

Digitaal Bewust

**12 THEMA'S OM DIGITAAL
WEERBAAR TE WORDEN**



politie.nl

Inhoudsopgave

1. Iedereen kan slachtoffer worden	5
2. Aan- en verkoopfraude	6
3. (bank)Helpdeskfraude	7
4. Beleggingsfraude	8
5. Phishing	9
6. Hacken	10
7. Ransomware	10
8. Datingfraude	11
9. Sextortion	12
10. (Cyber)pesten	13
11. Doxing	14
12. Gaming & Social Media	15





Iedereen kan slachtoffer worden!

Bedenk eens bij hoeveel handelingen in het dagelijks leven computers en internet een rol spelen. Vaak is het zelfs onmisbaar in onze dagelijkse uitvoering. Ook criminelen maken daar steeds slimmer misbruik van.

Al geruime tijd is er een verschuiving gaande van de traditionele naar de digitale criminaliteit. Gedigitaliseerde criminaliteit en cybercrime nemen een enorme vlucht en vereisen een nieuwe manier van aanpak en benadering. Er is ook een zichtbare verschuiving te zien in het karakter van jeugdcriminaliteit. Criminelen gaan steeds slimmer te werk en bedenken steeds iets nieuws. Maar ook een aantal meer traditionele vormen van criminaliteit krijgen een online karakter. Het blijft daarom opletten. In deze brochure leggen we uit welke maatregelen u allemaal kan nemen.

Toch zien we een patroon terug wanneer u of uw naasten benaderd worden. Is er contact met een medewerker van een instantie en het



gaat om geld? Wees dan extra alert. Criminelen gebruiken actualiteit, hoge urgentie, tijdsdruk en proberen vertrouwen te winnen met het benoemen van uw persoonlijke gegevens.

Hoe komen criminelen aan persoonsgegevens?

Dit kan op verschillende manieren. Denk aan identiteitsfraude, hacking of datalekken. Deze gegevens worden veelal doorverkocht op het anonieme internet zoals het Darkweb.

Een datalek wordt gedefinieerd als het opzettelijk of onopzettelijk vrijgeven van beveiligde informatie aan een onvertrouwd publiek. Gegevens van een webwinkel of van een systeem zijn onvoldoende beveiligd waardoor ze gemakkelijk buitgemaakt kunnen worden door onbevoegde. Ook gebeurt het dat medewerkers gegevens buitmaken en delen met criminelen.

Online criminaliteit of cybercriminaliteit zijn criminele delicten waarbij digitale technologie een rol speelt.



Aan- en verkoopfraude

Elke maand kopen en verkopen miljoenen mensen online goederen. Meestal gebeurt dit naar volle tevredenheid van alle partijen. Helaas zullen er altijd mensen zijn die de boel moedwillig oplichten. Criminelen proberen via onder andere, neppe webshops mensen op te lichten.

Wat kunt u doen?

- Overhaast uw aan- of verkoop niet!
- Nepwebwinkels lijken vaak op dat van een betrouwbare webwinkel. Ze kopiëren hierbij logo's of laten het webadres lijken op de echte aanbieder. Controleer het bedrijf in online zoekmachines en kijk naar klantbeoordelingen. Op politie.nl kunt u zien of er meldingen bekend zijn over de webshop.

- Controleer of de webwinkel is aangesloten bij een betrouwbare belangenvereniging. Zoek op de website van het keurmerk naar een vermelding van de webwinkel.
- Wees alert als de webwinkel het volledige bedrag vooraf wil ontvangen. Betaal bij voorkeur achteraf of via creditcard.
- Wilt u een grote aankoop doen op een tweedehands website? Dan is ophalen en gelijk oversteken een van de mogelijkheden.

Als iets te mooi lijkt om waar te zijn, is dat meestal ook zo. Laat u niet overhalen met kortingen of acties met tijdsdruk. Maak een overwogen beslissing.



Helpdeskfraude

(Technical Support scam)

U krijgt een telefoontje, sms-bericht of melding op uw computer, van iemand die aanbiedt om problemen op uw computer te verhelpen. Vaak is dit iemand die Engels spreekt en zich voordoet als medewerker van een softwarebedrijf. De medewerker belooft tegen betaling "niet-bestaande" softwareproblemen op te lossen of verzoekt u software te installeren om toegang te krijgen tot uw computer.

Bankhelpdeskfraude

Fraudeurs leggen contact met u en doen zich voor als bankmedewerker. Soms bellen ze met een telefoonnummer dat vertrouwd lijkt of lijkt op dat van de bank (spoofing). De oplichters wekken vertrouwen omdat ze uw persoonlijke gegevens weten en de tijd nemen. Ze maken u wijs dat er verdachte transacties zijn geweest. De fraudeur vraagt om uw medewerking voor het installeren van programma's op uw computer of telefoon. Dit voor overname van uw computer om in uw internetbankieren te komen.

In andere gevallen komt er een

persoon de pinpas 'met spoed' bij u thuis ophalen en wordt de pincode tijdens het telefoongesprek ontfutseld. Hierna wordt het er snel geld gepind. Soms hebben deze internetcriminelen dagenlang contact met slachtoffers.

Wat kunt u doen?

- Bankmedewerkers, Politie of andere bedrijven komen nooit langs om uw pinpas of sieraden op te halen!
- Een bank of andere instantie zal nooit uw pincode of saldo vragen, ook niet als controlevraag.
- Een bank zal u nooit vragen om geld over te maken naar een andere rekening, 'kluisrekening' of 'veilige rekening'. Deze rekeningen bestaan helemaal niet.
- Verbreek bij twijfel altijd de verbinding en bel uw bank op het u bekende nummer.
- Installeer geen (overname) software om uw computer.

Let op!

Banken, Politie of andere instanties vragen nooit om uw inloggegevens of pincodes. Bij twijfel direct ophangen en zelf de echte bank bellen.



Beleggingsfraude

Slachtoffers worden benaderd met als doel geld te laten investeren of te laten beleggen, ook wel bekend als boilerroomfraude. Beloofde rendement is altijd hoger dan elders. (Te mooi om waar te zijn!). De rendementen worden echter niet of beperkt uitbetaald. Soms wordt na een korte periode al een mooi rendement “behaald”, waarna een extra investering gevraagd wordt. Uiteindelijk blijken de investeringen of beleggingen waardeloos en bent u uw geld kwijt. Deze vorm van fraude komt veelal voor bij investeringen in cryptocurrency.

Wat kunt u doen?

- Doe onderzoek naar de partij waarmee u contact heeft.
- Veelal is het een Engelstalige medewerker (broker) maar ook Nederlandstalige frauders zijn

actief.

- Stop direct met verder investeren om het verlies te beperken. Informeer uw bank als uw rekeninggegevens bij de fraudeurs bekend zijn.
- Neem contact op met de toezichthouder (AFM). Zij kunnen onderzoek doen en waar nodig maatregelen treffen.
- Doe altijd aangifte bij de Politie.

Let op!

Wanneer u stopt met beleggen en dit kenbaar maakt kan het zijn dat advocaten of andere bedrijven u benaderen voor bemiddeling.

Dit zijn in alle gevallen (dezelfde) oplichters! (Recovery scam)



Phishing (e-mail, WhatsApp of sms)

U krijgt via e-mail, WhatsApp of sms een bericht van een crimineel die zich voordoet als vriend, familielid of medewerker van een organisatie. Het bericht ziet er betrouwbaar uit, maar via een link of bijlage in dat bericht kunt u opgelicht worden.

Voorbeeld van oplichting:

"Wij adviseren u zo spoedig mogelijk uw identiteit te verifiëren via deze link. Daarna kunt u weer direct gebruikmaken van uw creditcard."

"Hoi pap. Ik heb een nieuwe telefoon en kan daardoor nu niet internetbankieren. Maar ik moet vandaag echt iets betalen."

Wat kunt u doen?

- Klik nooit zomaar op een link en open nooit zomaar een bijlage.
- Deel nooit zomaar uw persoonlijke gegevens.
- Controleer de afzender van het bericht op echtheid.
- Probeer persoonlijk contact te maken. Let op: gebruik niet de contactgegevens in het bericht, maar bijvoorbeeld via het telefoonnummer dat bij u bekend is.



Phishing via een betaallink

U krijgt een betaalverzoek van een klein bedrag. Wanneer u op deze link klikt, proberen criminelen uw bankgegevens te bemachtigen. U kunt bijvoorbeeld via Marktplaats te maken krijgen met deze betaallinkfraude.

Voorbeeld van oplichting:

"Beste verkoper, ik ben onlangs opgelicht dus wil ik zeker weten dat ik u kan vertrouwen. Kunt u via deze betaallink eerst € 0,01 overmaken voordat ik u betaal?"

Wat kunt u doen?

- Maak nooit zomaar geld over.
- Doe bankzaken altijd via de eigen bankomgeving.
- Doe nooit betalingen via openbare wifinetwerken.

Tip!

Goede internetbeveiligings software kan helpen bij het ondervangen van phishing of infecties op computer, tablet of telefoon.



Hacken

Hackers zijn digitale inbrekers. Ze stelen informatie of bestanden van uw computer, zoals wachtwoorden, profielen op sociale media of gebruikersaccounts van bijvoorbeeld webwinkels. Afpersing of pesten kan ook een doel van hacken zijn. Maak het hackers oninteressant om u te hacken en ga verantwoord om met wat u digitaal bewaart en deelt.

Wat kunt u doen?

- Laat nooit zomaar uw gegevens, zoals bankrekeningnummers, een kopie van een identiteitskaart of creditcardgegevens achter op een website of in uw e-mailaccount.
- Gebruik sterke wachtwoorden, zoals een hele zin en wijzig deze regelmatig.
- Gebruik zoveel mogelijk verschillende wachtwoorden. Dit zodat bij een datalek de rest van de wachtwoorden wel veilig zijn.
- Deel uw wachtwoorden met niemand, ook niet met bekenden.
- Een wachtwoordmanager kan helpen bij het veilig onthouden van wachtwoorden.



Ransomware

Ransomware, ook bekend als gijzelsoftware, kan geïnstalleerd worden op uw computer nadat u op een link of bijlage hebt geklikt. U krijgt dan een bericht dat uw computer geblokkeerd is of uw bestanden versleuteld zijn. In ruil voor (digitaal) losgeld, bijvoorbeeld crypto/bitcoins, verwijdert de cybercrimineel soms (maar meestal niet eens) de kwaadaardige software.

Wat kunt u doen?

- Installeer een antivirusprogramma.
- Installeer altijd updates van software- en besturingssystemen.
- Maak regelmatig een back-up van uw bestanden en bewaar deze op een externe harde schijf.
- Open nooit zomaar linkjes en kijk naar de herkomst.

Tip!

Goede internetbeveiligings software kan helpen bij het ondervangen van hacking of het herkennen van ransomware op computer, tablet of telefoon.



Datingfraude

Datingfraudeurs maken via datingsites en andere social media platformen contact. Er wordt op geraffineerde wijze een “relatie” tot stand gebracht (fraudeurs blinken uit in het geven van aandacht). Foto’s van internet worden gekopieerd en gebruikt om de fake-identiteit mee op te bouwen (catfishing). Het slachtoffer wordt zo snel mogelijk naar andere contactkanalen geleid zoals Whatsapp.

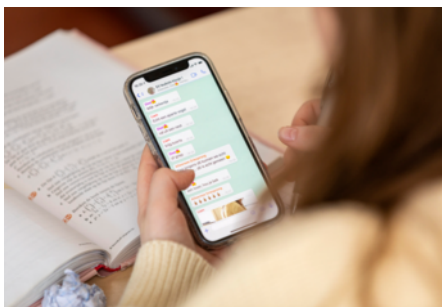
Vervolgens vraagt de oplichter zijn virtuele datingpartner met een smoes geldbedragen over te maken. Vaak wordt deze fraude uitgebreid in zogenaamde investeringsmogelijkheden, veilig stellen van erfenissen of financiële steun. Daarnaast kan het voorkomen dat het slachtoffer afgeperst wordt met pikante foto's (sextortion).

Wat kunt u doen?

- Probeer de identiteit te verifiëren of maak een fysieke afspraak met eventuele hulp.
- Videobellen of een kopie van een identiteitsbewijs kan gemanipuleerd zijn.
- Denk goed na welke informatie of foto's u deelt.
- Maak melding bij de datingsite om andere slachtoffers te behoeden.
- Beperk eventuele schade door contact te leggen met uw bank.

Tip!

Iemand kan zich anders voordoen. Zorg voor een fysieke ontmoeting. Deze vorm van fraude heeft ook de naam romance scam.



Sextortion

Sextortion is afpersing met een seksueel getinte foto of video van een slachtoffer. Het kan ook zijn dat (webcam)beelden van iemand zo gemonteerd worden dat het lijkt alsof het slachtoffer seks heeft met iemand, terwijl dit in werkelijkheid niet is geweest. Bijvoorbeeld seks met een minderjarige. Hiermee chanteren ze een slachtoffer en dreigen ze met het online zetten of verspreiden van deze beelden. Dit is allemaal strafbaar.

De afperser wil meestal geld of juist meer pikante foto's of video's van het slachtoffer. Vaak zijn de foto's en video's gestolen vanuit een cloud (online opslag), door het overnemen van een webcam (camera) of door gewoonweg via rondsturen. Een naaktfoto kan natuurlijk gestuurd worden naar iemand die in eerste aanleg vertrouwd lijkt. Het doorsturen van een naaktfoto of ander seksueel getint materiaal heeft de naam ; Sexting.

Wat kunt u doen?

- Denk goed na bij het delen van pikante foto's of video's.
- Wat is er op de foto of video te zien en wie krijgt ze te zien?

- Probeer de identiteit te achterhalen van de ontvanger, oplichter of afperser.
- Ga niet in op de bedreigingen of afpersingen. Bij betaling zal de afperser meer gaan vragen. Het is geen garantie dat de chantage stopt als jij doet wat er gevraagd wordt.
- Verzamel bewijs. Bewaar berichten en maak screenshots. Alles kan helpen bij een onderzoek.
- Verwijder en blokkeer de persoon zoveel mogelijk.
- Leg contact met de Politie.
- Komt u een foto of video online tegen? Neem dan zo snel mogelijk contact op met die site. Leg de website-eigenaar of beheerder duidelijk uit dat er geen toestemming is gegeven voor het plaatsen van de foto of video. Leg hiervoor eerst contact met de Politie. Dit zodat sporen eventueel tijdig veiliggesteld kunnen worden.

Wat denkt u?

Is de persoon met wie u praat daadwerkelijk wie hij/zij zegt te zijn?



(Cyber)Pesten

Cyberpesten is online pesten. Online pesten kent andere nadelen als klassiek pesten. Het is altijd beangstigend en vernederend voor het slachtoffer. Online kan de dader gemakkelijker anoniem werken. Het cyberpesten kan daarnaast 24/7 blijven doorgaan. Zeker bij een bereik van een grote groep pesters of meelopers. Pesten komt veelal voor bij jongeren, maar ook volwassenen worden slachtoffer van pesten.

Wanneer het pesten blijft doorgaan en steeds verdergaat, kan het strafbaar worden. Bijvoorbeeld als bij een bedreiging of fysiek geweld. Ook stalking, smaad en laster zijn strafbaar. Ook online! Meld het bij de Politie of doe aangifte. Hoe dan ook, praat erover met iemand die u vertrouwt.

Het posten van sexy foto's en filmpjes van een vriend(in) kan dan strafbaar zijn. Als hij of zij onder de achttien is, wordt dit gezien als (het maken en) verspreiden van kinderporno.

Wat kunt u doen?

- Neem iemand in vertrouwen en maak de situatie kenbaar.
- Blokkeer accounts of telefoonnummers.
- Maak melding bij school, werkgever of andere instanties.

Een hulpvraag doen roept een gevoel van mislukking of schaamte op. Door er over te praten kunnen we zorgen voor de juiste hulp.



Doxing

Doxing is kortweg het met kwade bedoelingen verzamelen of (verder) verspreiden van privé-informatie zoals woonadres, telefoonnummer, een foto, paspoort, naam werkgever en gegevens van familie of combinaties. Doxing kan o.a. een gevolg zijn van pesten, sexting of ander incident wat heeft plaatsgevonden.

Doxing speelt zich vooral online af en via sociale media en heeft het oogmerk iemand vrees aan te (laten) jagen, ernstige overlast aan te (laten) doen of ernstig te (laten) hinderen in de uitoefening van zijn ambt of ander beroep.

Deze gedragingen kunnen een enorme inbreuk hebben op de persoonlijke levenssfeer van slachtoffers en hun sociale omgeving. Doxing kan

omvangrijke vormen aannemen en ontwikkelt zich soms tot mediastormen en online heksenjachten. Doxing is per definitie persoonlijk van aard en kan een sterk ontregelend effect op de privésituatie van het slachtoffer en zijn/haar omgeving hebben.

Wat kunt u doen?

- Maak melding bij de Politie, school, werkgever of andere instantie.
- Maak het bespreekbaar in uw privéomgeving.
- Vraag het platform om het bericht offline te halen.

Tip!

Wat deelt u online en wat heeft u allemaal openbaar staan?



Gaming

Jong en oud vinden gamen leuk. Gamen biedt voor jongeren veel mogelijkheden om zich zelfstandig en zelfverzekerd te voelen. Ze merken dat ze beter worden en meer bereiken in de game.

Zo kent deze wereld ook enkele gevaren. De meeste games zijn online en hebben in-game-aankopen. Spelers kunnen dan voor echt geld, in het spel spullen kopen waardoor ze iets unieks, beters of mooiers kunnen krijgen. Hiermee kunnen ze zich onderscheiden van anderen. Daarnaast is het bij veel online games mogelijk om (anoniem) te chatten. Dit gaat tegenwoordig met VoIP (Voice over Internet Protocol).

Wat kunt u doen?

- Weet wat jongeren online doen, kijk soms mee en vraag eens met wie ze chatten/praten.
- Spreek duidelijke game tijden af om verslaving te voorkomen of beperken.
- Weet dat bepaalde games agressie opwekken.
- Deel nooit persoonsgegevens, foto's of social media accounts met andere gamers. Zij kunnen kwade bedoelingen hebben.



Social Media

Ongeveer 85% van de Nederlanders zit op social media. Ieder platform richt zich op een bepaalde doelgroep. Het algoritme zorgt ervoor dat u content te zien krijgt waar u (mogelijk) interesse in heeft. Onder jongeren kan social media gebruik zorgen voor een niet realistisch beeld van de werkelijkheid en het nastreven van perfectie. Dit kan zorgen voor een laag zelfbeeld of verslaving.

Ook criminelen zijn te vinden op de socials. Social media platformen worden gebruikt als wervingspagina voor bijvoorbeeld geldezels en slachtoffers van sextortion. Maar ook malafide verkoopadvertenties worden op social media aangeboden.

"Het is belangrijk om social media en gaming gevaren te kennen en herkennen. Praat erover. Verbieden is niet altijd de oplossing!"

Hulp en informatie

Spoed 112

voor doven en slechthorenden
0800 – 8112

Geen spoed, wel politie 0900 – 8844

voor doven en slechthorenden
0900 – 1844

Informatie en aangifte 0900 – 8844

voor doven en slechthorenden
0900 – 1844

Opsporingstiplijn 0800 – 6070

Meld Misdaad Anoniem 0800 – 7000

geen onderdeel van de politie

politie.nl

Sociale media

