‘Ruim 2 miljoen mensen dupe identiteitsfraude’
– De Telegraaf

‘Enkele tonnen gestolen door identiteitsfraude via DigiD’
– De Volkskrant

‘Eén kopietje van je paspoort en je identiteit is gejat’
– NRC Handelsblad

‘Identiteitsfraude zeer ernstig’
– NOS Nieuws

‘Hackers maakten duizenden valse LinkedIn-accounts’
– Knack

‘Campagne om identiteitsfraude bij kinderen
op sociale media tegen te gaan’
– Dutchcowboys.nl

‘Kabinet: Nederlanders niet alert op identiteitsfraude’
– Security.nl

‘Wie het slachtoffer wordt van identiteitsfraude belandt
in een horrorscenario, waarin deurwaarders, incasso-
bureaus en opsporingsambtenaren verbeten jacht maken
op een schaduw die altijd naar jou wijst’
– KRO Reporter

‘NSA kan vrijwel ieder mobieltje afluisteren’
– Algemeen Dagblad
‘Facebook downloadtool lekt contactinfo 6 miljoen leden’

– Webwereld

‘Kabinet wil actie tegen identiteitsdiefstal minderjarigen’
– Het Parool

‘Hackers stelen wereldwijd miljoenen wachtwoorden’
– Algemeen Dagblad

‘Persoonsgegevens niet veilig bij gemeenten’
– Binnenlands Bestuur

‘Afgedankte pc’s en laptops bevatten nog allerlei persoonlijke gegevens, zelfs als de harde schijf geformatteerd is’
– Recherchebureau Com-Connect
(gespecialiseerd in digitaal fraudeonderzoek)

‘ING-klanten overspoeld door phishingmails’
– Webwereld

‘Gemeenten springen onveilig om met persoonsgegevens’
– De Volkskrant

‘DigiD van 150 Amsterdammers gehackt’
– NRC Handelsblad

‘Rabobank offline na bizar privacylek’
– Webwereld

‘De snelst groeiende vorm van criminaliteit is identiteitsfraude’
– De Telegraaf

KOMT EEN VROUW BIJ DE H@CKER

MARIA GENOVA

KOMT EEN VROUW BIJ DE H@CKER

HOE JE IDENTITEIT GESTOLEN KAN WORDEN

JUST PUBLISHERS

Meer info over Maria Genova? Zie www.mariagenova.nl

14e herziene druk, januari 2018
15e druk, april 2018
16e druk, juni 2018
17e druk, juni 2018
18e druk, december 2018

Redactie en productie: Vitataal, Feerwerd
Opmaak: Studio Spade, Voorthuizen
Omslagontwerp: Ben Gross

ISBN 97890 8975 292 5
NUR 330 en 402

WWW.JUSTPUBLISHERS.NL

Inhoud

1

1737 auto's op je naam

'Nou, nu is het gebeurd. Het begon met een rekeningafschrift dat uit mijn brievenbus is gehengeld. Toen is er een bankpasje aangevraagd en daarna is mijn rekening geplunderd. Hoe kan de bank zomaar mijn geld aan iemand anders geven? Heb ik straks allerlei rekeningen en incasso's aan mijn broek? Ik vind het zo erg, naïeve tut die ik ben.'

Ik lees dat op een forum op internet. De angst en de onzekerheid van die vrouw spatten van het scherm. Dat lijkt me het lastigste: dat je niet weet hoe ver criminelen kunnen gaan. In het horrorscenario van identiteitsfraude neem je het vrijwel altijd tegen een onzichtbare vijand op.

Steven Romet is daar een mooi voorbeeld van. Hij krijgt vrijwel dagelijks boetes, aanmaningen en brieven van officiele instanties nadat iemand zijn rijbewijs in een discotheek heeft gestolen. In korte tijd zetten criminelen 1737 auto's op zijn naam. Romet wordt opgepakt en brengt maanden in de gevangenis door. Hij kan simpelweg niet bewijzen dat hij met zijn uitkering geen 1737 auto's kan kopen. Hij kan de Rijksdienst voor het Wegverkeer er niet van overtuigen dat het onmogelijk is om nieuwe auto's vanuit de gevangenis te registreren. De logica van een systeem blijkt sterker dan de logica van een individu. Zijn uitkering wordt stopgezet, want volgens de ambtenaar heeft iemand die in staat is zoveel auto's te kopen geen uitkering meer nodig.

Voordat de zaak definitief opgelost wordt, is Romet zeventien jaar verder, zeventien jaar vol angst en ellende. Pas in 2012 krijgt hij gerechtigheid van het Europees Hof voor de Rechten van de Mens. Als slachtoffer van een ambtelijke dwaling ontvangt hij negenduizend euro schadevergoeding.

Het ergste is dat je niet eens je rijbewijs hoeft te verliezen om slachtoffer van dit soort praktijken te worden. Er is een levendige internationale handel in kopietjes en die blijken even bruikbaar om fraude mee te plegen. Ik vraag me af hoeveel kopietjes van mijn paspoort en rijbewijs er rondslingeren. Hotels, autoverhuurbedrijven, overheidsinstellingen, banken, telefoonmaatschappijen, iedereen vraagt om een kopie. Op mijn paspoort staat een burgerservicenummer en tot voor kort wist ik niet eens dat ik het moet doorstrepen om fraude te voorkomen.

Mensen die slachtoffer zijn geworden van cybercrime klagen dat er bij de politie zulke digibeten werken dat ze er weinig van begrijpen. Op Twitter vind ik wel een 'Agent Digitaal', die voorlichting geeft over het onderwerp identiteitsfraude.

'Als ik wil, kan ik je identiteit zo stelen,' zegt de politieman als we elkaar voor het eerst spreken.

'Hoe dan?'

'Ik stuur je een betrouwbaar uitziende e-mail. Als je die opent, geef je me onbewust toegang tot je computer. Voor altijd.'

'Hmm.'

'Wil je misschien een voorproefje? Ik kan ook je LinkedIn-gegevens kopiëren en namens jou berichten naar allerlei personen sturen. Je kunt me niet voor identiteitsdiefstal aanklagen. Al die gegevens heb je zelf openbaar gemaakt, net als de meeste burgers. Ik steel ze niet, ik gebruik ze gewoon. Wil je me tegenhouden, dan moet je bewijzen dat je er schade van ondervindt en in de praktijk is dat niet zo simpel.'

'Dus mijn identiteit gebruiken is niet strafbaar?'

'In theorie wel, maar in de praktijk moet je eerst bewijzen dat het je schaadt.'

'Dat is toch logisch? Ik wil niet dat iemand me kloont en namens mij berichten verspreidt.'

Verbazing en boosheid strijden om voorrang. Ik probeer niet al te veel privé-informatie op internet te zetten, maar als je bij de bekende social media een profiel hebt, is dat gauw te veel. Ontbrekende gegevens worden simpelweg door andere sites aangevuld. De Kamer van Koophandel zet al mijn gegevens online omdat ik een bedrijfje heb, Google Maps gebruikt ze en laat iedereen op mijn huis inzoomen. Zelfs mijn telefoonnummer staat erbij, terwijl het niet eens op mijn naam is geregistreerd. Mijn gegevens worden aan elkaar gekoppeld, omdat ze geld waard zijn.

'Hoe ver kan iemand gaan met mijn gegevens?' vraag ik.

'Hoe ver wil je gaan?' reageert de politieman.

'Ik wil alleen maar weten wat er mogelijk is.'

Ik hoor een lachje aan de andere kant van de lijn. 'Ik mail je wat informatie.'

2
Onschuldig in de bak

Een vrijstaand huis in een nieuwbouwwijk in Hoofddorp. Ron Kowsoleea doet de deur open en laat me binnen. Even later zegt hij: 'Je spreekt nu met mij in mijn huis, maar eigenlijk zit ik vast in de gevangenis.'

'Hoe bedoel je, je zit vast?'

'Degene die mijn identiteit gestolen heeft zit vast. Dus op papier zit ik nu in de gevangenis.'

'Wat maf. Konden ze deze fout niet terugdraaien toen ze de identiteitsfraude ontdekten?'

'Nee, want dan moesten ze die man vrijlaten.'

'Bizar.'

'Mijn hele leven is bizar. Sinds de identiteitsfraude tenminste. Daarvoor was er niets aan de hand.'

Wat Ron Kowsoleea is overkomen, is haast onvoorstelbaar. Een harddrugscrimineel heeft in 1994 bij een aanhouding zijn naam opgegeven. Sindsdien staat Ron in allerlei overheidssystemen als crimineel geregistreerd.

'Politie en Justitie beloofden steeds dat het goed zou komen, maar ik werd keer op keer aangehouden en in de handboeien geslagen. Soms op straat, soms op Schiphol en een keer vielen ze mijn huis binnen. Ik zou drugsgeld hebben witgewassen. Om gek van te worden. Een officier van justitie stelde voor dat ik een andere identiteit aanneem om van de problemen af te zijn. Maar ik ben ik. Ik wil niet iemand anders zijn,' zegt de 52-jarige Ron.

Het begon allemaal met een dagvaarding. 'Ik zou voor een drugsdelict zijn aangehouden door de Amsterdamse politie,' zegt Ron. 'Ik was stomverbaasd, want ik was nergens aangehouden, laat staan voor drugs. Ik ben naar het politie-

bureau gegaan. Ik zie nog de verbijstering op het gezicht van de politieagent die bij de balie zat. Hij was namelijk dezelfde politieman die mij enkele weken daarvoor zou hebben opgepakt. Toen kwamen ze erachter dat de man die ze hadden aangehouden mijn naam had opgegeven. Het bleek een kennis van de lagere school.'

Justitie beloofde zijn dossier op te schonen en Ron dacht dat het allemaal achter de rug was. Daar leek het ook op tot hij jaren later werd aangehouden bij een verkeerscontrole.

'Ik werd in de handboeien geslagen en afgevoerd in een politiebusje. Je kunt je er geen voorstelling van maken wat dat met je doet als je niks gedaan hebt.'

'Lijkt me verschrikkelijk.'

'Ja, je wordt gefouilleerd en in een cel gezet. Je moet de veters van je schoenen en je riem afgeven. "Meneer, dat ben ik niet." "Ja meneer, dat zeggen ze allemaal." En de celdeur gaat dicht.'

Toen de Rotterdamse politie ontdekte dat het om identiteitsfraude ging, lieten de agenten hem vrij, met tal van excuses voor de slechte behandeling. 'Ik dacht alleen maar: eindelijk naar huis,' zegt Ron. Als hij dat zegt, worden zijn ogen een beetje vochtig.

Omdat de overheid de foute gegevens niet uit de computers kon halen, werd hij keer op keer aangehouden. In totaal meer dan tweehonderd keer. Ron zegt stapels compromitterende materialen tegen de overheid te hebben als het om identiteitsfraude gaat. Ik mag ze bij onze volgende afspraak allemaal inzien en er kopieën van maken.

Als we afscheid nemen, zegt Ron: 'Ik geloof trouwens niet in complotten. Anders was ik allang kapot. Ik geloof in mezelf. Ken je het lied van Shaggy "It wasn't me"? Dat geeft me kracht.'

Het eerste wat ik thuis doe, is mijn computer opstarten. De e-mail van Agent Digitaal is binnen, een rapport met triestе en schokkende gevallen van identiteitsfraude. Bijvoorbeeld Sven, die een rekening van dertienduizend euro voor een maand bellen ontvangt. Zijn identiteitsbewijs uit zijn gestolen portemonnee blijkt voldoende voor telefoonabonnementen, leningen en bestellingen bij postorderbedrijven. Sven kan geen huis kopen omdat hij geregistreerd staat als wanbetaler. En hij kan ook niet meer slapen.

Ook bij de 24-jarige Niels zijn de gevolgen groot. Zijn nieuwe identiteitsbewijs verdwijnt tijdens het transport naar het gemeentehuis. Fraudeurs registreren namens hem een bedrijf bij de Kamer van Koophandel. De schade is al tot honderdduizend euro opgelopen als Niels de fraude ontdekt. Hij krijgt hartkloppingen en raakt in een depressie. Door zijn medische klachten moet hij stoppen met werken en daardoor komt hij in financiële problemen.

De lijst van de politieman is behoorlijk lang: een man op wiens naam een valse uitkering is aangevraagd door misbruik te maken van zijn burgerservicenummer, een vrouw bij wie de buurvrouw de sleutel van haar brievenbus heeft gekopieerd en veel producten op haar naam heeft besteld, een man van wie de wraakzuchtige ex allerlei contracten op zijn naam zet en die uiteindelijk bij de psycholoog eindigt omdat het zo moeilijk blijkt om alles ongedaan te maken.

'Fraaie voorbeelden,' mail ik de politieagent.

Zijn antwoord laat niet lang op zich wachten: 'Geloof je nu wel dat het ook jou kan overkomen?'

'Misschien. Ik ben vrij voorzichtig.'

'Dat waren die andere mensen ook.'

'Kun je het echt niet voorkomen?'

'Lastig. Controleer in elk geval geregeld je bankafschriften op vreemde transacties. Vaak begint het met kleine bedragen. Als je vermoedt dat iemand je identiteit heeft gestolen, koppel dan je computer helemaal van het internet af. En doe aangifte.'

'Het schijnt dat de meeste agenten grote digibeten zijn en dat een aangifte vaak nergens toe leidt.'

'Nou, er zitten gelukkig ook goede tussen,' mailt Agent Digitaal. 'Maar de pakkans is klein. Anonieme mensen op internet zijn lastig op te sporen.'

Opeens komt Agent Digitaal met een vreemd idee op de proppen: 'Waarom huur je niet een hacker in? Dan zie je met eigen ogen wat die gasten allemaal kunnen. En nog een tip: zoek wel een betrouwbare hacker uit.'

Een betrouwbare hacker? In mijn oren klinkt dat niet als een logische combinatie. Maar de politieman heeft gelijk: als ik echt wil weten wat er op het gebied van cybercrime en identiteitsfraude mogelijk is, dan moet ik iemand vinden die heel diep in de materie zit, iemand die dingen kan doen die van de wet niet mogen. Komt een vrouw bij de... hacker.

Na de mailwisseling met Agent Digitaal ben ik een stuk voorzichtiger aan het worden. Alle informatie die ik binnenkrijg, bekijk ik met argusogen voordat ik ergens op klik. Cybercrime-specialisten kijken met verbazing naar het gemak waarmee mensen hun gegevens aan criminelen doorspelen. We schijnen massaal op besmette linkjes te klikken. Het gaat allemaal zo simpel: je hoeft alleen maar in te loggen om

een ontvangen wenskaartje te zien en dan hebben de hackers toegang tot al je gegevens. Een 24-jarige hacker verzamelde op deze manier naaktfoto's uit honderden computers, die hij vervolgens online publiceerde met vermelding van de echte namen van de slachtoffers.

Maar ook als je niet op besmette linkjes klikt, als je helemaal niets bijzonders doet, ben je niet veilig. Mensen kunnen zich simpelweg voor jou uitgeven en soms zelfs een identiteitsbewijs op je naam aanvragen. Dat overkwam bijvoorbeeld profvoetballer Kwasi Appiah, die in België speelde. Toen hij naar het buitenland vertrok, deed een illegale man zich als hem voor en meldde dat hij zijn identiteitspapieren kwijt was. Met zijn nieuwe identiteit sloot hij leningen en contracten af op de naam van de profvoetballer. Toen de echte Appiah naar België terugkeerde, werd zijn identiteitskaart in beslag genomen en werd hij een maand lang in een gesloten instelling opgesloten. De politie dacht dat hij de identiteitsdief was.

Komt een vrouw bij de hacker... Het idee laat me niet los, maar ik vind het behoorlijk eng om het uit te voeren. Wie wil nou dat een onbekende in haar computer gaat wroeten en misschien lang vergeten gevoelige informatie vindt? Normaal gesproken laat ik al niemand in mijn tas kijken en de inhoud van mijn harde schijf is waardevoller dan honderd van die tassen bij elkaar.

Aan de andere kant kan een hacker misschien dingen vinden die ik wel graag wil weten. Of mijn computer bijvoorbeeld door criminelen gebruikt wordt om spam en porno te versturen. Die kans bestaat, want veel computers zijn aangesloten op criminele computernetwerken, uiteraard zonder dat de eigenaren dat weten. Dat betekent dat ze in princi-

pe ook je e-mails kunnen lezen en je foto's kunnen bekijken. Daar merk je niets van, behalve misschien dat je computer soms te traag is. Dat kreng van mij is vaak te traag. Of ben ik te ongeduldig?

Er zijn trendwatchers die voorspellen dat het vrije internet op den duur opgeblazen wordt door de toegenomen cybercrime. Maar ik waan me veilig achter mijn computer, net als de meeste mensen. Het beklemmende idee dat iemand met een paar muisklikken van alles over je weet, is nog steeds een ver-van-mijn-bed-show. Maar ik weet inmiddels dat de echte computerexperts geen risico's nemen: ze herinstalleren om de zes maanden hun hele computer.

Wij digibeten zijn zelfs te lui om een nieuw wachtwoord te verzinnen. Misschien omdat we geen idee hebben hoe kwetsbaar we achter zo'n scherm zijn. Een computer op een afstandje besmetten en overnemen is een fluitje van een cent. Het slachtoffer hoeft alleen maar op een foute link te klikken. Of iemand stuurt je een bestandje met een verborgen keylogger. Die registreert je toetsaanslagen en verstuurt de opdrachtgever al je e-mails. Zo'n programmaatje kan zelfs het nummer van je creditcard na een betaling onderscheppen, inclusief veiligheidscode en vervaldatum. Als je wachtwoord niet sterk is, kan iemand je e-mails omleiden en jou worden op internet. Dat komt doordat veel diensten een e-mail gebruiken om wachtwoorden te resetten.
Terwijl je dit leest, kan iemand bezig zijn op mijn naam of op die van jou spullen te kopen, telefoonabonnementen af te sluiten of zelfs een hennepplantage te exploiteren. Onmogelijk? Meestal ontdek je het pas maanden en soms zelfs jaren later.

Mensen die werken, worden in duizenden databestanden geregistreerd. Als je als kluizenaar leeft, blijken je persoonsgegevens in 'slechts' 250 bestanden te staan.

Waarom willen zo veel instanties zo veel over ons weten? Op zoek naar het antwoord kom ik bij een mooi vrijstaand huis in een rustig stadje aan. Hier woont de eerste Nederlander die veroordeeld werd voor het schenden van de privacywetgeving in opdracht van bedrijven.

Wie een grote boef verwacht, komt bedrogen uit. Michel Kraaij is een charmante man van middelbare leeftijd met een joviale glimlach en ook nog behoorlijk idealistisch voor een boef. Toch heeft hij een halfjaar in de cel gezeten omdat hij persoonlijke gegevens op verboden manieren verkreeg.

'Het is helemaal niet zo moeilijk om aan informatie te komen die je niet mag hebben,' zegt Kraaij. 'Dan heb ik het bijvoorbeeld over al je rekeningen inclusief saldi, je geheime telefoonnummer, je salaris, hoeveel auto's je hebt, of je schulden hebt, of je ooit veroordeeld bent en ga zo maar door. Ik heb onderzoeken gedaan naar oplichters en moordenaars, maar ook naar bekende Nederlanders.'

'En al die jaren wist je niet dat je iets strafbaars deed?'

'Ik bevond me in een soort grijs gebied. Als je weet wie je opdrachtgevers zijn, dan waan je je min of meer veilig. De landsadvocaat, alle grote banken, verzekeringsmaatschappijen, bekende tv-programma's en tijdschriften. Ik was gewoon een kleine vis en ik verwachtte niet dat justitie juist achter mij aan zou gaan en de rest met rust zou laten. Het was allemaal zo bizar: ik zat in de bak en het bureau waar ik voor werkte ging gewoon verder met het verhandelen van informatie. Inmiddels weet ik hoe rekbaar het recht is. Wacht, ik kan het je allemaal laten zien,' zegt Kraaij en hij staat op.

Even later komt hij terug met een stapel ordners.

'Kijk, ik heb alles bewaard.'

Kraaij haalt er diverse faxen en brieven uit. Fortisbank vraagt een overzicht van de banksaldi van een man en wil weten of hij gezocht wordt door Justitie. Uiteraard is dat geen informatie die je op een legale manier kunt verkrijgen. Een ministerie vraagt om de bezittingen van iemand op te sporen die verontreinigde grond aan de gemeente Tilburg heeft verkocht. In de brief staat: 'Via de Fiscale Recherche te Roosendaal is getracht de mogelijkheid te onderzoeken om op legale wijze informatie te verkrijgen over de financiële gegevens van V. Dit bleek niet het geval.'

'Zie je het?' zegt Kraaij. 'Het ministerie schrijft zelf dat de informatie niet op legale manier te verkrijgen is, dus moet ik het op een illegale manier doen. Ze hebben me hier 2500 euro voor geboden als het me binnen drie weken zou lukken. Ik was binnen vier uur klaar. Toen had ik zijn adres, al zijn bankrekeningen, de saldi en de kentekens van zijn auto's.'

Kraaij laat ook een van de vele faxen van de landsadvocaat Pels Rijcken & Droogleever Fortuijn zien. 'Ze vragen of ik iemand wil opsporen die nergens ingeschreven staat.'

'Waar begin je dan?'

'In dit geval ben ik bij de banken begonnen,' zegt Kraaij, terwijl hij zijn aantekeningen bestudeert. Bij Fortis had ik beet. Ze vertelden me naar welk adres zijn bankafschriften werden gestuurd. Daar kon ik helaas geen telefoonaansluiting vinden. Toen belde ik de buren en ze vertelden me dat die man er al een tijdje samen met een weduwe woonde. Voor dit klusje heb ik veertig euro gerekend.'

'Wil je zeggen dat alle banken informatie over de rekeningen en de adressen van hun klanten aan je doorgaven?'

'Allemaal. Je hoeft alleen maar te zeggen dat je een collega van een andere afdeling bent en dat je computer platligt. Dan geven ze je alles wat je vraagt. Ik heb het slechts een paar keer meegemaakt dat ik op mijn bek ging, maar dat was geen probleem, want vijf minuten later kon ik de informatie via een andere afdeling ontfutselen. Dat geldt overigens niet alleen voor de banken, maar ook voor de FIOD, de Belastingdienst en de uitkeringsinstanties. Soms stonden medewerkers tientallen sofinummers te dicteren zonder argwaan te krijgen.'

'Bijzonder.'

'Voor mij was het helemaal niet bijzonder. Dat was gewoon mijn werk.'

Kraaij laat nog meer brieven zien. 'Hier vraagt de advocaat van de Rabobank of ene meneer Lochan rekeningen bij andere banken heeft. Hij is de Rabobank geld schuldig en ze willen beslag leggen op zijn rekeningen. Een accountantskantoor heeft blijkbaar een vergelijkbaar probleem met dirigent Jaap van Zweden, want in deze brief vragen ze of ik zijn bankrekeningen wil traceren. En hier moet ik het geheime nummer van een crimineel achterhalen. Als je mijn aantekeningen kunt lezen is dat ook gelukt en daar heb ik twintig euro voor gerekend. Ik belde de KPN, de afdeling die de geheime nummers kan inzien, ik deed me voor als een collega van de afdeling incasso en toen kreeg ik zijn telefoonnummer en ook zijn adres. Simpel hè? Alles staat geregistreerd in systemen.'

Kraaij bladert verder in zijn fascinerend omvangrijke archief. 'Kijk, een brief van Dirk Scheringa. Hij vraagt of er een gerechtelijk vooronderzoek naar hem loopt.'

'Maar je kunt toch niet in de systemen van Justitie komen?'

'Soms wel. Ik doe me gewoon als een collega van een ander parket voor en dan krijg ik alle informatie. Zo kom ik ook te weten of iemand eerder veroordeeld is.'

'Is het nog steeds zo gemakkelijk om aan persoonlijke gegevens te komen?'

'Ongetwijfeld.'

Op dat moment wordt Kraaij gebeld. Na enkele minuten hangt hij op: 'Sorry, ik moet gaan.'

Als ik het huis verlaat, bekruipt me een gevoel van onbehagen doordat het kennelijk zo simpel is om iemands gegevens te verzamelen.

3

De perfecte hacker

Wie zijn de hackers? De eerste naam die me te binnen schiet is Anonymous, waarschijnlijk omdat ze massale aanvallen op netwerken van bekende bedrijven uitvoeren. In mijn verbeelding zijn dat types die volledig ondergronds opereren. Het laatste wat ik verwacht is dat iemand van Anonymous zelf contact met mij gaat zoeken naar aanleiding van een blog. Hij schrijft me een mailtje dat hij een primeur heeft, een hack bij Justitie. Of ik die in de publiciteit wil brengen? Ik geef hem mijn telefoonnummer en hij belt me vrijwel meteen. Als ik hoor waar het over gaat, verwijs ik Anonymous naar twee collega's die op redacties werken die goede advocaten kunnen betalen. Maar ik gebruik ook meteen de gelegenheid om hem te vertellen dat ik met een zoektocht naar de mogelijkheden van hackers bezig ben.

'Bijzonder,' reageert hij. 'De meeste mensen laten sporen in cyberspace na, sporen die ze liever niet terugzien.'

'Ook niet als je computer goed beveiligd is?'

'Elke beveiliging kun je omzeilen. Meestal is dat niet zo moeilijk. Je stuurt bestandjes naar de computer die de firewall misleiden. Computers zien ze voor updates van belangrijke programma's aan en de meeste apparaten zijn zo ingesteld dat ze automatisch nieuwe updates ophalen. Als je computer dat gedaan heeft, kan ik alles lezen.'

'Nogal creepy. Maar ik heb begrepen dat het wat lastiger is bij een Apple.'

'Klopt. Bij een Windowscomputer kost het me zo'n tien minuten om binnen te komen, bij een Apple is dat een kwartier.'

Stilte.

'Dus je kunt mijn computer hacken?'

'Daag je me uit? Dit is vrij riskant voor je,' klinkt er aan de andere kant van de lijn.

'Ja, maar iemand moet wel proefkonijn zijn om te beschrijven hoe zoiets in zijn werk gaat en of het zo gemakkelijk is. Voor zover ik weet zijn er geen andere liefhebbers.'

'Ja, ik ben persoonlijk nog nooit gevraagd om iemands computer te hacken. Meestal kies ik zelf mijn slachtoffers uit.'

'Dus? Gaan we afspreken?'

Anonymous gaat akkoord om in een café af te spreken.

Als ik heb opgehangen, bekruipt me toch een grote twijfel. Wie zegt dat hij te vertrouwen is? Eerlijk gezegd vind ik dat best eng: met iemand die ik niet ken in een internetcafé afspreken en hem de sleutel tot mijn privéleven geven.

Na een dag nadenken hak ik de knoop door: ik ga een andere hacker zoeken, iemand die achteraf gemakkelijk te traceren is voor het geval dat er iets misgaat. En ik ga niet ergens in een café afspreken. Het liefst wil ik dat de hacker me in zijn huis uitnodigt, want dan heb ik zijn adres.

Als ik tegen mijn man vertel dat ik mijn computer wil laten hacken, kijkt hij me verschrikt aan.

'Hacken? Ben je gek geworden? Straks ligt alles van jou op straat. En dan krijgen je vrienden en duizenden onbekende volgers op Twitter van die leuke linkjes waar ze op kunnen klikken. Daar moet je echt niet aan beginnen.'

'Ja, maar ik wil uit de eerste hand weten hoe hackers te werk gaan. Ik wil kijken wat ze met mijn bestanden zouden kunnen.'

'Wat een risico. Gekkenwerk.'

'Het is allemaal theoretisch hoor, de hacker gaat niets met de informatie doen.'

'En dat geloof jij?'

'Daar ga ik van uit. We maken van tevoren afspraken.'

Mijn man kijkt niet bepaald happy. 'Wees alsjeblieft voorzichtig,' zegt hij. 'Mensen veranderen soms van intentie, ondanks hun goede bedoelingen.'

In mijn zoektocht naar de perfecte hacker bekijk ik tientallen profielen op social media. Wie kan ik vertrouwen? Soms vergroot ik hun foto uit, maar ik weet uit ervaring hoe weinig bepaalde gelaatstrekken iets zeggen over betrouwbaarheid. Koele blik, dunne lippen, harde uitstraling: vaak zit het allemaal tussen je oren. Een vriendelijk uitziend iemand kan juist heel glad blijken. Als ik ook nog een paar verhalen over doorgedraaide hackers lees, slaat de twijfel nog meer toe. Vooral het verhaal van ene Emma vind ik eng. Iemand stalkt haar en bedreigt haar al een tijdje, maar ze heeft geen flauw idee wie hij is. Haar belager mailt haar een 'plan van aanpak' waarop te lezen valt hoe ze door een vriendin zal worden meegelokt en vervolgens verkracht. De dader heeft ook een seksadvertentie met het telefoonnummer van Emma op internet geplaatst.

Een bevriende hacker helpt haar om zo veel mogelijk informatie te verzamelen. Hij is de enige die Emma in deze donkere periode helpt. Ze durft niet eens meer haar beste vrienden te vertrouwen.

Als de datum van de aangekondigde verkrachting nadert, gaat Emma naar een geheim adres. Maar ook daar wordt ze bedreigd. Dat brengt de politie op een spoor, want de be-

vriende hacker en haar ouders zijn de enigen die het geheime adres weten.

Bij het eerste verhoor ontkent de hacker alles, maar het net sluit zich bij zijn tweede verhoor. Zijn motief: het lukt hem niet om Emma op een gewone manier voor zichzelf te winnen, dus hoopt hij dat zij zich aangetrokken voelt tot hem als hacker en redder in nood. Hij krijgt uiteindelijk een werkstraf en een proeftijd van drie jaar. Emma heeft nog een lange tijd nachtmerries en heeft psychische hulp nodig.

Na zo'n verhaal vraag ik me af of ik ook niet op de een of andere manier last kan krijgen als ik een hacker carte blanche geef om in mijn gegevens te neuzen, uiteraard vooropgesteld dat het hem lukt om mijn computer te hacken.

Ik zet mijn zoektocht door, maar wel iets minder enthousiast. Ik volg al tientallen hackers op Twitter en Rickey lijkt me op de een of andere manier betrouwbaar. In zijn profiel staat 'High Tech Crime/Forensics'. Hij schrijft blogs die ik als digibeet kan volgen en daarom heb ik goede hoop dat hij me alles zonder al te veel vaktermen uit kan leggen.

Ik zie dat hij ergens 'criminal brought to justice' over zichzelf schrijft. Opmerkelijk, hij is dus veroordeeld en vast wel heel eerlijk om dit met iedereen te delen.

Ik stuur Rickey een berichtje: 'Ben je veroordeeld voor hacking?'

Het antwoord laat niet lang op zich wachten: 'Ja.'

'Kan ik je misschien hierover spreken? Voor een boek.'

Als ik Rickey aan de telefoon krijg, blijkt hij inderdaad heel open. Hij schaamt zich niet voor zijn veroordeling, hij ziet die als een jeugdzonde en als een levensles.

Rickeys verhaal is best apart. Hij is zestien als hij met het hacken van computers begint. Hij leest ergens 'Hack the world' en die drie woorden blijven in zijn hoofd spoken. Hack the world. Hij maakt alvast een beginnetje door alle Nederlandse universiteiten en hbo-instellingen te hacken. Als ze 'op' zijn, verlegt hij zijn grens naar Europa. En daarna naar Amerika. Hack the world.

Rickey komt overal binnen, beschikt over de wachtwoorden en de e-mails van de studenten, kan cijfers wijzigen, kan van alles op afstand doen. Maar hij doet er niets mee, want zijn doel is niet om schade aan te richten, zijn doel is 'Hack the world', gewoon om te bewijzen dat geen enkel systeem voor hem veilig is. Een soort jongens-ego-spel.

Rickeys droom is om later digitaal rechercheur te worden om cybercrime op te lossen. Hij denkt dat het niet zo veel kwaad kan als hij aan de andere kant van de wet wat ervaring opdoet. Hij gelooft sowieso niet dat hij opgepakt wordt. Maar de FBI traceert zijn spoor en schakelt de Nationale Recherche in. Ze vallen om zes uur 's ochtends zijn studentenwoning binnen.

Rickey denkt eerst dat het een geintje is, hij ziet zichzelf niet als crimineel. Pas als hij hoort dat hij voorlopig niet vrijkomt, beseft hij hoe ernstig de situatie is. Als Rickey uiteindelijk voor de rechter komt en zes jaar cel tegen zich hoort eisen, stort zijn hele wereld in elkaar.

'Zes jaar! Terwijl ik me voor een hacker belachelijk braaf heb gedragen,' zegt Rickey. 'Het enige wat ik fout heb gedaan was ruimte op servers aan vrienden beschikbaar stellen voor het gratis uploaden van films, muziek en games. Ik gaf ze geen toegang tot de wachtwoorden van de netwerken, ik

zette de computers alleen 's nachts op afstand voor ze aan. Ik keek vrijwel nooit naar al die films en ik ben nooit een gamer geweest, dus ik heb daar nauwelijks van geprofiteerd.'

Braaf of niet, Rickey wordt aangemerkt als staatsgevaarlijk en de eis is zes jaar gevangenis. De rechter ziet het echter anders. Hij vindt dat Rickey in de lange periode van afwachting van zijn proces heeft laten zien dat hij geen crimineel is. De straf is slechts drie maanden voorwaardelijk met een proeftijd van een jaar.

'Mijn proeftijd loopt nog,' zegt Rickey.

Wow, denk ik bij mezelf, de gedroomde hacker. Als hij mijn computer met mijn toestemming hackt is hij niet strafbaar, maar als hij de gegevens misbruikt, dan verdwijnt hij zo de bak in, omdat hij in zijn proeftijd zit.

Ik kan Rickey wel zoenen, maar dat weet hij natuurlijk nog niet. Eerst moet ik hem als hacker zien te strikken voordat ik juich dat ik de perfecte hacker heb gevonden.

'Kun je elke computer hacken?'

'Waarom vraag je dat?' reageert hij enigszins achterdochtig.

'Gewoon, nieuwsgierigheid.'

'Misschien niet elke computer, maar de meeste wel als ik daar voldoende tijd voor krijg. Ik kan niet snel typen en ik ben niet goed in spelletjes, maar de computers en ik begrijpen elkaar vanbinnen. De huidige generatie hackers hoeft de computers niet eens te begrijpen, er is zo gigantisch veel software beschikbaar om hacks uit te voeren en gegevens te stelen. De meeste hackers die ik ken zijn heel jong en ze denken dat ze ongrijpbaar zijn. Laatst waarschuwde ik een jongen van zeventien. 'Mij pakken ze niet,' zei hij. We hebben

een weddenschap om een biertje afgesloten. Hij heeft toen een database met privégegevens van politieagenten gehackt en gepubliceerd, inclusief hun bankrekeningen en telefoonnummers. Ze hebben hem gevonden. Het biertje was voor mij.'

'Je zit in je proeftijd, maar je blijft contact houden met mensen die strafbare dingen doen.'

Rickey zucht: 'Ik hoor nu eenmaal bij de hackersscene. Maar ik voel geen behoefte om zelf wat te doen.'

'En als iemand je vraagt om zijn computer te hacken?'

'Hmm. Waarom?'

'Om te zien wat er allemaal mogelijk is en hoe jullie hackers te werk gaan.'

'Gevaarlijk plan, ik zit in mijn proeftijd.'

'Als ik je zwart op wit toestemming geef om mijn computer te hacken is dat niet strafbaar.'

'Ik moet erover nadenken,' zegt hij.

Als ik een paar dagen later hoor dat Rickey het aandurft, spring ik van blijdschap door de kamer. Mijn man kijkt me niet-begrijpend aan. 'Wat mankeert jou?'

'Ik heb de perfecte hacker gevonden: hij heeft een strafblad en zit in zijn proeftijd.'

'Zo perfect klinkt dat anders ook weer niet,' zegt mijn man. 'Ik vind het nog steeds een stompzinnig plan dat je jezelf wilt laten hacken en dan ook nog door iemand die veroordeeld is.'

'Proeftijd, lieverd, dat is een magisch woord. Beschermt beter dan een wachtwoord van vijftien karakters.'

'Volgens mij ben jij niet verder gekomen dan een wachtwoord van vijf karakters.'

'Zeven inmiddels. Ik heb er twee cijfers aan toegevoegd.'

'Je geboortedatum zeker?'

'Ben ik zo voorspelbaar?'

'De helft van de mensheid is wat dat betreft voorspelbaar.'

Mijn man is heel erg wat de computerveiligheid betreft. Hij verzint onmogelijk lange wachtwoorden en onthoudt ze ook nog. Elke keer als hij zijn computer opstart, moet hij zo'n ellenlang wachtwoord intypen. Alleen al als ik ernaar kijk, raak ik gefrustreerd.

'Ik ga mijn computer beter beveiligen voor ik hem laat hacken,' beloof ik.

'Je kunt beter de meest gevoelige informatie en foto's op een USB-stick zetten en ze ook van de harde schijf wissen in plaats van beveiligen,' reageert mijn man nijdig.

4

Slordige instanties

De volgende keer dat ik bij Ron Kowsoleea aanbel, heeft hij een stapel belangrijke documenten klaargezet. Allemaal bewijzen hoe hij door identiteitsfraude van eigenaar van een farmaceutische groothandel tot drugscrimineel werd gedegradeerd. Ron laat me heel wat brieven en faxen zien: van de FIOD die zijn zakenrelaties bezoekt om hem in diskrediet te brengen tot het Openbaar Ministerie dat zegt dat het onmogelijk is om na te gaan in welke overheidssystemen een burger geregistreerd staat.

'Ik vind het onbegrijpelijk dat de overheid geen zicht heeft op wat de overheid registreert,' zegt hij. 'Dit heeft mijn leven geruïneerd.

Ron wijst naar een aangrenzende kamer: 'Kom. Ik laat je mijn archief zien.'

Als notoire weggooier zet ik grote ogen op als ik al die dozen en mappen zie.

'Jeetje, bewaar je echt alles?'

'Ik moet wel. Bewaren en sorteren, dat is de enige manier om niet te verzuipen. De overheid is een ster in het kwijtraken van documenten, maar ik heb ze allemaal. De FIOD deed hier een inval en nam alles mee. Ze dachten dat ik niets meer had, maar ik had alles ook digitaal. Dus ik heb het opnieuw uitgeprint en gesorteerd.'

Als ik in de onderwerpen cybercrime en identiteitsfraude duik, tref ik heel veel slordige instanties, die niets om goede beveiliging van privacygevoelige data lijken te geven. Sommige voorbeelden zijn haast lachwekkend. Zo ontvangen de leden van het Brusselse parlement een heel gemakkelijk te raden wachtwoord bij een update van hun accounts. Het gaat om de eerste letter van de achternaam, gevolgd door de

eerste letter van de voornaam en een uniform woord. Wie de naam van een parlementslid weet, kan dus al zijn e-mails lezen. Een paar parlementsleden nemen de proef op de som en ja, het werkt.

Het gemak waarmee databanken gehackt kunnen worden is ook verbijsterend. Het klinkt bijna als een mop: wat is de gemakkelijkste manier om een overheidssite binnen te dringen? Een ambtenaar om zijn inloggegevens vragen. Toch gebeurt het. Twee studenten doen zich voor als medewerkers van de gemeente Enschede die bezig zijn om het computersysteem sneller te maken. Binnen een uur geven een paar ambtenaren zonder slag of stoot hun wachtwoord en inlognaam aan de studenten. En daarmee toegang tot het computersysteem.

De hoeveelheid persoonlijke gegevens die bedrijven van ons hebben, verdubbelt om de drie jaar. De beveiliging is meestal een sluitpost. Zo komen door een lek in het beheersysteem van de publieke omroep ruim twee miljoen persoonsgegevens, zoals namen, e-mails en functie op straat te liggen. Met het lekken van slechts één wachtwoord blijken 160 websites van tv-omroepen en radiostations toegankelijk.

LinkedIn blundert met een iPhone-app en daardoor worden de privémailadressen van veel mensen openbaar, zelfs die van Barack Obama en Bill Gates. En Sony bewijst dat ook grote concerns hun zaken niet op orde hebben: de accountgegevens van miljoenen PlayStationgebruikers worden gestolen, omdat Sony de wachtwoorden niet versleuteld heeft.

Het meest gênante datalek is waarschijnlijk van YouPorn, een van de meest bezochte sites ter wereld. Via een slecht be-

veiligde server belanden duizenden e-mails en wachtwoorden op straat. Veel mensen blijken dezelfde naam of hetzelfde wachtwoord ook voor andere, niet-pornografische sites te gebruiken en worden herkend als 'liefhebber'.

Experts beweren dat er slechts twee soorten bedrijven zijn: bedrijven die al het slachtoffer geworden zijn van hackers en bedrijven die dat in de toekomst gaan worden.

Eigenlijk is het onvoorstelbaar wat zelfs digibeten met de moderne digitale technieken kunnen. Op een grauw industrieterrein in Nieuwegein staat het walhalla voor mensen die meer met hun computer en mobieltje willen doen, namelijk afluisteren. Vaak zijn dat heel gewone mannen en vrouwen, die bijvoorbeeld hun partner niet vertrouwen. In zo'n spywebshop kijk je als digibeet je ogen uit. Voor nog geen honderd euro heb je software om een gsm af te luisteren en met een soort stekkerdoos kun je gesprekken in bijvoorbeeld de slaapkamer volgen. Er is ook software die je dagelijks een rapport stuurt wat iemand precies doet op internet. Sommige werkgevers gebruiken het om te zien wat hun werknemers typen. Ze kunnen je e-mails lezen en ook zien welke websites je onder werktijd bezoekt.

Deskundigen verwachten dat steeds meer internetters in databanken met persoonlijke gegevens gaan neuzen. Het werkt simpel: je betaalt om te mogen wroeten in het digitale privéleven van wie je wilt. Met slechts een e-mailadres kan een dienst als Spokeo je een enorm gedetailleerd profiel van iemand geven, van zijn filmbeoordelingen tot de foto's die hij gedeeld heeft op Flickr en van zijn Twitterberichten tot zijn commentaar op een groot aantal sites. Het bedrijf kreeg een boete van 800.000 dollar omdat de meeste gegevens op

geen enkele manier gecontroleerd werden voordat ze doorgespeeld werden naar de abonnees.

Gek genoeg lijkt er niet veel veranderd: als ik op de naam van mijn zus zoek (en betaal), kan ik nog steeds zien waar ze woont, wat voor werk ze doet, hoeveel haar geschatte vermogen is, op welk van haar huizen een hypotheek rust en wie haar familieleden zijn. Zelf heb ik geen 'klantprofiel' bij Spokeo, wel bij dataverzamelaar Experian, uiteraard zonder dat ik ooit klant ben geworden. Op basis van dat profiel besluiten tal van bedrijven of ze zaken met me willen doen. De vraag is hoe betrouwbaar dat soort databanken zijn en wat er gebeurt als je gegevens niet blijken te kloppen.

Zonder al te veel moeite stuit ik op een gedupeerde. Ralph Hupkens wil een abonnement bij KPN afsluiten en krijgt te horen dat dit niet kan vanwege 'negatieve kredietinformatie'. Die blijkt gebaseerd op de vorige bewoner van zijn koopwoning, maar dat is nooit in het systeem veranderd.

Als ik mijn 'dossier' bij Experian opvraag, zie ik dat de telefoonmaatschappijen Vodafone en T-Mobile verschillende keren informatie over mijn financiën opgevraagd hebben. Gelukkig blijken mijn gegevens te kloppen. De oude man die in mijn huis woonde voordat ik het kocht, was blijkbaar een brave betaler, want ik heb nooit last gehad van zijn digitale schaduw. Behalve dat ik nog jaren brieven en rekeningen op zijn naam bleef ontvangen. Een paar keer kreeg ik ook een kerstpakket, dat was dan wel weer aardig.

Ik ben benieuwd of Kraaij als handelaar in persoonsgegevens Experian kent. Hij blijkt ervaring te hebben met een onderneming die door Experian is overgenomen. 'Ik parkeerde

mijn auto voor de deur en vroeg om bepaalde informatie, overigens niet onder mijn eigen naam,' zegt Kraaij. 'In die korte tijd hadden ze blijkbaar mijn kenteken nagetrokken, want ze kwamen melden dat ik meneer Van den Berg niet was. Dat was de eerste keer dat ik ondervond hoeveel instanties over me weten, zelfs als ik een valse naam gebruik.'

Als handelaar in persoonsgegevens wist Kraaij ook behoorlijk veel over de mensen die hij moest natrekken. Hij laat me een paar van zijn standaard 'verhaalrapporten' zien. De meeste tellen zo'n vijf pagina's en dan staan er zinnen in als 'Er is een telefoonaansluiting met een geheim nummer'. En dan wordt het geheime nummer vermeld. Verder nog waar die persoon werkt, of hij in gemeenschap van goederen is getrouwd, wat zijn netto-inkomen is en bij welke banken hij een rekening heeft.

'Toen de politie me van fraude verdacht en ging aftappen, groeide de informatie de agenten boven het hoofd,' zegt Kraaij. 'Mijn dossier telde 1200 pagina's, inclusief de taps. Wil je er een paar zien? Die geven letterlijk weer hoe ik aan die informatie kwam.'

Ik pak een van de politietaps aan. Na allerlei coderingen lees ik het begin van het gesprek:

> 'Michel belt ABN Amro in Bennebroek. Hij krijgt ene Hilda aan de lijn. Michel stelt zich voor als Peter. Hij zegt dat hij een overschrijving heeft, maar dat de opdrachtgever vergeten is het rekeningnummer in te vullen. Hilda geeft het rekeningnummer door en Michel vraagt of er toevallig ook een telefoonnummer bij staat. Hilda gaat even kijken in het andere systeem. Het telefoonnummer is 0229-... Vervolgens

geeft Michel nog een postcode en huisnummer door. Hilda geeft het volgende rekeningnummer door.'

Een ander tapgesprek is mogelijk nog curieuzer. Kraaij belt namens Ordina Sociale Zekerheid met ene Bianca van het UWV. Ze geeft hem heel veel sofinummers door en laat ook weten of die mensen een dienstverband hebben.

Ik leg het blaadje met het tapverhoor neer. 'Dus een medewerker van het UWV geeft je in slechts één gesprek 150 sofinummers door?'

'Ja, ik hing zo'n drie kwartier aan de lijn om die op te schrijven.'

'Moest je het vooral van zulke mutsen hebben?'

Kraaij kijkt beledigd: 'Nee hoor, de meeste medewerkers die ik aan de lijn kreeg, waren heel behulpzaam. Ik moest ze gewoon laten praten om niet te veel argwaan te wekken. Een keer belde ik namens een vrouw, terwijl ik dacht dat die naam bij een man hoorde. De medewerker aan de andere kant zei meteen: "U klinkt niet als een vrouw."

"Ik heb me recentelijk om laten bouwen," antwoordde ik. Ik kuchte even en vervormde meteen mijn stem. Toen kreeg ik de gevraagde informatie.'

'Hmm, een omgebouwde handelaar in persoonsgegevens.'

'Waarom niet?' lacht Kraaij. 'Alles is mogelijk.'

5

Antihackmaatregelen

De dag dat ik met Rickey afgesproken heb nadert en ik word steeds zenuwachtiger. Ik ken hem tenslotte helemaal niet en ik ga hem al mijn informatie in mijn computer toevertrouwen. Van wachtwoorden voor webshops tot bankrekeningen en van correspondentie met mensen tot de foto's van mijn kinderen. Ik ben zelf al behoorlijk veel in de publiciteit geweest, bijna standaard na elk boek, maar mijn gezin heb ik er grotendeels buiten gehouden. Mijn man is heel huiverig als het om privacy gaat. Nu geef ik iemand de sleutel tot alle bestanden. Of althans de toestemming om die sleutel te gebruiken als hij die vindt.

Voor de zekerheid pas ik mijn wachtwoord aan. Nu is het niet meer zo simpel. Voor mijn gevoel was het al niet simpel, want ik gebruikte geen bestaand woord, maar volgens mijn man kon het veel beter.

Computerspecialisten staan versteld over hoe vaak mensen gewone woorden als wachtwoord gebruiken. Bijvoorbeeld 'geheim', 'wachtwoord' of 'toegang'. Willekeurig iets uit het woordenboek kiezen biedt overigens net zo weinig bescherming, want de computerprogramma's van hackers screenen eerst alle woorden uit het woordenboek. Als een hacker een wachtwoord ontcijfert, dan past deze sleutel meestal op meerdere 'deuren', want veel mensen gebruiken hetzelfde wachtwoord voor meerdere sites. Ik ook trouwens, laat ik dat maar eerlijk toegeven.

In de Verenigde Staten kun je je tegen identiteitsfraude verzekeren. De verzekering probeert preventief op te sporen of iemand gebruikmaakt van je identiteit door honderden publieke bronnen van informatie op misbruik te scannen. Een van de verzekeraars werft met de tekst: 'Je bent uniek, zorg ervoor dat het zo blijft.'

Tja, ik ben uniek, maar zo moeilijk is het niet meer om me te klonen als iemand een van mijn wachtwoorden steelt. Wil ik dit voorkomen, dan moet ik in de toekomst een speciale pil slikken. Ik weet dat het gek klinkt, maar de ontwikkelingen staan niet stil en er wordt al met een wachtwoordpil geëxperimenteerd door Googledochter Motorola. Je hoeft hem alleen maar te slikken om toegang te krijgen tot je pc of tot je bankrekening als je bij een pinautomaat staat. Ook al ben ik een groot voorstander van 'gemak dient de mens', ik zie er toch tegen op om een pil te slikken waarin een chip en een zendertje zitten. Best een geinige uitvinding dat je maagzuur als brandstof voor dat minuscule computertje werkt, maar ik vind het toch gek dat ik min of meer gerobotiseerd moet worden zodat ze mijn identiteit niet stelen. Motorola heeft natuurlijk een veel fraaier verhaal bij de uitvinding: de wachtwoordpil voorkomt fraude en bespaart ons tijd. We schijnen gemiddeld 39 keer per dag ergens in te loggen. En als je tot de zware computergebruikers behoort, kan dat oplopen tot honderd keer per dag. Geen idee of ik tot de zware computergebruikers behoor, maar mijn man heeft mijn computer zo ingesteld dat ik elke keer weer in moet loggen. Uit veiligheidsoverwegingen uiteraard, maar dat betekent dat ik elke keer als ik de vaatwasser afgeruimd heb of de krant heb gelezen opnieuw een wachtwoord in moet typen. Gelukkig hoef ik maar zeven tekens in te typen en die kan ik inmiddels wel dromen. Dus ik wacht nog even met de wachtwoordpil. Die is trouwens ook nog niet op de markt, maar in Amerika mogen ze die al op mensen testen.

Als alternatief kan ik een tatoeage met sensoren en een antenne overwegen. Hoe hip wil je zijn? De bedenkers denken dat het vooral bij jongeren aanslaat, een stoere tattoo die

al je wachtwoorden onthoudt. En die de ouders vast heel lelijk vinden, maar ja, dat maakt het natuurlijk nog aantrekkelijker. Mijn pubers maken zich echter geen grote zorgen om hun digitale veiligheid. Dat hebben ze vast van mij en niet van hun vader.

Ik weet niet hoe veilig mijn wachtwoorden voor hackers zijn zonder een wachtwoordpil, maar voor een tap van de politie blijk ik bepaald niet veilig. Er zijn programma's die op basis van je socialmediacontacten berekenen hoe groot de kans is dat je afgeluisterd wordt. Met 23.000 volgers op Twitter en duizenden contacten op LinkedIn en Facebook is mijn uitkomst niet zo verrassend: honderd procent kans dat ik nu of in de toekomst afgetapt word.

De officier van justitie moet altijd toestemming geven om iemand af te tappen, maar daarvoor hoef je niet zelf verdacht te zijn. Geregeld contact hebben met een verdachte is al voldoende. Via de social media word ik door de vaagste types benaderd. En ik reageer altijd, omdat ik niet arrogant wil lijken. Als ze opnieuw schrijven, reageer ik weer, ook al probeer ik het op een vriendelijke manier af te kappen. Kun je een verdenking creëren door onschuldige informatie aan elkaar te koppelen en dingen verkeerd te interpreteren? De experts zijn eensgezind: ja. Tunnelvisie bij Justitie is geen onbekend fenomeen. En er zijn steeds meer data beschikbaar die aan elkaar gekoppeld kunnen worden.

Dus honderd procent kans dat ik nu of in de toekomst afgeluisterd word? Misschien zou dat geen verrassing moeten zijn, maar toch schrik ik van de uitkomst van deze test. Als brave burger vind ik het een griezelig idee. Het tolerante

Nederland is afluisterland nummer één ter wereld met zo'n tweeduizend afgeluisterde telefoons per dag. In de meeste andere landen wordt dat als een te grove inbreuk op de privacy gezien en nauwelijks toegepast. Hier doen niet zo veel mensen moeilijk als het om de politie als hacker gaat, niet bij telefoons en ook niet op het internet.

Ik vind het geen prettig idee dat de overheid mee kan lezen wat ik typ en alle door mij bezochte websites kan zien. Uit nieuwsgierigheid en voor research beland ik soms op foute sites en ik ben benieuwd wat voor risicoprofiel ik dan krijg. Mijn zoon speelde laatst op mijn computer en kwam met een paar muisklikken op een site met allemaal wapens.

'Cool, mama, ik heb nog nooit zo veel wapens gezien.'

Ik vond het helemaal niet cool, maar het staat vast mooi in mijn risicoprofiel: heeft onlangs ook een site voor wapens bezocht.

Als brave burger denk ik nog steeds dat de kans dat ik ooit in de bak beland nihil is, maar Nederland heeft de twijfelachtige eer om van alle EU-landen het vaakst onschuldige mensen op te pakken. In tien jaar tijd hebben we met z'n allen 79 miljoen euro betaald aan schadevergoeding voor mensen die ten onrechte hebben vastgezeten.

6

Leeggeplunderd

Rickey stuurt me een berichtje: 'Wat voor computer heb je?'

'Een Apple.'

'Dan weet ik niet zeker of het doorgaat. Ik ben gespecialiseerd in Windows. Niet dat de Applecomputers zoveel moeilijker te hacken zijn, maar ik heb me er niet mee bezig-gehouden.'

Koortsachtig denk ik na. Alles leek in kannen en kruiken en nu dreigt mijn droomhacker me in de steek te laten. Opeens bedenk ik dat ik nog een oude laptop heb die op Windows draait. Waarom heb ik daar niet eerder aan gedacht? Daar staat vrijwel geen gevoelige informatie op.

'Ik stuur je een e-mail vanaf een Windowslaptop,' zeg ik tegen Rickey. 'Die wordt je doelwit. Die gebruik ik overigens niet draadloos en die is ook beveiligd met een wachtwoord. Dat maakt het waarschijnlijk iets moeilijker voor je. Ik ga vanavond eerst alle blote foto's van mij van die laptop verwijderen.'

'Hoeft niet. DIE HEB IK AL,' verschijnt er in grote letters op mijn scherm.

Lolbroek.

Ik check wat er op de laptop staat: veel vakantiefoto's, maar verder geen belangrijke informatie. Mijn zoontje is net begonnen met een werkstuk voor school. Best een bijzonder onderwerp: de pissebed. Rickey verwacht vast geen informatie over pissebedden. Ik krijg steeds meer pret bij de gedachte dat hij juist dat soort teksten te zien krijgt. Een paar gehackte pissebedden, dat kan geen kwaad. Dan kan Rickey zien dat de mannetjespissebedden een groot probleem hebben, want de vrouwtjes kunnen bevallen zonder te paren.

Wat ook best geinig is: de pissebedden plassen niet en drinken water met hun achterwerk. Rickey kan zich hier hopelijk mee vermaken, want de vakantiefoto's ga ik wissen.

Op dat moment rinkelt de telefoon en mijn glimlach is snel verdwenen als ik hoor hoe overstuur mijn vriendin Marjan klinkt.

'Ze hebben mijn rekening leeggeplunderd. Wat moet ik doen?'

'Wie zijn "ze"?'

'Alsof ik dat weet,' reageert Marjan. 'Tijdens het internetbankieren kreeg ik een foutmelding op de bankpagina. Ik logde opnieuw in en even later was al mijn geld verdwenen. Ik heb even op internet gezocht hoe dat kan. Waarschijnlijk had ik een banking Trojan-virus in mijn computer.'

'En je hebt niet je gegevens in een of ander phishing-mailtje ingevoerd?'

'Uiteraard niet,' protesteert Marjan. 'Waar zie je me voor aan? Met de site van de bank leek ook niets mis. Die was versleuteld. Daar let ik altijd op.'

'Wat vervelend. Maar waarschijnlijk krijg je de schade vergoed.'

'Dat is maar de vraag,' zegt Marjan.

Ik vraag me af hoe Marjan aan zo'n Trojaans paard is gekomen. Ik ken haar als een vrij voorzichtig iemand, ze klikt niet zomaar op vreemde linkjes. Maar ja, besmette linkjes vind je overal, zelfs betrouwbare sites als Nu.nl en Telegraaf.nl bleken een virus opgelopen te hebben die de nietsvermoedende bezoekers verder verspreidden. Misschien heeft Marjan het ook via een betrouwbare site in haar computer binnengehaald. Met zo'n virus is het voor criminelen een fluitje van een cent om haar internetgedrag te bespioneren en be-

dragen weg te sluizen als ze gaat internetbankieren. Een virusscanner helpt niet, want de nieuwste malware wordt niet herkend. De duizend euro die je overmaakt, is opeens vijfduizend geworden en de rekening van de ontvanger is veranderd.

De Europese toezichtorganisatie ENISA zegt dat de banken ervan uit moeten gaan dat alle computers besmet zijn, maar dat doen ze dus niet. Ze worden juist strenger en verschuiven de aansprakelijkheid naar de consument, omdat internetcriminaliteit ze klauwen met geld kost. Alle banken eisen dat je zelfs op vakantie je saldo controleert, want dat moet je elke twee weken doen. Anders ben je 'grof nalatig' en kun je bij fraude zelf voor de schade opdraaien. Maar de meeste mensen lezen niet de kleine lettertjes waarin staat dat ze eens per twee weken moeten inloggen.

Ik vind het belachelijk dat de banken ons kunnen verplichten om op vakantie te computeren. Even offline zijn is heerlijk en het laatste waar ik aan denk is mijn saldo checken. Veel mensen doen het via draadloze netwerken waardoor cybercriminelen met gemak je hele dataverkeer onderscheppen en dan zijn de consumenten weer de pineut.

Tot voor kort vertikte ik het om laptops en iPads op vakantie mee te slepen, maar daar ben ik van teruggekomen. Niet vanwege het checken van mijn banksaldo trouwens, dat doe ik nog steeds niet, maar ik merkte dat mensen van je verwachten dat je op z'n minst je e-mails beantwoordt en als het even kan ook op vragen via social media reageert, zelf doen ze het tenslotte ook. Velen schijnen verslaafd te zijn aan hun inbox en dat heeft zelfs al een naam gekregen: internet addiction disorder, een psychische aandoening.

Ik ben niet verslaafd aan mijn inbox, maar de reden dat

ik die ook tijdens vakantie begin te checken, is dat ik anders na thuiskomst honderden berichten moet afhandelen. Alles in de virtuele prullenbak kieperen gaat niet, want er zitten ook belangrijke dingen tussen, maar die kun je niet vinden als je niet alles doorneemt. Degene die een manier verzint om automatisch het kaf van het koren te scheiden, wordt vast miljonair.

Natuurlijk kun je de standaard 'out of office'-mededeling terugsturen, maar dat kan pas nadat je een mail hebt ontvangen en die blijft gewoon op je wachten. Eigenlijk ben ik een voorstander van een radicalere oplossing, een tekst die bijvoorbeeld luidt: 'Tot 20 augustus is deze mailbox gesloten en alle e-mails worden automatisch vernietigd.' Ik geef toe dat het niet zo vriendelijk klinkt, maar als we het met z'n allen doen, dan wordt het vast snel geaccepteerd en dan kunnen we na de vakantie weer rustig beginnen met werken, zonder in de e-mailstress te schieten. Bill Gates krijgt trouwens vier miljoen e-mails per dag, maar hij heeft een complete afdeling personeel in dienst om die te selecteren en te ordenen.

Zo'n zeventig procent van al het e-mailverkeer schijnt spam te zijn, maar gelukkig houden de providers de meest evidente exemplaren tegen. Toch klik ik nog steeds dagelijks verdachte e-mails weg. Als ik er al weer eentje ontvang, blijven mijn ogen iets langer op de inhoud gefixeerd. Dit mailtje is zo slecht geschreven dat ik het haast aandoenlijk vind.

'Geachte klant,
Wanneer we ontdekken onregelmatige activiteiten, om ons te helpen te voorkomen criminaliteit, moeten we uw identiteit te bevestigen. Dit betekent bewijzen

> die je bent en waar je woont. In eerste instantie gebruik gemaakt van een online verificatie en indien dit succes, dat is alles wat we moeten doen. Met betrekking tot dit klik HIER om te bevestigen je identiteit. Internet Support Team ABN Amro.'

Met een glimlach op mijn gezicht klik ik het weg. Met zo'n beroerde vertaling kunnen ze waarschijnlijk niet eens een tachtigjarige digibeet verleiden om zijn inloggegevens bij de bank prijs te geven. Toch boeken de cybercriminelen opvallend vaak succes, zelfs na vertaling met Google Translate, die er niets van bakt.

Geld is tegenwoordig niets meer dan data opgeslagen in elektronische bits en bytes. Wie de macht over de computers heeft, heeft de macht over de economie. De banken nemen elk jaar miljardenverliezen door cybercrime voor lief om het vertrouwen van de consument niet kwijt te raken.

Alweer een 'ping'. Op mijn scherm verschijnt een waarschuwing dat oplichters nep-mails versturen namens ABN Amro. De bank vraagt om medewerking, ik moet voor de zekerheid mijn oude gegevens ter controle invoeren.

Uiteraard is dat opnieuw een e-mail van dezelfde oplichters, alleen de manier van schrijven is een stuk professioneler. Deze keer trappen er vast meer mensen in en worden hun rekeningen leeggetrokken. Dat gebeurt elke dag, ondanks alle waarschuwingen.

Soms snak ik naar de goede oude tijd, toen phishing nog een onbekend fenomeen was en de spam nog zo onschuldig: goedkope Rolexen, middeltjes voor eindeloze erectie of een gratis universitair diploma. De huidige spam is heel tricky.

Je volgt de berichten over een concert en opeens zie je op Twitter een link met foto's. Leuk! Als je erop klikt, zie je helemaal geen foto's, maar reclame. Je klikt die geërgerd weg en denkt dat er niets aan de hand is, maar door dat ene klikje heb je ze toegang gegeven tot je computer. En dan zie je jezelf tweets versturen over afslankmiddelen. Voordat ik het zelf doorheb, heb ik al heel wat argeloze slachtoffers besmet, die op hun beurt andere mensen besmetten. En met slechts 23.000 volgers ben ik nog redelijk onschuldig. Het account van Lady Gaga werd ook gehackt. Haar miljoenen volgers ontvingen tweets waarin gratis Appleproducten werden beloofd. Binnen de kortste keren klikten duizenden mensen op de besmette linkjes.

Als je denkt dat spam redelijk onschuldig is omdat de meeste weldenkende mensen die wegklikken, dan is de statistiek over de bestedingen naar aanleiding van spam vast een eye-opener: 160.000 euro per dag. En dat is alleen het behaalde resultaat van slechts één spam-verzender: het Russische netwerk Glavmed.

Wie op zo'n link klikt, stelt meestal ongemerkt zijn computer beschikbaar om nog meer spam te verspreiden. Een klein netwerkje kan een miljoen spamberichten per uur verzenden. De Spaanse politie rolde een reusachtig spamnetwerk op: 12 miljoen geïnfecteerde computers in 190 landen. De politie betitelde de drie opgepakte Spanjaarden als 'beangstigend gewoon'. Ze hadden alle drie nog geen strafblad. Zo'n netwerk wordt onder meer gebruikt om belangrijke sites offline te zetten en de bedrijven te chanteren, net zo lang tot ze betalen. Hiermee worden miljoenen verdiend.

Terwijl we de deuren van onze huizen goed sluiten om inbrekers buiten te houden, doen we dat niet als we online zijn. Daarom gaan steeds meer criminelen digitaal inbreken. Genoeg open deuren. Sommige mensen weten niet hoe ze die moeten sluiten, andere denken nog steeds dat het hun niet zal overkomen. Ondertussen brengt cybercrime meer op dan de illegale handel in marihuana, cocaïne en heroïne samen. Als de fraude-industrie een staat was, dan was deze staat de vijfde sterkste economie ter wereld.

Mijn bankrekening kan leeggeplunderd worden, mijn pinpas nagemaakt en zelfs mijn auto kan gekloond worden. Een kennis maakte het onlangs mee. De kentekenplaten van zijn Renault Twingo werden gestolen. Hij ontdekte dat een dag later en deed aangifte. Toen kwamen er hoge bekeuringen voor snelheidsovertredingen en die moest hij betalen, want hij was even te laat met zijn aangifte. De dieven hadden de kentekenplaten ook voor een zwarte Twingo gebruikt. Precies dezelfde auto met precies hetzelfde kenteken, ga maar bewijzen dat die niet van jou is.

Identiteitsfraude is vrijwel altijd lonend en moeilijk aan te pakken. Ik ken alleen één geval waarbij het niet lonend bleek. Een automobilist gaf tijdens een verkeerscontrole in Den Haag een verkeerde naam en geboortedatum op om onder een bekeuring uit te komen. Het resultaat: dat bleek iemand te zijn die nog zeven bekeuringen open had staan.

7

Beroemd

Komt een vrouw bij de hacker... Rickey belt op en zegt dat hij op de afgesproken datum niet kan. Balen, want zo houdt hij mij nog langer in spanning of het lukt. We maken een nieuwe afspraak.

Ik zoek de narigheid vrijwillig op, maar als ik zelf een kwaadwillende nerd zou zijn, zou ik gericht te werk gaan. Gewoon een bankier privé hacken, iemand die net een bonusje van een miljoen heeft opgestreken in plaats van een schrijfster die anderhalve euro per boek verdient.

Uiteraard ben ik niet zo slim om als enige te bedenken dat er veel meer te halen valt bij dat soort mensen. Twee Amerikanen noteren de namen van het lijstje rijken uit het blad *Forbes*, sprokkelen vervolgens zo veel mogelijk persoonlijke gegevens van beroemdheden zoals Steven Spielberg en Oprah Winfrey bij elkaar, kruipen in hun huid en achterhalen hun creditcardnummers.

Hoe kom je in de computers van the rich and famous? Ik weet het niet zeker, maar de kans is groot dat ze ook gewoon de naam van hun lievelingsdier plus bijvoorbeeld hun trouwdatum als wachtwoord gebruiken. De meeste mensen delen heel veel persoonlijke informatie via social media en al hun voorkeuren leiden tot tips over mogelijke wachtwoorden. Beroemdheden delen misschien minder uit zichzelf, maar ze worden zo vaak geïnterviewd dat al die korreltjes informatie ook tot bruikbare tips leiden als je ze bij elkaar brengt.

De fraude komt pas aan het licht als de 32-jarige bedenker ervan 10 miljoen dollar wil overschrijven van de rekening van een van de slachtoffers. Wel stom dat je dat in één keer probeert af te schrijven; als niet-nerd had ik het in minder opvallende bedragen verdeeld.

De bank wordt bij dat bedrag achterdochtig en dat leidt tot een onderzoek. De arrestatie zou in een film niet misstaan: een politieman kruipt via het open dak van de rijdende auto van de crimineel naar binnen. De agent slaat hem in de handboeien, terwijl hij zelf ondersteboven hangt.

Je hoeft helemaal geen hacker te zijn om op een oneerlijke manier miljonair te worden met behulp van een computer. Een Belgische douanier ontdekt dat dit gewoon met een paar muisklikken kan. Tim D. heeft eerst financiële problemen en opeens bestelt hij flessen champagne van honderden euro's per stuk. Zijn uitbundige levensstijl begint op te vallen. Boze tongen fluisteren dat hij in de drugshandel zit, maar niemand heeft een idee wat en hoe. Tot Justitie na een tip onderzoek gaat doen. En zo ontdekken ze dat zeecontainers vol met drugs ongecontroleerd de haven verlaten. Tim D. krijgt informatie in welke containers partijen drugs zijn verstopt en vinkt in de computer aan dat de container reeds gecontroleerd is. Daarna kan de container gewoon door de criminelen opgehaald worden.

Inmiddels hebben heel veel mensen bewezen hoe simpel cybercrime in de praktijk werkt. Hackers krijgen steeds meer middelen in handen om je het leven zuur te maken. Maar veel hackers doen dat niet, ze noemen de criminelen 'crackers' om zich van hen te onderscheiden. Het lijkt me best leuk om een keer met een 'ethische hacker' af te spreken om te kijken wat er zo ethisch is aan hacken.

Na wat googelen valt mijn keus op Jeroen van Beek. Op de site van CNN zie ik dat hij enkele jaren geleden met een vervalst paspoort de modernste scanapparatuur op Schiphol

wist te misleiden. Het paspoort was voorzien van een foto van Elvis Presley en Jeroen had de chip zo gemanipuleerd dat de scanner de gegevens verifieerde. Leuke grap om als Elvis bij de douane te verschijnen, olie op het vuur voor al die mensen die geloven dat de King of Rock-'n-roll nog steeds leeft.

Jeroen wacht op me in een restaurant, hij heeft zijn laptop opengeklapt om me te laten zien hoe simpel het is om een persoon of een bedrijf te hacken. 'Als je niet steeds de nieuwste updates van je computerprogramma's uitvoert, dan ben je kwetsbaar,' zegt hij. 'Het simpelst is om iemand een e-mail met een uitnodiging te sturen voor iets wat voor hem mogelijk interessant is.'

'En hoe weet je dat dan?'

'Ik stuur je namens je uitgever een uitnodiging voor het Boekenbal, omdat ik weet dat je boeken schrijft. Klik je die wel of niet open?'

'Normaal gesproken stuurt de organisatie van het Boekenbal geen digitale uitnodigingen.'

'Maar ze gaan met de tijd mee. Klik je die wel of niet open?'

'Oké, waarschijnlijk wel.'

'Dan zit ik op dat moment in je computer, kan ik al je e-mails lezen, al je passwords zien en misschien zelfs een kopie van je paspoort vinden, want geloof het of niet, veel mensen hebben die ergens in hun computer opgeslagen.'

Hmm. Ik moet schuld bekennen. De laatste keer dat ik een kopie van mijn paspoort naar een instantie moest mailen, heb ik die daarna niet uit mijn computer verwijderd.

'Heb je je paspoort bij je?' vraagt Jeroen.

'Ja, maar wat moet je ermee?' Ik begin wantrouwender te worden.

'Ik wil het even zien.'

Als ik hem mijn paspoort geef, kijkt hij erin en noteert iets. Daarna legt hij mijn paspoort dicht op de tafel en plaatst zijn mobieltje erop. Het duurt slechts een paar seconden, dan laat Jeroen me het schermpje van zijn mobiel zien. De binnenkant van mijn paspoort is gescand, terwijl het paspoort niet open lag!

'Kijk,' zegt Jeroen. 'Alles is van een heel hoge resolutie, ik kan er zo een kopie van maken.' Hij vergroot mijn foto om het te laten zien.

Ik ben te verbaasd om te reageren. Ik staar naar mijn foto en bedenk opeens dat die in kleur is, terwijl de foto in mijn paspoort gewoon zwart-wit is. Ik sla de bladzijde open om dat te checken. Het klopt.

'Wat maf, je hebt mijn foto in kleur!'

Jeroen glimlacht. 'Sommige digitale kopieën zijn beter dan het papieren origineel. Mijn mobieltje heeft gewoon de gegevens uitgelezen die op de chip staan. Die chip hadden ze ooit bedacht om de paspoorten veiliger te maken.'

'Aha.'

'Overigens zijn de paspoorten vrij goed beveiligd vergeleken met bijvoorbeeld de ov-chipkaart en allerlei toegangspasjes tot bedrijven en instellingen. Als ik de chip van zo'n pasje kopieer en op een blanco pasje zet, dan heb ik onbeperkt toegang tot bijvoorbeeld ministeries.'

'Gaat het zo simpel?'

Jeroen knikt. 'De blanco pasjes zijn gewoon te koop, de software is gratis te downloaden.'

Jeroen wordt niet alleen ingehuurd om computersystemen te hacken, maar ook om kantoren binnen te komen met nagemaakte pasjes. 'Moet je het ongeloof op de gezich-

ten van de directie zien als ik eenmaal binnen ben,' zegt hij.

'Hoe weet zo'n directie dat ze je kunnen vertrouwen? Voor hetzelfde geld steel je gevoelige informatie.'

'Klopt, dat weten ze niet. Ik heb een verklaring van goed gedrag dat ik niet veroordeeld ben, maar verder...'

'Verder ben je niet te vertrouwen.'

'Ha, als ik jou was zou ik voor de zekerheid geen enkele hacker vertrouwen. En zeker niet de hackers die beweren dat ze te vertrouwen zijn,' glimlacht Jeroen. 'Maar in mijn geval is het simpel: ik heb een heel leuke baan, verdien prima als beveiligingsconsultant en zo loop ik ook geen risico om problemen met Justitie te krijgen. Als ik één uitglijder maak, dan is dat mooie leven voorbij.'

Ik moet even naar het toilet. Ik laat mijn tas altijd op de grond slingeren, maar deze keer neem ik die mee. Al die pasjes in mijn tas en iemand die ze in no time kan scannen lijkt me geen goede combinatie. Vertrouwen is goed, voorkomen nog beter, dat is tenslotte wat Jeroen me net probeerde te vertellen.

'Ik wil je iets anders laten zien,' zegt Jeroen als ik terug ben. 'Hoe slordig veel bedrijven met je persoonlijke gegevens omgaan.'

Hij typt in Google iets met 'filetype:pdf paspoort site.nl' en '1900'. Het hele scherm vult zich met persoonlijke gegevens en kopieën van paspoorten. Ik ben met stomheid geslagen, vooral als ik ook de naam van mijn notaris in die lijst zie staan.

Ik wijs op zijn naam. 'Dit kantoor ken ik. Daar heb ik het koopcontract voor mijn huis afgesloten.'

'Ha, wat toevallig,' zegt Jeroen. Hij zoomt verder in. 'Wat een prutser is dat, hij heeft zijn computers blijkbaar niet goed beveiligd, kijk maar: rijbewijsnummers, paspoorten, adressen. Op dat soort lekkende sites vind je alles wat banken vragen als ze je identiteit willen verifiëren.'

Niet te geloven, mijn notaris met zijn poenerige kantoor. Misschien moet ik die beste man een e-mail sturen dat ik hem geen duizenden euro's betaald heb om mijn gegevens te laten lekken.

Jeroen kijkt er helemaal niet van op. Voor hem is het business as usual.

'Minstens de helft van alle databanken is lek,' zegt hij.

'De helft? Maar dan zijn onze privégegevens toch helemaal niet veilig?'

'Klopt.'

Terwijl we nog druk aan het praten zijn, geeft de ober me een draadloos pinapparaat aan om de rekening mee te betalen.

'Zou je dat wel doen?' vraagt Jeroen. 'Draadloos betekent dat iedereen met een laptop het signaal uit de lucht kan plukken. Hoe weet je zeker dat ze je pincode niet onderscheppen?'

'Ik heb een keer een slimme tip gekregen, ik typ eerst een foute pincode in. Dan weet ik zeker dat ik verbinding met de bank heb.'

'Slim, maar dat is nog geen garantie, want ze kunnen bij de tweede poging ook je pincode onderscheppen.'

'Kan best, maar niet betalen vindt de ober vast niet leuk.'

Na de ontmoeting met Jeroen ben ik opeens heel zuinig op mijn identiteitspapieren. Waar zo'n ethische hacker al niet

goed voor is! Ik ben nog niet eens gehackt en ik begin mijn leven al te beteren. Maar het valt niet mee, want allerlei bedrijven en instanties vragen om een kopie van mijn legitimatiebewijs en ik weet niet wanneer dat wel en niet verplicht is. Hoe de instanties de kopieën bewaren, zodat ze niet in handen van criminelen vallen, is me helemaal onduidelijk. Voor de zekerheid schrijf ik erop dat het een kopie is en noteer ook wanneer die gemaakt is. Ik streep mijn burgerservicenummer nog even door, want meestal mogen ze dat nummer niet gebruiken. Geen kopie accepteren de instanties niet, maar een bekladde kopie wel.

Als mijn identiteit ooit gestolen wordt, merk ik het waarschijnlijk niet meteen. De meeste slachtoffers ontdekken het te laat. Hun vrienden ontvangen e-mails die ze niet verstuurd hebben, van hun rekening worden producten afgeschreven die ze nooit besteld hebben, ze ontvangen een brief van een deurwaarder of hun aanvraag voor een hypotheek wordt geweigerd vanwege schulden waar ze niets vanaf weten. Het kan ook op tal van andere manieren ontdekt worden, want sommige mensen blijken opeens op een ander adres bij de gemeente ingeschreven te staan of ze ontdekken dat iemand een uitkering op hun naam aangevraagd heeft, een nieuw profiel op social media aangemaakt heeft of hun computer verrijkt heeft met bestanden die ze niet kennen.

Ik durf mijn oude mobieltjes en computers niet meer aan een goed doel te schenken sinds ik laatst gelezen heb hoe gemakkelijk het is om gewiste gegevens te herstellen. Het hele adresboek en sms-verkeer op mijn mobieltje zijn terug te halen. Ook het leegmaken van de computer is redelijk zinloos, aangezien alles met een simpele internettool te her-

stellen is. Alleen de harddisk kapotmaken schijnt te helpen, maar dat is wel een radicale manier om baas over mijn gegevens te blijven.

Ik kijk mijn oude computer vertwijfeld aan. Durf ik het wel of niet? Hij staat al een tijdje in de weg en ik wil hem kwijt, maar ik heb nooit gedacht aan een gewelddadig afscheid. We hebben best goede tijden samen gehad. Toch moet ik het doen, om mijn eigen privacy te beschermen. Ik loop naar de garage en pak een hamer.

'Mam, ga je het echt doen?' vraagt mijn jongste zoon.

Ja dus. Meteen een goede manier om mijn kinderen te waarschuwen voor de digitale gevaren. Mijn goedbedoelde adviezen slaan ze waarschijnlijk in de wind, maar een moeder met een hamer maakt vast indruk op ze.

Daar gaat mijn computer, eerst openschroeven, de harde schijf eruit halen en vervolgens zo hard mogelijk slaan. Na enkele rake klappen is hij aan diggelen. Mijn kinderen kijken me met grote ogen aan. Als ik de hamer neerleg, durven die twee dichterbij te komen om de schade te inspecteren. Alles is nu weg: van mijn eerste onzekere passen op computergebied tot het manuscript van mijn eerste boek. Ik moet toegeven dat ik het best erg vind: sommige onbruikbare spullen hebben een sentimentele waarde, zelfs voor een notoire weggooier.

Als regelrechte flapuit vertel ik op social media dat ik mijn oude computer heb vernietigd en ook dat ik met een cybercrimeboek bezig ben. De reacties stromen binnen. Een vrouw vraagt of ze me mag bellen. Als ik haar mijn telefoonnummer doorgeef, belt ze meteen.

'Ik heb een groot probleem. Mijn ex laat van alles en nog wat op mijn adres bezorgen,' zegt zij.

'Dat kun je toch terugsturen?'

'Ik doe niets anders dan terugsturen. Wasmachines, bedden, banken... Je wilt niet weten hoe boos de bezorgers reageren. Alsof het mijn schuld is.'

'Ben je al naar de politie geweest?'

'Ze kunnen niets voor me doen, want ik kan niet bewijzen dat mijn ex al die spullen laat bezorgen. Ze willen niet eens mijn aangifte opnemen. Een paar keer moest ik de rembourskosten betalen. En ik denk dat dit pas het begin is.'

'Waarom doet hij dat?'

'Hij wil op de een of andere manier een rol in mijn leven blijven spelen. Mijn ex heeft me nu ingeschreven voor rijlessen, die je verplicht bent te betalen. Als je dat niet doet, sturen ze een deurwaarder. Bij het politiebureau halen ze alleen maar hun schouders op en zeggen dat dit soort dingen vaak gebeuren, maar dat ze daar weinig aan kunnen doen. De politie ontvangt gemiddeld 3500 meldingen van internetoplichting per maand. Kun je nagaan hoe hoog het aantal slachtoffers is, want veel mensen gaan helemaal niet naar de politie. Misschien hebben ze gelijk, want het kost je tijd en vaak schiet je er niets mee op.'

Ik kan haar geen goed advies geven. Navraag bij het Centraal Meldpunt Identiteitsfraude levert geen hoopgevende informatie op. 'Bij identiteitsfraude neemt de politie vaak geen aangifte op. Terwijl schuldeisers meestal een aangifte eisen. Zo zit je klem.'

Nou, fijn om te weten. Ik moet dus zorgen dat ik nooit een wraakzuchtige ex krijg. Misschien krijg ik dat wel voor elkaar, maar hoe zit het met niet-exen die het op je gemunt hebben? Niet omdat je zo interessant bent, maar omdat ze

via de Kamer van Koophandel heel gemakkelijk aan je gegevens kunnen komen als je een bedrijfje hebt.

Een van de mensen die reageren, jaagt me de stuipen op het lijf. 'Maandagmiddag kreeg ik een telefoontje van Vodafone,' schrijft ondernemer Dirk-Jan Huizingh. "Goedemiddag meneer Huizingh, rare vraag, u heeft niet toevallig vorige week drie nieuwe iPhones plus abonnementen besteld en veel gebeld dit weekend?" Uiteraard had ik dit niet gedaan. Eerst mensen aansluiten en daarna pas verifiëren, heel handig. Schadebedrag: drieduizend euro. Vodafone had een machtigingsformulier waarmee ik ene Roy K. machtig om namens mij te handelen. Voorzien van een handtekening die totaal niet overeenkwam met die van mij. Roy had ook een scan opgestuurd naar Vodafone van mijn paspoort. De grap is dat ik geen paspoort heb, maar een ID-kaart. Valser kon het haast niet, maar het werkte blijkbaar wel. De telefoons werden bezorgd op mijn kantooradres. Roy heeft de koerier opgewacht en ervoor getekend. De koerier had een scan van zijn ID-kaart gemaakt. Dat leek me dus een kant-en-klare zaak voor de politie, want nu wisten we wie Roy was.'

Als ik dat zo lees, dan krijg ik het idee dat de zaak toch minder gemakkelijk oplosbaar is dan het op het eerste gezicht lijkt. Dirk-Jan bevestigt mijn vermoedens. 'Met al die informatie ben ik naar de politie gegaan om aangifte te doen. Twee weken later kreeg ik een telefoontje of ik benadeeld was. Huh? Nou, de financiële schade was in dit geval voor Vodafone, maar deze grap heeft me wel veel tijd gekost en ik vind het beslist geen prettig idee dat iemand een nep-paspoort van me heeft. De politie had daar begrip voor, maar ze

konden meneer K. niet vinden. Hij stond al in hun systeem geregistreerd wegens andere oplichtingspraktijken. Hoe kan iemand onvindbaar zijn? Binnen no time had ik het 06-nummer van zijn vader op internet gevonden, alles op een presenteerblaadje. Maar de politie vond het niet nodig om contact met zijn vader te zoeken. Dat heb ik zelf even gedaan. Zijn vader reageerde niet verrast. Het laatste woord van de politie? "Tenzij u benadeeld wordt, bijvoorbeeld doordat deze meneer opnieuw uw identiteit misbruikt, doen wij er niets aan. Den Haag heeft ons andere prioriteiten meegegeven."

En dat was het. Te zot voor woorden. Iemand scoort mijn gegevens via het handige bestand van de Kamer van Koophandel, flanst een nep-paspoort in elkaar, stuurt dat naar Vodafone op, die niet de moeite neemt om mijn handtekening, geboorteplaats of wat dan ook te controleren en vervolgens eindig ik bij de politie, die ook andere prioriteiten blijkt te hebben. En dan zijn ze allemaal verbaasd dat honderden mensen per dag slachtoffer van identiteitsfraude worden. Hoe zou dat nu komen?'

Als ik twitter over hoe weinig grip je tegenwoordig op je privacy en identiteit hebt, adviseert iemand me om mijn postcode en huisnummer naar 8118 te sms'en. 'Dan zie je hoeveel informatie je binnenkrijgt. Die informatie kan iedereen over jou opvragen met een simpel sms'je.'

Ik pak mijn mobieltje en SMS de gegevens naar 8118. Vervolgens verschijnt de waarde van mijn huis op het scherm, hoe groot het huis is, wanneer het gebouwd is, voor hoeveel geld ik het ooit gekocht heb, en ook een schatting van hoeveel mijn huis nu waard is. Dat ik een gedeelte van mijn hypotheek al afbetaald heb, staat er nog net niet in, maar ik vind het nu al te veel informatie.

Mooi dat instanties informatie ontsluiten, maar niemand denkt aan de privacy. Databanken worden in een rap tempo aan elkaar gekoppeld. Zelfs als je anoniem op een internetforum reageert, weten ze vaak wie je bent. Een grote site stuurt me een brief van een commerciële organisatie die hun bestanden wil gebruiken voor 'wetenschappelijke analyse'. In die brief wordt duidelijk uitgelegd hoe die organisatie te werk gaat: 'Als gebruikers op meerdere websites een profiel of account hebben aangemaakt kunnen deze worden gekoppeld aan de hand van het e-mailadres, de gebruikersnaam of het IP-adres. Op basis van gekoppelde profielen kunnen systematisch data worden opgebouwd over deze personen.'

In de brief wordt bevestigd dat veel bekende forums deze organisatie al toestemming gegeven hebben om de data van de gebruikers te analyseren en te achterhalen wie er achter de anonieme profielen schuilgaan. Ik twijfel bij voorbaat aan het 'wetenschappelijke' karakter van een commercieel bedrijf, maar blijkbaar is dit niet iets wat de beheerders ter discussie stellen voordat ze onze gegevens vrijgeven.

Op het moment dat ik op internet kom, worden allerlei trackers wakker. Ze zitten op vrijwel alle bekende sites en volgen op de voet wat ik doe. Alles wat ze over mij aan informatie kunnen sprokkelen, slaan ze op. Heel veel bedrijven verdienen grof geld aan het verkopen van mijn persoonlijke gegevens. Dit is de grootste verborgen economie op internet.

Datajournalist Dimitri Tokmetzis nam de proef op de som met een nieuwe tool. Na nog geen minuut op nu.nl waren er al 29 trackers die met hem meekeken. Wat al die bedrijven met veelal onbekende namen precies aan gegevens verzamelen, weten we niet. Bekende sites geven ruiterlijk toe dat ze niet eens weten met welke derde partijen ze gege-

vens delen. Heb ik een keus? Nauwelijks. Soms weiger ik bepaalde cookies te accepteren en dan zegt een site: bekijk het maar, voor jou tien anderen die het geen probleem vinden dat hun voorkeuren opgeslagen worden. Bij sites die ik als betrouwbaar beschouw, accepteer ik de cookies, maar ja, hoe betrouwbaar zijn webmasters die geen idee hebben wat de adverteerders die me volgen met de verzamelde informatie doen? Volgens de wet zijn ze verplicht om dit aan mij door te geven. Dat wordt dan lastig bij iets wat je niet weet.

Stel dat je wist dat veel onbekende bedrijven achter de schermen informatie over je verzamelen, klik je dan nog steeds op 'ja, ik accepteer jullie cookies'? Misschien gaan iets meer mensen zich dan achter het oor krabben. Of misschien ook niet, want dit is wat de experts de 'privacyparadox' noemen. Mensen zeggen dat ze het verontrustend vinden dat trackers ze overal op de voet volgen, maar klikken zonder aarzeling en zonder verder te lezen op 'ja, ik accepteer cookies'. We accepteren nog veel ergere dingen uit naiviteit of onwetendheid. Elke dag worden zo'n vijfhonderd Nederlanders slachtoffer van identiteitsfraude. Wie denkt dat het vooral mensen met weinig kennis of een lagere opleiding betreft, komt bedrogen uit. Die zitten er ook tussen, maar de hoger opgeleiden trappen er twee keer zo vaak in. Er zijn heel veel slimme mensen die domme dingen doen met hun computer. Ze beantwoorden phishing mails en storten geld op rekeningen van criminelen die met een goed verhaal komen. Mannen overkomt het iets vaker dan vrouwen. Ik heb echt geen idee hoe dat komt. Zijn wij vrouwen voorzichtiger? Daar geloof ik niets van. Ik ben benieuwd wie een logische verklaring kan verzinnen.

8

Tussen de hackers

Zonder dat we het doorhebben, zijn we heel afhankelijk geworden van allerlei digitale apparaten die steeds geavanceerder worden. Bij televisies denk ik zelf niet aan virussen, maar via de meeste moderne tv's kun je tegenwoordig het internet op en dat betekent dat hackers ze net als gewone pc's met virussen kunnen besmetten. 'Simpele' apparaten zoals een printer zijn draadloos geworden en zo kan een kwaadwillende van een afstandje printopdrachten sturen en eerder geprinte documenten achterhalen. Ook meelezen met documenten die gescand worden is mogelijk.

Een webcam is ook op afstand te benaderen. Een crimineel kan je observeren zelfs op momenten dat je de webcam niet gebruikt. En via de microfoon kan hij meeluisteren.

De opmars van draadloze verbindingen met vrijwel elk apparaat lijkt niet te stuiten. Dat zorgt soms voor verrassingen. Er komt een vrouw bij de hacker en zij vraagt aan hem: 'Wat heb je vandaag gedaan?'

'Ik heb een wc via Bluetooth gehackt.'

'Au, tegenwoordig ben je ook nergens meer veilig. Maar wacht eens, ik snap het niet helemaal. Waarom moet een wc een Bluetoothverbinding hebben? De bedenker kan wat mij betreft de pot op.'

Waarom een wc met je mobieltje moet communiceren is voor mij ook een raadsel. De Japanse fabrikant Satis bedacht een luxe wc die door te spoelen is met een app. Geen idee wat de voordelen zijn, maar zodra het nieuws bekend werd, werd ook de luxe poeppot gehackt. Niet dat het veel voorstelt: met een wc kun je niet zo veel behalve eindeloos laten doorspoelen, maar grappig is het wel. Voor mij blijft de grote vraag: waarom moet een wc met apps communiceren? Volgens de hacker is het logisch: tegenwoordig communiceren

steeds meer apparaten met elkaar, dus waarom de wc niet? Het internet lijkt tenslotte ook verdacht veel op een ongefilterd riool.

Hackers kunnen de verwarming in je huis op bloedheet zetten, je garagedeur op afstand openen of je beveiligingsinstallatie uitschakelen. Probeer maar eens te doorgronden hoe dat werkt.

Vooral ouderen snappen er niets van. Ze krijgen een iPad van de familie cadeau om met de tijd mee te gaan en goede uitleg over hoe ze op de Facebookpagina van hun kleinkinderen kunnen kijken, maar geen uitleg over hoe ze zich tegen cybercriminelen kunnen beveiligen. We denken blijkbaar dat ze oud en wijs genoeg zijn. Misschien wel, maar niet als het om moderne apparatuur gaat. Soms ben ik uren bezig om mijn oma een of andere gadget uit te leggen en dan kijkt ze me nog steeds glazig aan. Op een gegeven moment heeft ze het wel begrepen, maar een week later weet ze niet meer precies hoe het moest.

Mijn oma is geen uitzondering. Ik moest smakelijk lachen toen ik laatst een berichtje in de krant las over een oude dame die steeds de alarmlijn 112 belde. De vrouw drukte de hele tijd op de afstandsbediening van haar televisie, maar kreeg die niet aan de praat. Ze bleek in plaats van de afstandsbediening haar mobiele telefoon in handen te hebben. Toen de politie een bezoekje aan de vrouw bracht, was ze opgelucht dat haar afstandsbediening niet kapot was.

Tien jaar geleden waren er zo'n vijftigduizend computervirussen. Dat aantal is inmiddels veertig miljoen. Virussen maken en verkopen is een winstgevende business geworden, maar wie zijn de makers? Op zoek naar het antwoord scoor

ik een kaartje voor een toonaangevende hackersconferentie. Aan de prijs te zien is het geen plek voor wannabe-hackers, want die zijn vast niet bereid om vele honderden euro's voor een kaartje te betalen.

Als journalist kom ik overal, van gevangenissen tot chocoladefabrieken, maar deze keer ben ik extra benieuwd. Hackers hebben mythische proporties in de ogen van een digibeet. Ik snap echt niet hoe die gasten wijs kunnen worden uit rijen cijfertjes en codes. Het gekke is dat ze hiermee grote banken miljoenen euro's lichter kunnen maken en de informatiesystemen van hele landen plat kunnen leggen, zoals in Estland en Georgië gebeurde. Niemand die dat kan voorkomen, want hun servers veranderen soms elke tien minuten van adres en locatie om ontraceerbaar te blijven. De gegevens worden steeds gewist en opnieuw opgebouwd.

De mogelijkheden van hackers zijn schier oneindig. Ze werken niet alleen aan de verkeerde kant van de wet, maar ook in opdracht van regeringen. Iedereen doet er geheimzinnig over, maar veel landen verzamelen informatie voor cyberaanvallen. Doelwitten zijn voorzieningen die veel burgers raken, zoals de banken, de telecom en het elektriciteitsnet. Veelzeggend is dat er al gesprekken zijn geweest tussen de Verenigde Naties, Amerika en Rusland over het beperken van het gebruik van internet voor militaire doelen.

Eigenlijk is digitale oorlogvoering helemaal niet zo moeilijk. Je verzint als geheime dienst een spel zoals Angry Birds, honderd miljoen mensen installeren het op hun smartphones en geven je onbeperkt toegang tot al hun contacten, netwerkverkeer en gps-gegevens. Ze kijken toch niet wie de maker is en in wiens handen al die informatie terechtkomt. Noch stellen ze vragen waarom je die gegevens nodig hebt

(meestal is dat niet voor de werking van het spel, maar de spelletjesmakers vragen de gegevens toch en ze krijgen ze).

Veel mensen downloaden gratis apps. De apps verzamelen bergen informatie over je. Ze hebben toegang tot praktisch alles, van je agenda tot je contactpersonen en van persoonlijke gegevens tot je locatie. Daarom krijg je advertenties van Amsterdamse bedrijven te zien als je in Amsterdam bent. Weigert een app-maker je locatie door te sluizen naar adverteerders, dan krijgt hij minstens de helft minder betaald.

Mijn smartphone maakt geregeld verbinding met diverse servers over de hele wereld, omdat er enkele bekende apps op staan. Dat wist ik wel, ik wist alleen niet hoe vaak dat gebeurde voordat de Britse zender Channel 4 een onderzoek deed om te laten zien hoeveel gegevens de consumenten 'lekken'. Een smartphone met 30 bekende apps wisselt tot 350.000 keer per dag gegevens uit met servers overal ter wereld. De informatie wordt vooral naar adverteerders doorgespeeld. Een telefoon die ongebruikt op tafel lag, maakte in nog geen uur al 30.000 maal verbinding met servers in onder andere de VS, Oekraïne, Singapore en China. Wat voor informatie de apps willen weten verschilt, maar sommige weten de unieke IMEI-code van je telefoon en kunnen constant volgen waar je bent.

We zijn bijna zonder het te beseffen heel afhankelijk geworden van mobieltjes en computers, we kunnen niet meer zonder. Ziekenhuizen, havens, vliegvelden, politiebureaus: ze functioneren dankzij computers, die vaak op Windows draaien zonder de laatste veiligheidsupdates. Terroristen of vijandige landen die deze systemen kunnen overnemen, hebben onze samenleving in een wurggreep.

In diverse gemeenten kan de bediening van gemalen, bruggen en sluizen via internet door kwaadwillenden overgenomen worden. Drinkwatervoorziening, energieopwekking, chemie en transport werken vaak met verouderde computersystemen. Hackers kunnen met een vrij simpele aanval deze systemen verstoren.

Servers die gebruikt worden voor criminele doeleinden, worden op de naam van nietsvermoedende burgers gehuurd. Zo wissen de daders hun sporen uit. Om met beveiligingsondernemer Kaspersky te spreken: 'Hoe wilt u een Chinese hacker vinden die Russische spionagesoftware op een server in Tonga laat draaien en de gestolen gegevens opslaat bij een provider op de Kaaimaneilanden?'

Op de internationale hackersconferentie hoop ik ze wel te vinden, want volgens het persbericht komen er honderden hackers uit allerlei landen. Ik moet zeggen dat ik het best spannend vind klinken: een digibeet tussen de hackers, alsof ik op een soort undercoveroperatie ga. Het liefst val ik niet op, maar ik heb geen idee wat hackers wel of niet dragen. Google weet vast raad, denk ik bij mezelf en ik typ mijn vraag zo concreet mogelijk in: 'Hoe kleden hackers zich?' Google heeft blijkbaar een inzinking, want in plaats van een stukje over favoriete kleding en accessoires krijg ik tips voor inrichting van een slaapkamer, een nieuwsbericht over een bekende overleden hacker en zelfs een link naar 'islam for dummy's'. Ik heb zelden zo'n verwarrende en curieuze top-tien gezien. Om niet per ongeluk op de islam-toer te gaan, laat ik Google voor wat het is en ga ik in mijn kledingkast kijken. Dat ik altijd zo goed nadenk over wat ik aantrek, heeft met een journalistiek trauma te maken. Toen ik net met het vak begonnen was, moest ik voor een artikel meevaren op een tanker. Zon-

der er goed over na te denken trok ik een rokje aan. Nooit geweten dat je op een tanker zo veel moet klimmen. De mannelijke bemanning hielp me een paar keer, maar ze vonden het in de meeste gevallen interessanter om onder aan de trap te blijven staan. Probeer maar eens op een steile ladder te klimmen en je benen bij elkaar te houden. Sindsdien bedenk ik me wel drie keer voordat ik weer iets aantrek wat wel bij mij past, maar niet bij mijn werk op dat moment.

Mijn vooroordelen over hackers zijn dat ze allemaal een brilletje hebben en zich slordig kleden. Een brilletje heb ik niet meer sinds ik mijn ogen heb laten laseren en als ik mijn kast open, zijn er maar weinig kledingstukken die in de categorie 'slordig' vallen. Ik ben nog steeds van de hoge hakken en de mooie jurkjes, al zijn ze niet meer zo kort als vroeger.

Uiteindelijk pak ik een zwarte broek en een groenige trui. Erg simpel, maar op de een of andere manier denk ik dat het geschikt zou kunnen zijn. Zelden heb ik er zo onopvallend uitgezien en heb ik zo lang voor de spiegel gestaan. Nu maar hopen dat het niet voor niets is geweest.

Voordat ik de deur uit ga, belt er iemand aan. Een pakketje. Het adres klopt, maar de naam niet. Voordat ik dat aan de postbode kan doorgeven, is hij uit het zicht verdwenen. Mooi is dat, nu zit er niets anders op dan het open te maken.

Ik pak een nieuwe laptop uit. Nog een computer in huis, over mijn lijk. Ons gezin is al gecomputeriseerd genoeg, dus sluit ik uit dat een van ons deze laptop bij Wehkamp besteld heeft. Maar wie dan wel? De naam op de factuur is van dezelfde onbekende vrouw en het adres is van mij. Op-

eens herinner ik me dat ik een keer iets gelezen heb over een soortgelijke truc met verkeerd bezorgde pakjes.

En dan gaat de bel. Dezelfde bezorger verschijnt aan de deur.

'Ik heb hier net een pakje bezorgd, maar dat is voor iemand anders.'

'Ja, maar ik zag dat de factuur op mijn adres staat.'

'Dat is een foutje, ik heb het goede adres al.'

'Prima, maar ik ga u het pakje niet geven.'

'Hoezo?' De bezorger kijkt me perplex aan.

'Ik stuur het pakje liever zelf terug naar Wehkamp. Dan heb ik bewijs.'

'Maar dat gaat u geld kosten, dan moet u zelf de porto betalen.'

'Anders gaat het me waarschijnlijk nog veel meer geld kosten. Ik regel het dus zelf. Een prettige dag verder.'

De man kijkt me eerst niet-begrijpend aan. Daarna wordt hij boos omdat ik hem in zijn werk frustreer. Nu twijfel ik er niet langer aan dat het om een oplichterstruc gaat: alles wijst erop. Nou ja, 'alles' is alleen een verkeerde naam, maar gekoppeld aan mijn adres kan dat betekenen dat het postorderbedrijf straks bij mij aanklopt voor de rekening. Dan moet ik zien te bewijzen dat ik de laptop niet heb. Het is je eigen schuld als je ontvangen spullen aan een vreemde meegeeft. Iedereen kan zich tenslotte als bezorger voordoen.

9

Kwetsbaar

'Wil je je webcam aanzetten?

'Nee, ik vind het nog te vroeg.'

'Dan ga ik je computer hacken. Maar je kunt natuurlijk ook je webcam aanzetten en even voor mij strippen.'

'Dat meen je niet!'

Dat meende hij wel.

Ik heb het gelukkig niet zelf meegemaakt. Een kennis wel. Haar vriendinnen kregen vreemde berichten. Ook haar Hotmail deed het niet meer. De hacker had al haar e-mails gelezen en stuurde haar weer een bericht.

'Strippen en je krijgt je wachtwoord terug.'

Sommige hackers hacken websites om persoonlijke gegevens te krijgen, ze lezen je e-mails en persen je af als ze bijzondere berichten tegenkomen, ze passen de tekst van je website aan of zorgen dat de hele inhoud van je website verdwijnt. Het probleem is dat ze op zo veel verschillende manieren in je computer kunnen komen dat het haast onmogelijk is om je overal tegen te wapenen. Ze gebruiken bijvoorbeeld namen van je vrienden op Facebook en sturen je een berichtje. Als je erop klikt, installeert je computer software waarmee de hackers alle belangrijke gegevens kunnen kopiëren. Uit onderzoeken blijkt dat de meeste internetters vroeg of laat slachtoffer van cybercrime zullen worden als de huidige trend doorzet.

De hackersconferentie is in Hotel Okura in Amsterdam. Ik arriveer vlak voor de lunch. Bij hackers denk ik aan gasten die snel een broodje wegwerken om weer achter de computer te kruipen, maar in het Okura is er geen sprake van een simpele broodjeslunch. Er is zelfs kaviaar. Zo te zien kunnen de hackers die niet waarderen, dus lunch ik met heel veel ka-

viaar. Ondertussen bekijk ik zo onopvallend mogelijk iedereen die voorbijloopt. De slordig geklede hackers zijn in de meerderheid, maar ik zie ook best veel mannen in pakken. En er zijn net zo veel hackers met bril als zonder bril, over vooroordelen gesproken...

In een grote zaal vindt een internationale wedstrijd plaats. Teams van drie hackers per land hebben opdrachten gekregen zoals zo snel mogelijk een website hacken of een programma downloaden en raden wat het doet. 'Hacken is niets anders dan begrijpen hoe iets werkt en dat gebruiken op een manier die ze niet verwachten,' zegt Dirk van Veen, die namens de organisatie een oogje in het zeil houdt. De hackers staren naar de computers en proberen dingen uit. Rijen met cijfertjes en codes schieten voorbij. Ze zijn de dag ervoor begonnen en ze doen dat acht uur per dag non-stop.

'Krijgen ze geen vierkante ogen?' vraag ik.

Dirk haalt zijn schouders op: 'Ach, die hebben ze allang.'

Ik zie dat veel hackers een drankje drinken dat ik niet ken. Als ik het etiket van het flesje bestudeer, begrijp ik waarom het hier zo populair is. Er zit vijf keer meer cafeïne in dan in een kop koffie en die hebben ze vast nodig om hun ogen na urenlang computeren open te houden.

Als digibeet ben ik bang dat ik de technische uitleg van tophackers tijdens de presentaties niet kan volgen, maar dat blijkt mee te vallen. Van al die codes begrijp ik inderdaad niets, maar wel hoe het werkt. In een van de zalen wordt bijvoorbeeld uitgelegd hoe je camera's kunt hacken die mensen kopen om hun huizen te beveiligen. De meeste zijn zo slecht beveiligd dat het mogelijk is om op afstand een extra gebruiker toe te voegen en te kijken wat er in de huizen gebeurt.

Ook de particuliere beveiligingsinstallaties blijken gemakkelijk te hacken. Iemand demonstreert hoe hij duizenden valse meldingen tegelijkertijd kan versturen, zodat de alarmcentrales en de politie compleet in de war raken. Daardoor gaan ze op dat moment ook niet op de echte inbraken af, want ze kunnen ze niet van nep-inbraken onderscheiden.

De engste demonstratie is misschien wel het hacken van de software van een vliegtuig. Daarmee kan de hacker vanaf de grond de besturing overnemen.

Verderop is er een zaal waar vooral leuke gadgets te zien zijn, zoals een zelfgemaakte 3D-printer. Ik krijg een roze plastic sleuteltje in handen gedrukt. 'Net gemaakt, voor het openen van politiehandboeien,' zegt de 25-jarige Peter-Paul.

'Je bedoelt voor speelgoedhandboeien?'

'Nee, het werkt op de echte politiehandboeien. Lijkt er niet op, hè?'

'Niet echt. Kan ik dat testen?'

'Ja, er loopt hier een beveiliger met handboeien rond. Misschien kun je het aan hem vragen.'

Gewapend met het roze plastic sleuteltje ga ik op zoek. De bewaker kijkt me glimlachend aan als hij me ziet aankomen.

'Je bent niet de eerste,' zegt hij. 'Net kwam ook iemand het testen. Het ziet er niet uit, maar het werkt echt.'

Tja, een roze plastic sleuteltje uit een printer kan alle politiehandboeien openen. De wereld verandert voor mij te snel, niets is wat het lijkt.

Als ik thuiskom, duwt mijn man een krantenartikel onder mijn neus. De titel is: 'Wilt u gehackt worden?' Omdat de schrijver niet verwacht dat iemand gehackt wil worden, geeft hij heel veel tips hoe je dat kunt voorkomen. Geen 123456

als wachtwoord gebruiken bijvoorbeeld. Dat doe ik gelukkig niet. Hackers maken elk jaar de meest gebruikte wachtwoorden openbaar om andere hackers te helpen. 'Password', '123456' en '12345678' schijnen al jaren favoriet te zijn. 'Jesus' en 'ninja' ook, maar die had ik zelf niet kunnen bedenken. Jesus, ik begrijp echt niet wie met het woord 'ninja' wil inloggen. 'Welcome' scoort ook hoog, omdat het vaak standaard wordt ingesteld op computers. Als je het niet wijzigt, dan zijn hackers inderdaad welkom.

Ik ben niet zo'n ster in het verzinnen van sterke wachtwoorden. Minimaal vijf keer achtereen iets nieuws, niet de naam van je partner, liefst helemaal niets wat voor een normaal mens leesbaar is en het moet uitroeptekens, cijfers en letters bevatten en als het even kan ook nog 34 toetsaanslagen lang zijn... Zucht. Leuk dat de beveiligingsexperts zulke dingen verzinnen, maar wie gaat zo'n wachtwoord onthouden? De meeste mensen kiezen voor iets simpels. Uit een onderzoek van Google blijkt dat niet alleen de namen van hun huisdieren hoog scoren als wachtwoord, maar ook de verjaardag van hun man of vrouw. Dat is vast omdat sommige partners anders vergeten wanneer dat is. Een stuk minder populair dan de namen van huisdieren zijn de namen van je eigen kinderen. Geen idee of dat iets zegt over de volgorde van belangrijkheid. Het grappigst vind ik dat ook de namen van exen als wachtwoord hoog scoren. Ik moet er niet aan denken om elke dag met exen geconfronteerd te worden, maar blijkbaar zijn er genoeg mensen die dat juist leuk vinden. Of ze wisselen zo vaak van partner dat het niet te doen is om steeds een nieuw wachtwoord te verzinnen.

'Heb je nou nog steeds geen nieuw wachtwoord?' vraagt mijn man. 'Ik zie dat je hetzelfde intypt.'

'Zeg, ik ga niet elke keer een nieuw wachtwoord verzinnen.'

'Nou, dat zul je wel moeten gezien je research.'

Ik weet dat hij gelijk heeft, maar ik vind het niet gemakkelijk om een sterk wachtwoord te verzinnen, laat staan om hetzelfde kunstje om de paar maanden te herhalen en ook nog bij meerdere sites. Uiteraard is daar iets op verzonnen: de Wachtwoord Wisselaar. 'Veel mensen zijn zich nauwelijks bewust van de risico's van gemakkelijk te achterhalen wachtwoorden,' staat er op de site. 'Klik op "start" en beantwoord een vijftal eenvoudige, persoonlijke vragen. De Wachtwoord Wisselaar combineert deze gegevens en laat je een veilige, unieke en sterke combinatie van letters, cijfers en tekens zien.'

Nou, ik ben heel benieuwd naar de vragen, maar vooral naar wat voor wachtwoord de computer me aanraadt. Daar komt vraag nummer één: 'Hoe heette je eerste liefde?'

Jeetje, dat weet ik niet meer, zo'n onuitwisbare indruk heeft-ie niet achtergelaten. Wat moet ik nou invullen? Eerlijkheid duurt het langst, toch? Ik vul 'Weet ik veel' in. Ik ben benieuwd of de computer 'Weetikveel' als een naam registreert.

Vraag twee is mogelijk nog erger: 'Wat is je streefgewicht?' Op een bepaalde leeftijd hoor je dat niet meer te vragen, maar ik geef al weer een eerlijk antwoord: 57 kilo.

Vraag drie is wederom lastig: 'Wat is je favoriete film?' Er zijn zo veel films die ik goed vind. Hoe kan ik een leuke komedie met een heftige actiefilm vergelijken? Ik besluit mijn keuze drastisch te beperken tot het onderwerp cybercrime en vul 'Het net' in, een van de eerste op internet gebaseerde films.

'In welke straat woon je?' vraagt de computer vervolgens. Eindelijk een vraag die ik zonder nadenken kan beantwoorden. Tot slot moet ik mijn favoriete teken uit een rijtje invullen. Zit niet veel soeps tussen, van sterretje tot dollarteken en van procent tot een uitroepteken. Een vraagteken past beter bij mij, maar dat staat er niet tussen. Dan maar het uitroepteken. En dan zijn we zover: mijn supersterke wachtwoord is klaar: Str57!hetn.

Eerlijk is eerlijk, zelf zou ik zoiets niet bedenken. Ik begrijp ook vrijwel meteen hoe het opgebouwd wordt: het Str van de naam van mijn straat, 57 van mijn streefgewicht (kan ik mooi elke dag aan denken), het uitroepteken dat ik niet wilde hebben en een afkorting van de filmtitel. Als ik die volgorde onthoud, dan is het geen slecht wachtwoord. Maar ja, nou heb ik het verraden, dus moet ik weer iets nieuws verzinnen.

Sommige mensen bedenken een ijzersterk wachtwoord, maar hebben er niets aan. Dat toont een jonge hacker, die een nep-website maakt en twitteraars belooft dat ze zouden kunnen zien hoeveel ze gemeen hebben met hun volgers. Als de slachtoffers inloggen, krijgt de opgetuigde nep-website toegang tot hun account. Bij het inlogscherm staat overigens letterlijk vermeld dat de website de mogelijkheid krijgt te twitteren namens de gebruiker, maar voor 20.000 twitteraars is dat toch geen belemmering om hun inloggegevens achter te laten. Vervolgens stuurt de hacker vanaf hun account een tweet met de tekst 'Hoe slecht gaan mensen met hun twitteraccount om... groetjes Damiaan Reijnaers'.

Ik heb niet het idee dat ik onvoorzichtig bezig ben op internet en toch blijkt mijn website gehackt. Iedereen die de site

bezoekt krijgt een malware-melding en Google zet me op een soort zwarte lijst. Rickey? Als ik contact met hem zoek, zweert hij dat hij er niet achter zit.

'Ik ga niets doen voordat we elkaar ontmoeten,' zegt hij.

Fijn is dat. Ik heb een hacker geregeld, maar iemand anders is hem voor. En ik heb geen flauw idee wie erachter zit. Ik weet best dat het met duizenden websites gebeurt, maar op de een of andere manier denk ik steeds dat het mij niet overkomt. Wie is nou geïnteresseerd in een website met boeken, waar geen persoonlijke gegevens en bankrekeningen te halen zijn?

Als ik via social media vraag wie me kan helpen om het lek te dichten, melden zich meteen enkele kandidaten aan. Dat is nou waar digibeten goed in zijn: zich omringen met mensen die wel verstand van computers hebben.

Ik geef mijn wachtwoord uit handen aan de eerste de beste wizzkid, weliswaar met tegenzin, maar ik kan het probleem niet zelf oplossen, dus veel keus heb ik niet.

Het gewraakte bestandje blijkt gek genoeg nergens te vinden. Na enkele uren speuren gooit de wizzkid de handschoen in de ring. Dan neemt iemand anders het over. Maar ook die kan niets vinden. Google stuurt me ondertussen een rood schermpje dat er behoorlijk eng uitziet. Nou durft zeker niemand meer een bezoek aan mijn website te brengen. Tijd voor grover geschut. Zijn er mensen die echt veel, maar dan ook echt veel verstand van computers hebben?

Een nieuwe groep experts meldt zich via de social media aan. Deze keer ben ik vastbesloten om mijn wachtwoorden niet aan de eerste de beste te geven. Eentje stuurt me een bericht dat goed klinkt. 'Ik ben Holger, veertig jaar jong, en ik werk al sinds mijn twaalfde met computers. Op mijn ze-

ventiende was ik al senior programmeur bij een automatiseringsbedrijf. Ik spreek 10+ programmeertalen, maar mijn Nederlands is knudde ;-)).'

Aan zo iemand durf ik mijn wachtwoorden toe te vertrouwen. Dus Holger krijgt ze. Hij gaat meteen kijken wat er aan de hand is en niet veel later krijg ik een bericht:

'Jij hebt een virtuele soa opgelopen doordat een plug-in niet goed beschermd was tegen de boze buitenwereld. Mijn plan van aanpak is het volgende: je site gaat tijdelijk offline, zodat er geen nieuwe infecties teruggezet kunnen worden. Ik maak een back-up van alle data en verander de wachtwoorden. Daarna zorg ik dat de methode die ze hebben toegepast om de virus in je site te injecteren, dichtgaat.'

Een methode kan niet dichtgaan, maar Holger zei al dat zijn Nederlands knudde is en dat hij heel veel verstand van computers heeft, dus vertrouw ik hem. Virtuele soa, hoe verzin je het.

Holger is trouwens heel goed in uitleggen, want ik begrijp min of meer wat hij gaat doen. Hij legt elke stap heel netjes uit. 'Ik moet ieder bestand doorlezen om dingen die toegevoegd zijn aan je site weg te halen. Dit moet heel nauwkeurig gebeuren. Als er maar één achterblijft, steekt die de rest van de bestanden weer aan. Als ik denk dat ik helemaal klaar ben, maak ik nog een back-up van je schone site, zodat we iets hebben om op terug te vallen als die weer gehackt wordt.'

'Als die weer gehackt wordt? Nou, één keer vind ik meer dan genoeg, hoor. Ze blijven niet aan de gang.'

'Dat weet je nooit van tevoren,' reageert Holger. 'Ik heb het ook wel eens gedaan, maar ik test alleen op eigen sites of test sites met medeweten van de eigenaar uit. Program-

meurs maken vrijwel altijd fouten en daar profiteren de hackers van. Gemiddeld zitten er minstens tien programmeerfouten in elke duizend regels code.'

'En hoeveel regels heeft een programma?'

'Dat hangt natuurlijk van het programma af, maar een beetje software telt één miljoen regels en dat kan zelfs honderd miljoen regels zijn.'

Wow, dan zijn tien fouten per duizend regels opeens een grote berg.

Binnen een paar uur heeft Holger de besmette plug-in ontdekt en verwijderd. Ik hoef al die technische details niet te weten, maar ik ben wel benieuwd of ik dit had kunnen voorkomen.

'Moeilijk te zeggen,' reageert Holger. 'Ik denk dat er iemand is geweest die jou als testmodel heeft gebruikt om zo een grotere website te infecteren.'

Ik ben in elk geval gerustgesteld dat niemand het persoonlijk op mij gemunt heeft. Het is maar een van de vele virussen in cyberspace. Wij digibeten moeten er als eerste aan geloven en sommigen van ons zijn zo naïef dat ze zelfs voor virussen betalen. Wie op een foute link klikt, krijgt de boodschap dat zijn computer geïnfecteerd is en dat alleen een bepaald type software dit virus kan verwijderen. De software is gewoon een nieuw virus, maar mensen weten dat niet en betalen er graag veertig euro voor. Deze deal blijkt zo succesvol dat de bedenkers speciale callcentra moeten oprichten om alle belangstellenden te helpen. Bij het installeren van het nieuwe virus, welteverstaan.

10

Cyberlovers en nep-personen

Veel mensen laten zich bij het kopen van een product beinvloeden door reacties van andere gebruikers. Ik ook: iets wat slecht aangeschreven staat, koop ik gewoon niet. Ik vind het wel verwarrend dat de reacties soms zo uit elkaar lopen. Hoe kan nu een hotel van iemand een 10 krijgen en van een andere persoon een 1? En wat te doen als sommige lezers een boek de hemel in prijzen terwijl andere lezers het volledig afkraken, kopen of niet? Mensen zijn kuddedieren, daarom zijn beoordelingen van andere gebruikers blijkbaar belangrijk. Als de meeste mensen vijf sterren geven, dan is het blijkbaar goed. Dat kan best kloppen, ware het niet dat veel van die recensies nep zijn. Bedrijven waarvoor online aankopen belangrijk zijn, maken soms gebruik van software die betrouwbare nep-personen creëert. Ze krijgen een volledig profiel, inclusief een verzonnen naam, e-mailadres, website en socialmediaprofielen. De software zorgt ervoor dat deze 'social bots' reviews plaatsen waarin ze de producten van het bedrijf aanprijzen en die van de concurrentie afkraken.

Uit onderzoeken blijkt dat veel recensies van hotels, restaurants en mobieltjes nep zijn en toch laten we ons beïnvloeden. We zijn tenslotte niet getraind om de nep-recensies van de echte reacties te onderscheiden. Zelfs Wikipedia, de site die velen als een heel betrouwbare encyclopedie beschouwen, ontkomt er niet aan. Mensen blijken op grote schaal artikelen aan te passen in opdracht van bedrijven, uiteraard tegen betaling. Een bedrijf uit Texas had zich onder driehonderd valse identiteiten aangemeld om artikelen aan te passen en duizenden bedrijven bleken bereid voor zo'n dienst te betalen.

Bedrijven gebruiken nep-personen, maar andersom gebruiken nep-personen ook de bedrijven door bijvoorbeeld namens hen te bellen om naar gegevens te vissen. Verschillende vrienden en kennissen hebben het al meegemaakt en vertellen lachwekkende verhalen, waardoor ik me een beetje gepasseerd begin te voelen. Maar dan gebeurt het.

De man aan de andere kant van de lijn is van Microsoft en hij spreekt Engels met een zwaar accent. De digitale lekken in mijn Windowssoftware zijn een probleem, maar gelukkig kan dat op een simpele manier opgelost worden. Ik hoef alleen maar mijn computer op te starten en zijn aanwijzigen te volgen.

Afpoeieren wordt een makkie, denk ik bij mezelf, want als Applegebruiker heb ik niets met de software van Microsoft te maken. Maar ik vergis me in de volhardendheid van de man aan de andere kant van de lijn. Hij houdt voet bij stuk dat ik wel Microsoftsoftware in mijn computer heb en dat ik gevaar loop als ik de veiligheidslekken niet dicht.

De hele discussie is bijna lachwekkend. Het doet me denken aan de marketeers die je tijdens het eten opbellen om je een product dat je helemaal niet nodig hebt aan te smeren. Ze kunnen uiteraard niet van tevoren weten wat ik wel en niet nodig heb, maar met een klein beetje psychologische kennis kunnen ze zien of doordrammen nut heeft.

'Spreek ik met mevrouw Genova?'

'Ja.'

'Ik wil u graag wat vragen stellen over uw computer. Uit een recent onderzoek blijkt dat de meeste mensen te weinig...'

'Sorry, ik ben niet geïnteresseerd.'

'Mag ik vragen waarom niet?'

'Ik heb het al goed geregeld.'

'Maar we bieden u een gratis check aan.'

'Mooi, maar ik heb geen interesse, want ik heb niet zo lang geleden met een expert aan tafel gezeten.'

'Het kost u weinig tijd, mevrouw Genova, en zo weet u het zeker.'

'Ik heb gisteren een mooie zwarte bank op Marktplaats te koop gezet. Heeft u daar interesse in?'

Ik hoor stilte aan de andere kant van de lijn. De man is blijkbaar in de war. Mooi.

Dan zegt hij 'nee'. Maar ik heb al beet en ik ben niet van plan om zo gemakkelijk op te geven.

'Mag ik vragen waarom niet?'

De vervelende marketeer weet niet hoe snel hij de verbinding moet verbreken. Tof. De volgende commerciële beller ga ik vragen of hij interesse heeft in de fiets van mijn zoontje. En ik heb vast nog meer dingen te koop.

Jammer dat deze strategie niet bij een nep-beller van Microsoft werkt. De volgende keer zeg ik gewoon dat ik geen computer heb. Kijken of hij me er dan nog steeds van probeert te overtuigen dat de software van Microsoft ergens in mijn huis op de achtergrond draait. Ophangen kan natuurlijk ook, maar ik ken mensen die al voor de vijfde keer gebeld worden. Ik ga liever op zoek naar een manier om ze zo wanhopig te krijgen dat ze me op een zwarte lijst zetten.

Ik vind het best opmerkelijk dat ik als digibeet steeds serieuzer over mijn veiligheid online ga nadenken. Het kan dus wel. Soms heb ik het idee dat ik een beetje doordraai. Ik ben zo bedacht op besmette linkjes dat ik alle verdachte bestand-

jes direct wis. Dan krijg ik een boze opdrachtgever aan de lijn: ik blijk het contract voor een lezing voor spam aangezien te hebben en hij wacht al die tijd op mijn antwoord. De volgende keer dat ik niet zo paranoïde reageer en er wel op klik, is het vast wel een computervirus.

Wat ik opeens ook verwerpelijk vind, is het gemak waarmee instanties ons mogen controleren omwille van onze veiligheid. In een zwembad in Tilburg vragen ze zelfs om mijn vingerafdrukken. Wil ik geen vingerafdrukken afstaan? Dan mag ik niet zwemmen. Al die camera's die daar hangen zijn blijkbaar niet voldoende om mijn veiligheid te garanderen, alleen vingerafdrukken schijnen te werken. Alle klanten criminaliseren om een paar raddraaiers op te pakken, is dit de toekomst? Dat ik overal met camera's gevolgd word is tot daaraan toe, maar vingerafdrukken om te mogen zwemmen, vind ik net een stap te ver.

Als getrouwde vrouw blijft één ding me in elk geval bespaard: cybercrime via datingsites. Daar lopen steeds meer criminelen rond die met geloofwaardige verhalen naïeve slachtoffers geld ontfutselen. Het aantal slachtoffers van datingfraude is volgens de Fraudehelpdesk al de 40.000 gepasseerd. De verhalen zijn heel divers, maar de afloop is steeds hetzelfde. Een kapitein uit de US Army blijkt bijvoorbeeld een Nigeriaanse oplichter. Maar voordat het slachtoffer dat ontdekt, is ze vele duizenden euro's armer, want ze heeft hem een bedrag voorgeschoten om zichzelf van het leger vrij te kopen. In ruil daarvoor en als garantie kreeg zij beschikking over zijn pensioenrechten (documenten getekend door bestaande generaals, dat had ze allemaal gecheckt).

Een kennis was met ene Dana op internet aan het daten, maar kwam er per toeval achter dat Dana anders heette en

veel ouder was. Hij verbrak de prille relatie, maar Dana begon hem te bellen, soms 150 keer per nacht. Ze maakte accounts op zijn naam aan en mailde al zijn vrienden. Uiteindelijk werd ze opgepakt en kreeg ze een taakstraf. Het meest frustrerende voor mijn kennis was dat hij zelfs na haar veroordeling niet wist waarom ze dat deed. Hij is er ook niet gerust op dat deze vrouw niet zomaar opnieuw begint.

Voor sommige mensen is internet een uitlaatklep: ze kunnen eindelijk zijn wie ze willen zijn. In het echte leven is dat blijkbaar te moeilijk voor ze. Ze jagen wel de mensen die erachter komen de stuipen op het lijf, want ja, hoe normaal is het dat iemand zo veel moeite doet om zich als iemand anders voor te doen, en met welk doel?

Laatst maakte ik het zelf mee: ik trapte in het zielige verhaal van iemand op Twitter. Ze vroeg of ze me in vertrouwen kon nemen en toen volgde een verhaal over een bijzonder gruwelijk verleden. Ze was net gevlucht voor de mensen die haar seksueel misbruikten en voelde zich heel eenzaam. Ze had niemand om mee te praten.

Ik weet uit ervaring dat Twitter een wondermiddel is als je iemand een steuntje in de rug wilt geven. Mensen die iets ernstigs meegemaakt hebben, verdienen zonder meer steun. Ik tweette dus dat Kate heel eenzaam is en binnen een uurtje had ze zeventig nieuwe volgers met wie ze druk ging chatten. Ik leunde tevreden achterover – zo simpel is het dus om eenzaamheid op te lossen –, tot ik een bericht van iemand kreeg dat die Kate waarschijnlijk ene Sanne is en ook nog ene Jeanine, een meid die elke keer met een nieuw zielig verhaal opduikt en als het te heet onder haar voeten wordt, gewoon weer van identiteit verandert. Hoe triest om steeds

iemand anders te moeten zijn omdat je blijkbaar niet gelukkig bent met wie je werkelijk bent.

Misschien heeft deze Kate/Sanne/Jeanine inderderdaad iets ernstigs meegemaakt en heeft ze een luisterend oor nodig. Misschien verdient dat soort mensen juist steun om te voorkomen dat ze gekke dingen doen, maar ik heb zo'n gruwelijke hekel aan liegen. Zo'n voorval slaat een deuk in je vertrouwen. Maar de vraag is niet of je je bedonderd voelt, de vraag is wat je de volgende keer doet als je denkt dat iemand hulp nodig heeft. Niet helpen is het makkelijkst, maar voor hetzelfde geld gaat het om een echt slachtoffer.

11

Op een James Bondlocatie

Bestaat toeval? Geen idee, maar ik vind het heel opmerkelijk dat ik internetoplichters op mijn dak krijg terwijl ik een boek over cybercrime aan het schrijven ben. Ze kiezen me als slachtoffer uit omdat ik mijn auto te koop heb gezet. Ene meneer Laurent Gauthier wil graag de vraagprijs betalen, want zijn vrouw is helemaal verliefd geworden op mijn auto. Nu kan ik me dat best voorstellen, want het is een opvallende cabrio die al een tijdje uit productie is, maar toch frons ik mijn wenkbrauwen als ik zijn e-mail lees. Wat ik me niet kan voorstellen is dat meneer Gauthier de auto naar Afrika wil verschepen, omdat hij daar tijdelijk werkt. Als je ooit in Afrika bent geweest en de gaten in de wegen hebt gezien, dan weet je waarom een fourwheeldrive een beter idee is dan een cabrio.

Maar goed, ik ben benieuwd naar zijn oplichtingstruc, dus beantwoord ik braaf zijn e-mail. En dan komt het: hij wil een kopie van de autopapieren en van mijn legitimatiebewijs. Uiteraard heeft hij ook mijn bankrekeningnummer nodig, anders kan hij het geld voor de auto niet overmaken.

Meneer Gauthier is wel erg gretig, want om fraude op mijn naam te plegen heeft hij niet zo veel gegevens nodig. Tijd om te checken of hij al als oplichter bekendstaat.

Als ik alleen op zijn naam googel, kom ik niet ver, maar in combinatie met 'auto' levert het meteen een goede link op. Op een forum discussiëren allerlei mensen over de werkwijze van deze man. Jeetje, hij heeft ook op een Fiat Panda geboden! Dan weet je zeker dat het een oplichter is, want wie wil er nou in een Fiat Panda rijden?

Sommige mensen zijn verder dan ik in het transactieproces en hebben al een kopie van zijn paspoort en dat van zijn vrouw ontvangen. Beiden zijn blank. Dat viel te verwach-

ten, de foto's zijn vast van een paar mensen die wel een kopie van hun legitimatiebewijs gestuurd hebben zonder te beseffen dat ze voortaan als Nigeriaan door het leven gaan.

Ik weet het niet helemaal zeker of er in dit geval Nigerianen achter zitten, maar zo heet deze vorm van fraude, '419 scam', naar het fraudeartikel in het wetboek van Nigeria. In elk geval hebben de Nigerianen deze werkwijze al vanaf het begin van het internet massaal omarmd. In 2005 wonnen ze er zelfs de Ig Nobelprijs voor literatuur mee. Een leuke parodie om aan te tonen dat de internetondernemers in Nigeria de literatuur verrijkt hebben met kleurrijke personages en in een korte tijd miljoenen lezers wisten te bereiken. Nu, zo veel jaar later, is deze vorm van mooie verhaaltjes vertellen nog steeds springlevend.

Sinds ik de waarheid over meneer Gauthier weet, twijfel ik even of ik op zijn e-mail zal reageren. Ik kan uiteraard zeggen dat ik geen scanner heb, misschien wil hij het geld voorschieten zodat ik mijn legitimatiebewijs en de rest kan scannen om aan hem op te sturen. Maar iets weerhoudt me ervan dat te doen. Eigenlijk weet ik wat dat is: dat hij ook op een Fiat Panda geboden heeft. Dit doet voor mij de deur dicht.

Nu maar hopen dat iemand anders de vraagprijs biedt en dat ik het geld ook daadwerkelijk krijg.

Terwijl ik op de afspraak met de hacker wacht, vraag ik me af hoe moeilijk het kan zijn om in de huid van iemand anders te kruipen. Ik heb inmiddels genoeg gelezen om te weten dat het kunnen ontfutselen van informatie belangrijker is dan de technische capaciteiten. Op het internet is zo veel informatie over personen te vinden dat ik die waarschijnlijk niet eens hoef te ontfutselen.

Ik kies een willekeurig iemand, ene meneer Hendriksen. Ik zie dat hij sinds kort een eigen bedrijf heeft, want de Kamer van Koophandel zet al zijn gegevens online, inclusief zijn adres, en zijn handelsnaam. Deze man vermeldt zoals veel ondernemers zijn btw-nummer op zijn site. Met deze gegevens kan ik bij diverse sites zakelijke telefoonabonnementen op zijn naam afsluiten of een computer bestellen. De websites gaan ervan uit dat de Kamer van Koophandel de gegevens al gecontroleerd heeft. De factuur sturen ze naar het bekende adres, maar ik mag zelf aangeven of ik de goederen op een ander adres wil ontvangen. Heel handig, want hij moet alleen de factuur krijgen en niet de spullen. Laat hem maar bewijzen dat hij niets besteld heeft.

Ik kan nog verder gaan door een Marktplaatsaccount namens Hendriksen te openen. Hij heeft zogenaamd een partij spullen voor een redelijke prijs over. Uiteraard zullen sommige mensen kijken hoe betrouwbaar ik ben. Geen probleem, ik stuur ze gewoon de gegevens van meneer Hendriksen die op de site van de Kamer van Koophandel te vinden zijn. De potentiële kopers zijn gerustgesteld, want ze hebben nu een adres waar ze heen kunnen, mochten ze de goedkope laptop niet in goede staat ontvangen.

Ze maken het geld over, maar ik stuur ze niets op. Als ze bij Hendriksen aankloppen, dan gaat hij vast beweren dat hij niet eens een Marktplaatsaccount heeft. Maar het wordt voor hem bijzonder lastig om aan te tonen dat hij niet de persoon is die de advertenties op Marktplaats heeft gezet. En de politie kan hem ook niet helpen, want deze vorm van fraude heeft geen prioriteit.

Op politie.nl (Thema's) staat wel een schat aan informatie: allemaal verdachte rekeningen, telefoonnummers en

e-mails. Als je iemand op Marktplaats niet vertrouwt, kun je bijvoorbeeld zijn e-mailadres of rekeningnummer invullen om te kijken of hij niet als fraudeur te boek staat. Maar ja, meneer Hendriksen stond ook niet te boek als fraudeur. Dat was ik, met zijn gegevens. Maar ik sta ook nergens als fraudeur geregistreerd.

De echte meneer Hendriksen ken ik niet en misschien ga ik hem ook nooit ontmoeten, maar een slachtoffer van identiteitsfraude bereiken is soms een hele toer. Na een tip probeer ik met ene Leo af te spreken. Hij neemt zijn telefoon niet op en ik stuur hem een e-mail of hij me terug wil bellen. Daarna volgt een merkwaardige e-mail terug.

'Ik wilde je bellen. Maar op dit moment heb ik geen bankrekening (is opgezegd door de bank), geen geld (want geen bankrekening) en geen beltegoed (want geen geld). Als je identiteit gestolen is, dan heb je dus echt een probleem. Je wordt van het kastje naar de muur gestuurd. Kun je me nog een keer proberen te bellen?'

'Prima, gelukkig hebben ze je internet niet afgesloten,' reageer ik.

Even later komt zijn antwoord: 'Dat hebben ze wel. Ik mag gratis gebruikmaken van het draadloze netwerk van mijn buurman'.

Hoe hopeloos het geval van Leo is, hoor ik de volgende dag. Bij hem is het allemaal met een kopie van zijn legitimatiebewijs begonnen.

'Geen idee hoe of waar die gemaakt is,' zegt hij. 'Ze vragen overal om een kopietje. Daarna valt het in verkeerde handen en beginnen de problemen. Iemand rijdt zwart en

geeft mijn adres op als hij een boete moet betalen, iemand bestelt een creditcard op mijn naam, iemand doet aankopen op mijn naam. Zonder dat ik het weet, sta ik op allerlei zwarte lijsten en komt de politie me oppakken. Ze hebben me uiteraard eerst gewaarschuwd om mijn boetes te betalen, maar ik wist helemaal niet waar het over ging, dus heb ik niet betaald. Toen hebben ze me opgepakt tijdens een netwerkborrel ten overstaan van al mijn zakelijke relaties. Driemaal raden of ze daarna nog zaken met je willen doen.'

Leo werd acht dagen opgesloten, zo lang duurde het voordat zijn advocaat genoeg bewijzen had dat het om identiteitsfraude ging. 'We hadden een map vol met bewijzen dat ik bijvoorbeeld niet zwartgereden kon hebben in het openbaar vervoer, aangezien ik op dat moment een lezing gaf aan de andere kant van het land.'

'En toen lieten ze je gaan.'

'Ja, om me twee jaar later weer op te pakken. Deze keer moest ik drie maanden zitten. Mijn advocaat bleek verzuimd te hebben om binnen een bepaalde tijd naar meerdere rechtbanken de bewijzen te sturen dat ik het niet was. De zaak was dus niet afgesloten, alleen de boete was opgeschort en nu konden ze me opnieuw oppakken.'

'En je hebt drie maanden onschuldig in de gevangenis gezeten?'

'Ja, in Lelystad. Je hoort af en toe mooie verhalen over de gevangenis, maar ik kan je nu uit eigen ervaring vertellen dat die niet kloppen, want ik ben niet zo lang geleden vrijgekomen.'

'Wat een nachtmerrie.'

'Mijn grootste nachtmerrie moet nog beginnen,' zegt Leo. 'Het gevecht tegen de instanties om alles te herstellen.

Helaas valt niet alles te herstellen, want ik heb nu een strafblad en met een strafblad kom ik niet aan de bak.'

Na het gesprek met Leo heb ik wat tijd nodig om zijn woorden te verwerken. Slechts een kopie van je legitimatiebewijs en je leven verandert in een hel. Ik wil even niet denken aan al die instanties waar ik ooit een kopie heb achtergelaten.

In mijn mailbox vind ik een uitnodiging voor een congres over cybercrime in een KPN-datacentrum waar de data van velen van ons opgeslagen zijn. De bezoekers krijgen ook een rondleiding door de vertrekken waar buitenstaanders normaal gesproken niet mogen komen. Ik besluit erheen te gaan.

De eerste spreker heeft veel kennis van computerbeveiliging, maar ook ervaring als slachtoffer. Hij vertelt dat hij een keer een e-mail van een vriendin ontving dat ze in het buitenland beroofd was. Hij maakte zo snel mogelijk het gevraagde bedrag voor een nieuw paspoort en een hotelovernachting over om vervolgens te ontdekken dat die vriendin helemaal niet in het buitenland zat. Iemand had haar e-mail gehackt en namens haar honderden van dat soort e-mails verspreid.

'Klik je op een e-mail die zegt dat je inbox vol is?' vraagt hij. 'Vier tot vijf procent van alle mensen klikt op phishingmails en vult alle gevraagde informatie in.'

Dat verbaast me niets. Ik ben eerder verbaasd dat dit cijfer niet veel hoger is als ik weet hoe digibeet veel mensen zijn. Zo belt een oudere man de helpdesk op en de medewerker zegt: "U moet afsluiten met een hekkie." De man begrijpt er niets van: 'Met een hekkie? Ik woon vier hoog!'

De sprekers op de conferentie zijn het met elkaar eens dat de meeste particulieren weinig verstand van computerbeveiliging hebben, maar wat nog erger is: bij de bedrijven is het net zo. Ze hebben hun computersystemen niet op orde, wat soms grote gevolgen heeft. Een schoolvoorbeeld is Diginotar, die met mogelijk onveilige certificaten hele branches ontregelde. Rechtszaken werden uitgesteld omdat advocaten niet bij de dossiers konden, de Belastingdienst kon niet meer innen of terugbetalen, notarissen konden geen onroerende-zaaktransacties aanleveren aan het Kadaster en er kon niet eens gegraven worden, want de aannemers waren afhankelijk van de digitale kaart van Nederland die toont waar alle kabels liggen.

Net als fysieke beveiliging is echte computerveiligheid een illusie. Een van de sprekers vertelt een waargebeurd verhaal om dat te illustreren: hij had zijn nieuwe huis met dure sloten beveiligd. Toen kwam er een barstje in een raam en de glazenzetter tilde binnen twee minuten het hele raam eruit. 'Ik stond vol ongeloof naar het gapende gat te kijken. Zoals die glazenzetter zonder problemen mijn huis kon binnenkomen, zo kan ik zonder problemen een computer binnendringen. Kan dat bij elke computer? Ja.'

Dan is het tijd voor de rondleiding: met eigen ogen zien hoe goed de servers binnen het enorme KPN-centrum beschermd worden. De deuren zijn uiteraard beveiligd en je kunt alleen met een pasje binnenkomen. Boven onze hoofden hangen spanningsrails die de kastjes vol data van twee kanten voeden. Als er iets met de ene bundel kabels gebeurt, pakt de andere het naadloos over. En als de netstroom uitvalt, nemen zes hightechmachines met een vliegwiel van zes ton het over. Het vliegwiel kan zo'n tien seconden stroom le-

veren, dan gaat er een koppeling dicht en starten de dieselgeneratoren.

De generatorenruimte is indrukwekkend. Vooral de herrie. Overal in het gebouw hangen camera's, zo'n tweehonderd in totaal. Met een groepje van tien man mogen we met de lift naar een hogere verdieping. De deuren sluiten, maar er gebeurt niets en na een paar keer drukken op de knop nog steeds niet. Dan maar lopend naar boven, zo hightech hoeft het ook weer niet. Als het maar veilig is.

De warmte die alle servers produceren wordt afgevoerd naar gigantische koeltorens op het dak. Dat is net zo groot als een voetbalveld. Als je daar tussen de grijze koeltorens loopt, waan je je op een soort James Bondlocatie. Maar ik heb het vage vermoeden dat je geen James Bond hoeft te zijn om dit servercentrum binnen te dringen. Een nep-liftreparateur lukt het vast ook. Elke beveiliging is net zo sterk als zijn zwakste schakel.

Als ik het gebouw verlaat, ontvang ik een sms: 'Gefeliciteerd! U bent de winnaar van de Dag'. Ik heb een iPad gewonnen en ik word doorverwezen naar een site. Een nogal doorzichtige spam, maar hoe komen die spammers aan mijn telefoonnummer? Ik vrees dat ik dat nooit te weten kom, want er zijn inmiddels te veel manieren om telefoonnummers te bemachtigen. Sommige bedrijven verkopen je gegevens gewoon door, terwijl andere ze slecht beveiligen. Zelfs winkels met een keurmerk kun je niet vertrouwen, want meer dan de helft blijkt je data niet goed beveiligd te hebben. Mijn 06-nummer kan ook in verkeerde handen komen wanneer vrienden hun adresboek koppelen aan een app. De gratis app 'Talking Tom Cat', waarin een virtuele kat je napraat, steelt je telefoonnummer en verkoopt het voor adver-

tenties. Meer dan vijftig miljoen mensen hebben die pratende kat al gedownload.

Ik wis het spamberichtje en werp een laatste blik op het gebouw waar veel van onze gegevens bewaard worden. Aan de buitenkant ziet het er aanzienlijk saaier uit, net zo grijzig en hoekig als de gemiddelde bedrijfsloods. Maar de digitale James Bond weet het vast te vinden.

12
Big Brother

De meeste mensen denken dat ze niets te verbergen hebben, en dat geldt zelfs voor mensen die dingen doen die niet door de beugel kunnen. Het wordt steeds gemakkelijker om te controleren of iemand iets verzwijgt. Uitkeringsgerechtigden die gaan samenwonen en dat niet melden, plegen fraude. De instanties kijken gewoon op Facebook voor aanwijzingen of vragen hun waterverbruik op. Gemeenten stoppen uitkeringen als mensen te veel of te weinig water gebruiken.

Hoewel het koppelen van gegevens soms tot grove fouten leidt, komen de grootste gevaren vanuit een andere hoek. Al die databanken, vaak slecht beveiligd, maken ons kwetsbaar. Nieuwe soorten virussen proberen onze identiteit te stelen. De Pixsteal Trojan bijvoorbeeld gaat gericht op zoek naar plaatjes op computers. Een scan van een rijbewijs of paspoort komt zo gemakkelijk in handen van criminelen. Pikantere plaatjes worden voor afpersing gebruikt.

Ik heb ook niets te verbergen, maar privacy is veel meer dan dingen uitspoken die van de wet niet mogen. Het is de vrijheid om zelf te bepalen welke informatie aan wie wordt doorgegeven en ook het recht om te doen wat je wilt zonder dat elke stap gevolgd, geregistreerd en uitvergroot kan worden.

De vrije wereld is helaas niet meer zo vrij. Onze vrijheid wordt geschonden om ons te beschermen tegen terroristen die onze vrijheid haten. Dat doet me aan Big Brother van Orwell denken, alleen hield toen iedereen het voor fictie.

Orwells boek *1984*, geschreven als waarschuwing tegen totalitaire regimes, schijnt opeens weer massaal gelezen te worden. Best gek als je bedenkt dat het boek in 1949 verscheen. De beroemde frase 'Big Brother is watching you' is uit het boek afkomstig. Big Brother is in het boek de al-

machtige leider die altijd meekijkt bij wat de mensen doen en zeggen. Met wie bel ik, hoe lang, van wie krijg ik een sms, op welke trefwoorden googel ik... al mijn stappen kunnen ze volgen. Tussen degene die me afluistert en mij kunnen duizenden kilometers zitten. Gemak dient de mens. En de technologie natuurlijk.

In de tijd van Orwell was het onvoorstelbaar dat er overal om ons heen camera's zouden hangen om ons in de gaten te houden. Maar nu is het allemaal een feit en we liggen er niet wakker van. In Nederland hangen zeker tweehonderdduizend camera's die toezicht houden op de openbare ruimte en in gebouwen. Bij bedrijven en particulieren is het aantal nog veel groter. In Amerika heeft de politie helmpjes met camera's om de gezichten van burgers snel te scannen. Het motto is: 'Vertel me niet wie jij bent, dat vertellen wij je wel.'

Als gewone burger ga ik er niet van uit dat de camera's tegen mij gebruikt zullen worden. Toch is dit steeds vaker het geval. Een Nederlandse politica die een collega in een parkeergarage bevredigde, zag later alles op internet terug. Ook een Belgische burgemeester werd in verlegenheid gebracht door een filmpje op YouTube waarin ze vrijend te zien was op een romantische plek.

De camera's van politie, gemeenten en zelfs van amateurfilmers houden ons constant in de gaten zonder dat we er erg in hebben. Of dat een inbreuk is op onze privacy zien we pas als iets uitlekt.

Tegenwoordig is iedere burger al bij voorbaat verdacht. De overheid controleert ons strenger, maar onzichtbaarder dan ooit. Gek genoeg levert dat geen betere samenleving op, want het gevoel van onveiligheid is juist toegenomen. Waar-

om vertrouwt de overheid ons zo weinig? Ik wil toch ook niet weten wat er op de computer van de minister van Justitie staat en ik vraag hem ook niet om zijn DNA af te staan voor het geval dat hij ooit iets verkeerds doet? Toch is dit wat de overheid de laatste tijd wil: totale controle vooraf.

De Rotterdamse politie ging kentekens van onschuldige burgers verzamelen en bewaren tot die teruggefloten werd, want dat was in strijd met de wet. Vervolgens werd de wet gewoon aangepast: voortaan mocht de politie dat doen. Onze medische gegevens voor Justitie beschikbaar stellen is tegenwoordig ook bespreekbaar, net als het hacken van computers door de politie. Grappig dat de minister van Justitie dat als een goede manier van boeven vangen ziet, alsof ervaren cybercriminelen geen programma's hebben om zich tegen hackende politieagenten te wapenen. Columnist Jeroen Weghs vond het een leuk gegeven voor een stukje op opinieforum DeJaap.nl.

'Met een dreun zet de minister zijn computer op het bureau van Fox-IT-directeur Ronald Prins. "Ronald," zegt hij, "jij hebt verstand van computers. Kijk even naar de mijne, wil je?" Prins sluit de bak aan en vraagt wat er aan de hand is. "Hij doet gek," antwoordt de minister. "Hij ratelt, is zo traag als een ambtenaar op maandagmorgen en nu ben ik ook nog eens bestanden kwijt. O, en een hoop letters zijn zoek. Ik heb alleen nog maar hoofdletters."

Prins drukt op 'Caps Lock', opent een terminal en roffelt lange rijen code uit zijn vingers. "Ik zie het al," zegt hij, "u bent gehackt door Justitie."

"Gehekt zeg je? Wat is dat voor aperte nonsens?"

"De politie heeft bij u ingebroken en spyware geïnstalleerd."

"Wel voor den drommel! Hoezo? Welk onbenul heeft daar opdracht toe gegeven?"

"Nou... feitelijk u zelf, minister. Met de wettelijke verruiming van opsporingsbevoegdheden om cybercrime aan te pakken."

Prins bladert wat door de e-mail van de minister, doet een zoekactie op zijn eigen naam en opent een mailtje. "Hier, de aanbestedingsbrief. Hierin staat precies beschreven wat de software doet."

Het imposante lijf van de minister van Veiligheid en Justitie ploft in een van de stoelen. "Jaja, iets met ie-pee en het doorbreken van vuurwallen en dan een paard installeren... dat zegt mij toch helemaal geen fluit, jongeman! Spreek Nederlands! De helft van mijn rapporten is verdwenen. Die maatregel is bedoeld om levensgevaarlijke cybercriminaliteit een halt toe te roepen, niet om de minister het werken onmogelijk te maken."

"Dat begrijp ik, meneer, maar zoals ik u voordien al zei: de echte cybercriminelen gaan we er niet mee pakken. Echte internetcriminelen zijn te sluw om zomaar spyware te installeren. Het zijn de digitale kruimeldieven die we hiermee pakken. Maar ik installeer logging tooltjes, een port scanner en wat honeypots, zodat u weer veilig op uw systeem kunt werken."

"Bazel niet, Prins. Wat ben je in godsnaam aan het doen?"

"O, ik zorg ervoor dat de inbreker, de politie dus, niet op uw computer kan. Hij wordt er net zo hard weer afgeschopt.'

Zo is de minister gerustgesteld. De vraag is of hij wel doorheeft hoe cybercriminelen werken. Hackerscollectief Anonymous kraakte de computersystemen van VISA en

Mastercard, en viel zelfs de FBI, de CIA en de NAVO aan. Anonymous doet veel uit protest, omdat de overheid steeds vaker Big Brother-methodes toepast.

Computerbeveiliger Prins vindt de beschreven situatie best grappig, maar hij begrijpt ook waarom de politie meer digitale bevoegdheden wil. 'Anders lopen hun onderzoeken elke keer vast,' zegt hij. 'Cybercrime is heel internationaal. Wil je een botnet ontmantelen, omdat er duizenden besmette Nederlandse computers aan hangen, dan moet je rechtshulpverzoeken bij verschillende landen indienen. Dat werkt niet. Daarom begrijp ik de behoefte bij de politie om computers te mogen hacken. Tegelijkertijd moeten we oppassen dat die bevoegdheden niet te ruim worden en de privacy van de burgers gaan bedreigen.'

Het schrikbeeld van Prins is waarschijnlijk de Amerikaanse afluisterdienst NSA en ik moet zeggen dat ik door zijn toedoen ook aardig geschrokken ben. Hij gaf me zijn e-mail om een afspraak te maken en wie mailde ik? Juist, de NSA. 'Dat geintje maakt bij veel mensen indruk,' zegt Prins.

'Hoe kom je aan een e-mailadres van de NSA?'

'Eerlijk gekocht. Een bedrijf regelt voor 139 dollar zo'n e-mail voor je. Het enige verschil met de echte is dat je NSA-mailadres op '.org' eindigt, maar dat valt de meeste mensen niet op.'

Klopt, mij was het in eerste instantie ook niet opgevallen. Ik dacht dat Prins het NSA-mailadres via een achterdeurtje had bemachtigd. Nu ik weet dat het officieel te regelen is, lijkt het me een leuk verjaardagscadeau. Dan ben ik misschien ook verlost van al die spam, want ik denk niet dat de NSA heel geliefd is bij mensen die met louche zaken

bezig zijn. Of zal de NSA werkelijk alleen maar in terroristen geïnteresseerd zijn om miljoenen burgers af te luisteren?

Nu ik meer over cybercrime weet, valt het me op hoe gemakkelijk het allemaal gaat. Je hoeft er bijna niets voor te doen om slachtoffer te worden. Boudewijn Duijvesteijn kreeg een brief van de politie dat hij zich op het bureau moest melden voor overtreding van de opiumwet. Foutje, dacht hij. Maar de politie maakte een foto van hem en nam zijn vingerafdrukken af. Vervolgens werd hij urenlang verhoord. Ze vroegen of hij een bepaald adres kende, of hij hennep teelde en of hij mensen kende die dat deden.

Duijvesteijn had geen flauw idee waar ze het over hadden. Hij werd naar huis gestuurd, om enkele maanden later opnieuw verhoord te worden voor hennepteelt op een ander adres. Ook deze woning bleek op zijn naam te zijn gehuurd.

Als verdachte merkte hij hoe snel hij de schijn tegen had. Goede vrienden begonnen aan hem te twijfelen en zelfs zijn vriendin vroeg een keer: 'Je hebt het toch niet gedaan, hè?'

'Je kunt je niet voorstellen hoe machteloos je je op zo'n moment voelt,' zegt Boudewijn. 'Vooral als je ook nog een energierekening van ruim vijftienduizend euro krijgt en een notering als wanbetaler bij het Bureau Krediet Registratie. Dan vraag je je af: wat is dit allemaal, hoe kan dat?'

Inmiddels wist Boudewijn dat hij slachtoffer was geworden van identiteitsfraude, alleen niet wat hij ertegen kon doen. Hij wist ook hoe dit gekomen was: met een kopie van zijn paspoort konden de criminelen van alles op zijn naam uitspoken. 'Hoe die kopie in hun handen is gekomen? Geen idee,' zegt hij. 'Als burger laat je op heel veel plekken een kopie achter. Zoals zo veel mensen bewaarde ik ook een di-

gitale kopie van mijn paspoort in mijn computer. Achteraf niet echt veilig.'

Mensen zijn geen rationele wezens. We weten vaak wat goed voor ons is, maar doen het niet. Iedereen vertelt ons dat we geen kopie van ons legitimatiebewijs in de computer moeten bewaren en dat we niet overal dezelfde wachtwoorden voor moeten gebruiken en toch doen we het.

Als ik mijn computer probeer te beveiligen ben ik net een topkeeper uit de voetbalwereld. Uit een onderzoek blijkt dat de topkeepers weten dat ze de grootste kans hebben om een penalty tegen te houden als ze midden in het doel blijven staan. Maar dat doen ze niet. Maar liefst 94 procent duikt naar links of naar rechts. Zo houden de keepers de schone schijn op dat ze hun best gedaan hebben. Als keeper van mijn computer doe ik dat ook: dingen doen waar ik van weet dat ze niet verstandig zijn. Zoals af en toe een kopie van mijn paspoort vergeten te wissen nadat weer een of andere instantie gevraagd heeft of ze die mogen hebben. Laatst schreef ik een stukje voor een tijdschrift en ja hoor: hun financiële administratie wilde mijn factuur niet betalen zonder een kopie van mijn paspoort. Het is vast wettelijk zo geregeld, want ik krijg die vraag van vrijwel alle bladen waar ik voor werk. Ik weet alleen niet waar al die kopietjes verdwijnen. Ik wis ze meestal na een tijdje van de harde schijf van mijn computer, maar ik vraag me af of de bladen dat ook doen. Ik weet vrijwel zeker van niet.

Uiteindelijk werd Boudewijn aangeklaagd door het Openbaar Ministerie. Hij moest voor de politierechter verschijnen, inclusief een dure advocaat.

'Gelukkig werd ik vrijgesproken, omdat hun "bewijzen"

niet stevig genoeg waren voor een veroordeling,' zegt hij. 'Maar de gevolgen van de identiteitsfraude zijn nog steeds merkbaar. Ik werd niet geaccepteerd als vrijwilliger bij een buurtpreventieteam en mijn vermelding als wanbetaler is nog steeds niet weggepoetst. Het ergste is het dreigende gevaar. Je weet nooit wanneer het weer begint. Je kopie hebben ze al en niets let ze om die opnieuw te gebruiken.'

Dit is de grootste nachtmerrie voor veel mensen: je hebt een onzichtbare vijand en je weet niet wanneer die weer toeslaat. Iemand dient valse aangiftes namens jou bij de Belastingdienst in en je merkt dat pas als je een bericht ontvangt dat je rekeningnummer gewijzigd is. Maar dan is het te laat, want alles wat je terug ontvangen hebt, is bij de bank contant opgenomen.

Elk jaar worden er honderdduizenden Nederlanders slachtoffer van identiteitsfraude en oplichting, en de cijfers laten een flinke stijging zien. Bij postorderbedrijven hoef je vaak alleen maar je naam en adres in te vullen om zaken te doen. Die zijn meestal gewoon te googelen.

Wat je steeds vaker ziet, is dat hele webwinkels zomaar verdwijnen. Op internet regent het klachten over digitalshop-online.nl. Het vreemde is dat die webwinkel voor zijn verdwijning bekende webkeurmerken had, die niet eens nep waren. 'Balen,' schrijft ene Sjaak, die voor honderden euro's een mobiele telefoon bestelde. 'Webkeurmerken en het Kamer van Koophandel-nummer gecontroleerd, gezocht op reviews en gekeken of de betaalmogelijkheden goed waren. Alles klopte.'

Een andere bekende praktijk is het werven van thuiswerkers voor het ontvangen van retourpakketten. De opdracht-

gever wil een kopie van je legitimatiebewijs. Dat klinkt niet vreemd, want hij wil ook zekerheid. Maar dan begint het: hij maakt een nep-e-mail met je naam erin en bestelt van alles en nog wat op je naam.

Het postbedrijf komt de pakketten brengen en je tekent ervoor omdat je denkt dat dit de retourpakketten zijn. Je labelt ze met de stickers die de opdrachtgever opgestuurd heeft. De pakketten gaan naar het buitenland en je krijgt de rekeningen voor laptops en iPhones. Ze zijn op jouw adres besteld. Sterker nog, je hebt ervoor getekend.

Bij de stichting Opgelet op Internet regent het klachten van gedupeerden waar de politie niets mee kan. Ze zien een trend in misbruik van identiteiten. Oplichters kijken op sites zoals Marktplaats om te zien wie wat zoekt en reageren daarop. Aanbetaling hoeven ze niet, ze willen alleen een kopie van het identiteitsbewijs van de koper ontvangen. En de argeloze koper ziet het probleem niet. Maar dan pas begint het hele spel. De identiteitsdief maakt een e-mail met de naam van die persoon aan en stuurt honderden e-mails naar mensen die iets zoeken. Hij heeft al die spullen te koop en hij kan bewijzen dat hij betrouwbaar is, want hij mailt een kopie van zijn id en de naam is dezelfde als in zijn e-mail. De rekeningnummers zijn van katvangers en dat zijn vaak mensen die op advertenties over zogenaamd huiswerk reageren. Klinkt ingewikkeld, maar het werkt feilloos en duizenden mensen trappen erin. Als de gedupeerden aankloppen bij degene van wie de identiteit misbruikt wordt, blijkt die van niets te weten. De echte oplichters zijn meestal onvindbaar.

De meeste consumenten hebben geen flauw idee uit welke hoek het gevaar kan komen. De ene keer wordt hun identiteit gestolen door mensen die weinig tot niets over computers weten, de andere keer door hackers die heel anders werken. Een paar kennissen ontvingen laatst een berichtje dat ze 'getagd' zijn op een foto. De link leidde naar een site, die een programma installeert om de afbeelding te bekijken. Het programma doet echter iets anders: het geeft de aanvallers toegang tot je Facebook-, Twitter- en e-mailaccount. Voordat Google en Facebook de kwaadaardige links wisten te verwijderen, waren er al 800.000 gebruikers geïnfecteerd geraakt met het virus.

In de toekomst zullen veel banken en andere belangrijke instellingen platgelegd worden, omdat de cybercriminelen dankzij naïeve burgers over een toenemend aantal zombie-computers beschikken. Als ik een simpele mixer koop, krijg ik een boekwerk met veiligheidskeurmerken, instructies en waarschuwingen, maar als ik een pc koop, zit er geen enkele beveiliging tegen virussen en malware op. De boodschap is duidelijk: zoek het maar uit.

Met mijn geringe computerkennis moet ik dus een goed antivirusprogramma en een firewall installeren en ook systeembeheerder in het klein spelen, omdat bij nieuwe computers alles standaard openstaat. Hoe moet ik dat doen als niemand me ooit geleerd heeft hoe dat werkt?

Ik ben misschien van de oude generatie die niet opgegroeid is met computers, maar als ik kijk naar wat mijn zoons op school over digitale veiligheid leren, dan is dat ook bitter weinig. Als ik lezingen op scholen geef, steken de meeste jongeren hun hand op als ik vraag of ze hun inloggegevens

voor een transactie naar het buitenland zouden geven in ruil voor vijftig euro. Degenen die hun hand niet opsteken kunnen niet uitleggen waar het gevaar in schuilt. Welkom in de moderne samenleving waar jongeren achter de computers opgroeien zonder de gevaren te zien.

Als ze hun bankrekening voor zo'n transactie laten gebruiken, zijn ze medeplichtig aan het doorsluizen van crimineel geld, want daar wordt het voor gebruikt. Uiteraard wordt hun rekening ook leeggetrokken.

Ze zien me vast als een moraliserende tante, maar ze zijn opmerkelijk stil. In een van de klassen krijg ik bijval uit onverwachte hoek. Een jongen steekt zijn hand op en zegt: 'Ik doe het niet, want mijn broer raakte op deze manier tweeduizend euro kwijt.'

Dan zijn alle ogen op hem gericht, want iedereen wil weten hoe zijn broer zo stom kon zijn. Maar net vonden ze het bijna allemaal geen probleem om me hun bankpasje even te lenen in ruil voor geld.

13
Digi-stalker

Op social media zijn heel wat voorbeelden van identiteitsfraude, van mensen die een account met jouw naam en foto aanmaken en namens jou van alles rondbazuinen. Soms is dat alleen maar storend, een andere keer ronduit walgelijk. Een politicus uit Arnhem die in opspraak raakte als pedofiel, heeft in zijn profiel staan: 'Eens kijken hoe ik wat interessante volgertjes kan krijgen. Lieve kinderen, ik heb een hele kamer vol speelgoed! Volg mij via Twitter en misschien kunnen we 'n keer wat afspreken. Blijft ons geheimpje.' Uiteraard is dit een nep-account dat gebruikmaakt van een echte foto.

Ik zie ook nep-profielen van schrijvers opduiken. Die van Kader Abdolah onder de Twitternaam @stinkturk is helemaal verschrikkelijk: 'Ik hou van m'n schnorr. WNTB. HVJ. XOXOXOXOXOXO. Fuck deze afkortingen, iedereen weet dat ik geil ben.'

Als ik een halfjaar later ga kijken, bestaat het nep-account nog steeds. En dit is nou het probleem: vaak weet het slachtoffer het niet. Ik weet ook niet dat iemand een nep-account op mijn naam aangemaakt heeft tot een oplettende kennis me een berichtje stuurt: 'Dat ben je niet, hè?'

Nou nee, zo'n Twitterbio schrijf ik niet eens als ik goed dronken ben. @MariaGenova3 lijkt als twee druppels water op mij, want mijn foto is van mijn website gejat. Verder is mijn profiel vrij compleet, want ook de link naar mijn website werkt. Mijn bio is een bijzondere variatie op de titel van mijn boek *Man is stoer, vrouw is hoer* (over vrouwenhandel in Nederland). Die variatie luidt: 'Ik ben gewoon een hoer, maar hier doe ik stoer. Zelfs in Bulgarije liet ik mij tegen betaling al neuken, al was het maar voor een pakje peuken.'

Vreemd genoeg is het eerste wat ik denk: ik heb nooit ge-

rookt, dus wat doet dat pakje peuken in mijn bio? Dat is nou het domme: je hersenen proberen een logische verklaring te vinden, terwijl iedere gek zo'n profiel op jouw naam aan kan maken. Bij collega Rhijja Jansen kopieert iemand haar foto van internet, doet zich als haar voor en vraagt vrouwen of ze aan een liefdesboek willen meewerken. Binnen de kortste keren heeft die man bij verschillende vrouwen beet en zij vertellen hem tot in detail over hun seksleven.

Het kan nog erger: iemand stuurt racistische tweets namens jou, dat je 'misselijk wordt van al die moslims' op de universiteit. Daar schrik je van, maar waar je vooral bang van wordt zijn de reacties erop: "Natalja Laurey, ik snij je keel open als ik erachter kom wie je bent. Ik snij je in stukken.'

Erachter komen wie Natalja is, is niet zo moeilijk. De dader gebruikt immers haar echte naam en een foto van haar, gekopieerd vanuit de site van de universiteit. Zij is doodsbang voor de gevolgen. Natalja doet aangifte, maar dat wordt haar volgende lijdensweg. Het Openbaar Ministerie legt de zaak op de grote stapel en weigert in eerste instantie om de gegevens van de mogelijke dader bij Twitter op te vragen. Na een tijdje gebeurt dat wel, maar nu zijn het de Amerikanen die moeilijk doen en medewerking aan het rechtshulpverzoek weigeren.

Natalja is onthutst dat het zo simpel is om iemand digitaal te klonen en zo moeilijk om het allemaal terug te draaien. Haar nep-account werd in slechts een paar uur tijd verwijderd, maar als ze zichzelf googelt, komt ze vooral racistische uitspraken tegen die ze nooit gedaan heeft.

De impact van de social media vind ik geweldig, maar ook

heel eng. Social media vergroten alles uit, soms op een oneerlijke manier. Als je een saai verhaal leest en je vraagt je af waarom zo veel mensen het aanbevelen, dan kan de verklaring vrij simpel zijn. Een schrijver biecht het op: hij heeft voor de meningen van al die mensen betaald. Voor twee dollar per uur heb je een botnet, die duizenden mensen spamt met het verhaal. Voor vijf dollar delen tweeduizend mensen je verhaal via Facebook en voor hetzelfde bedrag koop je vijfhonderd tweets.

Ongeveer tachtig procent van de spam-accounts wordt binnen een dag uit de lucht gehaald, maar vrijwel onmiddellijk vervangen door nieuwe.

Het nep-account van Transavia had binnen 24 uur meer volgers op Twitter dan het officiële. Klinkt als humor, maar bedrijven die het overkomt, vinden het zelden grappig. Zo verscheen er op Twitter een volledig nagemaakte pagina van De Telegraaf met hot nieuws: 'PVV'er Van Bemmel opgepakt voor naaktlopen.' De tekst werd als lopend vuurtje verspreid. 'PVV-Tweede Kamerlid Jhim van Bemmel is zondagmorgen in zijn woonplaats Zoetermeer opgepakt voor verstoring van de openbare orde. Van Bemmel liep onder invloed van alcohol spiernaakt door de straat waar hij woont en riep daarbij verschillende beledigende leuzen. Hij zou onder andere geroepen hebben: "Islam? Islam? Ik is lam!"'

Hoe kan de grootste krant van Nederland berichten rondsturen waar niets van klopt? Simpel: het volledige Twitteraccount van *De Telegraaf* blijkt nagemaakt. En Van Bemmel wordt waarschijnlijk jarenlang achtervolgd door het 'naaktloopincident' als hij zichzelf googelt. Het ijzersterke geheu-

gen van het internet maakt helaas geen onderscheid tussen waar of onwaar.

Op het internet wemelt het van de nep-verhalen, nep-personen en helaas ook van mensen die op forums reageren met als enig doel anderen te kwetsen. Deze 'internet-trollen' schijnen te kicken als iemand toehapt en boos wordt. In de hersenen van zo'n treiteraar komt een chemisch stofje vrij dat zijn stress en frustraties tijdelijk afzwakt. Hij voelt zich dus goed omdat andere mensen boos worden. Je zou je haast afvragen wat al die mensen deden toen internet nog niet bestond.

Toen Zuid-Korea verplicht stelde dat alle burgers bij het registreren op een website hun naam, burgerservicenummer en adres opgaven, nam het aantal aanvallen en beledigingen op internetfora met vijftig procent af. Ook al konden de internetters een code in plaats van hun eigen naam gebruiken, het feit dat de website-eigenaar wist wie ze waren, was blijkbaar genoeg om hun gedrag te veranderen.

Het klinkt als een mooi systeem, maar de Zuid-Koreaanse overheid gaat het afschaffen, want daardoor stalen hackers de ID-gegevens, namen, adressen en telefoonnummers van miljoenen internetters.

Zelf reageer ik niet op kwaadwillenden, bang om verzeild te raken in eindeloze discussies. Maar niet reageren helpt niet tegen mensen die erop kicken om anderen te pesten en zwart te maken. Een man uit Arnhem maakt zo veel slachtoffers dat hij haast beroeps lijkt. Ook al negeer ik hem volledig en ook al heb ik zijn account geblockt, hij blijft me met vervelende tweets bestoken. Ik kan ze dan niet zien, maar er zijn altijd mensen die me erop wijzen en vragen waarom die

man zo naar over me tweet. Dat is nou het absurde ervan: als een boze ex zoiets doet, dan kan ik me er nog iets bij voorstellen, maar deze man ken ik nauwelijks. Dat weerhoudt hem er niet van om mijn foto's te kopiëren en honderden tweets en zelfs blogs over mij te schrijven. 'Wat is Genova toch een dom Bulgaars rund', 'Genova heeft bloed aan haar handen', 'Ik ben bang dat Genova de volgende keer bij kop en kont de gracht op de Wallen wordt ingemikt', schrijft hij allemaal op Twitter. Als dit alles was, had ik mijn schouders opgehaald. Maar hoelang kun je je schouders ophalen als deze meneer na anderhalf jaar nog geen tekenen van opgeven vertoont? Die man brengt me zelfs in verband met een Bulgaarse bende die fraude met huurtoeslagen pleegt. Niet dat ik ooit een huurtoeslag gehad heb, maar dat maakt uiteraard niets uit.

Blocken en zelfs een slot op mijn account helpen niet, want hij volgt me via verschillende nep-accounts. Ik kan moeilijk alle nieuwe volgers gaan weren omdat hij achter elke mogelijke naam kan schuilen. Negeren helpt ook niet, terwijl ze zeggen dat dit de beste remedie is tegen stalkers.

Mijn enige troost is dat ik niet zijn enige slachtoffer ben, want hij valt constant mensen aan en maakt ze voor alles en nog wat uit.

Van de wet mag hij behoorlijk ver gaan. Cyberpesten is niet strafbaar en stalking is altijd lastig te bewijzen, zeker via social media.

Als schrijver en journalist moet ik tegen een stootje kunnen, vind ik, maar mensen beginnen te vragen of het geen tijd wordt voor een aangifte. Ik twijfel, want ik hoor vooral ontmoedigende geluiden van kennissen die ook lastiggevallen worden via social media en die door de politie niet seri-

eus worden genomen. 'Ze sturen je gewoon terug', 'ze gaan je aangifte niet opnemen', 'verspilde moeite, want ze zullen zeggen dat je ruzie met hem hebt en dat ze er niet zijn om ruzies op te lossen'.

Zelfs mensen die het gelukt is om aangifte te doen, geven me geen hoop: 'Ze zeiden dat ik niet op die nare blogs over mij moet reageren,' klaagt een vrouw. 'Ik reageer om te voorkomen dat mensen gaan denken dat wat hij schrijft waar is, maar daar heeft de politie geen begrip voor. Niet reageren, of je hebt geen zaak.'

Dit klinkt niet best, want soms reageer ik ook op de blogs van mijn digi-stalker, om precies dezelfde reden. Dingen die ergens op internet over je geschreven worden, kunnen je jarenlang blijven achtervolgen, ook al klopt er niets van. Wat ik nooit doe is op zijn tweets reageren, zo kan het in elk geval niet op een ordinaire onlineruzie lijken. Denk ik. Maar misschien denkt de politie er het hare van en willen ze ook mijn aangifte niet opnemen.

Ik bel eerst met het politiebureau om te informeren of het überhaupt nut heeft. Na het aanhoren van mijn verhaal zegt de agente dat het haar verstandig lijkt om aangifte te doen. In mijn woonplaats hebben ze blijkbaar geen geschikte agenten die zo'n aangifte kunnen opnemen, dus word ik naar Beverwijk doorverwezen.

Ik hoop dat ik bij een gespecialiseerde rechercheur terechtkom, maar als ik zie dat de agent 'van de oude generatie' is, vrees ik het ergste. Natuurlijk zijn dat vooroordelen, maar helaas kloppen mijn vooroordelen best vaak.

'Heeft u verstand van social media?' vraag ik nog voordat ik ga zitten.

'Een beetje,' zegt de politieagent.

Dat klinkt niet bepaald geruststellend. Zeker niet als hij met het opnemen van de aangifte begint en vraagt of 'tweets' een echt woord is.

Een halfuur verder zijn we nog nergens. De agent weet niet of het lukt om aangifte van zowel smaad als stalking te doen, want dingen aan elkaar koppelen in het verouderde computersysteem van de politie schijnt niet mee te vallen. Hij zoekt heel lang naar het juiste invulveld. Op een gegeven moment moet ik vertellen waar het zich afgespeeld heeft.

'Op het internet,' zeg ik.

De agent staart naar zijn scherm. 'Deze optie is er niet. Zullen we maar je privéadres invullen?'

'Mijn privéadres? Daar heb ik geen last van die stalker.'

'Ik begrijp het, maar ik moet iets invullen, anders mag ik van het systeem niet verder.'

Ik word niet lastiggevallen op mijn privéadres, maar dat maakt niet uit, als we maar verder komen met de aangifte.

De agent tikt met twee vingers en het duurt zo lang dat ik een belangrijke afspraak dreig te missen. Aangezien ik 21 pagina's met bewijzen van laster en stalking van tevoren heb uitgeprint en zelf een kort verhaaltje over de gang van zaken op papier heb gezet, dacht ik in anderhalf uur klaar te zijn.

De politieagent merkt dat ik onrustig begin te worden.

'Misschien is het verstandig dat we een nieuwe afspraak maken, want zo'n aangifte kan lang duren,' stelt hij voor.

Oké, die man is niet bepaald geschikt voor deze taak, maar hij is wel heel vriendelijk en behulpzaam.

We spreken over twee dagen af en ik ren naar mijn afspraak.

14

DigiD voor dummies

De overheid weet dat duizenden Nederlanders hun DigiD-inlogcodes onbedoeld naar een reclamebureau sturen. Niemand krijgt een waarschuwing, maar André Elings, eigenaar van reclamebureau Digi-D, heeft al ruim twintigduizend gebruikersnamen en wachtwoorden in handen. Daarmee kunnen burgers zich bij honderden organisaties identificeren.

Door de naamsverwarring, het scheelt maar één streepje, krijgt het reclamebureau elke week tientallen vertrouwelijke e-mails. 'Mensen spreken ook de meest persoonlijke dingen op ons antwoordapparaat in,' zegt Elings. 'Ik vraag me af wat er met burgers gebeurt die hun belastingaangifte niet op tijd inleveren omdat hun vragen bij ons komen en wij niet reageren. Krijgen ze een boete? Ik vind het triest dat de overheid het niets kan schelen dat dit soort bijzonder privacygevoelige gegevens in handen van derden komt. De media hebben al aangetoond hoe gemakkelijk het is om hiermee fraude te plegen.'

Veel databanken van de overheid zijn gekoppeld, maar dat wil niet zeggen dat fouten automatisch doorgegeven worden. Daar weet Michel Savelkoul van het Centraal Meldpunt Identiteitsfraude alles van. 'Het gaat soms om verschrikkelijke zaken,' zegt hij. 'We zijn heel lang bezig geweest met een man die 51 strafbare feiten op zijn naam had staan zonder de wet overtreden te hebben. Hij werd om de haverklap door de politie opgepakt en onderging zelfs een gewapende inval thuis. Ook op vliegvelden hielden ze hem aan, want hij stond in de systemen als crimineel en wanbetaler geregistreerd. Soms moest hij een boete betalen om het land binnen te komen.'

'Is dat de zaak van Ron Kowsoleea?' vraag ik.

'Nee,' zegt Savelkoul. 'Dit is een andere man. Eigenlijk vind ik zijn zaak triester, want hij is er bijna aan onderdoor gegaan. Die man schaamde zich kapot omdat hij steeds opgepakt werd door de politie en zweeg tegenover zijn vrienden en collega's. Zijn eigen vrouw heeft hem uiteindelijk verlaten, want op een gegeven moment geloofde ook zij niet meer in zijn onschuld. Hoe kun je immers zo vaak in botsing met de autoriteiten komen als je zegt dat je niets verkeerds doet? Hoe kun je anderen ervan overtuigen dat criminelen gebruikmaken van je identiteit en dat dit zo'n lange tijd kan doorgaan? Uiteindelijk is het ons gelukt om zijn dossier op te schonen en hij kreeg officieel excuus van Justitie. De woorden "Het is niet uw schuld" zwart op wit waren voor hem ontzettend belangrijk, waarschijnlijk belangrijker dan de schadevergoeding die hij toegekend kreeg.'

Volgens Savelkoul hoef je niet bijzonder onvoorzichtig te zijn om slachtoffer te worden van cybercrime. 'Dat is juist het enge ervan, het kan iedereen overkomen. De slachtoffers zijn vaak geheel willekeurig gekozen. Misschien ben je morgen zelf aan de beurt, want je laat vast ook wel ergens een kopie van je paspoort of rijbewijs achter.'

Ik knik. Kopietjes genoeg. Bij verhuurbedrijven, bij sportclubs, bij opdrachtgevers, bij hotels...

'Vaak mogen bedrijven helemaal niet je paspoort kopieren, maar de meeste mensen weten dat niet. Als het gevraagd wordt, dan doen ze het gewoon. Laatst wilde ik een Bijenkorfkaart aanvragen en wat moest ik invullen? Mijn burgerservicenummer. Ik schreef op: "Dat mag u niet vragen." Geen probleem, ik kreeg de klantenkaart.'

Bij de gemeente kun je zelf aangeven of ze je gegevens mogen delen met andere organisaties, maar dat weet zowat niemand. Uitkeringsinstantie UWV deelt gegevens met zevenhonderd partners, uiteraard alleen wat relevant is per geval. Op de site overheid.nl kun je zien wat de overheid van je weet. Overigens is slechts een klein gedeelte van de informatie openbaar. UWV registreert dat je een uitkering hebt, de RWD dat je in een Mercedes rijdt. De losse data zeggen op zich niets, maar als je ze in een databank stopt, dan kom je tot interessante conclusies. Welke bijstandtrekker kan zich een nieuwe Mercedes veroorloven?

Savelkoul ergert zich aan grote postorderbedrijven zoals Neckermann, Otto, Wehkamp en H&M. 'Ze doen niet veel om de klanten te beschermen tegen fraude. De telefoonmaatschappijen hebben een paar jaar geleden het pinnen van één cent bij aankoop van een mobieltje als preventiemaatregel ingevoerd en sindsdien zitten ze niet meer bij de fraudetop. De postorderbedrijven beginnen er niet aan, omdat ze bang zijn om klanten kwijt te raken in het bestelproces. Maar die ene cent kan voorkomen dat ik iets op jouw naam bestel.'

'Hoe simpel is het om iets op mijn naam te bestellen?'

'Simpeler dan je denkt,' zegt Savelkoul. 'Ik geef jouw naam op en mijn eigen adres voor de bezorging van bijvoorbeeld een laptop. Ze sturen me de laptop op en een acceptgiro, maar ik betaal niet. Na enkele dreigbrieven schakelen ze een incassobureau in en nog later een deurwaarder. Die komt bij mij aan de deur, maar ik wijs ze op de naam boven de bestelling: 'Deze mevrouw woont hier niet. Ik heb nooit een laptop besteld of ontvangen, dus komen ze na wat speurwerk bij jou terecht.'

'Maar dan zeg ik toch dat ik ook niets besteld heb, dat dit niet eens mijn adres is.'

'Natuurlijk zeg je dat, maar je wordt gevraagd om te bewijzen dat je niets hebt gedaan. Ik heb meegemaakt dat mensen de rekening gewoon maar betaalden, omdat ze niet voor de rechter wilden verschijnen.'

'En als ik de rekening niet betaal?'

'Dan gebeurt er niets, want ze kunnen het geld niet innen. Het jaar daarop verhogen ze opnieuw de prijzen omdat ze steeds meer winst door deze vorm van fraude missen.'

Het overgrote deel van de slachtoffers die Savelkoul ontmoet, kan volgens hem niet voorkomen dat ze slachtoffer worden. 'Tenzij ze draconische preventiemaatregelen nemen, maar dat kun je van gewone burgers niet verwachten. We zien de gekste gevallen: zelfs mensen die zich voor andere mensen uitgeven en uiteindelijk officiële papieren krijgen dat ze de ander zijn. En dan heb je ook al die mensen die bij het Bureau Krediet Registratie als wanbetalers te boek staan, omdat iemand spullen op hun naam heeft besteld of een lening heeft afgesloten. Vaak weten ze dat niet eens, maar als ze een huis willen kopen, dan komen ze erachter dat ze geen hypotheek krijgen omdat ze als wanbetaler geregistreerd staan. Voor het regelen van een hypotheek krijg je meestal niet meer dan enkele weken. Voordat de fraude opgelost is, kan je droomhuis aan je neus voorbijgaan.'

Volgens Savelkoul is veel van de identiteitsfraude onzichtbaar en ongrijpbaar. 'Als je je paspoort verliest, plakken fraudeurs er andere gegevens overheen. Dan kun je als Maria Genova in bijvoorbeeld Nigeria of Argentinië door het leven

gaan. Je weet gewoon niet hoeveel klonen er van je rondlopen en wat voor sporen ze achterlaten. Je mag hopen dat de politie je niet komt oppakken voor misdrijven waar je geen weet van hebt.'

'Ik kan me haast niet voorstellen dat er klonen van me rondlopen, het klinkt zo gek.'

'De meeste mensen geloven niet dat ze gekloond zijn. Laatst hadden we een zaak van een man die zich dat ook niet kon voorstellen. Iemand bleek zijn paspoortgegevens in Spanje te gebruiken voor criminele activiteiten. De fraudeur leek trouwens helemaal niet op zijn slachtoffer, maar de fraude werd niet ontdekt. Toen de Nederlander op vakantie ging naar de Canarische Eilanden, werd hij meegenomen voor verhoor over strafbare feiten. Hij bleek niet het enige slachtoffer. De dader gebruikte 26 aliassen.'

Daar zit ik weer, in de kale verhoorkamer tegenover dezelfde digibete politieagent.

Hij glimlacht vriendelijk. 'Kun je uitleggen wat een "block" is en waarom het niet werkt bij deze man?'

Waarom? Omdat hij een mafketel is. Maar dat zeg ik dan niet. Ik probeer het op een simpele manier uit te leggen: dat een 'block' betekent dat je de gordijnen dichttrekt, maar dat een inbreker je woning binnendringt om de gordijnen open te trekken om naar binnen te kunnen blijven gluren. Dat de inbreker vervolgens ook een trucje uithaalt met nepaccounts, waardoor je deur niet meer goed sluit, zodat hij al je gesprekken met andere mensen kan volgen.

Terwijl ik praat, trekt de muismat van de politieagent mijn aandacht. Daarop staat met grote letters "Pilot aanpak cybercrime Kennemerland". Als dat geen humor is: een

korps dat zelfs via de muismatten aandacht voor cybercrime vraagt en agenten die met twee vingers typen en weinig tot niets over social media en cyberstalking weten.

Maar goed, na nog een paar uur is mijn aangifte compleet en ga ik met een heel tevreden gevoel naar huis. Of het wat wordt, weet ik niet, maar ik ben in elk geval blij dat ik het niet hierbij gelaten heb.

Ik ben nauwelijk thuis of een van mijn beste vriendinnen belt. Ze is helemaal van streek, want haar bankrekening is leeggehaald.

'Ik kreeg problemen bij het internetbankieren en toen werd ik gebeld door een medewerkster van ABN Amro. Ze wilde me helpen om het probleem met het inloggen op te lossen. Ze zei dat ze geen passwords van me nodig had en dat ik die sowieso aan niemand moest geven,' zegt Anna met een gebroken stem. 'Ik moest mijn apparaatje voor het internetbankieren pakken en de code intoetsen die ze me gaf. Vervolgens moest ik haar de responscode geven.'

'Ik weet genoeg. Dat is zowat gelijk aan je pincode weggeven, ook al waarschuwen ze er minder voor.'

'Daar ben ik inmiddels ook achter,' zegt Anna. 'Wat moet ik nu doen?'

'Zo snel mogelijk je pas laten blokkeren en daarna de bank om hulp vragen.'

'Moet ik ze de waarheid vertellen? Straks weten ze dat ik eraan meegewerkt heb.'

'Denk je dat ze dat niet weten? Volgens mij maken ze dat honderden keren per maand mee. Als het niet meer is. Waarschijnlijk kom je er met een kleine boete vanaf. Ik weet dat verschillende banken zo'n bedrag als eigen risico incasseren.'

Ik kan niet uitsluiten dat ik ooit zelf slachtoffer word. Vooral niet als ik lees dat in een test van de Consumentenbond slechts vier procent van de deelnemers alle phishingfraude doorzag. Die mensen waren van tevoren gewaarschuwd!

Alles wat iemand nodig heeft om je identiteit te stelen, is binnen een uur online te vinden. In veel landen is identiteitsfraude een van de grootste problemen op dit moment. De 26-jarige Amerikaan Rogelio Hackett leefde 10 jaar lang van gestolen creditcards zonder opgemerkt te worden. Hij spendeerde maar liefst 36 miljoen dollar. Hackett kreeg de creditcards in handen via hacken, maar je kunt natuurlijk ook zeggen dat je hond een creditcard nodig heeft. Dat klinkt absurd, een hond met een creditcard, maar pas als je het probeert, weet je dat het mogelijk is. Het begon met een e-mailadres dat een man voor de gein voor zijn hond maakte. Al gauw kreeg Clifford J. Dog een offerte voor een creditcard. De man stuurde het ingevulde formulier terug en verzweeg niet dat het om een hond ging. Blijkbaar was er niemand die de juistheid van de gegevens controleerde: de hond kreeg de creditcard toegestuurd.

Kan iemand met een fractie van mijn gegevens iets voor elkaar krijgen, bijvoorbeeld alleen met mijn naam en rekeningnummer? Jeremy Clarkson, de ex-presentator van het bekende programma *Top Gear*, vindt de ophef over datalekken overdreven en publiceert zijn rekeningnummer in een van zijn columns om te laten zien dat kwaadwillenden er niets aan hebben. Binnen de kortste keren wordt een aanzienlijk bedrag van zijn rekening afgeschreven. Het geld is via een eenmalige machtiging overgemaakt aan een goed doel. De bank kan hem niet garanderen dat dit niet vaker gaat gebeuren.

Hoewel ik identiteitsfraude met internetbankieren nog niet zelf aan den lijve heb ondervonden, heb ik al meer dan genoeg computerblunders op mijn naam staan. Zo kwam ik een keer in de verleiding om een consumentenenquête op internet in te vullen. Ik kon er vijfhonderd euro aan cadeaubonnen voor mijn favoriete winkel mee winnen. Ik vond het niet vreemd dat ik uiteindelijk niet won, maar wel dat ik meteen daarna door allerlei bedrijven werd gebeld. Blijkbaar waren mijn gegevens doorverkocht.

Een van mijn andere computerblunders had met een app te maken, waarmee ik zogenaamd kon zien wie mijn Twitterprofiel bekijkt. Voor ik het wist, had ik die foute applicatie toegang gegeven tot mijn gegevens en die verstuurde een tweet namens mij. Volgers die op de link klikten, verspreidden het virus verder. Als nieuwkomer op Twitter had ik mijn lesje geleerd: nooit meer op verdachte linkjes klikken. Ik moet toegeven dat het simpeler klinkt dan het is, want wat is verdacht? De linkjes zien er heel normaal uit en veel apps doen wat ze beloven. Dit is ook de reden waarom spam en virussen op social media zo'n enorme toevlucht hebben genomen: de goede links zijn vaak niet van de slechte te onderscheiden.

Een goed opgezette hack is niets anders dan social engineering: uitzoeken wat het slachtoffer interessant vindt. Als ik op social media iets over elektrische auto's deel, dan is het waarschijnlijk vrij simpel om me met een mailtje over de nieuwste elektrische auto's te verleiden.

Soms is het gewoon een toevalstreffer. Laatst reed ik naar het vliegveld om een vriendin op te halen en op dat moment kreeg ik een sms dat zij al aangekomen was en in

het Hilton-hotel wachtte. Ik had net de neiging om erop te klikken om te kijken waarom ze niet bij de gate stond toen ik me opeens bedacht. Ik las de sms nog een keer. Eigenlijk een doodnormaal gevalletje phishing, maar wat een perfecte timing! Later weer eentje, deze keer via mijn computer: 'You have exceeded the storage limit on your mailbox. You will not be able to send or receive new mail until you upgrade your email quota. Click the below link to upgrade your account.'

Waarom twijfelde ik bij zo'n bijna standaard-phishingmail? Omdat ik niet zo lang geleden een e-mail ontving dat ik de 'storage limit' van mijn website dreigde te overschrijden en dat bericht klopte. Toen heb ik een tientje meer betaald en kreeg ik extra 'storage'.

Ik kan me mijn eigen naïviteit moeilijk kwalijk nemen als zelfs mijn man, die tien keer voorzichtiger is op internet, erin trapt. Laatst stuurde hij me een e-mail door: 'Kun je even vertalen wat hier staat, iets in het Bulgaars.'

'Geen Bulgaars, maar een Russische spammail over juridische dienstverlening, gewoon weggooien,' mailde ik terug.

Maar manlief had al op de link geklikt, anders kon hij het bericht niet lezen. Hij vertrouwde het, omdat het gestuurd was door een goede kennis.

'En nu?' vroeg hij. 'Is mijn computer besmet omdat ik op dat linkje geklikt heb?'

'Geen idee, maar ik weet dat het soms voldoende is om malware op je computer te installeren. En dan kunnen ze best veel dingen op afstand, zoals je wachtwoorden jatten en de beveiligingscodes voor het internetbankieren afkijken.'

Mijn man twijfelde, hij had geen zin om alle program-

ma's op zijn computer opnieuw te installeren. Hoe groot is het risico dat je de pineut bent? Dat kan niemand met zekerheid zeggen.

Ik ben heel benieuwd of het Rickey lukt om mij te hacken en op welke manier. Als hij me een bestandje via e-mail stuurt, dan open ik het niet, omdat ik al weet wat hij van plan is. Hij weet waarschijnlijk ook dat hij iets creatievers moet verzinnen. Overigens twijfel ik geen moment aan de creativiteit van de hackers, want op internet lees ik over de meest bizarre hacks. Soms zijn ze zo bijzonder dat ik twijfel of het klopt. Wat te denken van een bericht over geluidssculpturen die gehackt zijn? Er is een filmpje bij, waarin de wethouder van de gemeente Enschede uitlegt wat er aan de hand is: de hacker verving de vogelgeluidjes uit de boxen met porno-gehijg. De gemeente is druk bezig om het probleem op te lossen. Het filmpje met voorbijgangers die zich allemaal omdraaien als ze de pornogeluiden horen is best geinig, maar is dat echt?

De reacties zijn interessant: van 'echte taboedoorbrekende geluidskunst' tot 'hoe symbolisch, nu weet de gemeente Enschede dat ze genaaid zijn om meer dan een ton voor deze geluidsinstallatie te betalen'.

Wat zo'n nep-berichtje geloofwaardig maakt, is dat een soortgelijke hack in de praktijk goed mogelijk is. De beroemde hacker Kevin Mitnick hackte bijvoorbeeld de geluidsboxen van een McDonald's drive-in. Hij zat in zijn auto om de reacties van de bestellers op de 'doorgedraaide' geluidsbox te observeren. Een vrouw bood hij een gratis hamburger aan als ze even haar borsten liet zien. Deze vrouw was zo verontwaardigd dat ze een honkbalknuppel uit haar

auto haalde en bij McDonald's naar binnen rende om verhaal te halen. Maar de medewerkers hadden geen flauw idee van wie de stem in de speaker was.

15

Foute instanties

Een kennis boekt een vakantiehuis via internet. Ze laat me het plaatje zien, een mooi chalet in Frankrijk.

'Heb je de aanbieder gecheckt?' vraag ik.

'Jij bent helemaal gehersenspoeld door je onderzoek naar cybercrime, hè?' reageert zij. 'Niet alle sites worden door oplichters bemand. Ik zag de advertentie in de krant, ik belde om informatie en ik werd heel vriendelijk te woord gestaan. Ik heb ook het adres van het bedrijf gecontroleerd. Het is hier in de buurt, in Uitgeest.'

Een paar weken later blijkt mijn kennis 483 euro armer. Vakantiehuisjeonline.nl is de zoveelste internetoplichter. De naam scheelde slechts één letter met die van een betrouwbare site: 'vakantiehuisjes' in plaats van 'vakantiehuisje'. De oplichter heeft zijn best gedaan om goed over te komen, met een vast adres, een bemand telefoonnummer en een inschrijving bij de Kamer van Koophandel.

Het telefoonnummer deed het uiteraard niet meer nadat de betaling van mijn kennis was ontvangen. Ze reed naar het adres in de buurt, maar de deur werd geopend door iemand die dat bewuste bedrijf niet kende. Blijkbaar misbruikten ze zijn adres, want hij kreeg rekeningen voor krantenadvertenties die hij nooit geplaatst had.

Een belletje naar de krant leert dat bedrijven een advertentie op rekening mogen zetten als ze een nummer van de Kamer van Koophandel doorgeven. Dat heeft dit bedrijf gedaan: het nummer van een ander bedrijf doorgegeven.

Overigens is het niet alleen in Nederland zo dat instanties heel slordig met de privacy van mensen omgaan. In Bulgarije stelen ze hele bedrijven met miljoenenomzetten via gegevens van de Kamer van Koophandel, want daar is ook alles

op internet te vinden. Ze veranderen 'gewoon' de naam van de eigenaar en schrijven het bedrijf opnieuw in. Zo heb je niets, zo heb je een winstgevend bedrijf op je naam.

Als ik tijdens een vakantie in Bulgarije aan enkele vrienden vertel dat ik met een boek over cybercrime bezig ben, krijg ik het ene na het andere bizarre verhaal te horen.

In de groep blijkt een ervaren hacker te zitten, Ivan. Ik ken hem verder niet en hij is best zwijgzaam, maar opeens beginnen verschillende mensen hem aan te moedigen om me iets over een 'pophack' te vertellen. Niet dat ik enig idee heb wat dat is en Ivan wil er in eerste instantie ook niet over praten. Maar zijn maten blijven aandringen en dan vertelt hij dat hij een van de belangrijkste sites voor popmuziek, een soort Top 100, gestolen heeft.

Ik schuif mijn stoel dichterbij.

'Gestolen? Hoe en waarom?'

'Normaal gesproken werk ik als computerbeveiliger en zit ik aan de goede kant van de wet, maar een bekende zangeres vroeg of ik die site kon ontmantelen, omdat ze elke keer vervelend over haar schreven. Ze heeft me betaald en toen heb ik het gedaan.'

'Maar hoe steel je een website?'

'Ik hackte ze, veranderde de wachtwoorden van de beheerders en stuurde ze een vriendelijke e-mail dat ik hun website tijdelijk overneem en dat ze die over twee jaar terugkrijgen.'

'En toen?'

'Toen werden ze natuurlijk heel kwaad, ze stuurden me diverse dreigmails, maar ja, ze wisten niet wie ik was, dus uiteindelijk hadden ze geen andere keus dan zich erbij neerleggen.'

Hmm, wat een moderne manier van censuur, denk ik bij mezelf. Schrijven ze iets slechts over je, huur je een hacker in en hij zorgt dat de hele website verdwijnt.

Wat ik ook een fascinerende ontwikkeling vind, zijn de drones, de kleine onbemande vliegtuigjes met een camera aan boord. Als ik de experts mag geloven, hebben we straks helemaal geen privacy meer en worden we voortdurend van alle kanten gefilmd. Drones zijn al zo betaalbaar geworden dat je ze zelfs bij speelgoedzaken kunt kopen: voor nog geen honderd euro heb je er eentje met een geheugenkaart waar je honderden foto's mee kunt schieten. Je haalt zo'n drone uit je zak en gooit hem in de lucht om opnames te maken. Je kunt er bekende Nederlanders mee achtervolgen of ermee in de tuin van je ex gluren. Enkelen van de rijkste Nederlanders waren woedend toen zakenblad *Quote* hun huizen en tuinen van heel dichtbij met zo'n drone fotografeerde en de beelden op internet zette. Ik vond hun reactie best begrijpelijk.

In diverse landen wordt er al discussie gevoerd over de impact van de drones en hun gebruik. In Amerika gaat het onder meer over de 'Burito Bomber', een drone die Mexicaans eten bezorgt. Het klinkt allemaal grappig, tot het vliegtuigje een storing krijgt en de hete bonen over passanten kiepert. Als je niet zelf het slachtoffer bent, kan het nog steeds grappig zijn.

De drones zijn bekend geworden door hun toepassingen in oorlogsgebieden. Toekomstige oorlogen zullen vooral met drones en computers uitgevochten worden en veel minder met wapens. Het land verdedigen met een toetsenbord en een joystick is al realiteit. Elke dag slaat Defensie ruim duizend aanvallen op de computers van het Nederlandse leger

af. De aanvallers kunnen virussen installeren die wapensystemen en de luchtverdediging verlammen.

De Belgische militaire inlichtingendienst heeft de Amerikanen onlangs om hulp gevraagd bij de verwijdering van een ingewikkeld computervirus. De Belgen hebben de berichten over de wereldwijde Amerikaanse spionage vast niet gelezen. Straks hebben ze er twee. Waarschijnlijk zijn hun militaire geheimen toch voor niemand geheim, want een hoge militair vertelt zonder gêne dat ze om de twee jaar groot netwerkonderhoud uitvoeren, zoals software updaten en virussen weghalen. Als je als consument je software eens in de twee jaar update, dan weet je zeker dat hackers al je bestanden meelezen.

Hackers maken zelden bekend dat ze in je computer zitten of het moet zijn omdat ze iets gevonden hebben waar ze je mee kunnen chanteren. Sommige computerexperts menen dat een derde van alle pc's geïnfecteerd is. Op internet kun je programma's downloaden die de infectie verwijderen. Veel programma's zijn echter nep en doen niets anders dan nog een virusje in je computer plaatsen, deze keer voor eigen gebruik.

Bij draadloze verbindingen ben je extra kwetsbaar. Ik heb met eigen ogen gezien hoe een volle zaal met mensen geïnteresseerd in het onderwerp privacy bedonderd werd. Ik mocht vertellen over het illegaal verzamelen van persoonsgegevens en toen was het de beurt aan hacker en journalist Brenno de Winter om aan te tonen hoe gemakkelijk cybercrime in de praktijk werkt. Hij bleek het signaal van zijn laptop 'KPN' genoemd te hebben en ja hoor: de meeste mensen in de zaal dachten dat dit Wi-Fi van KPN was. Veel appa-

raten zijn zo ingesteld dat ze bij een bekende naam automatisch inloggen. Vervolgens kon Brenno aanwijzen wie wat zat te doen: 'Jij twittert, jij hebt net een e-mail verstuurd en hij daar zit muziek te luisteren via Spotify...' Lesson learnt: vertrouw nooit op bekende namen van netwerken. En ook niet op onbekende.

Brenno deed de ultieme test om te laten zien hoe kwaadwillenden iemands gegevens kunnen misbruiken. Hij liep bijna negen maanden lang met een ongeldig legitimatiebewijs rond en kwam door elke mogelijke controle, van de Tweede Kamer tot aan het stemhokje.

Hij laat me zijn 'Lichtbildausweis' zien. Het is een kaartje met de afmetingen van een gewoon id, lichtblauw van kleur. Brenno heeft het op een hackersconferentie voor vijftien euro laten maken. Hij vond het er best stoer en grappig uitzien. Hij verwachtte niet dat veel instanties het zouden accepteren. Maar dat deden ze wel. Brenno haalde er simkaarten mee af bij T-Mobile en Vodafone. Ook de Tweede Kamer, de AIVD, drie politiekorpsen, het Europees Parlement en diverse ministeries accepteerden het kaartje als geldig legitimatiebewijs. Onder het mom van veiligheid moeten we steeds meer van onze privacy opofferen en uiteindelijk blijkt dat voor niets te zijn. Leve de schijnveiligheid.

Tal van organisaties beweren dat ze de bescherming van onze persoonsgegevens wel serieus nemen. Hun medewerkers worden getraind om te vragen naar verificatie zodat ze ook telefonisch kunnen vaststellen dat ik het ben en niet iemand die zich als mij voordoet. Maar ze stellen geen moeilijke vragen, want bij de meeste mensen zijn de gevraagde gegevens te googelen, bijvoorbeeld geboortedatum, voorletters en adres. De verificatie stelt dus niet veel voor, maar beter

dan niets. Dat denk je tenminste tot je zelf meemaakt hoe het in de praktijk werkt.

Ik bel namens een Bulgaarse vriendin zorgverzekeraar FBTO om te vragen waarom zij enkele maanden premie met terugwerkende kracht moet betalen. Omdat ze nog nauwelijks Nederlands spreekt, heb ik haar geholpen met het aanmelden en nu voel ik me schuldig omdat ze zo'n gepeperde rekening krijgt. De telefoniste voert de extra veiligheidscheck uit: voorletters en geboortedatum. Nadat ik denk dat ik geslaagd ben voor de controle vraagt ze opeens of mijn vriendin op dit moment bij mij is.

'Nee, ze werkt, ik moest alleen informeren of het klopt.'

'Nou, als ze niet bij u is, mogen we niets over haar doorgeven.'

Teleurgesteld hang ik op.

'Jeetje, kon je niet doen alsof ik bij jou in de kamer was?' zegt mijn vriendin als ze dat hoort. 'Hoe moeilijk kan dat zijn?'

'Geen idee.'

Ik besluit nog een poging te wagen. Deze keer doe ik alsof ik mijn vriendin ben, identiteitsfraude dus. Ik voel me heel erg ongemakkelijk, maar ik beantwoord de veiligheidsvragen. En ja hoor, nu krijg ik opeens alle informatie. Blijkbaar is het lonender om oplichter te spelen dan om te vertellen dat je je vriendin probeert te helpen. En de beveiliging van de persoonlijke gegevens blijkt... tja, een wassen neus. Zo ben ik al weer een illusie armer.

Dat dit niet alleen bij zorgverzekeraars mogelijk is, toonde 'Lektober' aan: hackers lieten een maand lang elke dag zien

bij welke organisaties de privacygevoelige gegevens van klanten op straat liggen. Het waren hacks waarvan velen zeiden: 'Ja, maar dat is niet zo ingewikkeld.' Dat maakt het juist zo eng, dat zo veel mensen het kunnen. Zelfs een kind dat niet kan lezen en schrijven, kan leren hacken. Bij het project One Laptop Per Child lieten onderzoekers dozen met tablets in afgelegen dorpjes in Ethiopië achter, zónder enige instructie. Ze verwachtten dat de kinderen met de dozen zouden gaan spelen. Dankzij de tracking-software zagen ze dat er iets heel anders gebeurde: de kinderen openden de dozen, vonden binnen de kortste keren de aanknop van de tablets en na een paar dagen gebruikten ze 47 apps per kind. Na enkele maanden hackten ze het besturingssysteem van Android, terwijl ze niet konden lezen of schrijven.

Brenno schakelde een keer een bejaarde in om te laten zien hoe onveilig de ov-chipkaart is. Ook de bejaarde lukte het om die te hacken, voor het oog van een draaiende camera. Dat was overigens niet als een geintje bedoeld, want sinds de invoering van de ov-chipkaart hebben de reizigers geen privacy meer. Het systeem volgt voortdurend waar je in- en uitstapt.

Ik gebruik het openbaar vervoer niet meer sinds alles zo veranderd is. Vroeger was het simpel: je kocht een papieren kaartje en stempelde de datum. Maar het stationsloket is opgedoekt om plaats te maken voor EVA, een NS-assistent die alle kennis paraat heeft.

Ik ken EVA niet, maar meneer Braakenburg wel. Hij wil graag informatie over het afschaffen van de papieren keuzekaartjes bij een voordeelurenabonnement en EVA is altijd bereid om te helpen.

'Klopt het dat u wilt weten wanneer u gebruik kunt maken van Keuzedagen?'

'Nee,' zegt Braakenburg.

EVA: 'Oké, dat was niet wat u bedoelde. Wilt u informatie over wat keuzedagen zijn?'

Nee, dat wil hij niet.

EVA geeft niet op: 'U wilt informatie over de vakantiedienstregeling?'

Vakantiedienstregeling? Nou, die EVA raakt steeds meer de kluts kwijt.

'Oké, dat was niet wat u bedoelde. Bent u op zoek naar informatie over een Keuzedag 60+?'

En zo gaat EVA nog een tijdje door tot meneer Braakenburg geïrriteerd raakt en zegt: 'Nu stop ik ermee.'

Maar EVA is niet geprogrammeerd om te stoppen. 'Sorry, dat snapte ik even niet. Wat bedoelt u?'

Niet dat het hebben van een auto veel gemakkelijker is, want tegenwoordig zijn die ook gecomputeriseerd. Als ik de autosleutel per ongeluk meewas, blijkt het een heel gedoe om de nieuwe aan de praat te krijgen. Serieus, tegenwoordig moeten ze je sleutel met een speciaal apparaatje 'aan de praat krijgen'. Dat duurt in mijn geval bijna een uur.

'Je hebt gewoon pech,' zegt de monteur. 'Vaak lukt het sneller.'

Ondertussen tikt het arbeidsloon door.

Natuurlijk is het handig dat ik mijn auto op afstand kan openen, maar dat blijken dieven ook te kunnen. Ze onderscheppen het signaal, kopiëren het en dan kunnen ze mijn auto zonder inbraakschade openen. Dat kan bij veel modellen, maar ik schrik als ik in de krant lees dat vooral onze ge-

zinsauto gewild blijkt bij de bendes die op bestelling werken. In Rusland geven ze subsidie voor het rijden in een hybride en sindsdien worden veel hybrides zonder schade geopend en meegenomen. Ik kan het best afleren om autosleutels mee te wassen, maar hoe voorkom ik dat dieven het signaal van mijn sleutels kopiëren? Daar ben ik nog niet achter.

Ik googel Rickey wat uitgebreider, want ik wil meer over hem weten voordat ik me door hem laat hacken. Google bevestigt wat Rickey me zelf verteld heeft. In een nieuwsbericht staat te lezen dat het Team High Tech Crime van de Nationale Recherche vijf mannen heeft aangehouden die worden verdacht van een inbraak op internet bij de universiteit van Michigan. Bovendien worden zij verdacht van een reeks computerinbraken bij universiteiten in een groot aantal West-Europese landen.

De universiteit van Michigan ontdekte dat op de servers van het computernetwerk een programma was geïnstalleerd om illegale kopieën van computerspellen en films te verspreiden.

Als ik op Twitter meld dat ik met een hacker zaken ga doen, word ik direct gevolgd door een 'dataspecialist'. Eerst denk ik dat het iemand is die voor een commercieel bedrijf data over klanten verzamelt, maar zij blijkt voor de politie te werken. Wat Roos bijzonder maakt, is dat ze met al haar expertise over computercriminaliteit zelf slachtoffer is geworden van identiteitsfraude.

'Ik dacht altijd dat ik niet interessant genoeg was als slachtoffer,' schrijft ze mij in een privébericht. 'Het enige interessante aan mij is dat ik een nerd ben. Als een van de wei-

nige nerds met borsten kreeg ik soms een voorkeursbehandeling. En als ik dom keek, dan wilden ze me allemaal helpen.'

'Nou, ik kijk mijn leven lang dom als ik bij mannen iets voor elkaar wil krijgen. Dat werkt ook bij een digibeet. Maar vertel, hoe ben je slachtoffer van identiteitsfraude geworden als je zo veel over het onderwerp weet?'

'Eigenlijk op een standaardmanier,' zegt Roos. 'Ik gaf een kopie van mijn paspoort bij het afsluiten van een abonnement voor een mobieltje. Daar heeft iemand handig gebruik van gemaakt door het uit het systeem te halen. Daarmee zijn nieuwe telefoonabonnementen afgesloten en ik kreeg de rekeningen toegestuurd. Ik wist van niets toen de politie aan de deur kwam.'

'De conclusie?'

'Dat je niet moet denken dat je geen slachtoffer kunt worden omdat je niet interessant genoeg bent.'

Even later meldt Rickey zich. Hoewel Roos en ik de meeste berichten niet openbaar hebben uitgewisseld, heeft hij gezien dat we contact hebben gelegd.

'Vreemd, ik heb het gevoel dat deze vrouw me volgt. Hadden jullie het over mij?'

'Niet echt. We maakten grapjes over mannen in het algemeen. Als je je aangesproken voelt.'

'Roos werkt bij de politie. Ze duikt op het internet steeds op plekken op waar ik ook kom. '

'Verbaast me niets, de meeste nerds hebben gezamenlijke interesses, dus is het logisch dat jullie op dezelfde plekken komen.'

'Misschien wel, maar ik vind het toch een beetje griezelig dat ik gevolgd word door iemand van de politie.'

'Dat komt doordat je geen schoon geweten hebt. Je hebt ingestemd om mij te hacken, terwijl je in je proeftijd zit.'

'Wrijf het me niet te erg onder mijn neus, anders bedenk ik me.'

'Je had je moeten bedenken voordat je alle universiteitscomputers hebt gehackt. Iemand met toestemming hacken is niet strafbaar. Behalve als je daarna mijn gegevens misbruikt. Maar aangezien je in je proeftijd zit, heb je een goede stok achter de deur om dat niet te doen.'

'Je hebt het goed bedacht, hè?'

'Nou nee, het kwam gewoon zo op mijn pad. Een hacker in proeftijd scoren, dat had ik niet kunnen bedenken.'

Ondertussen ontvang ik een brief van de politie. 'U heeft aangifte gedaan van belediging gepleegd maandag 1 oktober jongstleden. Naar aanleiding van deze aangifte is er door de politie een onderzoek ingesteld. Het resultaat hiervan is dat tegen de dader proces-verbaal kon worden opgemaakt.' In de brief staat verder dat het nu aan de officier van justitie is om mijn strafzaak te beoordelen.

Wat een abracadabra-taal. Ik begrijp sowieso niet voor welke belediging hij een proces-verbaal heeft gekregen, dat waren er zo veel. Heeft de politie er eentje uitgekozen? En hoe zit het met de laster, smaad en stalking? Ik bel het bureau op, want ik wil niet met vragen blijven zitten, zeker niet als het om mijn eigen aangifte gaat.

Brigadier Daan is heel vriendelijk en bereid om uitleg te geven. Zijn uitleg is vrij simpel: 'De computer accepteert niet meer, dus we maken een keus.'

'Waarschijnlijk past er veel meer in jullie computers, maar die zijn niet zo geprogrammeerd.'

'Ja, ons systeem is een beetje ouderwets, waardoor je af en toe niet kunt doen wat je wilt doen,' geeft de agent ruimhartig toe.

'Ik kan er dus van uitgaan dat jullie alles naar de officier van justitie hebben gestuurd en niet alleen een of andere belediging op 1 oktober?'

'Dat klopt.'

Gerustgesteld hang ik op. Ik ben benieuwd of de officier van justitie hier iets mee doet. Van andere slachtoffers weet ik dat digitale pestkoppen, stalkers en ander gespuis bijzonder moeilijk aan te pakken zijn. Vaak krijgen de slachtoffers niet eens de kans om aangifte te doen. Ik heb tenminste die kans gekregen en daar moet ik blij mee zijn. Er zijn al een aantal aangiftes tegen die man en misschien denkt het Openbaar Ministerie op een gegeven moment dat het geen toeval meer is.

16
Afluisteren

Mijn moeder, die al jaren in de Verenigde Staten woont, wil niet op Facebook. Volgens haar is dat een spionage-vehikel. Ze zet nauwelijks dingen over zichzelf online. Als we skypen, schrijft ze liever in het Bulgaars dan in het Engels omdat ze niet wil dat onze berichtjes op een simpele manier door de Amerikanen gelezen worden. Ik verklaarde haar voor gek, tot de privacybom losbarstte met onhullingen over de wereldwijde afluisterpraktijken. De veiligheidsdiensten bleken toegang te hebben tot de data van Skype, Facebook, Google en verschillende andere grote bedrijven. Mijn digibete moeder had gelijk dat ze onze e-mails konden lezen, dat ze onze chats konden volgen en dat ze ook de foto's gestuurd in privéberichten konden zien. Ze hebben bergen data over je en als ze iets verkeerd analyseren, kun je zomaar als potentieel gevaarlijk aangemerkt worden. Ik kan maar beter geen grappige mailtjes met woorden als 'Allah' en 'bom' sturen om geen gedonder te krijgen. Eigenlijk is het van de gekke dat derden stiekem toegang hebben tot wat ik aan mijn moeder schrijf. Ze luisteren miljoenen mensen af in de hoop er een paar op te pakken, de verhouding lijkt volkomen zoek. En het werkt niet eens, want de inlichtingendiensten werden de afgelopen jaren vaak genoeg in de verlegenheid gebracht doordat ze terroristen die ze al in het vizier hadden niet konden tegenhouden.

Inmiddels is internet van een vrij podium in een spionage-instrument veranderd. Nu ik weet dat de inlichtingendiensten onze e-mails en privéberichten 'scannen', dat ze zelfs versleutelde boodschappen kunnen lezen en ook een kijkje hebben in onze smartphones, wordt het voor mij steeds lastiger om te geloven dat ik in het vrije Westen woon. Ik

groeide op in een communistische dictatuur waar de overheid alle burgers als potentieel gevaar beschouwde. De westerse landen struikelden zowat over elkaar om te verklaren hoe verwerpelijk zo'n systeem was en nu doen ze het zelf onder het mom van 'terrorismebestrijding'. De Amerikaanse inlichtingendienst NSA spant de kroon door elke dag miljoenen telefoontjes, zoekopdrachten en e-mails te tappen. In eerste instantie vonden veel hooggeplaatste Europese politici het overtreden van de privacywetten van hun land geen reden voor een diplomatieke rel, tot het duidelijk werd dat ook hun mobieltjes afgeluisterd werden. Toen waren ze opeens wel goed boos, vooral de Duitse Bondskanselier Angela Merkel. Misschien speelde het mee dat zij ook in een communistische dictatuur is opgegroeid.

De Amerikanen bleken zelfs de paus af te luisteren. De paus! Over hem was ik het meest verbaasd. Hoelang gaat het nog duren voordat de Amerikanen God gaan afluisteren? Of denken ze dat ze via de paus sowieso weten wat God voor ze in petto heeft? Maar misschien is de verklaring een stuk simpeler: de Amerikanen zijn er gewoon van overtuigd dat ze Gods zegen hebben om zich de geheimen van bedrijven en burgers toe te eigenen. En van alle bekende voetbalcoaches niet te vergeten. Gek dat de Amerikanen na zo veel illegaal afgeluisterde aanwijzingen en tactieken nog steeds zo slecht voetballen. Dat is juist het verschil van iets goed horen en iets goed gebruiken, daar worden veel fouten in gemaakt. Voetbal is voor mij een bijzaak, maar een voetbalvoorbeeld is de enige manier om aan de voetbalfanaten in mijn vriendenkring te laten zien dat het recht op privacy langzamerhand sterft. Ze willen niet dat het Nederlandse elftal van de Amerikaanse 'losers' verliest.

Als ik naar mijn vrienden kijk, zijn de meeste niet geïnteresseerd in privacy. Dat vinden ze maar een vaag begrip. Misschien dat een enkeling zich zorgen maakt, maar niemand haalt het in zijn hoofd om te protesteren. Hoe anders was de situatie in 1971 in Nederland toen een volkstelling werd aangekondigd. Mensen moesten een vragenlijst met persoonlijke vragen beantwoorden en ook hun naam, adres en geboortedatum vermelden. Velen protesteerden, want ze maakten zich zorgen om hun privacy en om de koppeling van gegevens. Ze wisten nog heel goed hoe het zorgvuldig bijgehouden bevolkingsregister de deportatie van vele duizenden joden vergemakkelijkt had. Maar deelname was verplicht en als je weigerde kon je een gigantische boete of veertien dagen hechtenis krijgen. Toch vulden velen de gegevens expres verkeerd in en 268.000 mensen weigerden om mee te werken aan de opslag van hun gegevens. Tegenwoordig vinden we het normaal dat de overheid honderden databanken heeft en dat die steeds meer aan elkaar gekoppeld worden. Het klinkt een beetje triest, maar de privacy is dood. Misschien zelfs definitief.

Als ik naar Amerika wil vliegen om mijn moeder te bezoeken moet ik al weer zo'n belachelijke lijst invullen: of ik geslachtsziektes heb, een psychische aandoening of een strafblad. Het begint me steeds meer te ergeren dat ik bij voorbaat als een crimineel word beschouwd. Horen de Amerikanen die informatie niet allang te hebben dankzij de mogelijkheid om al mijn internetverkeer te volgen en dankzij alle databestanden die ze van onze overheid cadeau krijgen? Ze krijgen zelfs onze rekeningen, terwijl uit onderzoek is gebleken dat terroristen geen afwijkend betaalgedrag vertonen.

Dat lijstje dat ik invul kost me veertien dollar en ook

voor mijn minderjarige kinderen moet ik hetzelfde bedrag betalen om te verklaren dat ze niet veroordeeld zijn en geen geslachtsziektes hebben. Ik kan er niets aan doen, maar ik denk dat ik met dat geld het illegaal vergaren van data sponsor, want vroeger was hetzelfde lijstje gratis. Miljoenen mensen afluisteren kost geld en iemand moet dat betalen.

Sommige mensen begrijpen niet waar ik me druk over maak als ik niets te verbergen heb. Nou, de afgelopen tijd gingen mijn ogen wijd open. Ik dacht bijvoorbeeld dat het onmogelijk is dat ik de Verenigde Staten niet in mag omdat ik een joint heb gerookt. Ik heb het twee keer gedaan, want ik wilde weten hoe het voelt om high te worden. De eerste keer gebeurde er helemaal niets en daarom wilde ik het nog een keer proberen. Als niet-roker kan ik niet zo goed inhaleren en ook de tweede keer stelde het niet veel voor.

Ik schreef er een grappig blogje over, want ik zag mezelf niet als drugsgebruiker. Kan zoiets kwaad? Ik dacht eerst van niet, maar de Canadese psychotherapeut Andrew Feldman mocht Amerika niet in nadat een douanier hem gegoogeld had en gelezen dat hij in de jaren zestig drugs heeft gebruikt voor een experiment met lsd. In de jaren zestig! Het internet heeft een eeuwig geheugen en onthoudt zelfs dingen van voor het computertijdperk. De Amerikaanse autoriteiten ontzegden Feldman voor een onbepaalde tijd de toegang tot de Verenigde Staten.

Afluisterprogramma's gebruiken alle informatie die over ons te vinden is en produceren verdenkingen op basis van algoritmen. Als je in het echte leven onschuldig veroordeeld kan worden, dan is het online nog gemakkelijker, want foutieve informatie corrigeren is vrijwel onmogelijk.

De echte gevallen laten zien hoe dat werkt. Voor de veroordeling van Lucia de B., de verpleegkundige die zes jaar onschuldig in de gevangenis zat wegens moord op patiënten, werden verschillende feiten aan elkaar gekoppeld. Ze lunchte of roddelde zelden samen met collega's, ze was exprostituee, ze had haar diploma voor de middelbare school vervalst en ze hield van tarotkaarten. Al die dingen hebben niets met moorden te maken, maar ze maakten haar verdacht in de ogen van de rechters. Belangrijk was ook dat een verpleegkundige na het overlijden van een baby meldde dat ze Lucia de B. in de buurt had gezien.

Met de moderne technologieën weet de politie altijd waar we in de buurt van een misdrijf zijn geweest, want onze mobieltjes registreren dat feilloos, ook al staan ze uit. Google slaat al je vreemde voorkeuren op en het plaatje is compleet: je bent in de buurt geweest en je voorkeuren laten te wensen over. Lucia de B. kon de rechters niet overtuigen van haar onschuld, waarom jij wel?

Ik vraag me af hoe online data geanalyseerd worden en of die analyses allemaal kloppen. Er zijn veel programma's op internet die inlichtingendienst in het klein spelen. Een computerprogramma als Tweetgenie beweert bijvoorbeeld mijn sekse en leeftijd te kunnen voorspellen alleen aan de hand van de woorden die ik in mijn tweets gebruik. Naar mijn naam, foto en profiel kijken ze niet en ze gebruiken alleen mijn laatste tweehonderd tweets.

Het programma kijkt naar combinaties van woorden die geassocieerd worden met man en vrouw en met oud en jong. Kenmerkende woorden voor vrouwen schijnen te zijn: 'mijn man' (daar tweet ik dus vrijwel nooit over vanwege zijn recht

op privacy), 'doei' (dat zeg ik tegen vrienden, maar niet op Twitter), 'omg' (blijf ik een gekke uitdrukking vinden, gebruik ik nooit), 'hihi' (ik ben een heel vrolijk iemand, maar 'hihi' gebruik ik zelden), 'mama' (daar tweet ik niet over), 'vriendinnen' (meestal mention ik ze niet op Twitter), 'nagels' (dat is zo'n beetje het laatste waar ik aandacht aan besteed). Van het hele rijtje vrouwelijke woorden gebruik ik alleen 'lief' en 'leuk'. Echt vrouwelijk kom ik dus niet over en ik ben benieuwd of het programma mijn sekse raadt.

Tweetgenie geeft ook voorbeelden van mannelijke woorden: 'bro', 'ajax', 'fifa', 'kerel', 'bier', 'nice', 'mijn vrouw', 'game', 'ouwe'. Van dat rijtje komt me nog minder bekend voor.

Op de site staan ook kenmerkende woorden voor jongere en oudere mensen. Jong: 'echt', 'haha', 'ik', 'jij', 'gewoon', 'oké', 'bedankt'. Als je dat leest vraag je je af waarom ouderen dat soort woorden niet zouden gebruiken, maar blijkbaar is daar onderzoek naar gedaan.

Dan de woorden voor ouderen: 'zoon', 'dochter', 'goedemorgen', 'goede reis', 'sterkte', 'dank', 'prachtig', 'prettig weekend', 'wens'. Oké, prachtig, ik ben beniewd naar mijn digitale leeftijd.

Het enige wat ik hoef in te vullen is mijn Twitternaam en het programma slaat aan het rekenen. In nog geen minuut is het resultaat bekend: ik ben een vrouw van circa 36 jaar. Ze zitten er niet ver naast.

Ook het programma Youarewhatyoulike beweert te kunnen voorspellen wie ik ben. Daarvoor gebruiken ze mijn 'likes' op Facebook. Als de data geanalyseerd zijn, krijg ik een scherm met veel informatie over mezelf, verdeeld in groepen.

Eerst kijken de programma-makers of ik eerder voor traditionele of voor nieuwe dingen kies en komen tot de conclusie dat ik 'intellectually curious' ben naar nieuwe dingen, ongeacht wat anderen ervan vinden. Daar zit wat in. Daarna gaan ze een uitspraak doen over wat voor type ik ben en ze raden het weer. Ik ben succesvol dankzij mijn doorzettingsvermogen, zeggen ze. Ook dat klopt volledig. Ik weet nog heel goed hoe graag ik journalist wilde worden in een taal die ik nauwelijks kon uitspreken. Geen realistisch doel, maar dat was nu eenmaal mijn droom. Dan heb je slechts twee opties: of je droom opgeven of met veel doorzettingsvermogen de taal op zo'n niveau leren dat kranten en tijdschriften je inhuren om voor ze te schrijven.

Volgens de test ben ik verder kalm, emotioneel stabiel en ik ben ook niet iemand die heel lang met negatieve gedachten blijft rondlopen. Ook dat klopt, want ik ben nogal vergeetachtig en dat komt ook bij problemen goed van pas. Ik los ze op of ik vergeet ze.

Youarewhatyoulike doet vervolgens uitspraken over de manier waarop ik naar mensen kijk en vrienden maak: ik ben vriendelijk, behulpzaam en geloof in de goedheid van de mens, zeggen ze. Ik moet toegeven dat dit nog steeds het geval is, ook al heb ik best vaak mijn neus gestoten door te veel op de eerlijkheid en fatsoenlijkheid van mensen te rekenen. Dus ja, door mijn 'likes' kent zo'n computerprogramma mijn kwaliteiten en zwakheden. Best scary eigenlijk, een psycholoog is er niets bij. En dit is nog een vrij onschuldig programma. De overheden van diverse landen weten nog veel meer over mij onder het motto 'Yes, we scan'. Mijn hostingbedrijf stuurde tot 2015 elke nacht de privégegevens van zijn klanten naar Justitie. Telefoonnummers, IP-adres-

sen, naar wie we allemaal gemaild hebben... al die data worden opgeslagen in een bunker van Justitie in Maasland en de overheidsdiensten maken er ruim twee miljoen keer per jaar gebruik van.

Als je het rapport van het afgelopen jaar opvraagt, dan zie je iets geks: 'In de helft van de gevallen is niet vast te stellen of het opvragen van gegevens rechtmatig gebeurde.' Huh? Zelfs dat kunnen ze niet garanderen. Volgens hostingproviders kan zelfs een boswachter die een cursus tot buitengewoon opsporingsambtenaar heeft gevolgd mijn gegevens inzien.

In Nederland worden we gevolgd door zo'n miljoen camera's, bevriende regeringen lezen onze e-mails, de kentekens van onze auto's worden op verschillende snelwegen automatisch herkend en als je ergens parkeert, kan dat doorgegeven worden aan de Belastingdienst.

Als iets schaars is, dan wordt het normaal gesproken meer waard, maar dat lijkt niet voor de privacy te gelden. De meeste mensen maken zich niet druk om de glijdende schaal, want ja, het is voor ons eigen bestwil. De bemoeizuchtige overheid vindt het prima: zodra een privacyschending niet al te veel protest oplevert, wordt al weer een volgende maatregel aangekondigd.

Sommige mensen gaan er blijkbaar van uit dat ze in het digitale tijdperk geen privacy hebben en zetten dan maar alles online. Ze schromen er niet eens voor om hun onwetendheid of zelfs pure domheid te etaleren. Er zijn sites die opmerkelijke status-updates van Facebook verzamelen. Zo vraagt ene Jessica: 'Wat is ook al weer de achternaam van Obama?' en wil iemand anders weten hoe de Nederlandse

schrijver van Anne Frank heet. Twee woorden met twee tikfouten is ook leuk, vooral als het gaat om hoe goed je het op school doet: 'Exsamen gehaalt'. En mijn persoonlijke favoriet: 'Jeeeej, ticket geboekt naar Spanje. Rome here I come!' Maar ook katten die puppy's krijgen, België dat een natte stad wordt genoemd en de moeilijke vraag hoeveel een oplaadkaart van tien euro kost, zijn best leuk voor een uurtje 'zet maar alles online'-vermaak.

Wat mensen over zichzelf posten moeten ze uiteraard zelf weten, kwalijker is hoe slordig veel instanties met onze privacy omgaan. Als ik een beetje pech heb, liggen al mijn persoonlijke gegevens op straat, inclusief mijn medisch dossier. Ik heb nog geen gênante ziektes gehad, maar toch vind ik het geen prettig idee dat iedereen kan zien waarvoor ik ooit bij de dokter ben geweest.

Hoe groot is de kans dat iedereen dat te weten kan komen? Eerst dacht ik niet zo groot, maar opeens kwamen medische en persoonlijke gegevens van meer dan driehonderdduizend werknemers van Praxis, Bijenkorf, V&D, een bekende voetbalclub en honderden andere bedrijven op straat te liggen door een lek in het computerprogramma Humannet. De gegevens waren maandenlang toegankelijk voor externen door de gebrekkige beveiliging. Verzuim, medische dossiers, en reïntegratietrajecten van werknemers: alles was zichtbaar.

Ook de gegevens van honderdduizenden patiënten van het Groene Hart Ziekenhuis in Gouda waren jarenlang toegankelijk op een nauwelijks beveiligde computer. Via internet konden belangstellenden opnamegegevens, diagnoses, behandelplannen en laboratoriumuitslagen raadplegen.

Sites die gehackt worden reageren meestal traag. LinkedIn lekte meer dan zes miljoen wachtwoorden en de gebruikers van de service kregen vrijwel meteen een waarschuwingsmail om nieuwe inloggegevens in te voeren. Mooie actie, ware het niet dat niet LinkedIn zelf, maar cybercriminelen erachter zaten. Toen het nieuws bekend werd, waren ze sneller dan LinkedIn zelf.

Hackers verdienen grof geld aan dat soort 'phishingacties', maar ook aan computergijzelingen. Een hacker versleutelde alle medische dossiers van een ziekenhuis in Illinois zodat de artsen ze niet meer konden gebruiken en vroeg om losgeld. Zo'n losgeldmethode is ook in Nederland niet onbekend. Als je computer besmet wordt met kwaadaardige software krijg je een scherm te zien dat je illegaal films, muziek of porno hebt gedownload. Daarom is je computer tijdelijk geblokkeerd en pas als je honderd euro boete hebt overgemaakt, wordt de computer weer gebruiksklaar. Toen het virus net nieuw was, betaalden ongeveer vijftig Nederlandse slachtoffers per dag de gevraagde boete. Niet echt slim, want de virusverspreider ontving op die manier meteen ook de rekeningnummers en de wachtwoorden.

Hoewel hackers heel veel manieren kennen om je leven zuur te maken, zijn er minstens zo veel manieren om ook zonder hackers slachtoffer van cybercrime te worden. Dat is ook de reden waarom de identiteitsfraude als misdaad zo explosief toeneemt: je hoeft helemaal geen verstand van computers te hebben om iemands identiteit over te nemen.

Vera is pas 24 als ze met identiteitsfraude te maken krijgt en haar grootste nachtmerrie is dat zoiets haar haar leven lang achtervolgt. 'Ze hebben immers mijn persoonlijke gegevens en mijn handtekening. Daar kunnen ze van alles mee

doen, ook al heb ik inmiddels een nieuwe identiteitskaart gekregen,' zegt Vera. Het ergste vindt ze dat ze niet eens iets verkeerds gedaan heeft om slachtoffer te worden.

Vera sluit een mobiel abonnement bij Telfort af en ze moet een kopie van haar legitimatie scannen en e-mailen. Dat gaat allemaal goed, maar opeens worden er bedragen niet alleen namens Telfort, maar ook namens Vodafone van haar rekening afgeschreven. Ze zoekt meteen contact met de telefoonmaatschappij en krijgt te horen dat iemand twee abonnementen op haar naam afgesloten heeft. Twee nog wel! Haar adres blijkt helemaal niet te kloppen, wel haar bankrekening. Bij nieuwe abonnementen vragen de telecommaatschappijen om een cent te pinnen als bewijs dat de opgegeven bankrekening van jou is. Dit lijkt een goede extra controle tegen identiteitsdieven die meestal niet over het bankpasje van het slachtoffer beschikken. In het geval van Vera pinde de identiteitsdief die ene cent van een andere rekening, maar gaf de rekening van Vera op voor het innen van 150 euro per maand. De medewerker viel het helemaal niet op dat het om een totaal andere rekening ging.

Vera gaat naar de politie om aangifte te doen, maar de politie stuurt haar weg. Die avond gaat de telefoon, iemand van de Koninklijke Marechaussee. Vera schrikt zich rot. 'Zij vertelden me dat er fraude is gepleegd met mijn identiteitskaart en ze adviseerden me om aangifte te doen bij de politie. Hoe komisch, daar was ik net weggestuurd! De Marechaussee was er niet blij mee. Ik moest toch terug naar de politie. Ik was er snel bij, ik heb meteen mijn identiteitskaart laten vernietigen door de gemeente en ik heb ook een nieuwe bankrekening geopend. Geen idee of de dader ooit ge-

pakt gaat worden. Ik heb in elk geval geleerd om nooit zomaar een kopie van mijn gegevens te sturen. Ik was echt geschrokken hoe gemakkelijk iemand je identiteit kan overnemen.'

17
Facebook en Google

We strooien constant met informatie die in onze ogen geen kwaad kan, maar die vaak genoeg gebruikt wordt voor identiteitsfraude. Waarom willen we zo graag aan Jan en alleman vertellen wat we aan het doen zijn? Misschien omdat alle andere mensen dat ook doen. Als iedereen een mobieltje bij zich draagt om altijd bereikbaar te zijn, wordt dat gauw normaal. Als iedereen op Facebook zet wat hij aan het doen is, dan denk je dat je zelf te bekrompen bent om dat niet te doen.

Ik zet niet op al die social media dat ik met vakantie ga, want dieven schijnen ook mee te lezen. Nou weet ik het niet meer voor de volgende vakantie: tweets en e-mails beantwoorden, terwijl je liever een weekje offline wilt zijn of accepteren dat ik in de stress raak bij het zien van de gigantische stapel onbeantwoorde berichten bij thuiskomst.

Soms wil ik mijn computer uit frustratie rammen, maar dan tel ik tot tien, terwijl ik aan de woorden van een bevriende computerexpert denk: 'Nooit een computer rammen, want die heeft een RAM-geheugen.'

Gelukkig bepaal je meestal zelf wat je deelt, maar inmiddels is zelfs dat aan het veranderen. In de Amerikaanse staat Louisiana moeten mensen die ooit veroordeeld zijn voor een seksueel misdrijf op hun Facebookprofiel vermelden dat ze 'sex offender' zijn. Als ze dat weigeren, dan kunnen ze tot tien jaar gevangenisstraf krijgen.

Facebook is inmiddels favoriet leesvoer voor advocaten, want mensen vertellen zonder enige schaamte over hun misstappen. Er zijn moeders die de voogdij over hun kinderen kwijtraakten omdat ze beweerden dat ze veel tijd aan hun kinderen besteedden, terwijl Facebook feilloos registreerde dat ze dagelijks urenlang computerspelletjes speelden.

Ik waan me op Facebook onder vrienden, maar tussen al die vrienden lopen heel wat adverteerders stiekem te snuffelen. Alles wat ik post, sprokkelt Facebook bij elkaar en al die data leveren zo'n betrouwbaar profiel van mijn interesses op dat de Amerikaanse multinational me waarschijnlijk beter kent dan ik mezelf ken. Die data verkopen ze aan derden. Positief over Las Vegas? Daar komt een advertentie voor een reis naar Amerika. Liefhebber van boeken? De nieuwste titels verschijnen op mijn scherm. O ja, en de jurkjes niet te vergeten. Eerst vroeg ik me af waarom ik zo veel advertenties van jurkjes zag, maar inmiddels is me dat duidelijk geworden. Mijn kast hangt vol met jurken en Facebook weet dat.

Normaal gesproken ben ik relatief zuinig met mijn 'likes', maar soms kan ik de verleiding niet weerstaan. Het is ook zo simpel om op een 'like' te klikken. Soms heb ik het idee dat vrienden en kennissen daar helemaal geen waarde aan hechten. Laatst had ik technische problemen met Twitter en toen schreef ik alleen het woord 'test' om te zien of het weer werkte. Dat verscheen op het scherm en omdat ik mijn volgers mijn onzintestje wilde besparen, heb ik mijn tweet meteen verwijderd. Wat ik volledig vergeten was, was dat ik kort daarvoor mijn tweets naar Facebook had doorgeschakeld. Een dag later zag ik allemaal 'likes' onder het woord 'test'. Huh?

Wat ik bij Facebook ook niet begrijp is waarom ik de foto's en de statusupdates van bepaalde vrienden vrijwel nooit zie. Sinds kort weet ik waarom. Facebook selecteert op basis van algoritmes wat ik wel en niet zie en filtert tachtig procent van wat mijn vrienden delen gewoon weg. De bedoeling is goed, dat we niet verzuipen in de hoeveelheid posts, maar

het stomme is dat ik vaak updates krijg van vage kennissen en niet van mijn zus. De ranking wordt volgens Facebook gebaseerd op hoeveel likes en reacties een bericht gekregen heeft, maar ook op 'de relatie die de gebruiker heeft met degene die het bericht heeft geplaatst'. Nou, die relatie zien ze blijkbaar over het hoofd.

Facebook weet waarschijnlijk meer over mij dan mijn beste vrienden, maar hoeveel eigenlijk? Dat kan ik opvragen en ik doe het uit nieuwsgierigheid. Ik ontvang een gigantische download met berichten, advertenties waarop ik ooit geklikt heb en foto's die ik ooit gepost heb. Eigenlijk is het bestand verbazend groot, aangezien ik niet heel actief ben op Facebook. De lijst met interessegebieden voor potentiële adverteerders is een openbaring. Bij veel dingen heb ik niet eens een herinnering dat ik er ooit iets over opgezocht heb, laat staan geschreven. Van local bike shop tot Bali en van house music tot application software, echt geen idee waarom Facebook die aan mij koppelt. Maar de meeste trefwoorden kloppen wel: Toyota (onze auto is een Prius), New York (op vakantie geweest), jewelry (bestel ik nooit online, maar Facebook weet blijkbaar dat ik mijn verzameling oorbellen steeds meer uitbreid), police station (in verband met aangifte tegen stalker?), Loesje (daar schreef ik een keer een artikel over), Boekenweek (behoeft geen nadere toelichting). Bij sommige onderwerpen begint het me te dagen dat ik er ooit iets over opgezocht heb, maar bij heel veel weet ik het niet meer. Facebook heeft wel een feilloos geheugen.

De macht van Google is ook enorm. De zoekdienst onthoudt mijn IP-adres en plaatst een cookie op mijn compu-

ter. Zo krijg ik een unieke code, waarmee ik voortdurend te volgen ben. Google heeft tal van diensten, zoals YouTube en Google Maps, en al die data worden gecombineerd en geanalyseerd tot er een pijnlijk precies profiel van mij ontstaat. Het College Bescherming Persoonsgegevens kwam tot de conclusie dat Google hiermee de Nederlandse wet overtreedt. Privacygevoelige gegevens over onze locatie, betalingsinformatie en surfgedrag worden samengevoegd in één overkoepelende database. Deskundigen verwachten dat deze verzamelde gegevens net zo veel over ons kunnen onthullen als het menselijk DNA.

Google is overigens niet de enige die heel veel gegevens over ons combineert en analyseert. Ook minder bekende bedrijven doen mee, zoals kredietverstrekker ZestFinance, die op basis van 'signalen' beoordeelt of iemand een lening waard is. Daaronder vallen je onlinevrienden, je taalgebruik en zelfs de tijdstippen waarop je websites bezoekt.

Het verzamelen van persoonlijke gegevens is een complete industrie geworden. De topmannen van Google hebben er nooit geheimzinnig over gedaan met uitspraken zoals 'We willen dat Google je derde hersenhelft wordt' en 'We weten waar je bent, we weten waar je was. We kunnen min of meer weten wat je denkt'.

Hoeveel Google over je weet, wordt misschien pas echt duidelijk als je denkt de perfecte moord gepleegd te hebben, zoals de 27-jarige chemicus Bart S. Zijn vriendin overlijdt door het eten van een broodje pindakaas geïnjecteerd met gif. De lijkschouwer gaat uit van een natuurlijke dood: hartfalen.

Bart S. trekt pas de aandacht als hij iets te vaak naar het onderzoek begint te informeren. De doorbraak komt als zijn computer in beslag wordt genomen. De politie ontdekt dat hij gegoogeld heeft naar de werking van de stoffen azide en cyanide, die in het bloed van zijn vriendin zijn gevonden. Natriumazide vormt bij aanraking met maagzuur een dodelijk en achteraf niet te traceren gas: stikstofoxine. Een perfecte moord, maar alleen als je niet googelt.

Bedoeld of onbedoeld strooien we met gegevens, omdat we 'niets te verbergen' hebben. Maar er zijn al heel wat mensen die een baan misgelopen zijn doordat buitenstaanders met andere ogen naar onschuldige foto's en teksten kijken. Wat veel mensen niet beseffen is dat niet alleen potentiële werkgevers maar ook uitkeringsinstanties en verzekeraars je in de gaten houden. Verzekeraar Aegon royeerde een klant die op zijn Facebookpagina schreef dat hij aan straatraces had meegedaan. Deze klant had niet eens schade.

Ook werkgevers kijken op internet om te zien wat voor vlees ze in de kuip hebben, vooral bij sollicitatiegesprekken. Dan komen ze heel wat gekke dingen tegen, want veel jongeren hebben een broertje dood aan privacy. Dat kun je ze ook niet kwalijk nemen, want de computer-educatie op school stelt weinig voor en de meeste scholen vinden het niet hun zaak wat hun pupillen op het internet uitspoken. Toch gek, want je onlinereputatie is tegenwoordig bij het zoeken naar een baan niet zelden belangrijker dan wat voor diploma je hebt. Een werkgever gaat niet testen hoe betrouwbaar je bent, hij kijkt gewoon op internet. Kandidaten worden afgekeurd omdat ze 'ongepaste' commentaren plaatsen of te uitbundige foto's van zichzelf op Facebook hebben gepost.

Facebookaccounts schijnen bijzonder geliefd te zijn: er wordt 600.000 keer per dag geprobeerd om een Facebookprofiel te kapen. Dat gebeurt vooral door middel van generatoren van wachtwoorden of door boze exen die de wachtwoorden raden. Slachtoffers gaan vaak door een hel. Bekend is het geval van de Belgische advocaat Bart De Maeseneir, die kinderporno op zijn site plaatste. In werkelijkheid wist hij van niets, want dat werd allemaal gedaan door een vrouw die een appeltje met hem te schillen had. Hij moest zich vervolgens voor iedereen verantwoorden. En hij kreeg ook ouders van tieners op zijn dak die beweerden dat de advocaat met hun jonge dochters aan het chatten was. De chats werden door dezelfde vrouw uitgevoerd.

Als je al die privacyverklaringen van Facebook leest, denk je dat ze rekening houden met je privacy, maar Facebook en concurrent Google spenderen miljoenen aan politieke lobby om te voorkomen dat de politici strengere wetten opstellen. Ze weten ontiegelijk veel over ons en dat willen ze zo houden. Zie maar dingen te verwijderen die over jou geschreven worden en niet kloppen. Er zijn vast ook dingen die wel kloppen, maar die je zo privé vindt dat je die niet wilt delen met een miljoenenpubliek. Voormalig Formule 1-directeur Max Mosley heeft een rechtszaak tegen Google aangespannen vanwege foto's van een sm-feestje die hem al heel lang achtervolgen. De rechtbank besloot dat de uitgelekte foto's een schending van zijn privacy zijn; nu Google nog. De mens tegen de machine.

Overigens hoef je helemaal geen bekend iemand te zijn om last te hebben van de moraliserende massa. Een meisje dat een vriendje pijpte tijdens een openluchtconcert werd net zo

hard aangepakt. Haar foto werd overal verspreid en de commentaren waren zo snoeihard dat ze met psychische klachten opgenomen werd in het ziekenhuis. Natuurlijk was het handiger als ze een betere plek had gezocht voor die seksuele actie, maar waarschijnlijk besefte ze niet dat het internet alles tig keer uitvergroot. Mijn generatie maakte ook zat misstappen, maar toen werd niet alles geregistreerd. Vroeger werd een misstap besproken en dan vergeten, maar het internet vergeet niets. Als je tien jaar geleden een foute opmerking op een forum hebt geplaatst, is die nog steeds te traceren. Soms met een paar muisklikken. Als je wat bekender wordt, zijn er ook mensen die bereid zijn om er meer moeite voor te doen. Eerlijk gezegd zie ik niet hoe we deze foute trend moeten omkeren. Nooit meer van mening veranderen, want alles is ergens vastgelegd en het kan tegen je gebruikt worden? Het lijkt me zo verschrikkelijk als je niets meer spontaan kunt doen en zeggen. Ik vind het juist heel waardevol dat je van mening kunt veranderen. Zoals Adenaur zegt: 'Je hoeft niet altijd hetzelfde standpunt in te nemen, want niemand kan je verhinderen elke dag verstandiger te worden.' Maar ik vrees dat de googelende moralisten daar geen oog voor hebben. Sterker nog: ze interpreteren wat je geschreven hebt op een verkeerde manier en vervolgens heb jij een probleem, want dan valt de massa over iets wat je niet eens gezegd hebt.

Dat overkwam Monique Burger, eigenaar van De Nieuwe Boekhandel. Ze schreef een openhartige blog over de armoede in Nederland, die ze voor het eerst duidelijk zag toen heel veel onbekende mensen het gratis *Droomboek* kwamen halen. Ze beschreef hoe onverzorgd en ruw haar nieuwe klanten waren en hoe groot het contrast was met de vaste

bezoekers van haar boekhandel. Na bijzonder veel grove reacties en een paar bedreigingen moest ze onderduiken. Haar winkel werd beklad.

Ik heb haar blog met stijgende verbazing gelezen. Was dit het stuk waar al die mensen zich druk om maakten? Ze sprak weliswaar over armen die er onverzorgd uitzagen, maar nergens schreef ze dat alle armen in haar ogen zo zijn. Dat hadden al die 'reaguurders' ervan gemaakt.

Jaren geleden moest ik voor een krant een artikel schrijven over gezinnen met schulden. Toen ik naar het opgegeven adres ging, ergens in Den Helder, kwam ik in een buurt terecht waar ik mijn ogen uitkeek. Niks verzorgde tuintjes met bloemen en struiken, maar allemaal gestolen winkelwagens, afval en zelfs vieze luiers op de stoep en in de tuinen. Deze mensen hadden een breedbeeld-tv, maar geen geld voor een minder gescheurde bank of om iets lekkers voor hun kinderen te kopen, vertelden ze. Ik was geschokt en schreef het op. Het was absoluut niet stigmatiserend bedoeld, ik schreef gewoon op wat ik zag. Het enige verschil tussen Monique Burger en mij? Toen had je geen social media en daardoor werd mijn huis niet beklad.

Het gekke is dat je helemaal geen controversiële mening hoeft te hebben om online aangevallen te worden door onbekenden. Soms is een foto al voldoende, zoals in het geval van de twaalfjarige Freek. Met behulp van zijn moeder maakt hij een Twitteraccount aan. Hij schermt zijn acoount af zodat alleen vrienden toegang hebben. Een paar weken later is zijn foto op veel (buitenlandse) sites te vinden met teksten die zijn uiterlijk bespotten. Freek heeft veel sproeten en loenzende ogen. Zijn gezicht wordt ook op naakte vrou-

wen opgeplakt en er komen steeds meer nep-accounts bij.

De foto's blijken lastig te verwijderen via de officiële weg, dus besluit de vader van Freek om berichtjes te posten op de tijdlijn van de nep-accounts met het dringende verzoek om de foto van zijn zoon te verwijderen. Als reactie daarop maakt de dader de echte identiteit van Freek bekend en er duiken ook nieuwe foto's van hem op. Die blijken van de Facebookpagina van zijn moeder te zijn gestolen. Inmiddels gaat ook Google de mist in door de echte naam van Freek aan nep-accounts en karikaturen te koppelen. Omdat het zo uit de hand is gelopen, overwegen zijn ouders om de naam van hun zoon te veranderen – een zeer extreme maatregel voor een probleem dat anders onoplosbaar blijkt.

Het verhaal van de vijftienjarige Angelina heeft raakvlakken met wat Freek meegemaakt heeft, want ook zij ervaart hoe gemakkelijk het is dat iemand je digitale identiteit steelt. Angelina verandert van een braaf meisje in een slet die smeekt om 'genomen' te worden. Degene die achter het nep-account zit, verpreidt pornoplaatjes namens haar. Angelina durft niet meer naar school, omdat opeens allerlei jongens op haar afstappen om te vertellen dat ze zo'n sexy chick best een beurt willen geven. Het enige wat Angelina kan doen, is iedereen ervan proberen te overtuigen dat haar identiteit gestolen is en dat ze al aangifte gedaan heeft.

Haar moeder is nog steeds boos over de manier waarop de aangifte verlopen is. 'De politieagente wist werkelijk niet wat ze ermee moest, ze ging eerst informeren of ze de aangifte überhaupt moest opnemen,' zegt haar moeder. 'Ze zeiden tegen ons dat we niets moesten verwachten, omdat identiteitsfraude geen prioriteit heeft. Ik begrijp best dat ze liever

woninginbraken oplossen, maar identiteitsfraude kan ook iemands leven kapotmaken en dat wordt onderschat. Na de aangifte stuurde de politie ons naar huis zonder ons tips te geven wat te doen. We moesten daarna zelf uitzoeken hoe je zo'n nep-account verwijdert.'

Ondertussen ging Angelina wel naar school, maar ze kwam bijna elke dag huilend terug. Ze had een vermoeden wie het gedaan kon hebben. 'Die naam hebben we aan de politie doorgegeven, maar ze zeiden dat het IP-adres van de computer geen bewijs is, want misschien heeft iemand anders ook deze computer gebruikt.'

Van het verwijderde seks-account van Agelina zijn nog steeds sporen te vinden op internet, maar die wordt niet aan haar echte naam gekoppeld. 'Gelukkig maar,' verzucht haar moeder opgelucht. 'Stel je voor dat je gaat solliciteren en je toekomstige werkgever dit soort grove plaatjes ziet, dan kun je ervan uitgaan dat je niet aangenomen wordt.'

Daar kan ze best gelijk in hebben: tegenwoordig ben je wat Google zegt dat je bent. Dat klinkt misschien te kort door de bocht, maar onlinereputaties worden steeds belangrijker. Het is geen overbodige luxe om jezelf af en toe te googelen.

18

Digibeet meets hacker

Sinds ik her en der vertel dat ik me laat hacken, krijg ik van alle kanten waarschuwingen. Niemand heeft er begrip voor, ze vinden het allemaal een te groot risico.

'Heb je het artikel van een zekere Mister Penenberg gelezen?' vraagt een goede vriend.

'Mister Penenberg? Dat zegt me helemaal niets.'

'Nou, hij wilde ook gehackt worden en hij had zijn hackers goed uitgekozen, een professioneel team gespecialiseerd in ethische hacks. Zijn identiteit is dus niet gestolen, maar ze gingen vrij ver. Ze googelden zijn interesses en ook die van zijn vrouw en ze kregen allebei een betrouwbaar uitziende e-mail. Zijn vrouw hapte als eerste toe en opende het bestandje. Zo kwamen ze met gemak in haar computer en daar waren ook veel gegevens over haar man te vinden.'

'Verbaast me niets. Als ze in de computer van mijn man komen, vinden ze waarschijnlijk ook veel bruikbaars, ook al versleutelt hij zijn wachtwoorden.'

'Het grappige is dat hun wachtwoorden ook niet zomaar toegankelijk waren,' zegt mijn vriend. 'De hackers maakten een nep-scherm dat steeds om het masterwachtwoord vroeg. Heel irritant. Na verschillende keren negeren heeft zijn vrouw het toch maar ingevuld.'

'Ik vrees dat ik op een gegeven moment ook toegegeven zou hebben,' mompel ik zachtjes. Ik denk daarbij aan Google, dat me de laatste tijd steeds om mijn telefoonnummer vraagt met de zinnen: 'Help ons uw account te beschermen. Bevestig uw mobiele telefoonnummer en wij zullen u op de hoogte stellen als we ongewone activiteiten opmerken op uw account.' Elke keer negeer ik het, maar Google geeft niet op. 'Bevestig uw mobiele nummer. De meeste mensen ontvangen nog geen drie waarschuwingen per jaar. Dit

nummer wordt alleen gebruikt voor veiligheidsdoeleinden.'

Fijn, maar ik hoef geen extra veiligheid als ik googel, dus blijf ik de vraag stug negeren. Tot Google me weer dezelfde vraag stuurt, maar deze keer is het vakje voor het telefoonnummer niet langer leeg. Ik zie de cijfers van mijn mobiel. De brutaliteit! Dat Google mijn mobiele nummer al weet, is misschien weinig verrassend, maar het voelt alsof ze willen zeggen: 'Oké, genoeg spelletjes, we weten al alles over je, dus klik maar op "bevestig" en dan ben je van ons af.'

Ik geef het op, het spel is niet leuk meer als een van de spelers vals speelt.

Sinds ik met het onderwerp cybercrime bezig ben, lijken heel veel mensen in mijn omgeving hier opeens ervaring mee te hebben. Waarschijnlijk niet meer dan vroeger, maar toen praatten we er gewoon niet over. Nu zijn ze allemaal bereid om te vertellen wat ze zelf meegemaakt hebben.

'Ik kreeg laatst een herinnering van mijn tandarts dat ik de volgende dag voor controle moest,' zegt Ivon. 'Tot mijn stomme verbazing zag ik in de e-mail mijn naam, adres, telefoonnummer en zelfs mijn burgerservicenummer staan. Die staan niet alleen in de e-mails die hij verstuurt, maar ook op servers die waarschijnlijk niet goed beveiligd zijn. Ik heb toch maar even geklaagd. Volgens hem was ik de eerste die zich zorgen maakte om de veiligheid van de gegevens.'

Anita ontdekte dat ze een onlinelening met slechts een kopie van een legitimatiebewijs kon afsluiten. Ze besloot te testen of dat op de naam van iemand anders kon. Ze gaf haar eigen adres op, maar stuurde de kopie van het legitimatiebewijs van een vriendin in, met een vervalste handtekening. Die vriendin wilde graag een lening, dus maakten

ze zich geen zorgen als de aanvraag geaccepteerd werd. De vervalste handtekening bleek geen probleem. Het geld werd keurig op de verkeerde rekening gestort.

Mijn webmaster maakte ook iets geks mee. Zijn vorige vriendin bleek spullen besteld te hebben, maar niet op tijd betaald. Ze waren al een tijdje uit elkaar, maar toch leverde dat hem een plek op de zwarte lijst van het Bureau Krediet Registratie op. Daar kwam hij pas jaren later achter, net op een moment dat hij voor een nieuwe hypotheek moest bewijzen dat hij geen betalingsachterstanden had.

Een kennis die muzikant is, klaagde dat elke horeca-uitbater in wiens zaak hij met zijn bandje speelt zijn legitimatiebewijs kopieert. Zonder kopie geen betaling. Eigenlijk hetzelfde verhaal als bij mij: als ik voor een tijdschrift schrijf, willen ze ook een kopie van mijn paspoort voordat ze mijn factuur betalen. Nu schrijf ik voor een beperkt aantal bladen, maar mijn kennis heeft inmiddels bij honderden cafés een kopie moeten achterlaten.

Veel mensen zien de gevaren niet en doen niet moeilijk over kopietjes, zeker niet bij officiële instanties. Maar de meeste bedrijven en organisaties mogen dat helemaal niet vragen. De hotels in Nederland mogen dat bijvoorbeeld niet. In andere landen weer wel en zo kan je identiteit vooralsnog in omloop komen en wereldwijd te koop aangeboden worden. Met een tip van een privacyfreak probeer ik dat sinds kort te voorkomen. 'Jullie mogen het nummer van mijn paspoort noteren, maar niet kopiëren,' zeg ik als we op de vakantiebestemming arriveren.

'Hoezo?' De hotelmedewerkster kijkt me vragend en enigszins achterdochtig aan.

'Nou, in Nederland is het verboden om paspoorten te

kopiëren en de staat kan jullie voor de rechter slepen omdat jullie de paspoorten van Nederlandse burgers kopiëren.'

Dit is een enorme bluf, maar de dame kijkt behoorlijk geschrokken. Het komt helemaal niet in haar op om te zeggen dat de Nederlandse privacywetten in het buitenland niet geldig zijn.

'Aha, oké,' mompelt ze. 'Dan neem ik het nummer gewoon over. In principe moet dat voldoende zijn.'

Ik kijk mijn man triomfantelijk aan, het werkt! Al weer een manier gevonden om een stukje van mijn privacy te beschermen.

Wat doe je als je privacy niet door onbekenden bedreigd wordt, maar door je eigen vriend met wie je samen een kind hebt? Het klinkt misschien vreemd, maar als het om identiteitsfraude gaat, lijkt niets gek genoeg. Anna Jansen ontdekte na een relatie van tien jaar dat haar vriend accounts op haar naam en met haar foto's had aangemaakt om biseksuele vrouwen te versieren. Hij verstuurde enkele naaktfoto's die ze speciaal voor hem had gemaakt naar onbekenden, soms ook naar mannen.

Op een gegeven moment kreeg Anna een berichtje van een bekende. 'Wat plaats jij pikante foto's op Facebook.'

Huh? Pikante foto's? Anna wist van niets. Maar ze kreeg een linkje doorgestuurd en zo ontdekte ze dat ze al zeven jaar een Facebookpagina had met honderden vrienden.

'Als je zoiets ziet, dan weet je helemaal niet wat je moet denken,' zegt Anna. 'Eerst had ik geen idee wie erachter zat. Ik kon me niet voorstellen dat mijn eigen vriend dat deed. Maar op de pagina stonden foto's die niet door iemand anders geplaatst konden zijn. Ze waren gewoon té privé. Ik

ontdekte dat hij ook op datingsites profielen van mij aangemaakt had om met biseksuele vrouwen te chatten.

Ik vertrok met ons vijfjarig dochtertje. Ik kon er niet tegen dat mijn eigen vriend mijn identiteit had gestolen. Ik deed aangifte, omdat ik op een soort morele genoegdoening hoopte, maar die aangifte werd geseponeerd, want ze zeiden dat het niet te bewijzen viel dat hij het gedaan had. Dat heeft hij trouwens aan mij bekend, maar daar had ik geen bewijs van.'

Anna ging naarstig op zoek naar nog meer nep-accounts van zichzelf en stuurde verzoeken om die te verwijderen. Maar dat bleek lastiger dan gedacht. Een enkele keer liet haar ex alles staan, maar veranderde gewoon haar naam, zodat ze zichzelf via zoekopdrachten lastig kon vinden. 'Dan pas merk je hoe groot het internet is en hoe kwetsbaar je bent. Iemand kan van alles over je online zetten en er is niemand die dat controleert.'

Wat me bij alle gesprekken met slachtoffers vooral opvalt is op hoeveel verschillende manieren je identiteit gestolen kan worden en hoe onvoorspelbaar de gevolgen soms zijn. De meeste slachtoffers die het overkomt zijn bang dat het opnieuw begint. Sommigen worden zowat paranoïde en vertrouwen bijna niemand meer.

De 31-jarige Linda Dummer had ook zo'n moment. Anna kwam er vrij gauw achter dat de dader alleen haar eigen vriend kon zijn, maar Linda tast al zes jaar in het duister. Ze heeft al meerdere aangiftes gedaan tegen haar onzichtbare vijand. Een paar keer moest ze voor de rechter verschijnen omdat ze het vertikte om spullen te betalen die op haar naam besteld waren. 'Maar hoe kan het dat op de be-

stelling uw naam, uw geboortedatum en uw adres staan?' vroeg de rechter. Tja, die gegevens zijn tegenwoordig niet zo moeilijk te achterhalen.

'Ik kon uiteraard beweren dat ik al die spullen nooit gezien heb, maar hoe moet ik dat bewijzen?' zegt Linda. 'Een paar keer moest ik dus betalen. En een paar keer heb ik die rekeningen betaald, omdat ik bang was dat de incassokosten verder opliepen en een deurwaarder beslag op mijn spullen kwam leggen. Je staat met je rug tegen de muur en je kunt alleen maar denken: waarom zou ik in godsnaam al die troep bestellen? Er zat zelfs mannenkleding tussen. Alles bij elkaar heb ik zo'n elfduizend euro moeten betalen voor iemand die op mijn naam flink aan het shoppen was geslagen.'

Linda wist niet wie ze moest verdenken. Ze vond een goede kennis een vreemd type, maar was deze vrouw tot zoiets in staat? Ze had een keer iets verdachts meegemaakt. De doktersassistente had een recept voor de slaappillen van Linda verwisseld met iemand die hetzelfde middel gebruikte. Dat werd snel rechtgezet, maar na een tijdje ging Linda naar de apotheek om haar pillen met een herhaalrecept op te halen en die bleken al door iemand anders te zijn opgehaald. Iemand die ze niet kende. Ze moest bij de huisarts zien te bewijzen dat zij het niet was. Dat herhaalde zich nog een paar keer tot Linda een blokkade instelde: voortaan mocht alleen iemand met haar paspoort in de hand de medicijnen komen afhalen. De rekeningen van het ziekenfonds moest ze zelf betalen, want een gedeelte van de medicijnen van de onbekende afhaler was voor eigen risico.

'Ik ben nu zo'n zes jaar bezig met het oplossen van de puinhopen van de identiteitsfraude,' zegt Linda. 'Laatst kreeg ik een bericht van de ING dat mijn betaalrekening

omgezet was naar een studentenrekening, waardoor ik recht had op krediet. Ik vloog naar de bank, hoezo krediet, ik wilde helemaal geen nieuwe schulden. Bovendien: hoe konden ze dat zonder handtekening regelen? Een telefoontje van een onbekende was blijkbaar genoeg. De medewerkster vond het vreemd, vooral toen ik vertelde dat ik door identiteitsfraude een negatieve codering heb bij het Bureau Krediet Registratie. Alles werd teruggedraaid en ik was gerustgesteld, tot ik weer dezelfde brief kreeg. Ik kon het haast niet geloven. De ING draaide het weer terug, ze zouden het uitzoeken. Geen idee wat ze uitgezocht hebben, maar onlangs was het al weer raak: iemand had opnieuw mijn betaalrekening naar een studentenrekening omgezet. Dat dit zomaar kan is al verbijsterend, maar dat dit drie keer achter elkaar gebeurt, daar heb ik echt geen woorden voor.'

Er lopen nog twee rechtszaken tegen Linda. 'De ergste is een hoog bedrag voor een mobiel abonnement. Ik heb een keer een abonnement betaald dat niet van mij was, maar dit is bij een andere maatschappij. Het is zo lastig om te bewijzen dat jij het niet bent, dat is het hele probleem met identiteitsfraude. Ik ben net niet doorgedraaid door alle ellende, maar er was wel een periode waarin ik totaal geen vertrouwen meer in de mensen had. Ik probeerde iedereen in de gaten te houden, kon niet meer helder nadenken. Iemand heeft de macht over je, maar wie? Mede dankzij de steun van mijn ouders werd ik wat nuchterder.'

Ik herinner me nog goed de tijd dat alles veel persoonlijker was en identiteitsfraude nauwelijks bestond. We konden niet via een website spullen bestellen op de naam van

iemand anders en ook de recepten werden niet digitaal naar de apotheek doorgestuurd. Ik herinner me zelfs de tijd dat we helemaal geen computers hadden. Eigenlijk vind ik dat best bijzonder. Mijn zoons hebben die tijd niet meegemaakt en ze weten helemaal niet hoe je je urenlang, dagenlang en zelfs maandenlang prima kunt vermaken zonder computer.

Op een dag loop ik met ze door een museum waar oude computers tentoongesteld zijn.

'Vroeger had ik ook zo'n bakbeest,' zeg ik en ik wijs naar een van de exemplaren.

'Waar is dat gat voor?' vraagt de jongste.

'Voor de floppy's.'

'Voor wat?'

'Voor de floppy's. Daar kon je bijvoorbeeld spelletjes op bewaren, want onze computers hadden niet veel geheugen om zelf spelletjes te onthouden. En internet was ook nog niet uitgevonden om die online te spelen.'

'Dus jullie hadden geen internet? Waar gebruikten jullie dan de computers voor?'

Zijn vader en ik kijken elkaar aan. We zijn bijna in staat om in lachen uit te barsten, maar de vraag van onze zoon is bloedserieus. Tja, hoe leg je de jonge generatie uit dat je de computer vooral als tekstverwerker gebruikte en om bijvoorbeeld de namen van je elpees in tabellen te zetten? Dat is in zijn ogen een grote 'faal'. Als ouders hebben we al een suf imago en om nou ook nog zo'n faal erbij te krijgen?

'Ik speelde gewoon ook leuke spelletjes hoor,' probeert zijn vader hip te klinken.

Ons zoontje kijkt hem doordringend aan: 'Pacman zeker?'

Betrapt. We moeten toegeven dat er toen niet veel soeps

was vergeleken met de levensechte spelletjes die ze tegenwoordig spelen.

Ik probeer een voordeel van de goede oude tijd te bedenken, dat moet er ook vast zijn. Na zo'n faal kunnen we wat extra punten gebruiken om ons imago op te poetsen. Opeens weet ik het: 'We waren wel vrij veilig achter onze computers. Geen hackers en geen virussen.'

'Ja, duh, nogal logisch als er geen internet was. Hoe moeten ze anders in je computer komen?'

Mijn man buigt zich naar mij en fluistert: 'Dat kon ook via floppy's hoor, dat heb ik zelf meegemaakt, maar vertel dat maar beter niet aan hem.'

Een floppy is nergens in het museum te bekennen, dat scheelt uitleg, dus laten we het erbij.

De vraag van mijn zoontje maakt me wel nieuwsgierig. Wie waren de eerste hackers en wat moesten ze met een virus op een floppy als ze er toch geen gegevens mee konden ontfutselen? Waar deden ze het dan allemaal voor? Ik vind een boek over computergeschiedenis en ik lees het met stijgende verbazing. Als mijn generatie suf is, dan is die vorige helemaal suf. De foto's spreken boekdelen. De computers moesten bedienden hebben. Nu voel ik me af en toe ook een bediende van mijn computer, maar vroeger was dat letterlijk. Vrouwen sliepen meestal op een veldbed naast zo'n bakbeest, want als het zoemen stopte of anders klonk, dan moesten ze meteen ingrijpen. De computers waren supertraag in hun berekeningen en het was niet rendabel om ze uit te zetten. Zes vrouwen die dag en nacht voor een computer zorgen was geen uitzondering. Alleen maar vrouwen trouwens, want die bleken een stuk preciezer dan mannen

en met zo'n waardevol apparaat moest je uiterst voorzichtig omgaan.

Mijn kinderen kunnen wel zeuren hoe log en lelijk mijn eerste computer was, maar eigenlijk was het net een veertje vergeleken met zijn voorgangers. ENIAC, een van de eerste computers, woog 28 ton, net zo veel als 8 olifanten. Ik kan me dat haast niet voorstellen, laat staan mijn kinderen, die computers met een bolle toeter aan de achterkant al iets heel geks vinden.

En de hackers dan? Die waren op dat moment meer met de uitdagingen van de techniek bezig dan met virussen verspreiden. De eerste bug was ook niet door hackers bedacht. Deze werd ontdekt door een vrouw die wilde weten wat er mis was met de computer van de universiteit. Ze vond in de computer een geplette mot, daardoor was de computer vastgelopen. Ze lijmde deze in haar logboek en schreef er 'bug' onder, Engels voor 'mot'. De bugs die ik in mijn computer krijg zien er anders uit. Ik kan ze in elk geval niet zelf verwijderen, het 'debuggen' laat ik aan de nerds over.

Soms denk ik met nostalgie terug aan de goede oude tijd. Oké, de computers waren verschrikkelijk traag, maar we leken er niet veel last van te hebben, want ons leven draaide niet om de computer. We spraken af met vrienden voor een kop koffie in plaats van hun foto's op Facebook te liken. En we ontvingen geen bedreigingen via social media. Tegenwoordig worden er in Nederland zo'n 35.000 bedreigingen via Twitter geuit. Per dag. Ongeveer tweehonderd dagelijkse bedreigingen zijn zo ernstig dat de politie er werk van maakt. Een 'niet-OK'-knop is zo gek nog niet om men-

sen aan te geven die de social media voor asociale doelen gebruiken. Het lijkt weliswaar op het ouderwetse klikken, maar dan in een modern jasje voor het goede doel, want tijden veranderen. Vroeger moest je best veel moeite doen om iemand te bedreigen. Tegenwoordig kruip je gewoon achter je laptop of pak je je mobieltje. Er zijn mensen die blijkbaar niets beters te doen hebben dan de hele dag door digitaal pesten. Omdat het zo gemakkelijk is. Geef een domkop een laptop en hij verandert in een held. Binnen de kortste keren heeft hij meelopers gevonden die van relletjes smullen en ook gaan meedoen voor de lol.

19
Digi-dood

Alsof ik nog niet genoeg digitale zorgen heb, hoor ik tegenwoordig ook na te denken over mijn digitale dood. Dat adviseren althans grote partijen als Google en Facebook, maar ook tal van juristen die zich op de digitale dood gestort hebben. Er zijn ook initiatieven die juist de andere kant op gaan. Doodgaan hoeft niet meer definitief te zijn, althans niet volgens de website LivesOn. 'When your heart stops beating, you'll keep tweeting.' Is dat een grap? Ik hoef persoonlijk niet te blijven tweeten na mijn dood, lijkt me nogal luguber. Voor de mensen die het wel willen, belooft LivesOn automatisch samengestelde berichten vanuit het hiernamaals, die persoonlijk worden gemaakt door een analyse van je eerdere tweets en voorkeuren.

Veel gebruikers van social media en eigenaren van bedrijfsgeheimen in de cloud schijnen zich trouwens nauwelijks bewust te zijn van hun sterfelijkheid. Voor zover ik het weet heb ik geen geheimen in een cloud, met mijn 45 jaar besef ik donders goed dat ik sterfelijk ben, maar ik denk inderdaad niet na over wat er met mijn 'digitale bezittingen' gebeurt. Wat een lastig onderwerp. Hoe ziet een digitale begraafplaats eruit? Wie kan erbij?

Google en Facebook hebben inmiddels 'stervensapplicaties' gelanceerd om onze digitale dood bespreekbaar te maken en notarissen bieden speciale kluizen aan. De dood aangeboden door Google en Facebook is trouwens niets anders dan na een periode van inactiviteit al je gegevens automatisch wissen.

Ik ben benieuwd hoe je al je sporen op internet uitwist, volgens mij is het onbegonnen werk. Een Amerikaanse journaliste liet op een bijzondere wijze zien hoe de kruimeltjes informatie die her en der over ons te vinden zijn een giganti-

sche berg kunnen vormen. Ze googelde Googletopman Eric Schmidt bij elkaar en al die informatie over zijn aandelen, hobby's, politieke voorkeur en nog veel meer plaatste ze op de site news.com. Het resultaat: een briesende topman die klaagde over schending van zijn privacy en dat zelfs zijn veiligheid in het geding is, omdat iedereen opeens zo veel over hem weet. Voor het gemak zag hij even over het hoofd wie dat mogelijk maakt.

Google is onovertroffen, omdat we vaak verschillende Googlediensten gebruiken en al die informatie aan elkaar gekoppeld wordt. Neem nu een applicatie als Google Now, die je een seintje geeft als je te laat dreigt te komen op een afspraak die je in Google Calendar hebt gezet. De dienst kijkt naar waar je mobieltje zich op dat moment bevindt en kijkt op hoeveel kilometer rijden je afspraak is. Ruim van tevoren krijg je een herinnering om te vertrekken. De app kijkt ook naar de drukte op de wegen. Best handig, maar sommige mensen bleken onaangenaam verrast dat Google Now ze ook herinnerde aan verplichtingen die niet genoteerd waren in hun agenda. Huh, hoe weet Google waar je werkt en dat je nog een halfuur nodig hebt om op je werk te komen als je dat nergens genoteerd hebt? En hoe komt de dienst aan je privéadres?

Op zich is dat niet zo moeilijk, want de locatiegegevens van je telefoon zeggen heel veel over je. Als je elke avond terugrijdt naar dezelfde plek, dan is dat waarschijnlijk je adres. Als je op werkdagen veel uren ergens te vinden bent, dan is dat waarschijnlijk je werk. Google weet dus wat je werktijden zijn en welke dagen je te laat komt. Waarschijnlijk weet de zoekmachine ook wat je favoriete kroeg is en met een beetje pech ook hoe vaak je bij je minnaar of minnares

komt, mocht je die hebben. Maar ja, we zijn allemaal brave burgers en we hebben niets te verbergen, daarom vertrouwen we op Google. En voor het gemak natuurlijk, want handig is het wel. Als je bij je minnares uithangt en Google kent je vaste ritme, kun je een seintje krijgen dat het tijd wordt om naar je vrouw te gaan.

Google weet dat ik aangifte heb gedaan tegen mijn digi-stalker en is er sowieso van op de hoogte dat hij in alle toonaarden ontkent. Dat weet ik zeker omdat ik hem uit nieuwsgierigheid even googel om te zien of hij nog steeds met me bezig is. En ja hoor: hij verspreidt driftig het nieuws dat mijn zaak tegen hem geseponeerd is, omdat er niet eens 'een begin van bewijs' was. Woedend bel ik het Openbaar Ministerie: hebben mijn digi-stalker en Google de informatie over de geseponeerde rechtszaak eerder in handen dan degene die de aangifte heeft gedaan? De medewerker van het Openbaar Ministerie is best bereid om me aan de telefoon informatie te geven als ik mijn naam en dossiernummer zeg.

'Hoe komt u daarbij, dat de zaak geseponeerd is?' vraagt hij.

'Ik zag dat mijn stalker dat schrijft.'

'Maar het klopt niet. Zo te zien is er genoeg gebeurd. De politie heeft de zaak in elk geval niet geseponeerd en bij het Openbaar Ministerie is hij in behandeling.'

'En wat wil in behandeling zeggen, hoelang gaat dat nog duren?'

'Dat kan ik helaas niet zeggen. Maar het OM heeft twee indelingen: lichtere en zwaardere zaken. Ik zie dat uw aangifte eerst bij de lichtere zaken is beland, maar na beoordeling toch bij de zwaardere zaken is terechtgekomen.'

Ik luister enigszins verbaasd, want de stapel met lichtere zaken zou ik persoonlijk toepasselijker vinden. Er gebeuren tenslotte veel ergere dingen.

'Dus u kunt niet zeggen hoelang het gaat duren? Maanden, jaren?'

'Houd het maar op enkele maanden,' zegt de medewerker. 'En als je dan niets hoort, bel je ons nog een keer.'

Na mijn aangifte was mijn digi-stalker een stuk minder actief, maar opeens heeft hij een opleving, blijkbaar in de overtuiging dat mijn aangifte geseponeerd is. Ik zie al weer tientallen tweets over mij, waarin hij me voor alles en nog wat uitmaakt en me een rijtje psychische stoornissen toeschrijft. Knap dat mijn huisarts ze nog niet ontdekt heeft, maar hij wel. Je hebt van die mensen die van alle markten thuis zijn. Hij dicht me ook een 'secret lover' toe (dat moet ik vooral niet aan mijn man laten lezen). Ook leuk: 'Geruchten gaan dat Genova ex-paaldanseres was in Bulgarije,' schrijft hij. Was het maar waar, op zo'n spannend verleden kan ik niet bogen.

Laatst heb ik op Facebook de cover van mijn nieuwe boek laten zien. De volgende dag was de titel als website geregistreerd door mijn stalker, zodat ik die niet meer zelf kon gebruiken. Dat zag ik niet aankomen en toegegeven: origineel is het wel. De inhoud is helaas voorspelbaar: een dumpplaats voor al zijn gedachten over mij. Maar daar is iedereen een beetje op uitgekeken en het levert hem blijkbaar niet genoeg bezoekers op, dus moet hij met iets nieuws komen. En dan komt het: hij roept alle kankerpatiënten op om mijn boek te boycotten. Kankerpatiënten? Ja, want mijn boek heet *Komt een vrouw bij de hacker* en dat is gebaseerd op een beken-

de grap beginnend met 'Er komt een vrouw bij de...' en dat is vaak een dokter, dus gaat het over kanker, kijk maar naar Kluun. Huh? Knappe koppen die het nog kunnen volgen. Kanker en identiteitsfraude bij elkaar gebracht door de logica van een stalker die in alle toonaarden ontkent dat hij stalker is, maar wel een website met mijn boektitel registreert.

Overigens ontstond het idee voor de boektitel op het moment dat ik tegen mijn man voor de grap zei dat ik me ging laten hacken. Geen idee of ik het diep vanbinnen al meende. Ik geloof dat mijn moed nog moest groeien om het werkelijk te doen, maar ik had al een titel die de weg uitstippelde en dat was een goede stok achter de deur: Komt een vrouw bij de hacker...

Was het origineel genoeg? Geen idee, de meeste boektitels zijn niet origineel en je hebt veel boeken die precies dezelfde titel dragen, zoals *De duik*, *Gevangen* of *Overgave*. Je mag geen woorden of zinnen uit de Nederlandse taal claimen. Er is ook een boek dat *Komt een vrouw bij de sociale dienst* heet.

Ik ga niet naar de sociale dienst, ik ga niet naar de dokter, maar ik ga wel naar de hacker. Ik ben welkom in zijn woning in Amsterdam. Nog een paar dagen tot onze ontmoeting en ik ben heel benieuwd of we elkaars taal kunnen verstaan. De echte hackers zijn in mijn ogen nerds die in getallen denken, iets wat ik echt niet kan.

Mijn man is er overigens nog steeds op tegen. In het begin gebruikte ik de zin 'Komt een vrouw bij de hacker' om hem te plagen, maar hij weet dat het nu menens is en daar wordt hij onrustig van. Ik heb hem moeten beloven dat ik niet te ver ga. We hebben zelfs afspraken gemaakt over wat

wel en niet kan. Hij ziet het absoluut niet zitten dat iemand in mijn computer gaat grasduinen, omdat die niet alleen gegevens over mij bevat, maar ook over hem en onze kinderen. Point taken, ik wil mijn man niet kwijt. Maar ik wil wel zien hoe gemakkelijk het is om iemand te hacken. De afspraak met Rickey gaat dus zeker door.

's Avonds in bed zijn mijn ogen wagenwijd open en ook als ik ze dichtdoe, kan ik niet in slaap vallen. Hoe ziet de woning van een hacker op wie de FBI heeft gejaagd eruit? Is die volgestouwd met apparaatjes die ik niet ken?

Het blijkt minder spannend dan ik dacht: een rommelige studentenkamer zonder al te veel apparatuur. Een paar draden lopen over de grond en nodigen uit om te struikelen. Ik ga op het IKEA-bankje zitten en Rickey haalt zijn laptop tevoorschijn.

'Dus je weet het zeker dat je wilt dat ik je hack?' vraagt hij. 'Of wil je dat ik je alleen laat zien hoe ik het doe?'

'Ik wil live zien hoe het gebeurt en niet alleen theorie horen. Begin maar met mijn website, die is onlangs heel goed beveiligd door een expert.'

Rickey glimlacht: 'Door een expert nog wel. Oké, dat zullen we nog wel zien.'

Voordat Rickey aan de slag gaat, praten we over zijn nieuwste succes dat zelfs de pers gehaald heeft: hij heeft in de keuken van een groot Russisch botnet een kijkje genomen en daar kwam hij de gegevens van honderdduizenden Nederlanders tegen.

'Heb ik nou ook een Rus in mijn computer?'

Rickey trekt een wenkbrauw op. 'Dat weet ik niet, maar

die kans is niet ondenkbeeldig. De Russen hebben een overzichtelijke website en als je binnenkomt, zie je wat ze allemaal al weten. Soms zijn dat curieuze dingen, zoals de productiviteit van een bepaalde ambtenaar die heel wat uren op Facebook blijkt door te brengen. Maar de meeste zaken zijn een stuk ernstiger: bedrijfsgeheimen van een technologische onderneming, lopende zaken van advocaten, hoe de politie te werk gaat in een onderzoek, et cetera.'

Het digitale bestand is heel groot, vergelijkbaar met een bibliotheek met 37.000 kilometer aan boeken.

'De politie wilde in eerste instantie geen onderzoek doen naar het Pobelka-botnet,' zegt Rickey. 'Geen capaciteit en te weinig prioriteit.'

'Misschien zijn de gegevens toch niet zo indrukwekkend als ze op het eerste gezicht lijken?'

'Die gegevens kunnen dodelijk zijn als ze in verkeerde handen terechtkomen,' zegt hij. 'Via de besmette computers kun je controle krijgen over allerlei systemen, van chemie tot drinkwater. Zelfs het vliegverkeer platleggen is mogelijk.'

De lijst met besmette bedrijven en instellingen telt 120 miljoen pagina's met data. Ministeries, televisiezenders, advocatenkantoren, vliegmaatschappijen, technologische bedrijven... vrijwel alle sectoren blijken getroffen.

'Met de verkregen informatie kunnen de criminelen grote cyberaanvallen uitvoeren, maar ze lijken zich vooral op het manipuleren van financiële transacties te richten,' zegt Rickey. 'En nu gaan we naar jouw website kijken. Ik ben benieuwd of ik zwakheden kan vinden om binnen te komen.'

Hij roept mijn website op.

Ik heb de site onlangs zo goed laten beveiligen dat ik me eigenlijk geen zorgen maak. Dat heeft iemand gedaan die

bekende websites beveiligt en dagelijks aanvallen van hackers afweert, dus dat zit vast goed.

Rickey speurt met een programma Nmap naar zwakheden. 'Je site heeft 65.535 poorten. Als eentje niet goed dichtzit, dan heb je kans dat ik binnenkom. Wist je dat je server in Florida zit?'

'In Florida? Ik heb een contract met een Nederlands hostingbedrijf.'

'Ja, maar hij huurt servers in Amerika.'

Rickey tikt iets op zijn scherm. 'Tien poorten van je site staan open. Een poort moet je zo paaien dat die je binnenlaat.'

'Een poort paaien?'

Rickey lacht. 'Een computerpoort moet denken dat je een vertrouwde persoon bent om je binnen te laten. Ik zoek nu naar lekken in de software die me hierbij kunnen helpen.'

Rickey klopt bij alle poorten aan.

'Blocked by the firewall,' zegt hij even later. 'Goede beveiliging. Ze zien dat ik bij verschillende poorten geklopt heb en ze gooien me eruit.'

'Dus je kunt mijn website niet hacken?'

'Niet op de gebruikelijke manier. Maar ik kan wel de hele server proberen te hacken. Soms zijn andere websites op dezelfde server slecht beveiligd en dan kom ik zo ook naar binnen. Als ik de server hack, heb ik toegang tot alle websites, inclusief die van jou.'

'Een server hacken klinkt nog ingewikkelder dan een website.'

'Soms wel, soms niet,' zegt Rickey. 'Op je server draait het programma Pure-FTPd. Normaal installeren ze het op poort 21, maar hier staat het op een andere poort.'

In de tussentijd verschijnen er lange reeksen met getallen op het scherm. Voor een digibeet is het allemaal abracadabra, maar Rickey kijkt tevreden.

'Yes, ik zie hier een zwakke schakel, waarmee ik de hele server plat kan gooien. Dan is je website uit de lucht. Alle andere websites trouwens ook. Even kijken van wie die zijn.'

Ik lees met hem mee, de sites die aan mijn server in Florida hangen komen uit allerlei landen: van Engelse cricketteams tot een Indiase oliemaatschappij – 730 websites in totaal.

'Kijk eens hier,' zegt Rickey en hij wijst op het scherm.

'Je denkt toch niet dat ik hier iets van snap, hè?'

'Dit is precies wat ik zocht: software om deze server te hacken. Er zit zelfs een instructiefilmpje bij.'

'En dan heb je toegang tot al deze websites inclusief die van mij?'

'Yep.'

Ik ben met stomheid geslagen. Een sterk wachtwoord, een prima werkende firewall, zo veel moeite om mijn website te beveiligen en een hacker komt vrolijk via een omweg binnen.

20
Mogelijkheden

Een website hacken is misschien gemakkelijker dan mijn computer, denk ik. Rickey heeft geen tijd meer voor nog een uitdaging, maar ik spreek met hem af dat we het niet hierbij laten. Ik hoop nog steeds dat hij de pissebedden te zien krijgt en dat hij me uit kan leggen hoe hij door de beveiliging van de pissebedden is gekomen. Maar in eerste instantie hoop ik dat het hem niet lukt.

Websites hacken kan ik intussen ook, althans in theorie. Cyberaanvallen waarbij websites met grote hoeveelheden data worden bestookt, zijn gewoon te koop via internet. Een D-Dos-aanval kun je per uur bestellen en zo kun je bijvoorbeeld een grote bank offline zetten. ING maakte het in korte tijd verschillende keren mee en werd daarmee mikpunt van kritiek en van talloze moppen op social media.

Voordat ik zelf een bank ga hacken, is het verstandig om te weten hoe ik ontraceerbaar kan worden. Ik zie een workshop die dat belooft en schrijf me meteen in. Overigens is de workshop bedoeld voor brave journalisten en niet voor mensen die met snode plannen rondlopen. Waarschijnlijk ben ik daar de enige met 'boevige' gedachten, maar zolang ik die niet uitvoer is er niets aan de hand. Ik heb uiteraard een goed excuus: als ik iets boevigs doe, is het niet voor eigen gewin, maar uit nieuwsgierigheid of zoiets een digibeet ook lukt.

In het kantoortje van burgerrechtenbeweging Bits of Freedom tref ik een bont gezelschap journalisten en nerds aan. De bedoeling is dat de nerds de journalisten leren hoe ze hun computers beter kunnen beveiligen en hoe ze praktisch ontraceerbaar worden. Eis vooraf: laptops mee, maar geen tablets en mobieltjes, want die zijn per definitie onveilig.

Bits of Freedom stelt het heel duidelijk: de mobieltjes zijn afluisterapparaten waar je ook mee mag bellen. Als je zeker wilt weten dat je niet afgeluisterd wordt, is het niet voldoende om je telefoon uit te zetten, je moet hem in een koelkast of een andere stalen behuizing verstoppen. Zover heb ik dus nooit gedacht, maar tussen al die nerds lijk ik wel de enige die zich geen zorgen maakt over de spionagemogelijkheden van haar mobiel.

Als een van de sprekers is Arjen Kamphuis uitgenodigd, een veiligheidsconsultant die vertelt wat hij allemaal bij bedrijven aantreft als hij de toetsenborden optilt: heel veel voedselresten, maar ook gele plakbriefjes met wachtwoorden. 'En met één zo'n wachtwoord heb je meestal toegang tot het hele bedrijfsnetwerk.'

Kamphuis is goed in anekdotes vertellen. Hij reisde onlangs eersteklas met de Thalys en mocht in de trein gratis Wi-Fi gebruiken. Het viel hem op dat de inlogpagina niet beveiligd was. Hij zette zijn Wi-Fi-scanner aan en kreeg de wachtwoorden van al die vreemde medepassagiers te zien. 'Ik kan erom wedden dat de meesten geen speciaal Thalys-wachtwoord bedenken, maar een van de wachtwoorden invullen die ze ook voor privacygevoelige dingen gebruiken. Als cybercrimineel hoef je tegenwoordig alleen maar een Thalyskaartje te kopen om wachtwoorden te vangen. Een rijke oogst en voldoende materiaal voor identiteitsfraude gegarandeerd.'

Kamphuis leert de journalisten hoe ze hun nieuwe computer zo goed als ontraceerbaar kunnen maken. Je bestelt die niet via internet, maar in een winkel en je betaalt contant. Daarna sloop je de harddisk eruit en koop je een nieuwe harddisk bij een andere winkel.

Mijn ogen worden steeds groter. 'Is dit de enige manier waarop je een computer echt ontraceerbaar kunt maken?' Helaas voor mij blijkt dit wel het geval. De harddisk slopen van een nieuwe computer, dat had ik zelf niet kunnen bedenken.

Als ik bereid ben om wat meer risico te lopen, dan kan ik altijd nog encryptieprogramma's gebruiken om mijn berichten te versleutelen. De nerds blijken zelfs de simpelste boodschappen die ze elkaar versturen te versleutelen.

'Straks gaan we jullie allemaal bekeren zodat je het ook gaat doen,' zegt een van hen. 'Het klinkt misschien ingewikkeld, maar het stelt niet veel voor. Een gratis programma versleutelt en ontsleutelt je berichten en zelf hoef je niets te doen. Eigenlijk zou iedereen het moeten gebruiken gezien de afluisterschandalen van de afgelopen tijd.'

De nerds laten ons meteen het wondermiddel zien. Inderdaad, zelfs voor digibeten is het niet moeilijk. Verder krijgen we te horen dat we alle zoekopdrachten moeten spreiden over meerdere browsers. Voor de gevoeligste informatie is alleen het anonimiseringsnetwerk Tor geschikt. Wat ik nu doe, alleen Google gebruiken, is uiteraard goed fout, maar dat kon ik zelf ook bedenken.

De Windowssoftware op mijn computer wordt vervangen door een tijdelijke opstartversie van Linux, die zo aangepast is dat het startscherm op Windows lijkt. Niet alleen voor het gemak, maar ook om niet op te vallen in een internetcafé. 'Dan lijk je op een domme toerist en niet op een hacker of een journalist,' krijgen we als verklaring te horen.

Dan de wachtwoorden: dat hoofdstuk moeten we echt serieus nemen, goede wachtwoorden bedenken en af en toe veranderen. Arjen installeert het programmaatje LastPass.

Zelf heeft hij een paar honderd wachtwoorden. Als hij bijvoorbeeld op LinkedIn wil inloggen, zoekt het programma automatisch het juiste wachtwoord op.

'De meeste burgers zijn slordig met wachtwoorden, met het installeren van antivirusprogramma's en met het updaten van software,' zegt Arjen. 'De overheid doet schandalig weinig aan voorlichting. Ongeveer 35 procent van de Nederlandse pc's staat niet onder controle van de rechtmatige eigenaar. Vind je het gek dat het computeronderwijs op school vooral uit het typen in Windows bestaat? De oudere generatie moet het ook lekker zelf uitzoeken.'

Hoe serieus Arjen zijn digitale veiligheid neemt, kan ik zien als hij tijdens de demonstratie gebeld wordt. Hij haalt een heel oude Nokia uit zijn zak. Ik heb al een vermoeden waarom hij niet zoals zo veel mensen een mooie smartphone gebruikt. Even later wordt dat ook bevestigd: 'Dit type telefoon is te dom om afgeluisterd te worden,' zegt Arjen. 'Niet dat het onmogelijk is, maar het zal wat moeilijker zijn om op een telefoon uit 2007 software te installeren die microfoon en camera aanzet zonder dat ik het doorheb. Bovendien kan ik, in tegenstelling tot bij de iPhone, gewoon de batterij eruit halen.'

Voor de meeste mensen wordt het wel lastig om zo'n oude telefoon te scoren. Of je moet een reis naar Afrika maken, want daar zijn zulke oude mobieltjes nog steeds in roulatie.

Ik moet ervan uitgaan dat ik heel gemakkelijk op te sporen ben, want ik heb geen 'Afrikaans' mobieltje en voorlopig ben ik ook niet van plan om de harddisk van een gloednieuwe laptop te vervangen.

Meesteroplichter Frank Abagnale, die model stond voor de

rol van Leonardo di Caprio in de film *Catch Me If You Can*, zou een luizenleventje gehad hebben als hij iets later geboren was. In zijn tijd moest je slim en handig zijn om de identiteit van iemand te stelen, tegenwoordig kan iedereen het. Een kleurenprinter is voldoende voor een perfecte kopie en ook aan informatie geen gebrek, want vrijwel alles is op internet te vinden. Je maakt met je iPhone een foto van iemand op een vliegveld, laat vervolgens een app zoals PittPatt zijn gezicht herkennen en controleert of hij op internet te vinden is. Als hij geen Facebook heeft, dan staat zijn foto misschien op de site van zijn bedrijf of van zijn sportclub. Zo weet je binnen enkele seconden wie hij is. Als je ook zijn geboorteplaats en zijn geboortedatum kunt vinden (de meeste mensen maken er geen geheim van), kun je al zijn identiteit stelen.

Abagnale adviseert om nooit foto's gemaakt van voren van jezelf op internet te plaatsen. Alleen foto's met een groep of als je met iets sportiefs bezig bent, zijn geschikt, omdat ze niet gebruikt kunnen worden voor fraude. Dit is vast geen slechte tip, maar het probleem is dat de gevaren tegenwoordig van honderd kanten kunnen komen. Nigerianen en Russen sturen je phishing e-mails om je identiteit te stelen, terwijl Nederlanders je via internet met spullen verkopen oplichten. Als je dan denkt dat je de laatste aan kunt pakken, omdat de afstand kleiner is, dan kom je bedrogen uit. De wet zit zo gek in elkaar dat oplichters geen straf krijgen. Een Beverwijker verkocht bijvoorbeeld boeken en cd's op Marktplaats, maar liet na betaling niets meer van zich horen. Tientallen slachtoffers deden aangifte, maar volgens de rechter was dat geen oplichting of flessentrekkerij, omdat de man onder zijn eigen naam handelde. In het Wetboek van Strafrecht staat

dat er sprake moet zijn van een valse naam of hoedanigheid, dus als je mensen onder je eigen naam oplicht, dan word je vrijgesproken. De slachtoffers waren verontwaardigd, terwijl de man fluitend de rechtszaal in Haarlem verliet.

Als je niet eens oplichters die hun eigen naam gebruiken aan kunt pakken, lukt dat zeker niet bij anonieme daders. Van de rekening van Marcel Beerens wordt 4300 euro afgeschreven door iemand die zich achter een rekeningnummer van ING schuilt. Marcel weet niet door wie, want zijn bank zegt dat de privacyregels ook voor fraudeurs gelden.

Het gekke is dat Marcel geen virus in zijn computer heeft, hij ziet het gewone scherm van ABN Amro, met logo en slotje, en waant zich veilig tijdens het internetbankieren. Marcel is 39 jaar en heeft een eenmanszaak voor technische producten. Hij zit niet op social media, klikt niet op verdachte linkjes en hij heeft ook geen camera op zijn computer die hackers op afstand aan kunnen zetten, dus was hij hoogst verbaasd dat het juist hem overkomt. 'Ik kon op geen enkele manier sporen van hackers in mijn computer ontdekken, mijn virussoftware was up-to-date en ik heb ook een firewall, dus begreep ik niet aan welke voorwaarde van de bank ik niet voldaan heb. ABN Amro wilde niets vergoeden en ik mocht mijn eigen dossier niet eens inzien. Ik ging uiteraard ook naar de politie, maar de agent vond het niet de moeite waard om de aangifte op te nemen, want het ging 'maar' om 4300 euro.'

'Ik ben ontzettend kwaad op de bank dat ik het geld kwijt ben, terwijl ik niet weet wat ik verkeerd heb gedaan. Ik heb ze gebeld en gevraagd: Hoe moet ik de volgende keer als ik inlog zien dat ik op het originele scherm van de bank zit? De vorige keer was er tenslotte ook geen verschil te zien.' Ze zei-

den simpelweg dat het een kwestie van vertrouwen is. Vertrouwen! Sinds kort hebben de banken hun voorwaarden aangepast waardoor heel veel mensen aan den lijve gaan ervaren hoe gemakkelijk de bank zonder enig bewijs de schuld bij de consument legt.'

Beerens stuurt me zijn merkwaardige correspondentie met ABN Amro door. Hij heeft heel veel argumenten voor zijn onschuld aangedragen, maar de medewerker van de bank is onverbiddelijk: 'Alhoewel ik zeer sympathiek sta tegenover u en uw klacht, zal ik de klacht afwijzen.'

De politie heeft niet veel capaciteit voor dat soort zaken. Teleurgestelde slachtoffers laten vaak berichten op forums achter. Zo ook Ilse. Iemand misbruikt haar ING-bankrekening voor incasso's en eenmalige machtigingen door bedrijven die ze niet kent. ING doet er weken over om te kijken of de incasso's onterecht zijn, terwijl er steeds meer geld van haar rekening afgeschreven wordt. Alle via internet bestelde spullen gaan naar één adres en dat is niet het adres van Ilse. Ze verbaast zich erover dat de bedrijven haar handtekening helemaal niet nodig hebben, dat iedereen zomaar geld van haar rekening af kan schrijven.

Ilse doet aangifte van fraude en geeft het adres en het e-mailadres van de fraudeur aan de politie door, maar die man blijft haar rekeningnummer gebruiken. Hij krijgt de goederen en zij de narigheid, want zij moet elke winkel ervan proberen te overtuigen dat iemand haar identiteit misbruikt.

'Hij kocht allerlei dingen, zoals een Veronica-boodschappenpakket, een fiets en voor zevenhonderd euro aan spullen bij Ziggo, waaronder een basispakket, een erotiekpakket en een tablet. Dat kan blijkbaar gewoon, alleen met het aan-

vinken van een eenmalige machtiging. Met een terugboekperiode van nul dagen, dus niet terug te boeken. En iedereen vindt dat goed. Ik heb er geen woorden voor.'

Ilse laat uiteindelijk haar rekeningnummer volledig blokkeren voor incasso's. Dat kan als je het schriftelijk aanvraagt bij de bank. De oplichter kiest daarop vast een ander rekeningnummer, misschien dat van jou of van mij.

Cybercriminelen zijn geen kieskeurig volkje. Meestal maakt het hun helemaal niet uit wiens identiteit ze stelen en van wie ze geld ontvangen. Vaak mikken ze juist op grote groepen, omdat dit de kans van slagen vergroot. Sommigen pakken het zelfs met radioreclames via betrouwbare zenders aan, omdat de potentiële slachtoffers dan minder achterdochtig zijn. Zo trapten duizenden mensen in de mooie boodschap van mijngratisbox.nl, die via Sky Radio en de Ster adverteerde. Deze professioneel uitgevoerde fraude leverde naar schatting bijna een half miljoen euro op. De 'gesponsorde' artikelen werden nooit geleverd, terwijl vele duizenden consumenten de verzendkosten betaalden.

'Je hele leven staat online en dat kan tegen je gebruikt worden,' zeggen de Belgische banken in een filmpje dat waarschuwt voor de gevaren van internet. Als ik het filmpje voor het eerst zie, sta ik met mijn mond open. Een medium met paranormale gaven ontvangt diverse mensen en hij kan van alles over ze vertellen: wie te veel drinkt, wie een negatief banksaldo heeft, wie tatoeages met vlinders heeft, wie een boeiend liefdesleven met meerdere partners heeft, wie honderden euro's per maand aan kleding spendeert, hoeveel iemands huis heeft gekost... De mensen zijn allemaal geschokt: hoe kan iemand als Dave dat allemaal weten? Zelf zit

ik ook met die vraag. Ik wil best geloven dat sommige mensen paranormale gaven hebben, maar Dave raadt zelfs de rekeningnummers van willekeurige voorbijgangers. Aan het einde van het filmpje wordt het geheim van Dave onthuld: achter de schermen verzamelen hackers in een rap tempo gegevens over die mensen en ze fluisteren Dave de gevonden informatie in. Niets paranormaals aan, gewoon googelen.

In de toekomst wordt het alleen maar lastiger: zelfs gegevens die je niet prijsgeeft, zijn te vinden. De experts voorspellen computers die duizenden malen sneller zijn en elke beveiliging in enkele seconden kunnen kraken.

Hackers richten zich steeds vaker op het stelen van afbeeldingen. Ik heb alle kopietjes van documenten inmiddels van mijn computer verwijderd en ook oude foto's waarop ik uitdagend voor de camera van mijn toenmalige vriend stond te poseren. Plaatjes zijn voor hackers goud waard, want je kunt er identiteiten mee stelen of mensen mee onder druk zetten.

De FBI arresteerde niet zo lang geleden een 27-jarige man die computers van vrouwen hackte op zoek naar naaktfoto's en persoonlijke informatie. Hij deed zich als de vrouwen voor en voerde computergesprekken met hun vriendinnen, waarbij hij de vriendinnen overhaalde om naakt te poseren. Vervolgens chanteerde hij de vrouwen en dreigde hun foto's te publiceren als ze hem niet zouden voorzien van nieuwe naaktplaatjes van henzelf. Hij verspreidde een gedeelte van zijn buit via Facebook. De politie vond foto's van honderden vrouwen.

Ook zonder hackers zijn we kwetsbaar, want we strooien onbewust informatie rond die later niet verwijderd kan worden. Als het je lukt om iets van een site te verwijderen, blijkt

het ergens anders op het internet te zijn opgeslagen. Schrale troost: zo zijn we allemaal onsterfelijk geworden.

Voor mensen als Erik Wannee maakt het helemaal niet uit. Ik mag alles van hem weten, behalve zijn pincode en zijn DigiD. Niet alleen ik, maar de hele wereld mag dat weten, want hij plaatst het allemaal zelf online: zijn adres, zijn telefoon, zijn e-mailadres, zijn bankrekeningnummer, hoelang hij met Saskia getrouwd is, wat voor werk hij doet (keuringsarts) en noem maar op. De naam van Erik kom ik per toeval tegen op een internetforum waar hij zijn burgerservicenummer gepubliceerd heeft. Eerst denk ik dat het om een grap gaat en dat zijn burgerservicenummer niet klopt. Als ik hem googel en al die andere informatie zie, dan denk ik: als dit een grap is, dan is die al behoorlijk uit de hand gelopen.

Ik besluit om niet langer in het duister te tasten en Erik op te bellen. Hij heeft tenslotte niet voor niets zijn privénummer op internet gezet.

Erik is best bereid om een onbekende te woord te staan.

'Een grap is het zeker niet,' zegt hij. 'Dat zijn allemaal gegevens die van de meeste mensen op het internet te vinden zijn, alleen weten die het misschien niet.'

'Ik denk niet dat mijn burgerservicenummer op het internet staat. Ben je niet bang voor misbruik als je zo veel gegevens bij elkaar zet?'

'Niet echt,' zegt hij. 'Iedereen kan slachtoffer van identiteitsfraude worden, ook al zet je zelf niets online.'

'Eens, maar je maakt het de potentiële kwaadwillenden wel heel erg gemakkelijk.'

Heel even is het stil aan de andere kant van de lijn.

'Weet je, zie het als een statement. Niemand is onkwetsbaar. Ik ben zelf een keer slachtoffer van identiteitsfraude geworden, maar dat had niets te maken met het publiceren van al deze gegevens.'

'Hoe kwam dat dan?'

'Iemand bestelde van alles en nog wat en ik kreeg honderden e-mails dat ik de rekeningen moest betalen. Een milde vorm van identiteitsfraude, want zelfs mijn naam klopte niet, dus geen deurwaarder die achter me aan ging.'

'Dus je dacht: zet maar alles online, misschien maak ik de volgende keer iets spannenders mee.'

Erik lacht: 'Nee, dank je. Maar ik vind dat gegevens als bijvoorbeeld je burgerservicenummer niet geheim hoeven te zijn.'

'Maar dat is juist het nummer dat honderden organisaties vragen ter verificatie. Of je naam, adres en geboortedatum, maar die zet je ook online.'

'Het burgerservicenummer is niets anders dan een uniek getal dat bij een bepaalde persoon hoort, om uit te sluiten dat er verwisseling plaatsvindt. Als arts ben ik zelfs wettelijk verplicht om het burgerservicenummer van mijn patiënten te gebruiken in correspondentie met collega's.'

'Prima om verwarring te voorkomen, maar bij bewuste fraude lijkt het me juist heel handig om over zo'n uniek nummer te beschikken.'

'Ik weet niet of ze er zo veel mee kunnen. Net als met mijn bankrekening. Ik zet die op het internet, maar ze kunnen er niets mee, behalve geld overmaken. Zonder pincode is de bankrekening niet bruikbaar en mijn pincode maak ik écht niet openbaar!'

De stelligheid in zijn stem verbaast me. Ik heb nog nooit

iemands bankrekening misbruikt, maar deze keer krijg ik kriebels om dat te proberen. Ik wil Erik heel graag een privacylesje leren. Ik schrik van mijn eigen gedachten. Hoe ethisch is het om te frauderen om iemand een les te leren en waarom wil ik dat? Ik lijk net een privacy-Jehova's getuige, terwijl ik tot voor kort nog van die zwakke wachtwoorden gebruikte.

Erik onderbreekt mijn gedachten: 'Kijk, voordat je denkt dat ik een hopeloos naïef iemand ben: mijn baas wil al een tijdje dat ik mijn handtekening inscan om digitaal de brieven te ondertekenen. Lekker efficiënt, maar ik begin er niet aan. Het is kinderlijk eenvoudig om zo'n handtekening in te scannen en onder bijvoorbeeld een leningaanvraag te plakken.'

'Goed dat je in elk geval je handtekening beschermt. Volgens mij is dat volstrekt onvoldoende, maar ik ben vast van de oude stempel.'

Als we ophangen malen mijn gedachten verder. Natuurlijk ben ik ouderwets, ik hecht nog enige waarde aan mijn privacy en aan het verbergen van belangrijke data. Maar misschien heeft Erik gelijk dat dit geen nut heeft, omdat we uiteindelijk even kwetsbaar zijn.

21

De laatste zoektocht

Hoewel Rickey tot nu toe altijd serieus is geweest, laat hij me deze keer in de steek. Hij wordt de laatste tijd intensiever in de gaten gehouden door de politie en omdat hij nog in zijn proeftijd zit, durft hij niet verder te gaan.

'Ik hoop dat je het begrijpt,' schrijft hij.

Ik staar in de leegte. Ik had mijn zoektocht naar een betrouwbare hacker zo zorgvuldig voorbereid en nu durft mijn gedroomde hacker niet verder te gaan. Ik voel paniek opkomen. Als ik zou roken, dan zou ik op dit moment snakken naar nicotine. Maar ik rook niet, dus resteert het nagelbijten. Dat had ik recentelijk afgeleerd en daar was ik bijzonder trots op, maar nu doe ik het al weer. Nadat ik mijn nagels afgekloven heb, is de boodschap echt geland. Rickey kapt ermee, hij durft het niet meer aan, ook al heeft hij mijn officiële toestemming. Hij is al een tijdje zijn leven aan het beteren en hij wil niet langer problemen met de autoriteiten.

Is mijn zoektocht voor niets geweest? Nee, want Rickey heeft me al veel laten zien, maar af is het zeker niet. Het was niet de bedoeling dat hij zomaar afhaakt.

Ik begrijp Rickey wel, daar niet van. Als ik hem was, dan zou ik waarschijnlijk ook zeggen: 'Tot hier en niet verder.' Ik zou het ook niet prettig vinden om de hete adem van de politie in mijn nek te voelen, maar hoe kom ik aan een nieuwe betrouwbare hacker? Wie zegt dat de persoon die ik benader wil meewerken?

Opeens denk ik aan Holger. Hij heeft me toen heel goed geholpen met mijn digitale beveiliging, misschien kan hij me nu helpen om die juist te slopen? De beste beveiligers zijn zelf ervaren hackers en Holger liet een keer iets vallen dat hij ook aan de verkeerde kant van de wet was begonnen. Het probleem is dat ik hem nauwelijks ken, alleen van

berichtjes op social media. Ik weet dat Holger van computers en van hardlopen houdt, maar ik heb geen idee hoe betrouwbaar hij is. Kan ik hem zo veel informatie toevertrouwen?

Bij Rickey had ik toen hetzelfde dilemma, maar op een gegeven moment hakte ik de knoop door en besloot hem blindelings te vertrouwen. Eigenlijk is het best logisch om ook bij Holger niet te veel na te denken, maar mijn intuitie te volgen. Hij lijkt me een aardige vent en ik wil mijn hackproject afmaken. Komt een vrouw bij de hacker… bij een andere hacker.

Als ik Holger mail, krijg ik vrij snel een enthousiaste reactie terug. 'Je computer hacken? Geen probleem. Als je het leuk vindt, kan ik je leren hoe je zelf iemand kunt hacken, dit lijkt me persoonlijk een grotere uitdaging.'

Hmm, van een digibeet een hacker maken? Het klinkt inderdaad spannend, maar dan ben ik wel strafbaar bezig. Als ik betrapt word uiteraard.

De dagen voor de afspraak met Holger breek ik me het hoofd over wie ik zou kunnen hacken. Ik wil geen vrienden kwijtraken en bij onbekenden durf ik het al helemaal niet. Zonder het te weten plaatst Holger me met zijn enthousiaste aanbod voor een ethisch dilemma.

Ik kan uiteraard een van mijn vrienden van tevoren vragen of het mag, maar ik ben bang dat niemand het een leuk idee vindt dat zijn of haar e-mails gelezen kunnen worden. Als ik het van tevoren aankondig, loop ik bovendien het risico dat ze extra opletten en er sowieso niet in trappen.

Op de dag dat Holger naar mijn huis komt, voel ik de opwinding die mensen voelen als ze nieuwe werelden gaan verkennen. Tof dat iemand bereid is om me de geheimen van de nullen en de enen in mijn computer uit te leggen.

Een slanke man met stekeltjeshaar belt iets later dan het afgesproken tijdstip aan.

'Je huis is moeilijk te vinden,' zegt hij. 'Zelfs de navigatie raakt in de war.'

'Ik weet het, daar ben ik blij om. Ook Google zoomt er een stukje naast. Grappig is dat, dat ik toch een beetje privacybescherming heb zonder daar iets voor te doen.'

'Je maakt je zorgen om je privacy en je laat je hacken?' Holger kijkt me enigszins onbegrijpend aan.

'Nou, dat dient een hoger doel.'

'Vast wel, maar zo'n klusje is niet gebruikelijk. Meestal programmeer ik geen virussen. Hoewel ik dat vroeger heel veel heb gedaan. Toen moest je echt verstand van computers hebben om virussen te maken, tegenwoordig zoek je even op het internet en je vindt een enorm aanbod. Niks aan.'

'Ben je ook een van die mensen die beweren dat vroeger alles beter was?'

'Nee hoor, dat niet, maar de uitdagingen waren leuker.'

'Ik heb anders best een leuke uitdaging voor jou. Een laptop vol pissebedden.'

'Pissebedden?' Holger kijkt me aan alsof ik gek ben geworden. Maar ik weet wat er op de Windowslaptop staat die hij moet hacken: het werkstuk van mijn zoontje over hoe boeiend het is om een pissebed te zijn en voor de rest helemaal niets. Mijn man wist dat er een hacker zou komen en omdat hij niet in betrouwbare hackers gelooft, heeft hij alles gewist. Op de pissebedden na. Mijn man heeft ook de laat-

ste updates uitgevoerd en ervoor gezorgd dat er een nieuwe virusscanner op draait. Dat vertel ik aan Holger.

'In dat geval is het bijna onmogelijk om je computer te hacken,' zei hij.

Dat geloof ik graag, maar toch wil ik dat Holger een poging waagt. En daarna ben ik aan de beurt. Komt een digibeet bij de hacker en vraagt hoe ze zelf hacker kan worden... Geen idee of dat grappig afloopt, maar ik heb al een slachtoffer geregeld. Lina is iemand die niet zo bezig is met het onderwerp privacy. Ik heb het trouwens netjes gevraagd. 'Voor een experiment,' zei ik.

'Wow, en ik mag je proefkonijn zijn?' vroeg Lina. 'Ik voel me vereerd. Ware het niet dat ik niet in je hackerskunsten geloof.'

'Dan moet het helemaal geen probleem zijn om je computer beschikbaar te stellen.'

'Mij best. Stel dat het je toevallig lukt: ik wil niet dat je iets in mijn computer wijzigt.'

'Afgesproken.'

In mijn eentje lukt het vast niet om Lina's computer te hacken, maar Holger is niet voor niets gekomen. Hij installeert zijn laptop en laat me zijn programma met het virus zien. 'Vroeger hackte ik best vaak computersystemen uit nieuwsgierigheid,' zegt hij. 'Ik wilde gewoon weten wat onbekende computers verbergen. Soms was het best spannend, alle profielen op een erotische site bleken bijvoorbeeld niet versleuteld. De dames vertelden van alles over zichzelf en gaven ook hun privénummers in de veronderstelling dat alleen de beheerder toegang had tot dit besloten gedeelte van de site. Omdat ik het kwalijk vond dat hij zo slordig met hun gegevens omging,

stuurde ik hem een e-mail met uitleg hoe gemakkelijk het is om zijn website te hacken. Ik kreeg heel snel een antwoord: 'Fuck you.' Duidelijke taal. Toen wist ik wat me te wachten stond. Ik heb een laptop van een vriend geleend, ben naar een McDonald's gereden om gebruik te maken van hun Wi-Fi en ik heb de hele databank met meiden en klanten gewist.'

'Als dit verhaal bekend wordt, durft niemand je meer uit te schelden.'

Holger lacht. 'We zullen zien. Ben je er klaar voor?'

Ik knik en zet mijn laptop aan.

'Oké,' zegt Holger. 'Normaal gesproken hoef je niet mee te werken, maar vandaag wel, want we hebben niet veel tijd. Stel ik stuur je een linkje met een interessant cybercrime-spelletje, ga je dat openen?'

'Meestal negeer ik spelletjes, maar omdat het met cybercrime te maken heeft, word ik wel nieuwsgierig. Ik hoor wel aan je stem dat dit een truc is.'

'Juist. Als je zo'n e-mail van een onbekende ontvangt, verwijder je die meteen, maar niet als die van een goede kennis komt. De meeste mensen vertrouwen hun vrienden en kennissen en dat is juist de truc: degenen die zo'n e-mail sturen weten vaak niet dat hun computer misbruikt wordt om andere computers te besmetten.'

Ik open mijn e-mailprogramma en daar is het bewuste mailtje.

'Holger, ik heb gezegd dat ik erop klik en dat ga ik doen. Nu weet ik dat de inhoud besmet is, maar als je me niet van tevoren had gewaarschuwd, had ik er niets achter gezocht. Eerlijk is eerlijk.'

Eén, twee, drie. Eens even kijken hoe alert mijn virusscanner is.

Een seconde later verschijnt er een waarschuwing in beeld. Malware. Foute boel.

'Mijn scanner heeft je hackprogramma ontmaskerd,' zeg ik vrij triomfantelijk, alsof het mijn verdienste is.

'Daar was ik een beetje bang voor,' zegt Holger. 'Dit programma is een beetje oud en er zijn virusscanners die het herkennen.'

'Zullen we kijken of het op de laptop van mijn vriendin werkt?'

Holger knikt: 'Als ze niet vaak updates uitvoert, dan heeft het kans van slagen.'

'Ik hoop het, want ze lachte me al bij voorbaat uit en zei dat ik een waardeloze hacker zal zijn. Maar met zo'n kant-en-klaar programmaatje lijkt het me niet zo moeilijk.'

Ik kruip achter het toetsenbord en typ: 'Hoi Lina, ik mail je een heel bijzonder spel. Ik weet dat je niet zo van spelletjes houdt, maar dit heeft met je werk te maken. En jou kennende vind je het heel leuk.'

Ik druk op 'verzend'.

'Kun je het zien als ze het opent?'

'Uiteraard kan ik dat zien,' zegt Holger. 'Als ze het opent, zitten we in haar computer. Dat kan niet ongemerkt blijven. Nu gaan we wachten.'

'Koffie? Als het te lang duurt, ga ik haar even skypen dat ik haar een leuk spelletje gestuurd heb. Ik zie op Skype dat ze online is.'

'Niet te veel pushen, anders wordt ze misschien achterdochtig,' reageert Holger. 'Als je haar eerder gewaarschuwd hebt wat je gaat doen, dan is het helemaal niet handig om te bellen. Gewoon even geduld.'

Hackers hebben vaak bergen geduld, maar ik niet. Ik

wip onrustig heen en weer en daarna ga ik koffie zetten.

Even later hoor ik Holger roepen: 'Kom even kijken!'

'Zijn we binnen?'

'Nou en of. Ik heb haar camera op afstand aangezet.'

Gelukkig is Lina niet naakt. Ze loopt in haar huis richting de keuken. Haar laptop staat zoals gewoonlijk op de salontafel.

'Luister, ik wil niet uitgebreid in haar computer neuzen. Ik wil alleen weten wat voor bestanden je ziet en of je bijvoorbeeld haar wachtwoorden kunt onderscheppen.'

Holger typt 'stored passwords' in het virusprogramma.

'Geen passwords. Eigenlijk best bijzonder, want de meeste mensen bewaren wachtwoorden in hun computer.'

'Lina is niet zo actief op internet, dan hoeft ze er waarschijnlijk maar twee te onthouden.'

'Aha. Even kijken, wat hebben we nog meer? Wie is Alex?'

'Dat is haar vriend.'

Holger tovert een paar foto's op het scherm. 'Dit is vast Alex.'

'Ja, zo te zien een vakantiefoto. Maar laten we stoppen, ik voel me een beetje bezwaard.'

'Wil je haar e-mails niet zien?' vraagt Holger.

Wat een vraag! Natuurlijk wil ik dat. Ik wil alles, maar tegelijkertijd weet ik dat ik dit soort dingen niet moet willen. Wie wint: mijn nieuwsgierigheid of mijn verstand?

'Ik denk dat het beter is om het hierbij te laten, Holger.'

'Wacht, ik wil je nog iets laten zien,' zegt hij. Hij drukt op een knop en een minikeyboard verschijnt op zijn scherm. 'Kun je hier een melodietje op spelen?' vraagt hij.

Ik druk op een paar toetsen en ik zie Lina verschrikt kijken naar haar computer.

'Je meent het, hoort ze nu echt wat ik speel?'

'Natuurlijk, en vrij hard ook.'

'Arme Lina, zij heeft totaal geen verstand van computers en een computer die opeens muziek maakt, lijkt me best eng. Alsof het spookt in het huis.'

'Geen zorgen, we gaan haar straks uitleggen dat een computer geen eigen leven kan leiden.'

'Behalve als ik die als digibeet op afstand bestuur.' Je zou me moeten zien grijnzen. Het is zo leuk om iets te doen waar je totaal geen verstand van hebt en dat het lukt! Dat gebeurt me nou niet zo vaak.

We kunnen Lina inderdaad alles uitleggen en zelfs laten zien, want ik heb een week geleden met haar afgesproken dat ze vandaag rond drie uur voor een kop koffie langskomt. Ik gokte erop dat een paar uur genoeg zou zijn om in haar computer te komen en dat blijkt het geval. Lina weet ook dat ze haar laptop mee moet nemen, omdat ik iemand met verstand van computers geregeld heb die haar met een computerprobleem kan helpen. Als ze die maar niet vergeet.

We wachten met spanning op Lina.

'Wat we nu doen is eigenlijk heel ouderwets hacken,' zegt Holger. 'We maken ons kenbaar en als ze goed oplet, begrijpt ze wat er aan de hand is. Vroeger deden alle hackers dat, ze stuurden je bijvoorbeeld een virus waarmee je cd-lade spontaan openging en ze waren blij dat ze zo'n grap uithaalden. Van de aanwezigheid van de moderne hackers in je computer merk je meestal niets. Ze doen het niet voor de lol, maar voor het geld.'

Ik ben blij dat ik een ouderwetse hacker ben, dat vind ik al spannend genoeg. Nu nog de reactie van Lina afwachten.

Even later belt ze aan.

'Wat was dat voor een raar mailtje van jou?' vraagt Lina als ze binnen is. 'Ik heb je bestandje met de game geopend, maar het deed het helemaal niet.'

'Het bestandje deed het wel hoor, heb je je computer geen muziek horen maken? Dat was part of the game.'

Lina kijkt me verbluft aan. 'Hoe kan dat nou? Ik snap er niets van.'

'Ik ook niet, maar ik heb je gehackt.'

'Je meent het! Heb je ook mijn e-mails gelezen?'

'Ja, je hele liefdescorrespondentie met Alex.'

Het gezicht van Lina betrekt.

Holger grijpt in voordat het uit de hand loopt. 'Dat heeft ze niet gedaan, hoor. Ze was heel braaf en helemaal niet nieuwsgierig.'

'Niet nieuwsgierig? Dat is niets voor Maria.'

'Nou, ik ben altijd nieuwsgierig, maar ik weet wanneer ik moet stoppen. Ik wil dat we nog wat langer vriendinnen blijven.'

'Dit was wel de laatste keer dat je me hebt gehackt,' zegt Lina.

'O, je denkt dat ik de smaak te pakken heb? Zo erg is het niet, hoor.'

Holger probeert tussenbeide te komen voordat we in vrouwengeklets verzanden met hem als toehoorder. 'Weet je wat we gek vonden, Lina? Dat je geen wachtwoorden in je laptop bewaart.'

'Is dat gek?'

'Nee, dat is juist heel goed. Meestal vind ik wachtwoorden of kopietjes van documenten en jij bent een uitzondering.'

'Nou, ik doe niet zo veel op de computer. De paar wachtwoorden die ik heb, kan ik prima onthouden.'

'En die verander je uiteraard niet meer, dat is nou weer slecht,' zeg ik wijsneuzerig.

Holger kijkt me scherp aan:

'Hoe vaak verander jij je wachtwoorden?'

Uhh. Betrapt. Komt op mijn lijstje met goede voornemens naast meer sporten, meer boeken lezen, minder vaak op Twitter kijken, vaker 'nee' zeggen, minder vaak mensen proberen te pleasen, vaker met mijn kinderen over computers en veiligheid praten, nooit meer zomaar kopietjes van mijn paspoort laten maken en... De rest ben ik vergeten. Daar heb je computers voor. Ze onthouden alles wat ik niet kan onthouden, inclusief mijn rare nieuwe wachtwoord van zeventien tekens. Waarom zeventien? Omdat dit mijn geluksgetal is. Natuurlijk komt zeventien ook in mijn nieuwe wachtwoord voor. Omdat je niet genoeg geluk kunt hebben als het om identiteitsfraude gaat, dé misdaad van de toekomst.

Van de hackers heb ik in elk geval één ding geleerd: investeren in je digitale veiligheid loont. Vergelijk het met goede sloten op je deuren: inbrekers kunnen zelfs de meest beveiligde huizen binnenkomen, maar als je het ze moeilijk maakt, kiezen ze eerder voor een huis met slechte sloten. Digitaal gekloond worden is voor veel mensen een nachtmerrie. Je bent uniek, zorg ervoor dat het zo blijft.

Opmerking van de auteur

Ieder van ons is en blijft kwetsbaar. Na het schrijven van dit boek besef ik dat des te meer. Ik heb enkele slachtoffers van identiteitsfraude in dit boek geanonimiseerd, want zij hebben al meer dan genoeg meegemaakt.

Ik ben geen computerexpert, verre van dat, maar ik heb mijn best gedaan om het onderwerp identiteitsfraude op een toegankelijke manier toe te lichten.

'Kennis is macht,' zeggen ze. Daarom heb ik bij talloze experts aangeklopt om tips te verzamelen voor mensen die niet zo veel verstand van computers hebben. De lijst werd heel lang. Schrik niet, want je hoeft niet alles uit te voeren en sommige tips zijn zo simpel dat ze nauwelijks moeite te kosten.

Graag tot ziens op social media. Nee, ik ben niet zo geschrokken dat ik opeens al mijn profielen wis. Ik blijf een onverbeterlijke optimist, die denkt dat er voor elk probleem een oplossing is. En dat is nou het leuke van social media: we kunnen met z'n allen de mooie oplossingen in een mum van tijd verspreiden.

Twitter: https://twitter.com/genova2

Facebook: Maria Genova (books)
https://www.facebook.com/MariaGenovaBooks/?fref=ts

LinkedIN: Maria Genova
https://www.linkedin.com/in/maria-genova-528bb77

Tips

● Als je wachtwoord voor je e-mail niet heel sterk is, kan iemand anders je e-mails omleiden en jou worden op internet. Veel accounts gebruiken je e-mail om wachtwoorden te resetten. Verzin dus een heel sterk wachtwoord. Bewaar je wachtwoorden niet in je computer. Gebruik (gratis) programma's zoals KeePass, LastPass en 1Password, die ingewikkelde wachtwoorden voor je verzinnen en automatisch invoeren. Hiermee hoef je nog maar één wachtwoord te onthouden. Alle andere wachtwoorden worden door het programmaatje onthouden. Zorg ervoor dat het wachtwoord dat toegang geeft tot je wachtwoordmanager heel sterk en makkelijk te onthouden is.

● Pas op waar je wachtwoordprogramma's downloadt, want er bestaan ook onbetrouwbare kopieën. Doe het altijd via de officiële site https://lastpass.com en KeePass http://keepass.info of via de officiële app. Als je wachtwoordmanagers zoals Keepass gebruikt, hoef je niet geregeld je wachtwoorden te veranderen. Doe je dat niet, verander dan geregeld je wachtwoorden en kies verschillende wachtwoorden voor belangrijke sites.

● Het is overigens veel beter om zogenoemde wachtzinnen te gebruiken in plaats van wachtwoorden. Een wachtzin is een zinnetje dat je makkelijk kunt onthouden én dat door zijn lengte veiliger is dan een gewoon wachtwoord.

Bijvoorbeeld IkHebGeenTijdVoorGoedeWachtwoorden00! Zet in de zin ook leestekens, cijfers en hoofdletters, dan wordt je wachtwoord veel veiliger. Bewaar zo'n wachtzin niet in je computer of op je smartphone.

● Je kunt ook een standaard sterk wachtwoord gebruiken en dat elke keer aanvullen. Stel dat mijn wachtwoord Lezenhoudenvan1213? is en ik kom op Facebook, dan maak ik er FBLezenhoudenvan1213 of voor bol.com, waar ik bijvoorbeeld een boek bestel, BoekenLezenhoudenvan1213. Voor Eneco wordt het dan bijvoorbeeld Energie Lezenhoudenvan1213. Je standaardwachtwoord weet je dus en per site voeg je er iets aan toe wat met de site te maken heeft (kan ook de naam van de site zelf zijn). Een goed wachtwoord bevat geen namen en geboortedata, en bestaat uit minstens twaalf karakters.

● Check of je antivirusprogramma up-to-date is. Negeer geen updates van programma's, ook al gebruik je ze niet vaak. Hackers gebruiken verouderde versies van programma's om je computer over te nemen. Als je met een document bezig bent en je hebt geen tijd om een update uit te voeren en opnieuw de computer op te starten, klik de update niet weg, maar minimaliseer die zodat die in je gezichtsveld blijft. Aan het einde van de werkdag kun je de update uitvoeren voordat je de computer afsluit. Schakel de automatische updates van je antivirusprogramma in en laat het geregeld (eens per maand) alle apparaten scannen. Schakel een eventueel meegeleverde firewall altijd in. Sla je wachtwoorden niet in de internetbrowser op.

● Verstrek een kopie van je legitimatiebewijs alleen als dat wettelijk verplicht is, bijvoorbeeld aan overheidsinstanties. Veel bedrijven mogen het helemaal niet vragen; dat geldt bijvoorbeeld voor vrijwel alle commerciële bedrijven. Alleen je eigen werkgever, bank, notaris of casino en overheidsinstanties mogen een kopie maken, bij alle andere bedrijven kun je gewoon weigeren. Verhuurbedrijven, hotels en telecomaanbieders mogen bijvoorbeeld geen kopie maken, alleen enkele gegevens noteren. De instanties en bedrijven die hier wel om mogen vragen, moeten de data veilig opslaan en na verloop van tijd (maximaal vijf jaar) verwijderen.

● Werkgevers zijn verplicht om een kopie van je identiteitsbewijs in de loonadministratie te bewaren. Je kunt wel informeren hoe veilig die kopieën opgeslagen worden en of de database versleuteld is voor het geval dat hackers die aanvallen. Werk je voor een uitzendbureau, dan mag alleen het uitzendbureau een kopie van je identiteitsbewijs maken, het bedrijf waar je de arbeid verricht, mag dat niet. In het buitenland gelden vaak andere regels.

● Wanneer je een kopie moet verstrekken, doe dat dan veilig. Maak verscheidene gegevens onleesbaar, zoals je burgerservicenummer, je pasfoto en je handtekening. Het burgerservicenummer staat op twee plaatsen in je paspoort, ook in het lange nummer onderaan. Er zijn bij de ANWB speciale hoesjes of ID Covers te koop die de bewuste velden afschermen.

● Maak altijd een aantekening op een kopie van je legitimatiebewijs die aangeeft waarvoor deze kopie bestemd

is, bijvoorbeeld 'kopie voor autoverhuurbedrijf Olymp'. Zo maak je het min of meer onbruikbaar voor fraude, want fraudeurs hebben liever een schone kopie. Stuur geen kopie als een koper of verkoper op sites zoals Marktplaats.nl dat vraagt, want er wordt veel fraude mee gepleegd. Als je toch besluit om een kopie te mailen, maak dan de genoemde gegevens onleesbaar en noteer dat het een kopie is.

● De overheid heeft een speciale app ontwikkeld voor het maken van een veilige kopie van een identiteitsbewijs: KopieID. Na het maken van een foto van het paspoort of de kaart kunnen gegevens onleesbaar worden gemaakt en kan een watermerk worden toegevoegd. De app kun je gratis downloaden.

● Op https://www.politie.nl/themas/internetoplichting.html kun je checken of iemand als oplichter bekendstaat. Op de site van de politie kun je checken of bankrekeningen, telefoonnummers en webadressen bekend zijn. Een check op Google levert vaak ook klachten op als het om een onbetrouwbare aanbieder gaat.

● Klik nooit op linkjes die je niet helemaal vertrouwt, zelfs niet als die afkomstig zijn van goede vrienden. Wees zeker voorzichtig bij Engelstalige teksten of wenskaartjes.

● Banken en andere financiële instellingen sturen je geen e-mails met vragen over persoonlijke gegevens. Als je zo'n e-mail ontvangt, kun je ervan uitgaan dat het om phishing gaat. Voer ook geen updates uit van programma's die je via de mail ontvangt. Door slechts een klik op een besmet linkje kan je hele computer overgenomen worden. De laatste update van

een programma kun je meestal gratis via de officiële site van het programma ophalen.

● Gebruik in plaats van Google die je digitale sporen niet opslaat, zoals Startpage, DuckDuckGo of Epic, www.startpage.com, www.duckduckgo.com of www.epicsearch.in. Gebruik Tor als browser voor geanonimiseerd surfen, www.torproject.org.

● Controleer of het e-mailadres van de afzender van het bedrijf is. Criminelen gebruiken soms wel adressen die op de echte lijken: bij @abnambro.nl plaatsen ze een letter b tussen. Bedrijven gebruiken geen gratis mailboxen als @Hotmail.com, Outlook.com of @gmail.com.

● Een link in een email kan op het eerste gezicht betrouwbaar lijken, maar controleer voordat je op een link klikt waar deze naartoe leidt. Dit kun je zien door met de cursor boven de link te hangen, zonder erop te klikken. Als er een verkorte link wordt gegeven (bijvoorbeeld http://bit.ly/28M1lbJ), kun je naar http://urlxray.com/ gaan om te kijken welke bestemming er achter die link zit.

● Zit er een bijlage bij de e-mail die je moet openen of downloaden (bijvoorbeeld om software te 'updaten'), dan is dit een manier om een virus op je computer te krijgen. Als je aan de echtheid van een e-mail twijfelt, kun je het beste contact opnemen met het bedrijf dat de e-mail gestuurd heeft en vragen of het klopt. Twijfel je of een website gevaarlijk is, of dat een bestand dat je wilt downloaden een virus bevat? Dan kun je een second opinion opvragen bij VirusTotal Virustotal.com. Virustotal is een website die je bestanden

controleert en door verschillende bekende virusscanners laat analyseren. Je krijgt dus de mogelijkheid om al deze virusprogramma's tegelijk te 'gebruiken' zonder deze te hebben geïnstalleerd.

● Om veilig te surfen op het internet kun je de HTTPS Everywhere en Privacy Badger installeren. HTTPS Everywhere forceert wanneer het kan een beveiligde https-verbinding, Privacy Badger blokkeert advertenties en trackers die je op het internet volgen.

● VeraCrypt is op dit moment een van de beste gratis en open source programma's om bestanden te versleutelen. Je creëert een soort extra harde schijf op je computer, een zogehete 'container'. Na het invoeren van je wachtwoord verschijnt de externe harde schijf op je computer en kun je er bestanden in slepen. Zo'n container-bestand kun je vervolgens naar de cloud uploaden.

● ProtonMail is een gratis e-maildienst, die de e-mails tussen de gebruikers standaard versleutelt. Ook je gehele inbox wordt versleuteld, ProtonMail zelf heeft geen toegang tot jouw e-mails.

● Zet je e-mailadres niet op (openbare) websites en wees voorzichtig met het invullen van online formulieren. Klik nooit op (afmeld)-links in spamberichten, want daarmee bevestig je juist dat het e-mailadres in gebruik is en krijg je nog meer spam.

● Om de gevolgen van ransomware te voorkomen moet je regelmatig een externe kopie van je bestanden maken. Automatische back-ups zijn niet aan te raden, want die

kunnen ook versleuteld worden. Werk de software van je computer altijd bij met de laatste updates, aangezien oude software lekken bevat waar de gijzelingssoftware van profiteert.

- Op de site Veilig Internetten vind je veel tips en kun je je computer gratis laten schoonmaken: https://veiliginternetten.nl/maakjecomputerschoon/

- Via http://www.boefproof.nl kun je je gestolen smartphone waardeloos maken voor dieven en je privacy beschermen.

- Op myaccount.google.com kun je instellen dat Google je zoeklocatie en YouTube-geschiedenis niet meer opslaat en aan derden verkoopt. Je kunt ook de al opgeslagen gegevens wissen en Google verbieden om advertenties te koppelen aan je interesses.

- Check welke apps persoonlijke informatie van je binnenhalen: https://www.mypermissions.com.

- Betaalde antivirus-software scoort meestal beter, maar er zijn genoeg gratis mogelijkheden die bescherming bieden, zoals Avast, Avira en Panda Free Antivirus. Ze tonen uiteraard reclame of proberen je over te halen om de betaalde varianten te kopen.

- Voor versleuteld mailen kun je GPGTools gebruiken, bij een Apple https://gpgtools.org en Thunderbird. Bij een Windowscomputer www.gpg4win.org, www.mozilla.org/thunderbird.

● Met de gratis app G-Data Secure Chat kun je veilig chatten: je sms'jes, foto's en berichten worden versleuteld en de gegevens worden verder ook niet op een server bewaard. Voor versleuteld chatten kun je ook www.pidgin.im gebruiken.

● Wis apps die je niet langer gebruikt en wees op je hoede bij het downloaden van nieuwe apps, vooral als die gratis zijn. Er zijn apps die je hele mobiel leegtrekken. Lees de voorwaarden. Bij sommige apps kun je de locatie en het delen van contacten uitzetten, zelfs achteraf.

● Leeg geregeld de prullenmand op je computer, want documenten in je prullenmand blijven kwetsbaar voor virussen.

● Wis je webgeschiedenis, zodat sites die je tracken die niet kunnen lezen. Je kunt je computer ook zo instellen dat je browser dat automatisch doet. Wis ook je cookies (zoek op 'internet-cache'). Een handig programma om de rommel in je computer op te ruimen is https://ccleaner.nl.softonic.com.

● Google biedt een extra beveiligingscode die naar je mobiel wordt gestuurd (de zogenaamde 2-factor identitificatie die je bij de instellingen kunt aanzetten door middel van een vinkje). Ook andere internetbedrijven bieden deze mogelijkheid. Met zo'n extra beveiligingscode kunnen hackers niet meer zo gemakkelijk bij jouw gegevens komen, ook al hebben ze je wachtwoord kunnen achterhalen. De code wordt immers naar jouw telefoon gestuurd, niet naar die van de hacker.

- Bij Facebook kun je de *two-factor authentication* inschakelen. Als iemand inlogt van een onbekende computer, dan krijgt de gebruiker een sms'je met een code om de nieuwe computer aan te merken als een veilige locatie. De volgende keer hoeft de extra authenticatie niet.

- Ook je LinkedIn-account is beter te beveiligen met een dubbele verificatie. Je moet een code invoeren als je inlogt vanaf een niet-herkend apparaat of zoekmachine. Deze code ontvang je in een sms.

- Twittergebruikers kunnen ook hun account beveiligen met een extra verificatiecode bij het inloggen. Ze krijgen een zescijferige code in een sms.

- Als je iets impulsiefs zegt op social media, wis het dan zo snel mogelijk. Zo blijft de schade beperkt.

- Als je een computer buitenshuis gebruikt voor social media of internetbankieren, vergeet dan niet uit te loggen. Vink sowieso de functie om je wachtwoord te onthouden af. Sommige browsers onthouden je wachtwoord, dus wis voor de zekerheid de geschiedenis van de browser.

- Voor internetbankieren kun je het best een speciale browser gebruiken. Bitdefender Safepay is afgeschermd van Windows, zodat je geen virussen en malware oploopt.

- De app Wickr (gratis) belooft hyperveilige communicatie. Je kunt een bericht wissen als het gelezen is.

- Via de site disconnect.me kun je voorkomen dat Facebook je activiteiten elders op het internet volgt.

● Als je de cookie notices in je browser(s) aanzet, kun je zien welke sites cookies plaatsen. Je kunt de cookies blokkeren. Ook kun je de cookies die je volgen verwijderen. Google helpt je op weg via https://support.google.com/accounts/answer/32050.

● Gebruik de Tracker Trackertool als je wilt zien welke trackers op welke websites je onlinegedrag registreren: https://wiki.digitalmethods.net/Dmi/ToolTrackerTracker.

● Als je geen trackers wilt, kun je programma's als Ghostery, Adblock en Do Not Track Me inschakelen.

● Controleer een link voordat je erop klikt (dat kan door met je rechtermuisknop erop te gaan staan om te zien waar de link naartoe verwijst).

● Loop je privacy-instellingen van Facebook na. Mogen je vrienden alles delen? Mogen ze je op foto's taggen? Mogen ze je albums zien? Op Facebook kun je met de optie 'Tijdlijn en taggen' kiezen wie er allemaal berichten op je tijdlijn kunnen plaatsen. Je kunt jezelf ook 'untaggen' op foto's op andere Facebookpagina's. Je kunt niet verbieden dat anderen foto's met jou erop posten (bijvoorbeeld van een feestje), maar untaggen maakt het moeilijker om zo'n foto te vinden.

● Facebook-apps verzamelen veel informatie over je, dus probeer het gebruik daarvan te beperken. Bij elke app zie je een knop 'Instellingen bewerken'. Als je erop klikt, kun je zien naar wie deze app posts verstuurt en wat die nog meer in jouw naam mag uitspoken. Vrienden maken ook van alles over jou openbaar door simpelweg Facebook-apps

te gebruiken. Bij 'Apps die anderen gebruiken' kun je dat allemaal zien. Alle punten die hier aangevinkt staan, van je biografie tot je statusupdates, worden te grabbel gegooid. Je kunt alle vakjes uitvinken als je op je privacy gesteld bent.

- Googel jezelf af en toe om je onlinereputatie te checken. Stel ook een Google Alert op je naam in zodat je een seintje krijgt wanneer er iets over je op het internet verschijnt.

- Als je sexy foto's op je computer hebt: bewaar ze niet op de harde schijf, maar op een SD-kaart of een externe harde schijf. Bewaar ook geen kopie van je identiteitsbewijs in je computer, op een usb-stick is het veel veiliger. Je kunt ook een usb-stick kopen die je eerst moet ontgrendelen voordat je bij de informatie kunt komen.

- Heb je een gijzelvirus op je computer gekregen, kijk op de site https://www.nomoreransom.org of je dat kunt verwijderen zonder te betalen. Betalen is niet verstandig, omdat je hiermee deze vorm van fraude winstgevend maakt.

- In het dashboard van Google kun je zien welke gegevens het bedrijf over jou opslaat. Je kunt de activiteit van je account bekijken en ook wat mensen te zien krijgen als ze je googelen. Je profiel (en de bijbehorende Googlediensten) verwijderen is ook mogelijk. Op de site Me & My Shadow https://myshadow.org vind je nog meer tips en tools om je privacy te beschermen.

- Op de site www.beveiligmij.nl kun je een leuke test doen om te kijken hoeveel je weet over de onlinegevaren.

● Verwijder je verjaardag van Facebook. Heel veel datahandelaren zoals Experian, Acxiom en Rapleaf koppelen je 'likes' aan je geboortedatum en dan weten ze bijna zeker wie je bent, zelfs als je naam veel voorkomt.

● Wees voorzichtig met je privégegevens en zet nergens op internet je 06-nummer, je geboortedatum en je woonplaats. Anoniem surfen kan via sites zoals Torproject.org en Anonymizer.com.

● Kinderen zijn heel scheutig met informatie over zichzelf, familie en vrienden. Ze zien de gevaren niet. Aan een onbekende op straat geven ze hun adres niet, maar op internet wel. Leer je kinderen om niet klakkeloos hun gegevens in te vullen op websites die dat vragen. Het enige wat echt moet kloppen, is meestal het e-mailadres, want daar wordt je wachtwoord naartoe gestuurd. Je echte naam hoeven de sites niet te weten en je adres evenmin.

● Scholen zouden kunnen helpen door jongeren voor te lichten over de gevaren van sexting (sexy foto's die naar een vriendje gestuurd worden, komen geregeld op pornosites terecht), over de gevaren van illegaal downloaden en te veel openheid op social media, over kindermisbruikers die jongeren via spelletjes benaderen en over waar ze meer informatie kunnen krijgen als er iets aan de hand is. Scholen hebben meestal zelf geen expertise in huis, maar er zijn genoeg professionals die workshops en lezingen geven. Op www.mariagenova.nl vind je info over het boek *Sexy selfies*, over het onlinegedrag van tieners en meer info over lezingen.

- Beveilig je brievenbus, zodat criminelen niet je post kunnen stelen.

- Gooi documenten met persoonsgegevens niet bij het oud papier. Koop een papierversnipperaar en haal alle documenten met vertrouwelijke informatie erdoorheen.

- Gebruik programma's zoals Eraser, Sure Delete en Wipe Drive als je je harde schijf wilt wissen. Vernietig de harde schijf als je computer naar de vuilstort gaat.

- Verstuur foto's via SnapChat http://www.snapchat.com als je wilt dat iemand ze ziet, maar niet wilt dat de foto's tot in de eeuwigheid beschikbaar blijven. Bij SnapChat kun je zelf instellen binnen hoeveel seconden na het bekijken de foto vernietigd wordt. Honderd procent zekerheid heb je niet, want zo'n foto kan ook heel snel opgeslagen worden voordat hij voorgoed verdwijnt.

- Geloof niet alles en iedereen op internet of nog beter: geloof zo min mogelijk. Het aantal nep-Twittergebruikers wordt geschat op twintig miljoen. Het internet wemelt van hoaxen en nep-personen met mooie verhalen en kwade bedoelingen.

- Check voordat je iets bij een webshop bestelt of die goed uitziende webshop niet nep is. De webshop moet telefonisch bereikbaar zijn en het btw- en KvK-nummer moeten vermeld staan. Als de webshop een keurmerk heeft, zoals 'waarborg webwinkel', dan moet dat logo aanklikbaar zijn, dus klik er voor de zekerheid op om te controleren of het echt is: een logo is te kopiëren, maar een hyperlink niet.

● Zoek ook op reviews en ervaringen van andere consumenten. WebWinkelChecker (http://webwinkelchecker.nl) is een gratis hulpmiddel om te checken of anderen negatieve ervaringen met een webshop hebben. Het waarschuwt ook voor faillissementen en misbruik van keurmerken.

● Werk voordat je online gaat winkelen of betalen je besturingssysteem bij met de nieuwste updates. Gebruik ook een goede firewall. Op de site van de Consumentenbond vind je geschikte gratis software.

● Kopen en betalen op internet kun je beter niet doen vanuit een internetcafé of vanaf een geleende laptop, want je weet niet of de beveiliging goed is.

● Bij webwinkels moet je bij je eerste bestelling een account aanmaken en een wachtwoord kiezen. Verzin een uniek en sterk wachtwoord dat je niet ook voor andere diensten gebruikt. Gebruik dus niet het wachtwoord van je e-mail.

● Voer persoonlijke informatie alleen op beveiligde websites in (met 'https://' in de adresbalk of een hangslotsymbool).

● Beveilig alle mobiele apparaten met een wachtwoord. Er zijn nog steeds veel mensen die hun mobiel met '0000' en '1234' beveiligen. Als je je mobiel kwijtraakt, dan kan de vinder alles lezen wat op je mobiel staat.

● Maak alleen verbinding met vertrouwde Wi-Fi-netwerken. Open Wi-Fi (bijvoorbeeld bij McDonald's) is per definitie onveilig, hackers kunnen al je berichten en wachtwoorden onderscheppen.

● Jaarlijks worden een kwart miljoen Nederlandse reisdocumenten en rijbewijzen als verloren of gestolen opgegeven.

Dat is een groot potentieel voor lookalike-fraude. Doe altijd meteen aangifte en vraag een nieuw document aan.

● Als je een e-mail met een bijlage ontvangt of met een ingekorte hyperlink of een verzoek om ergens in te loggen, doe het dan niet, zelfs niet als je de afzender kent. Het account kan gehackt zijn. Accepteer het bericht alleen als je met elkaar afgesproken hebt dat diegene mailt.

● Meer dan de helft van de ondernemers is al slachtoffer geworden van cybercrime. Als je een zaak hebt, controleer dan geregeld je rekeningafschriften op kleine bedragen, want identiteitsfraude begint vaak met kleine bedragen die afgeschreven worden. Deze tip geldt overigens ook voor particulieren.

● Sta geen bankmedewerkers te woord via de telefoon, want fraudeurs geven zich geregeld uit als medewerker van de bank en vragen naar je response-code.

● Beveilig je computer met een virusscanner en een goed beveiligde Wi-Fi-verbinding. Installeer apps voor mobiel of tablet uitsluitend via de officiële applicatiewinkels. Gebruik geen illegale kopieën in verband met virussen. Kijk ook goed naar de toegangsrechten van de app en naar ervaringen van medegebruikers.

● Sluit pop-ups met de toetscombinatie Alt+F4 af (op een Apple met Cmd + W). Klik nooit op akkoord of 'x' of 'nee' om een pop-up af te sluiten, want zo kun je per ongeluk malware installeren. Installeer eventueel een pop-upfilter om pop-ups te blokkeren.

- Maak back-ups op externe, losgekoppelde gegevensdragers (zoals een dvd, een USB-stick of een externe harde schijf).

- Doe aangifte als je toch slachtoffer wordt van identiteitsfraude. Identiteitsfraude herken je als je bijvoorbeeld een afwijzing voor een lening ontvangt, brieven krijgt die niet voor jou bestemd lijken of opeens geen post meer ontvangt.

- Het Centraal Meld- en informatiepunt voor Identiteitsfraude en -fouten (CMI), de Fraudehelpdesk en het Landelijk Meldpunt Internetoplichting geven voorlichting en helpen slachtoffers bij het doen van aangifte en het oplossen van hun zaak.

- Check op https://haveibeenpwned.com of bedrijven/websites je wachtwoord gelekt hebben en zo ja, verander zo snel mogelijk je wachtwoord (ook op alle andere websites waar je dat wachtwoord gebruikt).

- Een vreemd e-mailadres als afzender is vaak een aanwijzing voor phishing. Het deel achter het @-teken moet eindigen op de domeinnaam. De tekst voor de domeinnaam moet gescheiden zijn met een punt. Goed: nieuwsbrief@mail.ing.nl Fout: nieuwsbrief@emaillogin-ing.nl

- Wees voorzichtig met verkorte links in mail en op websites. Testen waar de link naar toe gaat, kan via www.unshorten.it

- De volgende bestandstypen zijn extra verdacht als ze in een mailbijlage staan: zip: een zip-bestand wordt gebruikt om de inhoud (vaak een .exe-bestand) te maskeren. exe: een programmaatje, nagenoeg altijd foute boel. js .ink .wsf

.scr .jar: Nooit openen! Ze bevatten scripts die malware downloaden. doc is een Word-document en standaard niet gevaarlijk, maar als het bestand na openen vraagt om het inschakelen van macro's, doe dat dan niet. Helaas zijn de extensies (zoals .exe) in Windows standaard verborgen. Schakel bestandextensies in, zodat je ziet om wat voor bestand het gaat. Typ Windowstoets + R, typ in het venster 'control folders' en druk op Enter. In het tabblad Weergave verwijder je het vinkje voor 'Extensies voor bekende bestandstypen verbergen'.

- Twijfel je of je een virus op je toestel hebt? Doe een gratis online scan op een van antiviruswebsites , bijvoorbeeld ESET Online Scanner, F-Secure Online Scanner of Panda Cloud Cleaner.

- Heb je al bepaalde gegevens prijsgegeven aan een fraudeur, dan moet je direct bij de betrokken bedrijven of instanties aan de bel trekken. Waarschuw direct je bank, dat kom je waarschijnlijk in aanmerking voor compensatie van de schade. Heb je een wachtwoord ingevuld? Verander dit wachtwoord meteen. Heb je je mobiele nummer ingevuld? Meld je af voor ongewenste (sms) betaaldiensten via Payinfo.nl.

- Of een profielfoto van je wordt gebruikt op andere websites, kun je checken met https://images.google.nl

- Op https://myactivity.google.com kun je zien wat Google over je verzameld heeft. Geschrokken? Deze informatie kun je deels verwijderen. Gebruik de zoekfunctie en de filters.

- Zorg altijd dat je smartphone, tablet of laptop niet standaard naar wifinetwerken zoeken en verbinding maken

met 'bekende netwerken,' want die zijn misschien helemaal niet zo bekend als ze zich voordoen. Schakel de optie uit dat verbonden netwerken standaard worden onthouden.

● Maak regelmatig een back-up van de belangrijke dingen die op je telefoon staan. Op computers en laptops is het al doodnormaal, op telefoons nog niet: zet een antivirusscanner op je telefoon. Antivirus-apps zijn gewoon te vinden in de appstores, maar let op de beoordelingen. Ze kunnen je waarschuwen als apps zich verdacht gedragen.

● Is jouw telefoon besmet met de schadelijke software? Dan kun je het probleem oplossen door de fabrieksinstellingen te herstellen en je mobiel opnieuw op te starten. Ga hiervoor naar 'instellingen' en klik op 'privacy'. Selecteer 'fabrieksinstellingen herstellen' en kies tot slot 'herstel telefoon'. Let op: alle gegevens worden van je smartphone verwijderd, dus ook jouw persoonlijke bestanden.

● Soms is het niet mogelijk om je mobiele telefoon opnieuw op te starten. In dat geval is er een andere truc om het systeem te herstellen. Druk de volgende combinatie tegelijk in en houd deze handeling 10 seconden vast: geluid harder, home button en de aan/uit knop. Vervolgens wordt je mobiel opnieuw opgestart. Selecteer 'wis data' en klik op 'terug naar fabrieksinstellingen'. Ook nu raak je jouw persoonlijke bestanden kwijt.

● De gratis Kaspersky Anti-Ransomware Tool voorkomt gijzelingen van bestanden https://go.kaspersky.com/Anti-ransomware-tool.html

● Ga bij de instellingen van je telefoon naar 'beveiliging' en klik op 'versleutelen.' Als je je telefoon verliest, kunnen

anderen niet zomaar bij de inhoud van je smartphone komen. Ze hebben dan je wachtwoord nodig om de versleuteling ongedaan te maken. Een zeer uitgebreide site die privacy-tools vergelijkt: https://www.privacytools.io

● Een gedetailleerde uitleg hoe je tweestapsverificatie instelt om je social media-accounts te beveiligen vind je op: https://www.want.nl/tweestapsverificatie-online-accounts/

● Check of je internet-devices publiekelijk te vinden zijn http://iotscanner.bullguard.com

● Phishing wordt niet alleen via e-mail verstuurd, ook SMS en chat-apps worden misbruikt. Wees heel voorzichtig met het openen van links en het installeren van apps wanneer dit via een onverwacht bericht wordt gevraagd. Vul niet zomaar wachtwoorden op websites of in apps. Via de site https://breachalarm.com krijg je een melding als 1 van je wachtwoorden gelekt is.

● Wil je een keer een interactieve lezing over de nieuwste ontwikkelingen op het gebied van privacy en cybercrime bijwonen? Maria Genova geeft elke maand lezingen aan bedrijven en organisaties, waarvan een aantal openbaar. Meer info op http://mariagenova.nl/lezingen/

Handige links

Centraal Meld- en informatiepunt Identiteitsfraude https://www.rijksoverheid.nl/contact/contactgids/centraal-meld-en-informatiepunt-identiteitsfraude-en-fouten-cmi

Fraudehelpdesk: www.fraudehelpdesk.nl

Slachtofferhulp Nederland: https://www.slachtofferhulp.nl

In de toolbox van Bits of Freedom vind je handige instructies hoe je je laptop en mobiel veiliger kunt maken: https://toolbox.bof.nl

Test je phishing-kennis: https://onderzoek.consumentenbond.nl/csb517/Project/Completed

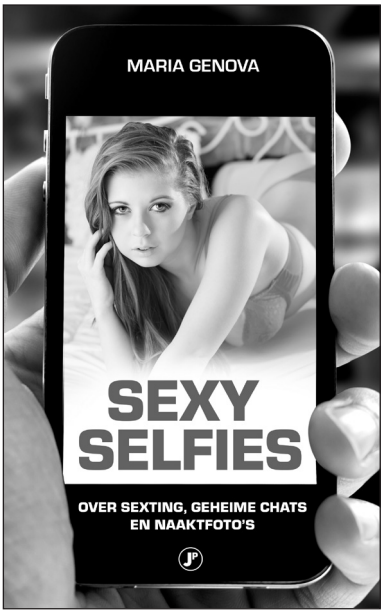
Opgelet op internet: http://www.opgeletopinternet.nl

Beveiligingtests en weetjes: http://www.beveiligmij.nl

En ten slotte iets leuks: bekijk het filmpje op http://www.safeinternetbanking.be/nl/dave-campagne

Ook op www.mariagenova.nl vind je een filmpje over identiteitsfraude, met een echt slachtoffer en een echte hacker. Op http://mariagenova.nl/lezingen/ vind je ook info voor het aanvragen van lezingen en awareness-sessies.

Lees nu ook



'Als je niet met mij naar bed gaat, zet ik je naaktfoto op alle pornosites...'
Wat doe je dan?
–
'We scoren naaktfoto's van meisjes en dan ruilen we ze met elkaar, net als de Panini-plaatjes.'

In *Sexy selfies* vertellen slachtoffers (m/v) over de gevolgen van het maken van onschuldige naaktfoto's. De slachtoffers worden zo erg gepest en bedreigd dat sommige tieners zelfmoord plegen. Maria Genova sprak tientallen tieners en kreeg hun geheime chats doorgestuurd. Ook daders vertellen waarom ze naaktfoto's doorsturen en soms zelfs verzamelen.

Sexy selfies bevat veel tips voor onzekere tieners en voor onwetende ouders. Kun je een sexy selfie maken zonder in de problemen te komen? Hoe pak je de pesters aan als je naaktfoto uitlekt? Hoe kun je voorkomen dat een foto verspreid wordt? En hoe kun je verhinderen dat je webcam wordt gehackt?

*Journaliste **Maria Genova** (1973) is auteur van een aantal succesvolle en taboedoorbrekende boeken. Zeer spraakmakend was **Het Duivelskind**: over foute ouders en falende jeugdzorg. In 2014 werd Maria Genova uitgeroepen tot schrijfster van het jaar.*

JUST PUBLISHERS