Dirkjan van Ittersum

De online fraude Survivalgids

Consumentenbond

1e druk, april 2022

Inlichtingen: Consumentenbond

Auteur: Dirkjan van Ittersum
Eindredactie: Dieneke Hengeveld
Verder werkten mee: Vincent van Amerongen, Ronald Kamp
Grafische verzorging: PUUR Publishers
Beeld omslag: PUUR Publishers
ISBN 978 905951 5055
NUR 988

Inhoud

Inleiding 9

1 Cybercriminaliteit 11
1.1 Toename 12
1.1a Slachtoffers 12
1.1b Schade bij banken 13
1.1c Coronacrisis 14
1.2 Steeds nieuwe vormen 15
1.3 Datalekken 17
1.4 Zo werkt en denkt de cybercrimineel 18
1.4a Motieven 18
1.4b Technische hulpmiddelen 19
1.4c Aanvalsmethoden 20
1.4d Verleidingstactieken 22
1.4e Doorpakken 23
1.5 Aanvallen voorkomen 25
1.5a Alert blijven 25
1.5b Technische maatregelen 26

2 Nepberichten en telefonische oplichting 27
2.1 Phishing 29
2.1a Link klopt niet 30
2.1b Onjuiste afzender 31
2.1c Valse QR-code 32
2.1d Onpersoonlijke aanhef 32
2.1e Urgentie en dreiging 33
2.1f Onrealistische belofte 34
2.1g Taalfouten 35
2.1h E-mail met bijlage 35
2.2 Spear phishing 35
2.3 Vriend-in-noodfraude 36
2.4 Frauduleuze telefoontjes 37
2.4a Bekende neptelefoontjes 37
2.4b Meekijksoftware 38
2.4c Nieuwe neptelefoontjes 38
2.4d Spoofing 40
2.4e Terugbelfraude 40
2.5 Winacties 42

3 Malafide transacties 43
3.1 Marktplaatsfraude 44
3.1a Herken de nepadvertentie 44
3.1b Verdachte handelaren 45
3.1c Contact en betaling 46
3.1d Maatregelen van Marktplaats 48
3.2 Valse betaalverzoeken 50
3.2a 1-cent betaalverzoeken 50
3.2b Nepbetaalverzoek 51
3.2c Nepwebsite voor verzendlabel 52
3.2d Neplinks herkennen 53
3.3 Nepshops 55
3.3a Nepshop herkennen 56
3.3b Online reviews 58
3.4 Crypto- en beleggingsfraude 58
3.4a Cryptofraude 59
3.4b Beleggingsfraude 60
3.5 Ticketfraude 61
3.6 Kwaadaardige apps 62
3.6a Malware 62
3.6b Fleeceware 63
3.7 Voorschotfraude 64

4 Overige fraude 65
4.1 Datingfraude 66
4.1a Foto controleren 67
4.2 Chantage 71
4.2a Sextortion 71
4.2b Dreigmails 71
4.3 Malware 72
4.3a Ransomware 72
4.3b Bankmalware 74
4.3c Cryptojacking 74
4.3d Scareware 75
4.3e Spyware 75
4.3f Adware 75
4.4 Identiteitsfraude 76
4.4a Zo herken je identiteitsfraude 77
4.4b Wanneer een identiteitsbewijs? 78
4.4c Een veilige kopie 78
4.4d Zo komen ze aan je identiteitsbewijs 79
4.5 Inzet als geldezel 79
4.6 Misbruik bedrijfsnaam 80
4.7 Spookfacturen 80

5 Apparatuur beveiligen 81
5.1 Updates installeren 82
5.1a Windows 82
5.1b MacOS 88
5.1c Android 89
5.1d iOS 91
5.2 Veilige wifiverbinding 93
5.2a Wifi beveiligen 93
5.2b Wifi onderweg 98
5.3 Scannen op malware 104
5.3a Symptomen 104
5.3b Scannen 104
5.3c Welke virusscanner? 105
5.3d Veilig downloaden op de computer 106
5.3e Veilig downloaden op smartphone en tablet 108
5.3f Gebruik een spamfilter 110
5.4 Veilige systeeminstellingen 110
5.4a Windows 110
5.4b MacOS 119
5.4c Android 121
5.4d iOS 123
5.5 Apparaten versleutelen 123
5.5a Windows 123
5.5b MacOS 125
5.5c Android 126
5.5d iOS 127
5.6 Back-up maken 127
5.6a Computer 128
5.6b Smartphone en tablet 131

6 Accounts beveiligen 133
6.1 Wachtwoord kiezen 134
6.1a Eisen aan een goed wachtwoord 134
6.1b Wachtwoorden onthouden 135
6.2 Tweestapsverificatie 136
6.2a Apple 136
6.2b Facebook 138
6.2c Google 139
6.2e PayPal 143
6.2f Twitter 144
6.2g WhatsApp 146
6.3 Wachtwoordmanager 147
6.3a Bitwarden 147
6.3b iCloud sleutelhanger 151
6.4 Online accounts beveiligen 152

6.4a Apple ID 152
6.4b Facebook 152
6.4c Google 153
6.4d Microsoft 155
6.4e Twitter 156
6.5 Online accounts verwijderen 157
6.5a Apple ID 157
6.5b Facebook 157
6.5c Google 158
6.5d Microsoft 158
6.5e Twitter 159
6.6 Bank-apps veilig instellen 160

7 Opgelicht! Wat nu? 161
7.1 Is het mis? 162
7.1a Op een phishinglink geklikt 162
7.1b Geld belegd of in crypto gestoken 162
7.1c Geld betaald aan (droom)prins 162
7.1d BSN doorgegeven 163
7.1e 1 cent overgemaakt 163
7.1f Vriend in nood geholpen 163
7.1g Bestelling gedaan bij nepshop 163
7.1h Bankgegevens uit handen gegeven 164
7.1i Malware gedownload 164
7.2 Neem direct maatregelen 167
7.3 Contact met de bank 168
7.3a Spoofing 168
7.3b Klacht indienen 169
7.3c Oplichter achterhalen 169
7.4 Melding maken 170
7.4a Beleggingsfraude melden 170
7.4b Nepshop melden 170
7.4c Identiteitsfraude melden 170
7.4d Vals sociale-media-account melden 171
7.4e Nepbestellingen en -contracten melden 171
7.4f Phishing en smishing melden 171

Register 172

Inleiding

In 2021 kwamen 2,5 miljoen Nederlanders in aanraking met online criminaliteit. Dat blijkt uit de cijfers van het Centraal Bureau voor de Statistiek (CBS).
Er is sprake van een trend: cybercriminelen maken de laatste jaren steeds meer slachtoffers. Tegelijk neemt de 'traditionele' criminaliteit af. Minder woninginbraak en diefstal dus, maar vaker identiteitsfraude, phishing, hacken en oplichting bij aan- of verkoop. Slachtoffers van online fraude zijn vaak grote bedragen kwijt.
Dit boek beschrijft hoe cybercriminelen te werk gaan en hoe je je tegen hen kunt wapenen. Deels ligt de oplossing in techniek: door een goede virusscanner te installeren, kun je al veel leed voorkomen. Maar minstens zo belangrijk is het om te doorzien welke tactieken oplichters hanteren. Cybercriminelen kunnen zeer overtuigende verhalen ophangen, waardoor zelfs een doorgewinterde IT'er het schip in kan gaan.

In hoofdstuk 1 leggen we uit hoe die tactieken van cybercriminelen eruit zien. Door de werkwijze van oplichters te herkennen, trap je minder snel in hun mooie verhalen. De hoofdstukken 2, 3 en 4 zijn gewijd aan de verschillende vormen van fraude. Om te beginnen vertellen we in hoofdstuk 2 welke trends er zijn bij phishing en telefonische oplichting. Criminelen gaan daarbij steeds brutaler te werk. Naast nepberichten, is telefonische oplichting aan de orde van de dag. De oplichters gaan zelfs zo ver dat ze een eerder slachtoffer nog eens opbellen, ditmaal namens 'de politie' om de kwestie 'op te lossen'. Weer volgt een geloofwaardig verhaal en weer maken ze geld buit.
Hoofdstuk 3 behandelt allerhande malafide transacties, ofwel oplichting tijdens aan- en verkopen. Marktplaatsfraude komt nog altijd regelmatig voor. Het zorgt voor veel schade. Met onze tips en adviezen leer je de trucs van een foute koper of verkoper te doorzien. In het vierde hoofdstuk zetten we alle overige fraudevormen op een rij, waaronder datingfraude, identiteitsfraude en malware.

Je kunt niet alle vormen van fraude met technische middelen voorkomen, maar het zo veilig mogelijk instellen van je apparatuur helpt wel. Zorg voor een goede virusscanner, installeer updates, maak back-ups en kies de juiste veiligheidsinstellingen voor al je apparaten. In hoofdstuk 5 lopen we het allemaal langs.
In hoofdstuk 6 behandelen we de accounts die je hebt, bijvoorbeeld bij Google, Facebook of WhatsApp. Ook die moet je veilig instellen om digitale inbraken te

voorkomen. Zo is tweestapsverificatie een belangrijke eerste verdedigingslinie. We leggen uit wat dat precies is en hoe je het instelt voor allerlei applicaties. In het laatste hoofdstuk lees je wat je kunt doen als het toch is misgegaan. Welke stappen moet je nemen om te voorkomen dat de schade (nog) groter wordt? Welke middelen staan je ter beschikking om de buit terug te halen? Ook vertellen we waar je online fraude kunt melden.

Met de praktische informatie, tips en stappenplannen in dit boek kun je je wapenen tegen online oplichting via pc, tablet en smartphone en daarmee het risico erop flink verminderen.

Gebruikte systeemversies

Dit boek bevat veel stappenplannen voor pc, smartphone en tablet, inclusief schermafbeeldingen. Er zijn afbeeldingen voor zowel Windows 10 als 11. We hebben de nieuwste versies van MacOS en iOS gebruikt. Voor Android zijn de schermafbeeldingen gemaakt met een Samsung-telefoon met Android 12, de meeste actuele versie bij het verschijnen van deze uitgave.

Foto : Michel Walraven

Dirkjan van Ittersum is IT-journalist en auteur van computerboeken. Hij verkent enthousiast de mogelijkheden van nieuwe technologie en geeft er graag uitleg over.

1

Cybercriminaliteit

Vrijwel dagelijks staan er berichten in de media over cybercriminaliteit. Het aantal aanvallen door cybercriminelen stijgt nog altijd. We bespreken de actuele trends en laten we zien welke methoden cybercriminelen gebruiken om slachtoffers te maken.

1.1 Toename

In Nederland kan iedereen bij de Fraudehelpdesk melding te maken van cybercriminaliteit. En dat gebeurt veelvuldig. In 2021 kwamen er 530.000 meldingen binnen, goed voor €47 miljoen aan schade. Een jaar eerder deden 350.000 personen een melding. Het schadebedrag was toen €41 miljoen. Vooral fraude bij online (ver)kopen viel in 2021 op. Het aantal meldingen daarvan steeg met 25%. Beleggingsfraude kwam ook veel voor. Het bijbehorende schadebedrag van €19,5 miljoen is ronduit schrikbarend, een stijging van 45% ten opzichte van 2020. Uit cijfers van de Fraudehelpdesk blijkt verder dat criminelen hun slachtoffers steeds vaker persoonlijk opbellen, bijvoorbeeld uit naam van de bank (zie par. 2.4). Een trend die sinds eind 2021 in opkomst is, zijn de geautomatiseerde telefoontjes. Deze zijn zogenaamd afkomstig van de politie of de 'Hoge Raad der Nederlanden'. Met deze neptelefoontjes proberen criminelen onder meer burgerservicenummers (BSN's) te achterhalen of je computer over te nemen.

Online fraude in cijfers

Dit was in 2021 de top drie van *fraudevormen*:

1. **Cybercrime: hacken, phishing, computervredebreuk en malware**
2. **Identiteitsfraude: met name WhatsApp-hulpvragen**
3. **Handelsplaats- en webwinkelfraude**

Het meeste *financiële leed* veroorzaakten deze drie fraudevormen:

1. **Handelsplaats- en webwinkelfraude (zie hoofdstuk 3)**
2. **Identiteitsfraude (zie par. 4.4)**
3. **Voorschotfraude (zie par. 3.7)**

De *hoogste schadebedragen* waren er bij onderstaande fraudevormen:

1. **Beleggingsfraude €19,5 miljoen**
2. **Voorschotfraude €10 miljoen: met name datingfraude (ruim €7 miljoen)**
3. **Identiteitsfraude rechtspersonen €7,2 miljoen: waarvan nep-banktelefoontjes €5,1 miljoen**
4. **Identiteitsfraude natuurlijke personen €3,2 miljoen: waarvan WhatsAppfraude bijna €2,5 miljoen**

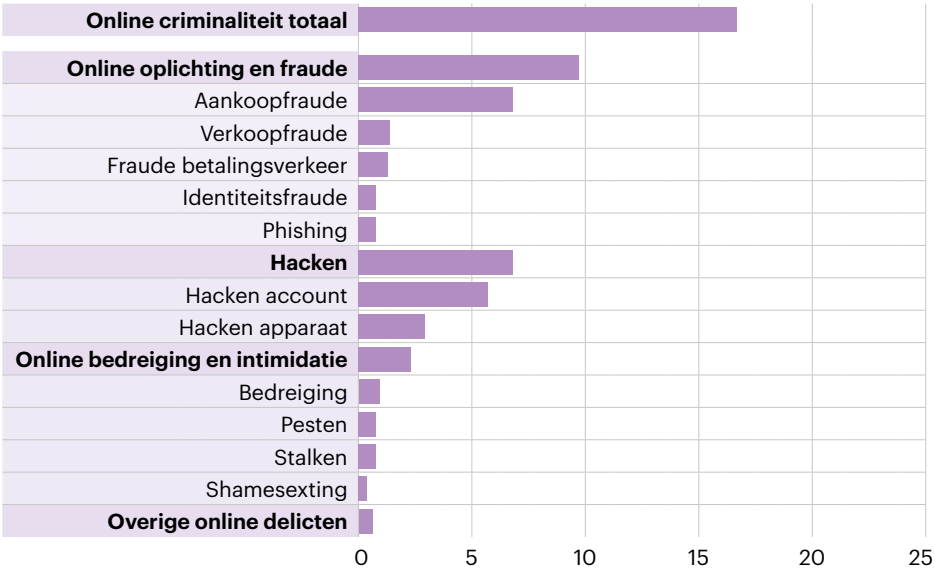
Bron: Fraudehelpdesk, cijfers 2021

1.1a Slachtoffers

Het CBS doet jaarlijks een eigen onderzoek naar het totaal aantal slachtoffers van online criminaliteit (dus niet op basis van meldingen, zoals bij de Fraudehelpdesk).

Daaruit blijkt dat afgelopen jaar 17% (ofwel 2,5 miljoen) van alle Nederlanders met cybercriminelen te maken kreeg. In de grafiek is te zien welke vormen van online criminaliteit het CBS vaak signaleert.

Slachtoffers online criminaliteit 2021



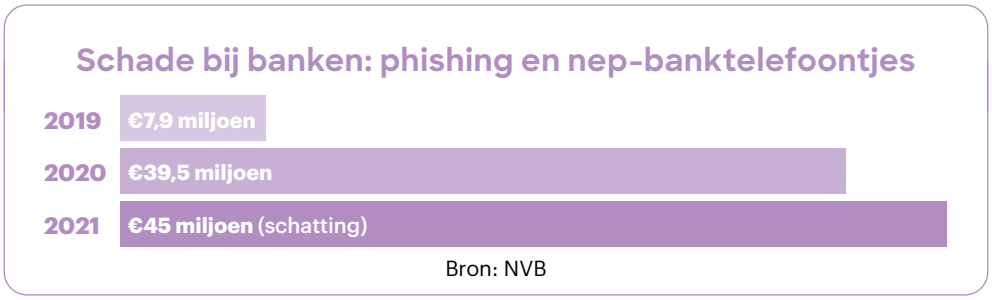
Bron: CBS

1.1b Schade bij banken

Ook de Nederlandse banken, verenigd in de Nederlandse Vereniging van Banken (NVB) registreren hoeveel schade cybercriminelen veroorzaken. De NVB becijferde dat het schadebedrag in de eerste helft van 2021 uitkwam op €22,5 miljoen. Het gaat hier om schade als gevolg van phishing (€6,1 miljoen, zie par. 2.1) en nep-banktelefoontjes (€16,5 miljoen, zie par. 2.4). Ter vergelijking: de schade was in geheel 2020 €39,5 miljoen. Cijfers over geheel 2021 ontbreken bij het ter perse gaan van dit boek.

De NVB noemt de hoogte van dit bedrag zorgwekkend. De organisatie pleit voor een gezamenlijke aanpak om het probleem te lijf te gaan. Daarbij zouden onder andere overheden, internet- en telecomproviders, big-techbedrijven, handelsplatformen en de politie betrokken moeten zijn.

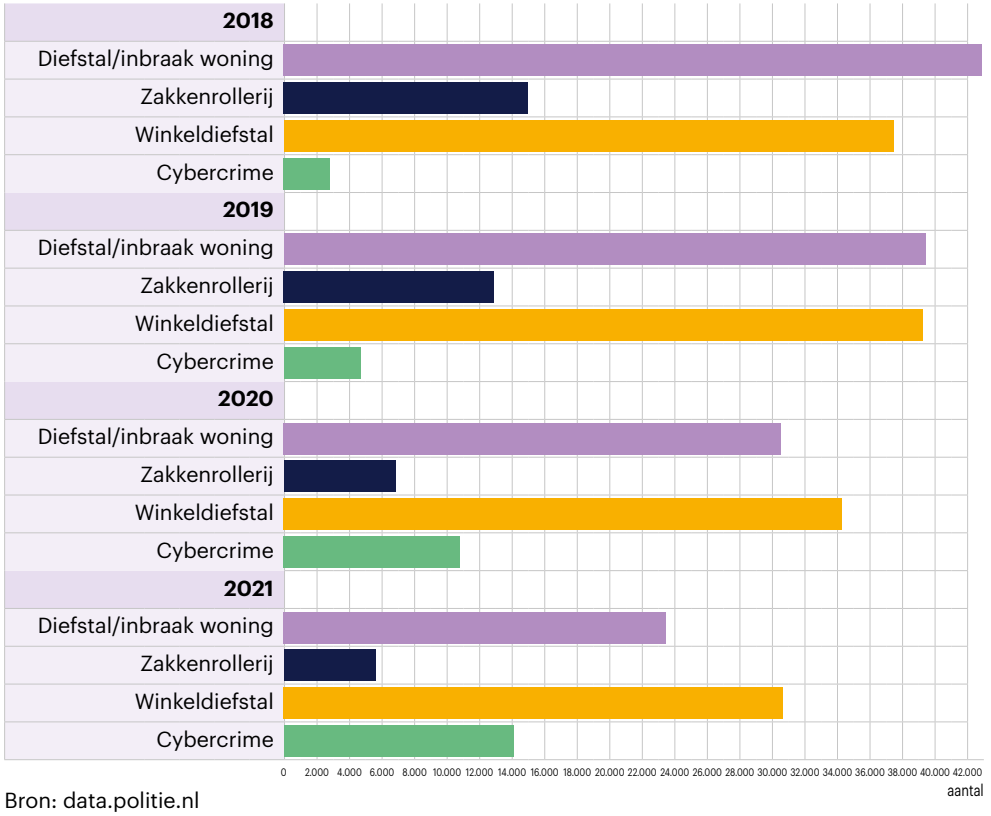
Banken hebben al maatregelen genomen om schade door cybercriminaliteit te voorkomen. Zo is sinds enige tijd de IBAN-Naam Check ingevoerd, waarbij banken controleren of naam en rekeningnummer overeenkomen. Ook is er de gelijk-oversteken-service bij online handelsplaatsen (zie par. 3.1) en zijn er mogelijkheden bij gekomen om banklimieten en tweestapsverificatie in te stellen (zie par. 6.2).



1.1c Coronacrisis

Als gevolg van de coronacrisis is er een verschuiving te zien in criminaliteit. Het aantal woninginbraken en winkeldiefstallen nam de afgelopen twee jaar af. In plaats daarvan richten criminelen zich meer op online fraude. De politie registreerde in 2021 14.000 gevallen van cybercriminaliteit, dat is zo'n 33% meer dan in 2020 en zelfs drie keer meer dan in 2019. Het aantal aangiften van woninginbraken en winkeldiefstallen nam af, maar is in absolute zin nog wel groter dan van cybercriminaliteit.

Gerigistreerde misdrijven en aangiften in Nederland 2018-2021



Bron: data.politie.nl

Op een andere manier heeft corona ook invloed op cybercriminaliteit. Oplichters misbruiken de angst voor corona. Zo zijn er sinds het begin van de coronacrisis nepmails in omloop die zogenaamd afkomstig zijn van het RIVM. Een bijlage zou belangrijke informatie bevatten over het virus. Als je de bijlage opent, kan de pc besmet raken met ransomware (zie par. 4.3a).
Ook bij phishing grijpen criminelen de coronacrisis aan (zie par. 2.1). Er gingen bijvoorbeeld e-mails en sms'jes rond die zogenaamd door de bank waren verstuurd. De berichten verwezen naar een formulier waarmee je een antibacteriële bankpas zou kunnen aanvragen. Ook verstuurden boeven berichten over onder meer vaccinatie-afspraken en de aanvraag voor coronasubsidie. Wie inging op deze berichten kreeg te maken met malware of kon het slachtoffer worden van digitale inbraak of identiteitsfraude.

Rabobank

Rabobank introduceert antibacteriële betaalpas

Beste klant/relatie,

Het coronavirus raakt inmiddels meer dan alleen onze gezondheid. De WHO spreekt over een pandemie en Corona raakt de wereldeconomie. De situatie brengt onzekerheid met zich mee en vanzelfsprekend maken we ons zorgen over wat er kan gebeuren. Het stelt u en onze medewerkers bloot aan nieuwe uitdagingen en dilemma's, die we zo goed als mogelijk en met elkaar het hoofd moeten bieden.

Het belangrijkste blijft uw en onze gezondheid. Als bank hebben we bovendien de verantwoordelijkheid om ervoor te zorgen dat u gebruik kunt blijven maken van onze dienstverlening. Dat u in de winkel uw boodschappen kunt afrekenen, mobiel kunt blijven bankieren en gebruik kunt blijven maken van een Rabo Betaalverzoek.

Om dit te kunnen blijven garanderen, hebben wij voorzorgsmaatregelen getroffen en is onze dienstverlening aangepast aan de nieuwe situatie. Een situatie die met het huidige verloop van het virus nog in beweging is. Rabobank volgt daarbij richtlijnen van het RIVM en de overheid. Daarbij staan de gezondheid en veiligheid van u en onze medewerkers voorop. We dragen bij om verdere verspreiding van het coronavirus zoveel als mogelijk tegen te gaan.

Hierbij introduceert de Rabobank antibacteriële betaalpas.U heeft tot 19 maart 2020 de gelegenheid om kosteloos deze betaalpas aan te vragen.

Na de genoemde datum brengen wij €44,99 kosten in rekening per nieuwe aanvraag.

De nieuwe betaalpas ontvangt u binnen 3 werkdagen per post.

Klik hier om uw nieuwe betaalpas kosteloos aan te vragen tot 19 maart 2020.

Tot slot: dat mensen steeds meer thuis werken sinds het begin van de coronacrisis zien criminelen als een kans. Ze vissen via e-mails, die zogenaamd afkomstig zijn van 'de directie', naar toegang tot het bedrijfsnetwerk. In de mails staat vaak een link naar een nagemaakte Microsoft- of Outlook-website.

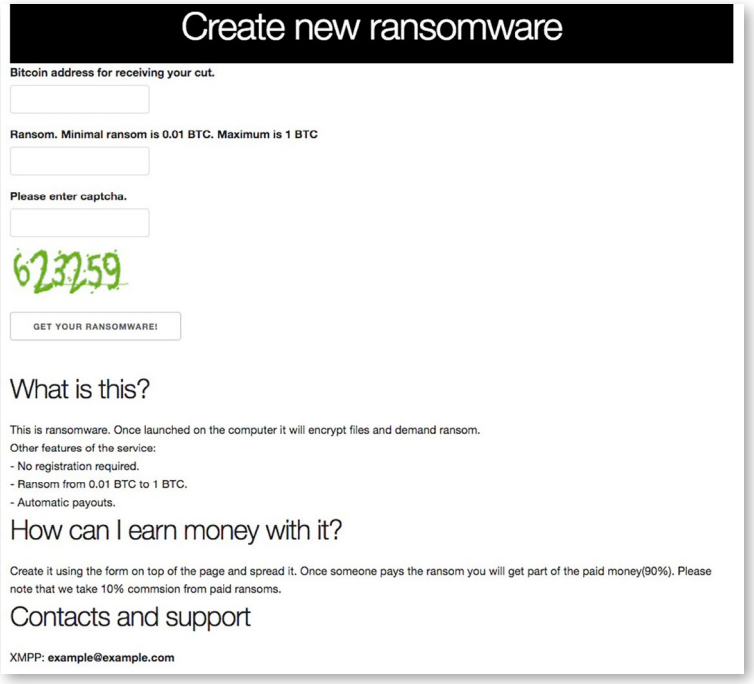
1.2 Steeds nieuwe vormen

Cybercriminelen vinden steeds nieuwe manieren om slachtoffers maken. In dit boek passeren diverse voorbeelden de revue. Bedenk dat er bijna dagelijks nieuwe varianten ontstaan. Criminelen zijn continu op zoek naar mogelijkheden om mensen op te lichten.
In veel gevallen gaat het om al langer bestaande fraude in een nieuw jasje. Een voorbeeld is zogeheten *spear phishing* (zie par. 2.2). Dit is een geavanceerde vorm van het aloude phishing (zie par. 2.1). Bij spear phishing kiest de crimineel zeer gericht een slachtoffer na onderzoek op bijvoorbeeld sociale media. Door de aanval goed voor te bereiden is de kans dat de opzet slaagt een stuk groter.
Wat ook opvalt is dat cybercriminelen hun werkterrein steeds verder uitbreiden.

Niet langer richten ze zich op uitsluitend computers en laptops. Ze richten het vizier ook op smartphones, tablets en smarthome-apparatuur (zoals 'slimme' verlichting of beveiligingscamera's). Zelfs de auto – steeds vaker voorzien van een draadloze verbinding – is niet veilig voor cybercriminelen.
Een recent fenomeen is dat slachtoffers tweemaal ten prooi vallen aan dezelfde groep oplichters. Nadat het slachtoffer bijvoorbeeld in de val is getrapt van een vals WhatsApp-bericht, belt een vriendelijke 'medewerker van de bank' op. De behulpzame stem legt uit dat er fraude is geconstateerd. Tijdens het gesprek wordt het slachtoffer er opnieuw van overtuigd geld over te maken naar een – zo zal later blijken – criminele rekening.

Ransomware via het dark web

Dat de online criminaliteit uitsluitend het werk is van getalenteerde (maar kwaadaardige) IT'ers is een fabeltje. Ook criminelen zonder IT-diploma kunnen een aanval opzetten. Goed verborgen op internet zijn er illegale marktplaatsen waar ransomware, DDOS-aanvallen of kraakprogramma's te koop zijn. De prijzen vallen mee. Op het zogeheten dark web koop je voor een paar honderd euro al ransomware.

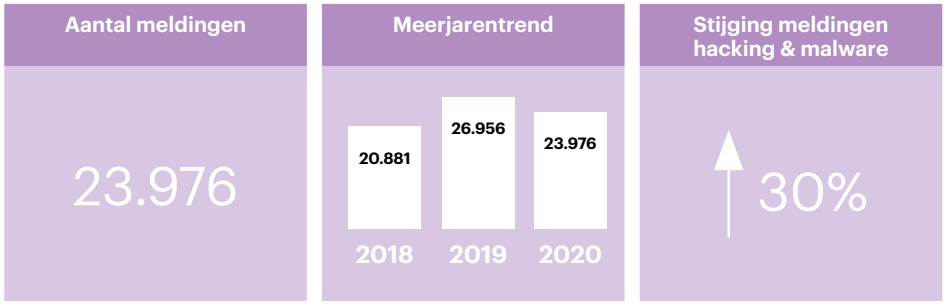


Bron: mcafee.com

1.3 Datalekken

Een aanhoudend probleem vormen datalekken bij bedrijven en organisaties. Regelmatig blijken gegevens niet goed beschermd, waardoor ze in verkeerde handen vallen. In 2020 ontving de Autoriteit Persoonsgegevens (AP) 23.976 meldingen van datalekken. Dat is 11% minder dan in 2019. Deze daling is het gevolg van het feit dat incassobureaus minder datalekken hebben gemeld. Zij hebben hun werkwijze aangepast, waardoor minder betalingsherinneringen bij verkeerde ontvangers terechtgekomen.
Het aantal meldingen naar aanleiding van hacking, malware of phishing-incidenten is gestegen met 30% vergeleken met 2019. In Nederland zijn bedrijven verplicht om een datalek te melden bij de AP.

Meldplicht datalekken: feiten en cijfers 2020



Bron: autoriteitpersoonsgegevens.nl

Als gevolg van datalekken zijn persoonsgegevens van miljoenen Nederlanders in omloop. Het gaat meestal om contact- en inloggegevens, maar soms ook om gevoeligere data. Uit een schatting door de Consumentenbond blijkt dat van ongeveer de helft van alle Nederlanders wel eens een wachtwoord is gelekt. Een deel van de gegevens is te koop op illegale marktplaatsen.
We spreken van een datalek als er onbedoeld persoonsgegevens zijn gedeeld, verloren, gewijzigd of vernietigd. Daar kunnen allerlei oorzaken voor zijn, bijvoorbeeld slechte beveiliging, menselijke fouten of (digitale) inbraak. Bedenk dat als er sprake is van een incident, het niet altijd zeker is dat gegevens zijn gelekt naar derden. Of dat is gebeurd, is vaak niet te achterhalen.
De gevolgen van een datalek kunnen verstrekkend zijn. De precieze gevaren hangen af van welke gegevens zijn gelekt en of ze gecombineerd kunnen worden met informatie uit andere lekken.
De belangrijkste gevaren na een datalek zijn:

- *Identiteitsfraude*: met gestolen persoonsgegevens kunnen criminelen een andere identiteit aannemen. Ze kunnen zich online uitgeven voor iemand anders of contracten afsluiten op andermans naam (zie par. 4.4).

- *Oplichting*: criminelen gebruiken persoonlijke informatie bij oplichtingspraktijken. Een slachtoffer gaat bijvoorbeeld sneller mee met een babbeltruc. Een voorbeeld is een nep-bankmedewerker die je burgerservicenummer (BSN) of bankrekeningnummer weet (zei par. 2.4).
- *Phishing*: criminelen gebruiken buitgemaakte gegevens bij het versturen van nepberichten. De informatie helpt ze de berichten gerichter en persoonlijker te maken. Denk aan een juiste aanhef of een correct kenteken bij een nepboete. Zo lijken ze geloofwaardiger (zie par. 2.1).
- *Hacks*: als je hetzelfde wachtwoord voor meer accounts, lopen die allemaal gevaar bij een hack. Met gelekte wachtwoorden kunnen criminelen bijvoorbeeld bestellingen doen op jouw naam of (crypto)valuta stelen. Soms lukt het criminelen om je telefoonnummer te kapen (*sim-swapping*). In dat geval lopen zelfs via sms beveiligde accounts gevaar.
- *Diefstal en inbraak*: kunnen criminelen bepaalde zaken koppelen aan je adres dan loop je een verhoogd risico op diefstal van je eigendommen. Denk aan bijvoorbeeld je auto als dat een gewild merk en type is.

Het is lastig om jezelf te wapenen tegen datalekken. Wie het internet opgaat, accepteert een zeker risico. Je kunt de gevaren wel verkleinen, bijvoorbeeld door zo min mogelijk accounts aan te houden, voorzichtig te zijn met wat je online plaatst en apparatuur goed te beveiligen. In dit boek gaan we uitgebreid in op al deze onderwerpen.

1.4 Zo werkt en denkt de cybercrimineel

Hoe gaan cybercriminelen te werk? Door oplichtingstrucs te doorgronden is de kans groter dat je ze ontwijkt.
Vrijwel iedereen kent de mailtjes, sms'jes of WhatsApp-berichten waarin criminelen hengelen naar geld of persoonlijke gegevens. Ook aanvallen met malware zijn bekend (zie par. 4.3). Vaak gaat het om ransomware, kwaadaardige software die persoonlijke bestanden in gijzeling neemt. In hun pogingen mensen op te lichten, kiezen criminelen steeds vaker een persoonlijke aanpak: ze bellen mensen brutaalweg op of ze versturen zeer gerichte mailtjes. Meer dan ooit is het belangrijk om je bewust te zijn van de gevaren.

1.4a Motieven

De achterliggende motieven van online criminelen zullen niemand verrassen.

- In de meeste gevallen zijn ze uit op je *geld of bezittingen*. Door bijvoorbeeld in te breken op je bankaccount, maken de criminelen geld buit. Of ze halen je per WhatsApp over om geld over te maken.
- In sommige gevallen is *reputatieschade* het doel: de crimineel wil schadelijke

informatie naar buiten brengen. Dit kan gekoppeld zijn aan geldelijk gewin. In dat geval kan het slachtoffer tegen betaling de reputatieschade voorkomen.
- Online criminaliteit kent nog een ander gezicht in de vorm van *bedrijfsspionage*. Hackers zijn uit op concurrentiegevoelige informatie. Dat lijkt niet relevant voor consumenten, maar het vele thuiswerken brengt nieuwe risico's met zich mee. De thuiscomputer kan toegang geven tot geheime bedrijfsinformatie.
- Een minder gekend gevaar zijn *hackers die werken voor buitenlandse overheden*. Zij zijn uit op gevoelige informatie van andere overheden of bedrijven. Of ze proberen met hun aanvallen tweespalt te zaaien in rivaliserende landen. Ook hier kan de thuiscomputer een toegangspoort zijn naar IT-systemen.
- Tot slot noemen we de '*hacktivisten*'. Dit zijn (meestal groepen) hackers met een activistisch doel. Ze willen een maatschappelijk probleem op de kaart zetten of politieke tegenstanders in een kwaad daglicht stellen. Ze breken – soms via de thuiscomputer van een medewerker – in bij bedrijven en overheden om bewijsmateriaal te verzamelen.

1.4b Technische hulpmiddelen

Cybercriminelen hebben een breed scala aan hulpmiddelen ter beschikking om slachtoffers te maken. In par. 1.2 stipten we het al aan: er is tegenwoordig weinig technische kennis nodig om online criminele activiteiten te ontplooien. Via illegale marktplaatsen is een ransomware-, DDOS- of phishingaanval zo gekocht.
Niet iedere cybercrimineel koopt kant-en-klare software. Er bestaan groepen hackers – vaak professioneel georganiseerd – die zelf technologie ontwikkelen. Er is sprake van een heuse industrie rondom online oplichtingsactiviteiten. Criminelen die zich ermee bezighouden, vinden elkaar online op afgeschermde plekken waar ze kennis en software met elkaar uitwisselen.
Andere fraudeurs zijn meer gelegenheidsdieven. Ze zien mogelijkheden om een internetdienst, app of software te misbruiken en slaan daar een slaatje uit. Denk aan criminelen die zich bezighouden met Tikkie- of Marktplaatsfraude (zie par. 3.1).

Professionalisering

In de afgelopen jaren is er sprake van een professionaliseringsslag onder cybercriminelen. Phishingmails met krakkemikkig taalgebruik komen nog wel voor, maar steeds vaker zijn het e-mails in perfect Nederlands. De aanvallen zijn zo perfect opgezet, dat zelfs een deskundige ze nauwelijks nog doorziet. Ook ransomware-aanvallen zijn steeds professioneler. Wie besluit losgeld te betalen om gegijzelde bestanden terug te krijgen, wordt vaak keurig te woord gestaan door de 'klantenservice'.