
- politie.nl

**Ben je slachtoffer geworden?**

Doe altijd een melding of aangifte bij de politie! Hierdoor kan het OM en de politie beter inzicht krijgen in de omvang, en de verdachten (sneller) opsporen en vervolgen.

**Richtlijn strafvordering cybercrime**

OPENBAAR MINISTERIE

# Phishing

## Wat is het?

Phishing is de verzamelnaam voor alle digitale activiteiten waarmee criminelen proberen persoonlijke informatie te pakken te krijgen. Zij proberen daarmee de controle over je bankrekening of inloggegevens te krijgen.

## Wat is er tegen te doen?

Ga nooit in op mails, sms'jes, apps of telefoontjes van onbekenden, waarin gevraagd wordt om je wachtwoorden, of een nieuwe bezorgafspraak te maken. Betrouwbare webshops, banken of creditcard maatschappijen zullen dat nooit vragen. Wil je betalen, log dan zelf in op je eigen banksite (géén link van een ander dus). Check een link via checkjelinkje.nl. Is je aanspreeknaam niet juist? Dan is de kans groter dat het om phishing gaat.

Link checken? Ga naar:
www.checkjelinkje.nl

## Welke straf kan het OM eisen?

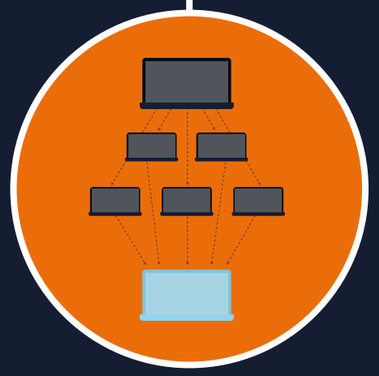
In 2019 werd een man door de rechtbank veroordeeld tot een gevangenisstraf van 42 maanden, en het (terug)betalen van een bedrag van 1 miljoen euro.

OPENBAAR MINISTERIE

# DDoS-aanval

## Wat is het?

Bij een DDoS-aanval sturen criminelen grote hoeveelheden dataverkeer naar servers, waardoor ze overbelastraken en niet meer (goed) werken. Hierdoor zijn bedrijven urenlang niet meer bereikbaar, wat grote gevolgen heeft. Denk bijvoorbeeld aan onderwijsinstellingen of overheidswebsites. Soms proberen criminelen bedrijven af te persen, onder dreiging van een DDoS-aanval.



## Wat is er tegen te doen?

- Zorg dat je je updates van je besturingsysteem up to date houdt.
- Er bestaan commerciële aanbieders van pakketten die beschermen tegen DDoS-aanvallen, zoals Nationale Wasstraat en Cloudflare.
- Slachtoffer geworden? Doe altijd aangifte bij de politie! En: betaal niet! Daarmee hou je het criminele verdienmodel in stand.

## Welke straf kan het OM eisen?

Onlangs werd in Midden-Nederland een verdachte door de rechter veroordeeld tot een (deels voorwaardelijke) celstraf van 3 jaar. Hij gebruikte de DDoS aanval om een bedrijf af te persen, en had ook een vuurwapen in zijn bezit.

OPENBAAR MINISTERIE

# Account Take Over (ATO)

## Wat is het?

Bij een Account Take Over (ATO) nemen criminelen - via een hack, datalek of phishing - je account bij een webshop over, en plaatsen bestellingen uit jouw naam.

## Wat is er tegen te doen?

- Zorg voor sterke en unieke wachtwoorden
- Gebruik niet overal hetzelfde wachtwoord
- Gebruik - waar mogelijk - twee factor authenticatie bij het inloggen. Naast een gebruikersnaam en wachtwoord vul je bijvoorbeeld ook nog een code in die je via SMS op je smartphone hebt ontvangen, of geef je een digitale vingerafdruk via je smartphone.
- Slachtoffer geworden? Doe altijd een melding of aangifte bij de politie!

Wil je weten of jouw mailadres ooit onderdeel is geweest van een datalek? Kijk dan op de site haveibeenpwned.

## Welke straf kan het OM eisen?

Begin 2021 is tegen een 27-jarige man een gevangenisstraf van 30 maanden geeist, evenals het betalen van een geldboete van 10.000 euro.

OPENBAAR MINISTERIE

# Ransomware

## Wat is het?

Ransomware is software die criminelen gebruiken om computers te versleutelen, waardoor je niet meer bij je gegevens kan. Pas na betaling van losgeld ('ransom') krijg je - doorgaans - de controle weer terug. Ook dreigen de criminelen met publicatie, om je nog meer onder druk te zetten om te betalen.

## Wat is er tegen te doen?

- Verander geregeld je wachtwoorden, voer tijdig noodzakelijke updates uit en investeer in online beveiliging, zoals antivirus-software en firewalls.

- Voor bedrijven: Zorg voor een goede basis IT hygiëne. Een ransomware aanval kan al starten via een simpele phishing mail aan een medewerker.

- Slachtoffer geworden? Doe altijd een melding of aangifte bij de politie en betaal niet! Daarmee houd je het criminele verdienmodel in stand.

Slachtoffer van een ransomeware aanval? Kijk op NoMoreRansom.org of er een digitale sleutel is, waarmee je toch bij jouw gegevens kan.

## Welke straf kan het OM eisen?

In 2018 werden 2 jongens door de rechtbank veroordeeld tot een maximale taakstraf, in combinatie met forse voorwaardelijke gevangenisstraffen. Het OM kan - voor een grootschalige ransomware aanval - een gevangenisstraf eisen van 3 jaar (voor een eerste veroordeling). Voor veelplegers kan dit oplopen naar 4 jaar.

OPENBAAR MINISTERIE

# Tech Support Scam (TSS)

## Wat is het?

Tech Support Scam (TSS) is een digitale babbeltruc. Criminelen doen zich – meestal telefonisch – voor als medewerker van een helpdesk, en proberen zo toegang te krijgen tot je inloggegevens.

## Wat is er tegen te doen?

- Scherm je contactgegevens goed af. Ga niet in op het aanbod van de helpdesk en geef anderen geen toestemming om je computer op afstand over te nemen.
- Slachtoffer geworden? Doe altijd een melding of aangifte bij de politie!

## Welke straf kan het OM eisen?

In een strafzaak waarbij verdachten zich hebben voorgedaan als medewerkers van helpdesk van een bank, zijn lange (deels voorwaardelijke) gevangenisstraffen opgelegd, evenals het terugbetalen van het onrechtmatig verkregen geld.

OPENBAAR MINISTERIE

# Criminele RAT's

## Wat is het?

Een RAT (Remote Access Trojan) is een programma waarmee je computer, tablet of telefoon volledig kan worden overgenomen, zonder dat je dit in de gaten hebt. Dit kan bijvoorbeeld leiden tot het overnemen of veranderen van bestanden, stelen en gebruiken van wachtwoorden, het besturen van je camera, muis of toetsenbord, en het verkrijgen van toegang tot je online cloud, Social Media account(s) of (crypto)rekeningen.

## Wat is er tegen te doen?

- De malware zit verborgen in een link in een e-mail, of illegale (gedownloade) software. Koop dus alleen legale software, via betrouwbare webshops en appstores.
- Doe altijd alle noodzakelijke updates, installeer een firewall en open nooit bijlages of URL's van onbekenden.
- Maak zoveel mogelijk gebruik van 2-factor authenticatie.
- Wees je er bewust van waar je je documenten en bestanden opslaat. Is deze locatie goed beveiligd?
- Gebruik een webcam cover.
- Slachtoffer geworden? Doe altijd een melding of aangifte bij de politie!

## Welke straf kan het OM eisen?

Er staan (forse) gevangenisstraffen op het hebben en gebruiken van een RAT. Onlangs is een man door de rechtbank veroordeeld tot een onvoorwaardelijke gevangenisstraf van 19 maanden.

OPENBAAR MINISTERIE

# VIN/WhatsApp fraude

## Wat is het?

Bij Vriend in Nood (VIN) fraude doen criminelen zich (vaak via whatsapp) voor als een vriend of familielid, en vragen om geld.

## Wat is er tegen te doen?

- Scherm je privégegevens (en je vriendenlijsten) online goed af (want daar halen criminelen informatie uit).

- Stuurt iemand je een verzoek via een 'nieuw' kanaal? Check dan via een ander - bekend- kanaal bij diegene of dit verzoek echt is.

- Slachtoffer geworden? Doe altijd een melding of aangifte bij de politie, óók als je niet betaald hebt! Maak screenshots van het gesprek en noteer het nummer.

## Welke straf kan het OM eisen?

In verschillende strafzaken zijn verdachten door de rechter veroordeeld tot jarenlange gevangenisstraffen, en het terugbetalen van het onrechtmatig verkregen geld.

OPENBAAR MINISTERIE

# BEC/CEO-fraude

## Wat is het?

Criminelen proberen bedrijven & organisaties op te lichten. Bijvoorbeeld door zich voor te doen als CEO (en zo betalingen af te dwingen). Maar ook door in de mailserver binnen te dringen en daar facturen aan te passen, zodat het geld naar de bankrekeningen van criminelen kan worden weggesluisd. Bij het zich voordoen als medewerker van het bedrijf wordt onder meer gebruik gemaakt van typosquatting - waarbij een mailadres sterk lijkt op het orgineel - alsook van spoofing (geen verschil zichtbaar).

## Wat is er tegen te doen?

- Neem bij afwijkingen in een factuur (bijv. nieuw rekeningnummer) altijd telefonisch contact op met de afzender
- Voer extra controles in (zoals het 'vier-ogen principe')
- Laat (via de softwareleverancier) veiligheidscontroles inbouwen
- Slachtoffer geworden? Doe altijd een melding of aangifte bij de politie!

## Welke straf kan het OM eisen?

Zo is onlangs een man door de rechtbank veroordeeld tot een jarenlange gevangenisstraf en de terugbetaling van honderdduizenden euro's.

OPENBAAR MINISTERIE

# Sextortion

## Wat is het?

Via seksueel getinte foto's of video's proberen criminelen je te chanteren of af te persen. Dit kunnen echte beelden zijn, of beelden die gemanipuleerd zijn.

## Wat is er tegen te doen?

- Verspreid nooit gevoelige beelden en scherm je identiteit goed af.
- Slachtoffer geworden? Doe altijd een melding of aangifte bij de politie, en schakel hulp in via bijvoorbeeld helpwanted.nl of Qpido.nl.

Slachtoffer van sextortion? Kijk op: internetsporen.nl/is/sextortion

## Welke straf kan het OM eisen?

Onlangs is een webcamafperser door de rechtbank veroordeeld tot een gevangenisstraf van 10 jaar. In deze zaak was er sprake van een groot aantal minderjarige slachtoffers.

OPENBAAR MINISTERIE

# Betaalverzoekfraude

## Wat is het?

Criminelen sturen (via FaceBook of Marktplaats) een betaalverzoek. Dit lijkt op een echt betaalverzoek of een tikkie. Maar pas op: dit kan een phishinglink zijn, waarmee ze toegang krijgen tot je bankrekening.

## Wat is er tegen te doen?

- Ga niet in op een verzoeken van onbekenden
- Geef je telefoonnummer niet rechtstreeks aan derden, communiceer alleen via de berichtenservice van bijvoorbeeld Facebook of Marktplaats zelf
- Gebruik (waar mogelijk) twee factor authenticatie bij het inloggen. Naast een gebruikersnaam en wachtwoord vul je bijvoorbeeld ook nog een code in die je via SMS op je smartphone hebt ontvangen, of geef je een digitale vingerafdruk via je smartphone.
- Slachtoffer geworden? Doe altijd een melding of aangifte bij de politie!

## Welke straf kan het OM eisen?

Onlangs zijn vijf verdachten veroordeeld tot een gevangenisstraf van 15 maanden, waarvan 5 maanden voorwaardelijk.

OPENBAAR MINISTERIE

# Bulletproof Hosting

## Wat is het?

Een bulletproof hosting provider maakt het uitvoeren van criminele activiteiten via het internet mede mogelijk. Bijvoorbeeld door serverruimte te verhuren of data te hosten van personen of organisaties, die dit gebruiken voor cybercrime. Denk bijvoorbeeld aan (online) verspreiding van kinderporno, of het hosten van ransom- of malware.

## Wat is er tegen te doen?

- Wanneer een hosting-bedrijf signalen krijgt van criminele activiteiten van één van haar klanten, dan wordt verwacht dat ze hier tegen optreden. Doen ze dit niet, dan zijn ze zelf ook strafbaar.
- De opsporing en vervolging is complex. Vaak zit de malafide verhuurder (evenals de criminele klanten) in een land ver over de Nederlandse grens.
- Het OM werkt samen met de politie en andere meldings-instanties om deze bulletproof hostingbedrijven aan te pakken.

## Welke straf kan het OM eisen?

De eigenaar van een hostingbedrijf werd onlangs door de rechter veroordeeld tot een gevangenisstraf van 5 maanden, voor het witwassen van geld. Door het OM was 5 jaar geëist, maar het met opzet verspreiden van kinderporno kon niet worden bewezen.