DIRKJAN VAN ITTERSUM

ONLINE VEILIGHEID

oprecht consumentenbond

1e druk, mei 2018

Auteur: Dirkjan van Ittersum
Verder werkten mee: Ronald Kamp, Peter Kulche en
Yvo Verschoor (Consumentenbond)
Eindredactie: Carlijn Brouwer (Mediaeval Tekst en Vorm)
Grafische verzorging: PUUR Publishers, Utrecht
Beeld omslag: PUUR Publishers, Utrecht

ISBN 978 905951 4157
NUR 988

INHOUD

INLEIDING

Internet biedt veel voordelen. Dat er ook gevaren zijn, bleef lange tijd onderbelicht. Zelfs vandaag de dag is veilig gebruik van internet niet vanzelfsprekend. Onderzoek door de Consumentenbond toont aan dat 123456, welkom en wachtwoord (!) nog altijd tot de populairste wachtwoorden behoren. Allerminst veilig dus!

Gelukkig raken steeds meer mensen doordrongen van het feit dat internet niet alleen maar gemak biedt. Kranten stonden afgelopen tijd bol van berichten over digitale inbraken en veiligheidslekken. Wie denkt dat er bij hem niets te halen valt, komt bedrogen uit. Iedereen kan slachtoffer worden van accountmisbruik. Een crimineel kan accounts overnemen, bekenden oplichten en aankopen doen met andermans geld. Ook identiteitsfraude is een probleem, waarbij de crimineel zich voor een ander uitgeeft. Dit kan zorgen voor veel schade.

Het gijzelen van computerbestanden of het inbreken in iemands computer om privéinformatie te stelen is eveneens een zeer reëel gevaar. Om dit te voorkomen is het belangrijk computer, tablet en smartphone stevig dicht te timmeren met wachtwoorden. Dat geldt ook voor andere apparaten zoals televisies en luidsprekers met internettoegang. Een onderschat gevaar vormen mailaccounts, waar meestal veel persoonlijke informatie uit te halen is. Bovendien: wie eenmaal binnen is kan internetaccounts (van bijvoorbeeld Facebook of Twitter) overnemen door een nieuw wachtwoord aan te vragen.

Gelukkig is er wat aan te doen. Het beveiligen van internetapparaten is niet ingewikkeld. Het is belangrijk enkele basisregels te hanteren. Slechts het installeren van een virusscanner is niet meer genoeg. Minstens zo belangrijk is

Cybercriminelen hebben het niet alleen op grote bedrijven voorzien. Iedereen loopt gevaar

het kiezen van goede wachtwoorden, het instellen van dubbele authenticatie en het installeren van updates. Ook het vermijden van risico's is noodzakelijk voor veilig internetgebruik: download geen bestanden van louche websites en wees alert bij links of bijlagen die per mail worden gestuurd.

Dit boek helpt internetgebruik stap voor stap veiliger te maken. In hoofdstuk 1 leggen we uit welke gevaren er op de loer liggen. Hoofdstuk 2 draait om de beveiliging van systeem en software. Wie gegevens kwijtraakt door internetcriminaliteit, moet kunnen terugvallen op een back-up. In hoofdstuk 3 beschrijven we hoe je die kunt maken. Adviezen om veilig te surfen op internet en accounts te beveiligen staan in hoofdstukken 4 en 5. De laatste twee hoofdstukken zijn gereserveerd voor het beveiligen van de internetverbinding en veilig online bankieren.

Dit boek bevat veel stappenplannen met uitleg over het wijzigen van instellingen. Software en webdiensten passen regelmatig hun beleid en werkwijze aan. Het kan daarom voorkomen dat bepaalde tips en instructies inmiddels achterhaald zijn of net op een iets andere manier werken. De achterliggende informatie blijft echter gelijk.

TIP

Ook op onze site is veel informatie te vinden over online veiligheid en online privacy. Zie www.consumentenbond.nl/veilig-online en www.consumentenbond.nl/internet-privacy.

Foto auteur: Michel Walraven

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

1

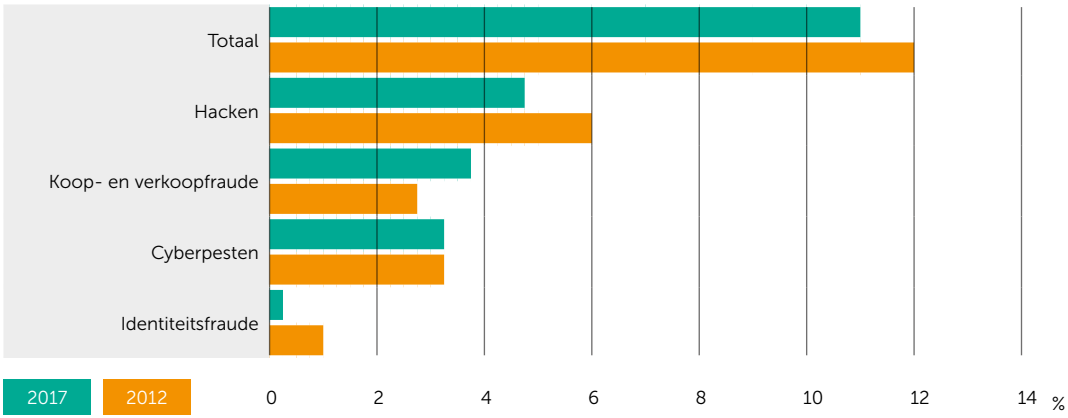
ONLINE RISICO'S

Internet biedt veel mogelijkheden, maar er zijn ook risico's. Hackers liggen op de loer. Ze zijn uit op geld of persoonlijke gegevens. Er zijn allerlei manieren waarop ze binnendringen. In dit hoofdstuk een overzicht van de gevaren.

Ons leven is verweven geraakt met internet. Een dag zonder is bijna niet meer voor te stellen. Bij een storing van Netflix, Facebook of Google regent het klachten. Voor het boeken van een reis, informatie opzoeken of chatten met vrienden: we zijn steeds afhankelijker geworden van internet.

Die afhankelijkheid brengt risico's met zich mee. Een tijdelijke storing zorgt voor irritatie. Echt gevaarlijk wordt het als je te maken krijgt met kwaadwillenden die internet misbruiken. Volgens het Centraal Bureau voor de Statistiek (CBS) was in 2017 11 procent van de burgers van 15 jaar of ouder slachtoffer van cybercrime. Het gaat om zaken als identiteitsfraude, inbraak op de computer, cyberpesten en fraude bij kopen via internet. Jongeren zijn relatief vaker slachtoffer dan ouderen.

SLACHTOFFERSCHAP CYBERCRIMEDELICTEN



1.1 Computercriminaliteit

Bedrijven, overheden en consumenten zijn het slachtoffer van cybercrime. Regelmatig staan er alarmerende berichten in de kranten. Een kleine greep: hackers maakten klantgegevens buit bij taxibedrijf Uber, banken gingen offline door cyberaanvallen en het Rotterdamse Havenbedrijf

moest tot tweemaal toe zijn werkzaamheden stoppen door virussen. Ook lezen we vaak over slachtoffers van internetcriminaliteit zoals ransomware (zie par. 1.5e en 4.4) of phishing (zie par. 1.5a en 4.2).

1.2 Steeds meer internetapparaten

Dat criminelen steeds vaker via internet opereren heeft te maken met de toename van het internetgebruik. Niet alleen via de computer, maar ook via smartphone en tablet zijn we continu online. Zelfs televisies, netwerkschijven, printers, mediaspelers en radio's beschikken over een internetaansluiting. Daarnaast is in steeds meer huizen een met internet verbonden thermostaat en verlichting te vinden.

Huishoudens veranderen in zogeheten 'smarthomes', waarin bijna elk apparaat voorzien is van een aansluiting, tot aan de stofzuiger en wasmachine aan toe. Het fenomeen van apparaten met een internetaansluiting wordt ook wel 'Internet of Things' (IoT) genoemd. Zonder tussenkomst van een gebruiker sturen ze continu informatie

het internet op. Dat kan handig zijn: je krijgt bijvoorbeeld bericht dat de was klaar is. Maar voor een hacker vormen die apparaten een extra mogelijkheid om binnen te dringen in het thuisnetwerk.

TIP

Smarthome goed beveiligd?
Vormen de met internet verbonden apparaten in uw huis een gevaar? Controleer het op de site iotscanner.bullguard.com.

Ieder apparaat dat is verbonden met internet levert een potentieel risico op. Via een slecht beveiligd apparaat kan een hacker de rest van het thuisnetwerk bespioneren, informatie stelen of zelfs geld buitmaken. Of een apparaat goed beveiligd is, kan een gemiddelde consument niet beoordelen. Een goede beveiliging van het netwerk wordt dus steeds noodzakelijker. Er zijn speciale routers (zie par. 6.3) te koop die hiervoor zorgen.

Een slimme speaker, zoals hier de Amazon Echo, biedt handige mogelijkheden, maar hackers kunnen er misbruik van maken.

1.3 Botnets

Een crimineel kan computerapparatuur ook onderdeel maken van een zogeheten 'botnet' waarmee hij aanvallen uitvoert. Een botnet bestaat uit vele duizenden tot soms wel miljoenen gehackte computers met als doel aanvallen uit te voeren op computers van (veelal) bedrijven en overheden. Meestal weet de eigenaar niet dat hij onderdeel is van zo'n botnet. Met een botnet kan een hacker DDoS-aanvallen uitvoeren. Via talloze gehackte apparaten stuurt hij tegelijkertijd internetverkeer naar een bedrijf of website. Het gevolg is dat die offline gaat door de enorme hoeveelheid verkeer. Dit type aanval werd bijvoorbeeld begin 2018 gebruikt om banken tijdelijk offline te halen. In zo'n geval ben je dus niet zelf doelwit van een hacker, maar wordt de computer gebruikt in een grotere aanval. Niet alleen banken worden slachtoffer van DDoS-aanvallen. Ook overheidsinstellingen en mediabedrijven hebben er geregeld mee te maken.

Niet alleen op computers

Tot een paar jaar geleden bestonden botnets vooral uit computers, maar dankzij de opkomst van smartphones en smarthomes is de aandacht van cybercriminelen verschoven. Botnets bestaan er nu ook voor mobiele en IoT-apparaten.

1.4 Waarom hackers hacken

Hackers breken om verschillende redenen in op computers. Er is niet altijd kwade opzet in het spel. Er zijn zogeheten 'ethische' hackers. Zij zoeken uit waar gaten in de beveiliging zitten en maken hier melding van bij de verantwoordelijke bedrijven. Sommige bedrijven geven een beloning voor dergelijke ontdekkingen. Google betaalde afgelopen jaar 2,9 miljoen dollar aan ethische hackers.
Gevaarlijke hackers zijn er ook. Zij hebben diverse motieven voor hun praktijken, waaronder:

- Diefstal
- Activisme
- Chantage
- Spionage
- Identiteitsfraude
- Cyberterreur
- Cyberpesten
- Cyberoorlog

Als consument krijg je niet direct met al deze zaken te maken. De kans dat je onderdeel wordt van een cyberoorlog is vrij klein, tenzij je computer onderdeel wordt van een botnet. Een groter risico is dat een hacker uit is op geld of vertrouwelijke informatie.

1.5 Verschillende soorten cyberoplichting

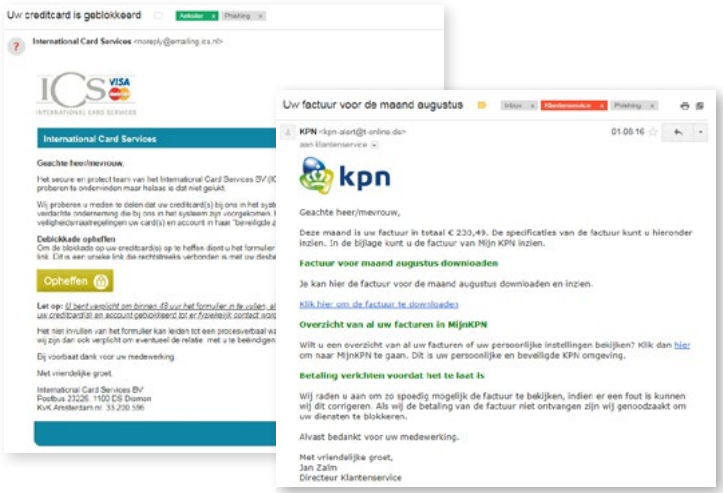
Cybercriminelen hebben verschillende manieren om iemand op te lichten. Hieronder bespreken we de meest voorkomende soorten.

1.5a Phishing

Een groot probleem op internet wordt gevormd door

phishing. Criminelen hengelen via nepberichten naar privéinformatie zoals inlogcodes. Dagelijks komen nieuwe meldingen binnen. In phishingberichten doen criminelen zich voor als een ander. Ze schrijven een bericht uit naam van bijvoorbeeld een bank, bedrijf of overheidsinstelling. Het komt ook voor dat criminelen zich voordoen als een vriend of bekende (zie ook par. 4.7 over identiteitsfraude). Een phishingmail bevat bijna altijd het verzoek om op een link te klikken of een bijlage te downloaden. Hiermee kan een crimineel privégegevens stelen of kwaadaardige software (malware) op de computer zetten.

Vroeger pikte je de mailtjes er zo uit door het knullige taalgebruik, maar tegenwoordig zijn phishingmails nauwelijks van echt te onderscheiden. In paragraaf 4.2 laten we zien hoe je ze toch herkent.



Voorbeelden van phishing per mail.

1.5b Voorschotfraude

Een veelgebruikte methode om mensen op te lichten is voorschotfraude. Een fraudeur doet een mooie belofte, bijvoorbeeld een grote som geld. Het slachtoffer moet daar wel iets voor doen, bijvoorbeeld een klein bedrag overmaken of waardevolle privégegevens sturen. Deze