WHAT THE HACK!

Maria Genova

Maria Genova © 2018
www.mariagenova.nl
ISBN: 978-90-814726-2-3

Uitgever: MG Books Media
Cover: Flavour
Illustraties: André Versteeg
Opmaak: Mira Loves Books
Fonts: Fontsquirrel

Eerste druk: december 2018

Maria Genova

WHAT THE HACK!

MG Books Media

1. GEHACKT

André moet een auto ontwijken, maar dat lukt op het laatste moment niet. De twee Formule 1-auto's knallen op elkaar. Er volgt een explosie. Gelukkig is het maar een game, denkt André, terwijl hij naar zijn laptop kijkt.

Opeens verschijnt er een scherm dat hij niet eerder heeft gezien. Het is een doodshoofd met de tekst 'Je bent gehackt!'.

Huh? André probeert het vreemde scherm weg te klikken, maar dat lukt niet. Het doodshoofd blijft hem met lege ogen aanstaren. Zijn hele computer is geblokkeerd.

Dit kan niet waar zijn, denkt André. Wat heb ik verkeerd gedaan? Hij probeert zich te herinneren waar hij allemaal op geklikt heeft. Er was een linkje naar een grappig filmpje. En hij heeft een nieuw spel gedownload. Er was ook een advertentie dat je een gratis iPhone kon winnen. Daar heeft hij niet op geklikt, want dat vond hij meteen verdacht.

André heeft geen idee hoe de hackers binnengekomen zijn. Wat ze willen, staat wel op het scherm: geld, te betalen in bitcoins. Als hij niet betaalt, wordt zijn hele computer gewist.

André probeert nog een keer de muis te bewegen. Zijn hand trilt. Ik ga die boeven niet betalen, denkt hij. Snel mijn vader vragen, volgens mij heeft hij niet zo lang geleden nog een backup gemaakt.

Zijn vader zit in de woonkamer de krant te lezen als André met een bezorgde blik binnenstormt en bijna een vaas omver gooit.

‘Pap, ik heb iets stoms gedaan, denk ik. Mijn laptop doet het niet meer.’

‘Ja, je laptop is vast de kluts kwijt na al die uren gamen. Misschien heeft-ie een burn-out gekregen en heeft-ie wat rust nodig om te herstellen.’

‘Pap, probeer niet van alles een grapje te maken. Ik ben gehackt.’

De ogen van zijn vader worden groot. ‘Gehackt? Hoe weet je dat?’

’Nou gewoon, dat staat op het scherm. Kom maar kijken.’

Zijn vader staat op en loopt mee.

‘Waar heb je allemaal op geklikt? Wat heb je gedownload?’

‘Ja hallo, onthoud je zelf waar je allemaal op klikt?’ reageert André gefrustreerd. ‘Er zijn een paar dingen waar ik achteraf aan twijfel, maar daar hebben we nu niets aan.

Pap, je hebt toch laatst een apparaat aangesloten om automatische back-ups te maken? Als dat goed werkt, ben ik niets kwijt.'

'Dat hoop ik voor je,' zegt zijn vader en haast zich naar zijn eigen computer om de back-ups te checken.

'Nee hè!' hoort André even later.

'Wat is er?'

'De hacker heeft ook de back-ups versleuteld. Via jouw computer heeft hij toegang gekregen tot alle automatische back-ups.'

André kijkt zijn vader ongelovig aan. 'Dus ik ben alles kwijt?'

'Ik vrees van wel.'

'Maar pap, ik heb honderden foto's op mijn laptop en heel veel games.' De blik van André is wanhopig, hij weet zich geen houding te geven en wiebelt nerveus van het ene been op het andere.

'Ik weet het ook niet,' zucht zijn vader. 'Ik vrees dat er geen oplossing is. Laatst werd een collega van me gehackt en hij heeft zijn laptop naar een computerwinkel gebracht in de hoop dat ze iets van zijn bestanden konden redden. Dat is niet gelukt. Uiteindelijk was hij alleen maar extra geld kwijt, want in de computerwinkel werken ze niet gratis.'

'Heeft hij de hackers betaald?'

‘Ja, 800 euro. Want hij wilde zijn foto’s en een aantal belangrijke documenten terug. Toen hij betaalde, werkte alles weer.’

‘800 euro?’ André kijkt verschrikt. ‘Dat heb ik helemaal niet.’

‘Zelfs als je het hebt, lijkt het me niet slim om boeven te betalen. Zo worden ze steeds rijker en zien ze dat misdaad loont.’

‘Is er geen kans dat ze opgepakt worden?’

‘Nauwelijks. Ik las net in de krant dat er vorig jaar drie miljoen Nederlanders slachtoffer zijn geworden van cybercrime. Je denkt toch niet dat de politie zo veel mensen in dienst heeft om al die zaken op te lossen? Je kunt beter jezelf beschermen.’

‘Maar pap, ik heb niet eens iets geks gedaan! Ik klik gewoon op linkjes en download af en toe een programma, dat doet toch iedereen?’

‘Ja, en dat is het probleem: er zijn tegenwoordig heel veel nep berichten en websites waarmee je een virus naar binnen haalt.’

André is helemaal niet blij met de uitleg van zijn vader. Er moet toch een manier zijn om te zien dat iets juist van een hacker komt? Gek genoeg hebben ze daar op school nooit een les over gekregen, terwijl al zijn vrienden

urenlang online zijn en overal op klikken. Laatst had Sanne uit hun klas ook ergens op geklikt en toen had een hacker haar webcam overgenomen. Hij filmde haar in haar slaapkamer, terwijl ze zich aan het uitkleden was. Daarna wilde hij geld. Anders zouden de foto's verspreid worden. Dat gebeurde ook. Eén van de foto's ging de hele school rond, vooral via WhatsApp. Iedereen kon haar bloot zien. André vond het heel erg voor Sanne, vooral de reacties: "Trut", "Ben je zo trots op je borsten?', 'Wat ben je een domme meid dat je op deze manier aandacht zoekt!' Alsof Sanne het expres gedaan had en al die negatieve aandacht leuk vond! Ze was al een week niet op school verschenen, omdat het pesten dagenlang doorging.

'Waar denk je aan?' vraagt zijn vader.

'Eh, niets bijzonders. Ik denk hoe we ons beter tegen hackers kunnen beschermen. Er moet vast een manier zijn.'

'Ja, er zijn genoeg manieren.'

'Misschien kan ik de beste manieren verzamelen en met mijn vrienden delen.'

'Dat lijkt me een goed idee,' zegt zijn vader en klopt hem op zijn schouder. 'Ga nu maar naar bed. Ik ga je laptop opnieuw installeren. Dan heb je een gloednieuwe laptop zonder al die rare schietspelletjes. Ruimt lekker op.'

André kijkt zijn vader woedend aan.

Zijn vader geeft hem een knipoog. ‘Ach, maak je je geen zorgen, ik weet dat het je binnen no time lukt om je laptop weer vol te krijgen.’

2. DE TOFFE PEER

Sanne is weer op school. André is blij om haar te zien. Hij vindt haar het leukste meisje van de klas, ook al heeft hij dat nooit aan iemand te durven vertellen. Ze ziet er nu wel ongelukkig uit en loopt met hangende schouders de klas binnen.

'Hé Sanne, ga je weer je shirtje omhoog doen?' hoort hij opeens iemand roepen. Sanne verkrampt en André kijkt wie dat geschreeuwd heeft. Joeri natuurlijk, de grootste pestkop. En hij gaat nog even door: 'Hoe gaat het met je hacker, Sanne? Heeft je pappie hem al opgespoord? Je vader zit toch bij de politie?'

André heeft de neiging om de pestkop een klap te verkopen. Maar dan gaat Joeri hem in elkaar slaan, want hij is een kop groter en twee keer zo zwaar. En de volgende dag gaat hij Sanne weer pesten, want zo is hij nu eenmaal. Al die anti-pest praatjes op school hebben niets geholpen. Gasten zoals Joeri denken alleen maar: 'Laat de meester maar kletsen.' Misschien hadden ze één van die keren kunnen praten over hoe je je tegen hackers kunt beschermen in plaats van tegen pestkoppen. Dan was het Sanne waarschijnlijk niet overkomen en zouden ze haar

ook niet pesten.

De bel gaat en meester Bas komt het lokaal binnen. Hij is een beetje maf, vindt André, draagt vaak twee verschillende sokken en hij denkt blijkbaar dat dit hip is. Hij probeert ook hip te praten met woorden als ‘chill’ en ‘ziek’. ‘Ziek man.’ Welke docent zegt nou zoiets? Dat werkt iedereen op de lachspieren, maar meester Bas denkt dat ze hem tof vinden. Laatst met het carnaval had hij zich verkleed als een peer, omdat hij zo graag wilde horen dat hij een toffe peer is. Tja, zijn er nou werkelijk mensen die een man verkleed als een peer tof vinden…?

‘En André, wat is jouw idee? Ik weet dat je heel creatief bent, dus misschien kun jij dat als eerste vertellen om de rest te inspireren.’

André schrikt zich rot. Waar heeft de meester het over?

‘Uuh...’

‘Je moet met een idee komen wat je voor de maatschappij kunt doen,’ fluistert Sanne.

‘Hackers,’ zegt André.

‘Hackers?’ Meester Bas kijkt hem met gefronste wenkbrauwen aan.

‘Uuh, ik bedoel dat we iets moeten doen om ons beter tegen hackers te beschermen. Vorig jaar zijn drie miljoen mensen slachtoffer geworden van cybercrime,’ herhaalt

hij wat hij van zijn vader heeft gehoord.

'De vraag is wat je persoonlijk kunt doen, André. Ik neem aan dat je geen computerprogramma hebt gemaakt om alle hackers te weren?' Meester Bas kijkt hem streng aan en wacht op antwoord.

'Nee, dat niet,' stamelt André. 'Maar misschien kan ik een soort gratis e-book maken over wat je moet doen om je computer en je mobiel tegen hackers te beschermen. Ik denk dat veel mensen dat niet weten.'

'En weet jij dat wel dan?'

'Uuh, nou nee, eigenlijk niet,' geeft André eerlijk toe en kijkt naar de grond.

'Hoe zie je dat dan voor je? Je geeft tips die je zelf niet kent? Worden die tips je door een hogere macht ingefluisterd of zo?' lacht de meester.

'Er zijn mensen die inderdaad stemmetjes horen, maar die zitten meestal in bepaalde klinieken,' roept Joeri. 'Sommigen denken dat ze God zijn, anderen denken dat ze een toffe peer zijn.'

De klas barst in lachen uit.

'Mag ik iets voorstellen?' Sanne steekt haar hand op. Iedereen kijkt haar verbaasd aan. Het is de eerste keer dat ze weer durft te praten sinds haar naaktfoto verspreid is.

'Als je maar niet over naaktfoto's begint,' joelt Joeri.

Enkele jongens liggen in een deuk. Sanne kleurt hele-

maal rood.

‘Jongens, we hebben al verschillende keren over pesten gesproken en hoe slecht dat is,’ grijpt meester Bas in. ‘Ik wil niets meer over die naaktfoto horen. Sanne kon er niets aan doen dat haar computer gehackt werd. Dat kan iedereen overkomen.’

‘Niet iedereen, maar zeker 80 procent van ons is een makkelijke prooi voor hackers,’ zegt Sanne zacht.

‘En hoe kom je aan die wijsheid?’ roept Joeri. ‘Ben ik volgens jou ook gemakkelijk te hacken?’

‘Waarschijnlijk wel,’ zegt Sanne.

‘O, mevrouw de wijsneus, ik heb toevallig een zeer goed antivirusprogramma.’

‘Dat gaat niet helpen,’ zegt Sanne. Haar stem klinkt plotseling niet meer zo onzeker. ‘Elke dag verschijnen er duizenden nieuwe computervirussen en er is geen enkel antivirusprogramma dat ze allemaal herkent. Dat weet ik omdat mijn broer ethische hacker is. Hij kan bijna elke computer hacken.’

‘Ha jongens, horen jullie dat ook?’ joelt Joeri. ‘Haar broer is een hacker en Sanne is laatst gehackt. Misschien hadden ze ruzie en wilde haar broer haar een lesje leren.’

‘Doe niet zo flauw,’ schreeuwt Sanne. ‘Natuurlijk heeft mijn broer dat niet gedaan.’

‘Joeri, ik zei dat het tijd wordt om te stoppen met

pesten,' probeert meester Bas weer.

Pff, denkt André, zolang de meester dat op zo'n milde toffe peer toon zegt, gaat er niets veranderen.

'Wat betekent ethische hacker?' vraagt Elise.

'Dat je iemand hackt, maar alleen om te testen of degene goed beveiligd is,' antwoordt Sanne. 'Verder mag je de gevonden gegevens niet misbruiken.'

'Ha, en waarom zou je dat testen?' vraagt Joeri. Hij klinkt opeens belangstellend.

'Dat doet mijn broer meestal in opdracht van bedrijven. Hij gebruikt dezelfde programma's die de kwaadaardige hackers gebruiken en laat dan zien wat voor schade ze zouden kunnen aanrichten. Daarna adviseert hij hoe ze de gaten in hun computers kunnen dichten. Hij wordt dus betaald om te hacken en hij is niet strafbaar.'

'Hoezo is hij niet strafbaar?' vraagt Elise.

'Omdat hij van tevoren toestemming heeft gekregen. En omdat hij de gaten in de beveiliging meldt en niet misbruikt.'

'Kan je broer mij ook hacken?' vraagt Joeri.

'Ja, maar dat gaat hij niet doen. Want dan is hij wel strafbaar. Je mag niet zomaar mensen hacken. Daar kun je een gevangenisstraf voor krijgen.'

André zegt de hele tijd niets, maar luistert wel geboeid. Een ethische hacker, dat is precies wat hij nodig heeft voor

zijn plan om de maatschappij veiliger te maken.

‘Wat zijn we ver afgedwaald,’ zegt meester Bas, ‘we zijn begonnen met maatschappelijke projecten om uit te komen bij… ‘

‘Perensap,’ roept Joeri. ‘Wie heeft er nog meer trek in perensap?’

De klas begint te lachen. Meester Bas heeft nog steeds niet door dat dit over hem gaat, maar hij stoort zich wel aan al die luidruchtige leerlingen.

‘Nu gaan we echt terug naar de les. Ik weet niet waarom Sanne opeens over hackers begon, terwijl André aan het woord was…’

‘Ik weet dat wel,’ zegt André. Iedereen kijkt hem nieuwsgierig aan, ook meester Bas. ‘Ik denk dat Sanne me een hint wilde geven. Ik zei dat ik een gratis e-book wil maken hoe we ons beter tegen hackers kunnen beschermen, maar eerst moet ik dat zelf leren. En haar broer weet dat, omdat hij op dezelfde manier werkt als de kwaadaardige hackers.’

‘Best een goed plan,’ zegt meester Bas. ‘Maar ik weet niet of haar broer wil meewerken.’

‘Ik denk het wel,’ zegt Sanne. ‘Mijn broer vindt het ook belangrijk dat mensen hun computers beter beschermen. Anders kan dat tot veel ellende leiden.’

‘Ja, hij hoeft alleen maar naar zijn zusje te kijken,’ joelt

Joeri.

‘Joeri!’ schreeuwt de leraar. Nu is hij echt boos.

Op dat moment gaat de bel.

‘Gered door de bel,’ mompelt André. ‘Wat oneerlijk.’

3. VLOG

André houdt zijn mobieltje in zijn hand, met de camera naar zich gericht. Hij twijfelt. Zal hij het doen? Hij heeft het heel vaak gezien, tieners die vloggen, maar durft hij dat zelf ook? Hij is in elk geval zo enthousiast over hoe de dag verlopen is dat hij toch op de opnameknop drukt. Hij ziet de camera lopen.

'Hallo iedereen,' roept hij enthousiast, terwijl hij in de camera kijkt en glimlacht. Mijn naam is André en dit is mijn eerste vlog. Ik ben net begonnen met een project. Het heet *What the hack!* Misschien denk je nu al "What the hack!", maar ik heb niet zomaar voor deze naam gekozen. Ik werd namelijk niet zo lang geleden gehackt. Ik weet nog steeds niet hoe, maar mijn hele computer werd versleuteld en ik was al mijn gegevens kwijt. De meeste van ons zijn simpel te hacken, gewoon omdat we veel dingen verkeerd doen online. Ik was vandaag op bezoek bij een ethische hacker en hij heeft me precies laten zien wat. Wil je dat ook weten? Volg dan mijn vlogs en je ziet hoe project *What the hack!* afloopt. Ik beloof je dat je aan het einde zo goed als onhackbaar bent. Want hackers werken net als gewone inbrekers: maak het ze iets moei-

lijker en dan gaan ze door naar de volgende.'

André drukt op stop om de opname te beëindigen. Zijn hart klopt in zijn keel. Heeft hij het goed gedaan? Was hij duidelijk genoeg? Zouden ze hem niet uitlachen? Vloggen ziet er best simpel uit, maar er is blijkbaar veel moed voor nodig.

Op dat moment komt een appje van Sanne binnen: 'En, is het gelukt met het filmpje? Mijn broer is heel enthousiast hoe je het wilt doen en ik ben benieuwd hoe het filmpje is geworden.'

'Ik zet het zo online,' appt André terug. Op dat moment beseft hij dat er geen weg meer terug is. Sanne vindt hem vast een lafaard als hij het opeens niet doet. André drukt snel op 'Upload'.

Het filmpje staat online. Andre houdt zijn adem in. Zullen ze het goed vinden?

Al vrij snel verschijnen enkele duimpjes omhoog. Gelukkig maar, hij haalt opgelucht adem. Dan verschijnt er een nieuwe reactie. 'Gehackt zei je? En je gaat ons leren hoe we ons moeten beschermen tegen hackers? Alweer iemand die denkt dat hij heel wat is, maar niet weet waar hij het over heeft. Doet me denken aan een ander iemand, een toffe peer. Die is gelukkig nog niet gaan vloggen, ook al zie ik hem daar wel voor aan.'

André hoeft niet eens naar de naam te kijken om te weten wie de reactie geplaatst heeft. Zelf gebruikt hij altijd een schuilnaam als hij op forums reageert, maar Joeri geeft blijkbaar niets om zijn privacy, want zijn volledige naam staat eronder met een duimpje naar beneden. André googelt hem even en ziet al snel veel informatie verschijnen. Hobby's: gamen (natuurlijk, wat anders?), sporten: fietsen (alleen dat kleine stukje naar school zeker?), beste vrienden: drie (heeft die pestkop drie echte vrienden?). Bij interesses heeft hij Netflix ingevuld. Zeker met een grote bak chips op de bank? Want die dikke buik moet toch ergens vandaan komen. Er is ook een foto met zijn hond Rex in zijn slaapkamer. Zijn wachtwoord is vast Rex gevolgd door zijn geboortedatum… Vooral één van de vele foto's trekt de aandacht: Joeri zwaait met een fles bier. Hij staat best voor paal, vindt André, vooral met zo'n bierbuik.

Even later verschijnt er weer een reactie: 'Leuk filmpje, ik wil hier meer over weten.' Die is van Elise. En Sanne reageert ook: 'Dit kan een mooi project worden, succes ermee! Ik heb een paar van de tekeningen die je voor het boek wilt gebruiken al op je Insta gezien: wow, wat kun jij tekenen!'

André glimlacht. Hij krijgt vaker te horen dat hij mooi kan tekenen, maar uit de mond van Sanne klinkt dat nog

leuker.

Er verschijnen nog meer duimpjes en ook een privé bericht van DarkHacker13. Als André het bericht leest, krijgt hij kippenvel. ‘Hey gozer, haal dat stomme idee uit je hoofd om al die digibete debielen cybersmart te maken. Wij verdienen er goed geld aan en dat laten we niet zomaar afpakken. Mocht je je project doorzetten, dan krijg je met ons te maken. We beginnen digitaal, maar als dat je nog niet afschrikt, ontmoet je ons offline.’

André krijgt er rillingen van. DarkHacker13, wie is dat? En meent hij dat nou echt? Zou Joeri onder een andere naam reageren om hem de stuipen op het lijf te jagen? Of heeft hij echt met hackers te maken die niet blij zijn met wat hij wil doen? Als dat zo is: hoe ver zullen ze gaan?

André pijnigt zijn hersenen, terwijl hij van tevoren weet dat hij daar geen logisch antwoord op kan verzinnen. Maar het dreigement houdt hem wel bezig. Hoe zet je je negatieve gedachten stop? Misschien gewoon wegklikken en iets anders gaan doen. Of op Facebook kijken, daar delen mensen vaak van die filmpjes waar je om moet lachen. Laatst eentje met voetballers die weggevoerd werden op brancards. En de verzorgers lieten ze allemaal vallen. Eén van die klunzige verzorgers verloor drie keer achter elkaar zijn evenwicht en ging op het gezicht van de voetballer zitten. Best zielig voor de gewonde voetballers,

maar André kon zijn lachen niet inhouden. Waar hadden ze al die klunzen gevonden?

Deze keer is het een stuk saaier op Facebook, vooral filmpjes van huisdieren. En ook enkele meisjes van zijn klas die verwikkeld lijken in een strijd wie de meest sexy selfie online kan plaatsen. Een aantal strooit met wijze spreuken en Sanne heeft ook zoiets gepost: 'Waarom we fouten bij anderen zo snel herkennen, is omdat ze ons zo bekend voorkomen.'

André geeft het een like. Het liefst wil hij Sanne een mooi berichtje sturen, een compliment, maar hij is bang dat ze dan gaat denken dat hij verliefd op haar is. Misschien is dat ook zo, maar dat hoeft ze niet te weten. Nog niet. Daar moet hij toch wat meer moed voor verzamelen. Het is eigenlijk nog erger dan een vlog. Een vlog kun je tenminste nog wissen en dan verdwijnen ook alle reacties, maar als Sanne hem afwijst, dan kan hij dat niet even snel wissen. Morgen ziet hij haar weer. Dan heeft hij een afspraak met haar broer om verder samen aan het e-book te werken. En dan gaat haar broer hem ook in de praktijk laten zien hoe hij hackt. André heeft hem toestemming gegeven om zijn laptop te hacken.

4. STIEKEM GEFILMD

Voordat André naar Rickey, de broer van Sanne, vertrekt, kijkt hij nog even of er nieuwe reacties op zijn vlog zijn. Hij ziet heel veel nieuwe duimpjes omhoog en een paar leuke reacties. En ook weer eentje dat behoorlijk creepy is: 'We houden je in de gaten. Check je webcam. Gemeend advies: stop dit maffe project. We gaan natuurlijk niet heel veel tijd aan je besteden, maar het is een kleine moeite om je dwaze plan te dwarsbomen.'

Het is alweer een bericht van DarkHacker13. Blijkbaar geen grap, anders gaat hij niet door met dat soort berichten. Aan wie moet hij dat vertellen? Zijn ouders zijn geen optie, die weten sowieso van niets. Sanne? Zij kan er niets aan doen, waarschijnlijk maakt hij haar alleen maar bang. Aan Rickey dan? Hij kent hem nauwelijks. Nee, beter aan niemand vertellen. DarkHacker13 heeft tenslotte nog niets gedaan. Misschien is het iemand die niet eens kan hacken, alleen maar kletsen. Deze gedachten geven André niet veel rust. Als hij naar zijn voorgevoel luistert, weet hij dat er iets niet klopt. Hij kijkt naar zijn webcam. Hij neemt zich al een tijdje voor een webcamcover te bestellen, maar komt er steeds niet aan

toe. Een pleister erop plakken kan natuurlijk ook, maar dat staat zo suf. Binnenkort toch maar een onopvallende webcamcover voor de zekerheid bestellen. Misschien vanavond nog.

Een uur later belt hij bij Sanne aan. Haar broer doet open. ‘Kom binnen,’ zegt Rickey. ‘Leuk om je weer te zien. Ben je er klaar voor?’

‘Voor wat precies?’ vraagt André.

‘Om gehackt te worden natuurlijk. Of dacht je dat ik een grapje maakte vorige keer?’

‘Nee, maar op de een of andere manier klonk het uit je mond niet heel spannend.’

‘Klinkt het spannender als DarkHacker13 dat zegt?’

André kijkt hem achterdochtig aan. ‘Hoe weet je dat? Heb je daar iets mee te maken?’

‘Niet echt.’

‘Maar hoe weet je het dan?’

‘Nou, de reacties op je filmpje zijn gewoon openbaar.’

‘Ken je die gast?’

‘Niet dat ik het weet, maar ik heb een beetje huiswerk gedaan. Ik zag zijn naam bij diverse forums op het Dark Web opduiken. Hij verhuurt botnets.’

‘Botnets?’

‘Een botnet is een netwerk van heel veel besmette

computers, soms honderdduizenden. Al die computers zijn besmet met een virus, zodat hackers ze kunnen aansturen. Daar vallen ze bedrijven mee aan, persen webshops af die ze eerst offline gooien en ze kunnen ook hele ziekenhuizen platleggen, waardoor de patiënten gevaar lopen.'

'Maar van wie zijn al die duizenden besmette computers?' vraagt André.

'Van iedereen, van gewone mensen. Van jou en van je vrienden. Terwijl jullie berichtjes uitwisselen zijn jullie laptops en mobieltjes bijvoorbeeld de banken aan het aanvallen. En dat lukt, ook grote banken gooien ze offline als ze met zo veel apparaten tegelijkertijd aanvallen.'

'Maar dat moeten we toch merken?'

'Meestal merk je er niets van. Als een hacker binnenkomt, zet hij het antivirusprogramma vaak uit. Hooguit wordt je laptop wat trager, omdat het meerdere taken tegelijkertijd uitvoert. Ik heb je trouwens een e-mail gestuurd. Heb je die al gezien?

André zet zijn laptop aan en ziet een e-mail met het onderwerp: 'Het tofste spel op dit moment'.

Hij klikt op de bijlage, maar dan ziet hij een scherm met een foutmelding.

'Volgens mij heb je iets verkeerds gestuurd, want ik kan het niet openen.'

‘Nee hoor, het is precies zo gegaan zoals ik dat wilde,’ glimlacht Rickey. ‘Je hebt de bijlage geopend en nu zit ik in je laptop en kan ik overal bij. ‘Hé, ik zie hier een foto van Sanne. Waarom bewaar je een foto van mijn zus?’

André schrikt zich rot. ‘Kun je nu echt alles op mijn laptop zien?’

‘Ja, ik kan alle mappen openen, al je foto’s bekijken, al je e-mails en je privé berichten op social media lezen, alles eigenlijk.’

Hij ziet André bijna opspringen.

‘Rustig aan, ik ga dat natuurlijk niet doen, ik zeg alleen maar dat het kan, want ik heb nu een volledige toegang tot je computer.’

‘En dit komt omdat ik de bijlage opende?’ vraagt André onzeker, ook al kan hij het antwoord raden.

‘Ja, dat is vrijwel altijd voldoende. Soms stuur ik een link en via de link kom je op een site waar een virus op je zit te wachten. Dat kan dus ook. Ik ga je zo uitleggen hoe je de kwaadaardige links en bijlagen kunt herkennen, maar eerst wil ik je iets op mijn laptop laten zien. Ik heb je namelijk de hele tijd gefilmd met de camera van je eigen laptop.’

André kijkt hem verbaasd aan. ‘Laat zien,’ zegt hij, omdat hij nog steeds niet kan geloven dat hij stiekem gefilmd is.

Rickey draait zijn laptop naar hem toe en laat hem het filmpje zien. André hoort zichzelf praten en ziet hoe geschrokken hij kijkt. Dat was toen Rickey vertelde dat hij een foto van Sanne op zijn laptop had gevonden.

Als André bijna twee uur later naar huis gaat, weet hij precies wat hij in zijn e-book gaat opschrijven om de andere kinderen te waarschuwen. En hij heeft ook een idee voor een nieuwe vlog.

5. DE AANVAL

‘Hallo iedereen. Dit is mijn tweede vlog. Ik was laatst op bezoek bij een ethische hacker en hij heeft mijn volledige laptop overgenomen. Hij heeft me zelfs gefilmd, terwijl ik dat niet doorhad. Dat was best een schokkende ervaring. Ik ga je nu vertellen hoe dat werkt. En ook hoe je kunt voorkomen dat je stiekem gefilmd wordt.’

Even later klikt André op ‘stop’. Hij heeft het idee dat hij het goed verteld heeft. Deze keer was hij een stuk minder zenuwachtig, alleen een beetje gespannen. Hij vindt vloggen nog steeds niet leuk, maar het is voor het goede doel. Als het straks klaar is, moeten zo veel mogelijk mensen het e-book weten te vinden en downloaden.

Dezelfde dag stromen de reacties binnen. Allemaal positief. Alleen Joeri laat zich weer kennen: ‘Hé, watje, ben je tegen je wil gefilmd? Waarom ga je niet bij je mama klagen, maar doe je dat online? Best zielig dat je geen vrienden hebt.’

‘Alsof jij zo veel vrienden hebt,’ sist André en klapt de laptop dicht. Er zijn altijd een paar jongens die met Joeri meedoen, maar volgens hem doen ze dat alleen maar

omdat ze zelf niet gepest willen worden. Meelopen loont blijkbaar. André is niet van plan om daar aan mee te doen. Dan maar ruzie. Voor die flapuit Joeri is hij niet zo bang, wel voor die onbekende die vorige keer reageerde. De reactie van DarkHacker13 laat niet lang op zich wachten: 'Ik heb je gewaarschuwd, maar je gaat blijkbaar door. Niet handig. Ik had je slimmer ingeschat. Wie niet horen wil, moet maar voelen.'

André voelt hoe zijn hart sneller gaat kloppen. Hij krijgt kippenvel. Dat klinkt als een serieus dreigement, maar wat is die gast precies van plan?

Dat ziet hij gauw genoeg, want nog dezelfde dag wordt hij bekogeld met phishingmails. 'Drie maanden gratis Netflix', 'win een waardebon van 100 euro voor Steam', 'update je Instagram-account in verband met nieuwe privacy voorwaarden'… De mails blijven binnenstromen. De hacker hoopt blijkbaar dat André op een moment van onoplettendheid ergens op klikt, maar André is al voldoende gewaarschuwd door Rickey en hij kijkt wel uit. Hij klikt elke keer op de afzender om te kijken of die klopt. Soms staat er gewoon steam@DH.com. DH staat vast voor Dark Hacker, hij doet het expres om hem te kunnen laten zien dat hij achter hem aan zit, om hem angst aan te jagen. Maar sommige phishingmails lijken te komen van een goede afzender, zoals 'Let op: aangepast lesrooster

deze week'. De hacker gebruikt gewoon het e-mailadres van de school. Rickey heeft hem uitgelegd dat mailadressen makkelijk na te maken zijn. Dan moet je op de link of op de bijlage letten. André zweeft met zijn muis boven de link en ziet dat het niet naar de schoolsite gaat, maar naar de website Aangepast-Rooster.nl. Klinkt best goed, maar het is niet logisch dat zijn school speciaal voor het aangepaste lesrooster een nieuwe website registreert. Dat heeft DarkHacker13 vast gedaan in de hoop dat hij op zijn site komt om zijn laptop met een virus te besmetten.

André verhuist het bericht naar de spam-map, opgelucht dat hij niet meer zo makkelijk te hacken is. Of is dat alleen maar schijn? Rickey had hem al gewaarschuwd: 'Als je mijn tips uitvoert, ben je voor de meeste hackers niet meer interessant. Maar bij een heel gerichte hack geef ik geen garanties. Weet je waarom de hackers zo succesvol zijn? Omdat je slechts een klein foutje hoeft te maken.'

'Hoi,' zegt Sanne als ze hem op school ziet. 'Gaat het goed?'

'Ja,' antwoordt André, niet helemaal overtuigend.

'Ik hoorde van mijn broer dat je nogal last had van een of ander duister type.'

'Ach, tot nu toe kan ik hem wel aan. Ik weet alleen niet wat zijn volgende stap wordt.'

‘Wees voorzichtig. Mijn broer heeft het een en ander over hem uitgezocht. Dat is geen lieverdje.’

‘Daar gokte ik al op, want zijn berichten zijn tot nu toe niet bepaald lief.’

‘Als je ergens over twijfelt, bel alsjeblieft Rickey. Hij gaat je zeker helpen.’

‘Ik weet het, maar voorlopig wil ik hem niet storen. Je broer heeft het druk genoeg en ik red me wel.’

‘Oké, maar neem geen risico’s. Er gebeuren gekke dingen online.’

‘Ik weet het, bedankt voor je bezorgdheid.’

Sanne draait zich om en loopt naar hun klas. André kijkt haar na. Wat is ze mooi in haar strakke jeans, en haar haarlokken lijken te dansen op haar rug. Opeens draait Sanne zich om: ‘Ik wil nog iets zeggen: dat project van je… ik vind het echt heel tof.’

‘Dank je,’ mompelt André. Hij weet niet meer zo goed welke kant hij op moet kijken.

Als André thuis is, gaat hij meteen werken aan het e-book. Zijn handen vliegen over de toetsen. Het idee in zijn hoofd wordt steeds duidelijker en tot zijn verbazing ook steeds groter. Misschien moet hij niet alleen een boek schrijven, maar ook een heel platform bouwen, met anti-hack games, met toffe video’s van ethische hackers en slimme

vragen. HackShield, dat lijkt hem een toepasselijke naam.

Hij ziet een nieuwe e-mail binnenkomen. Van Joeri. Huh, sinds wanneer stuurt die pestkop hem ook e-mails? Meestal leeft hij zich in de WhatsApp groep van hun klas uit. Het onderwerp is: nieuwe naaktfoto's van Sanne, klik op de bijlage.

Niet alweer, denkt André. Houdt het niet een keer op!

Als hij op het zip-bestand klikt, ziet hij een foto van een eend. Typisch iets voor Joeri om te denken dat dit grappig is. Ik ga hier echt niet op reageren, besluit André. Pesters kicken op aandacht, maakt niet uit of dat positief is of negatief.

Hij gaat verder met het schrijven van het boek, maar zijn concentratie is weg. Toch maar even in de WhatsApp-groep kijken, Joeri heeft waarschijnlijk meerdere mensen beetgenomen met die eend.

Hij leest van alles, maar daar ziet hij niets over. Vreemd.

Als hij een uurtje later weer wil kijken, ziet hij dat de beheerder hem uit de WhatsApp groep heeft gegooid. Huh? Hij heeft niet eens iets gezegd, laat staan iets kwetsends. Als ze zo streng zijn, dan hadden ze Joeri met zijn grote bek allang uit de groep moeten gooien.

Wat een vreemde dag, denkt André. Eerst de waarschuwingen van Sanne, dan die vreemde e-mail van Joeri en vervolgens wordt hij ook nog uit de WhatsApp-groep

gegooid, terwijl hij niets gedaan heeft. Een dag om snel te vergeten.

6. BETRAPT

Het schoolplein loopt weer vol. André is een beetje laat, tot diep in de nacht kon hij niet de slaap vatten en hij werd er helemaal gek van. Het ergste vond hij dat hij niet precies wist wat hem dwarszat.

Als hij het schoolplein op loopt, ziet hij dat veel leerlingen hem op een vreemde manier aankijken.

Wat nou weer? denkt hij. Ben ik misschien in de haast vergeten mijn haar te kammen? Iets anders kan hij niet bedenken. Zijn shirt en spijkerbroek zijn oké, waarom kijkt iedereen hem zo vreemd aan?

Hij signaleert Sanne en glimlacht naar haar. Normaal gesproken glimlacht ze altijd terug en dat maakt hem altijd blij. Maar deze keer niet: Sanne kijkt hem minachtend aan, met een frons tussen haar mooie wenkbrauwen. André heeft het voorgevoel dat er iets grondig mis is, maar wat? Hij heeft toch helemaal niets gedaan? Anders had hij het zelf geweten.

Als hij de klas in loopt, komt Joeri naar hem toe: 'Jij durft, sukkel'.

André kijkt hem met grote ogen aan. 'Wat durf ik? Jij stuurt me een foto met een eend, omdat je zo dom als

een eend bent en vervolgens ben ik de sukkel.'

'Ben je helemaal geflipt!' schreeuwt Joeri. 'Ik heb je helemaal geen foto met een eend gestuurd. Jij hebt ons allemaal rare berichten gestuurd.'

'Jij bent geflipt, niet ik. De foto kwam van jouw mailadres, zogenaamd nieuwe naaktfoto's van Sanne. Of ben je dat nu al vergeten?'

'Waarom zou ik nieuwe foto's van Sanne naar jou sturen?'

'Dat heb je ook niet gedaan; toen ik het bestand opende was dat een foto van een eend.'

'En die eend zit nu blijkbaar in je hoofd. Ten eerste heb ik je helemaal geen e-mail gestuurd en ten tweede heb je jezelf laten ontmaskeren als leugenaar. Ik weet niet wat voor bewijs je hebt dat ik je een eend heb gestuurd, maar kijk eens wat je ons hebt gestuurd.' Joeri opent WhatsApp op zijn mobiel en laat André de berichten lezen.

Dat kan niet waar zijn! Allemaal vreemde berichten verstuurd van zijn account! En de teksten zijn zo erg dat hij zich goed kan voorstellen dat iedereen hem opeens mijdt.

André staart naar zijn foto en leest wat hij verstuurd heeft: 'He, debielen, dachten jullie nu echt dat ik jullie wijs ga maken hoe je jezelf tegen hackers kunt beschermen? Dat was ik geen moment van plan. Maar ik wilde

kijken hoe lang ik een spelletje met jullie kan spelen.'

En nog een berichtje namens hem: 'Bedankt voor de toffe reacties op mijn vlogs, stelletje naïevelingen. The game is over. En ik heb nog een persoonlijke boodschap voor Sanne: ik dacht wat lol met jou te beleven, maar je bent een saaie muts.'

André kan wel door de grond zakken. Hoe moet hij iedereen wijs maken dat hij die vreselijke berichten niet gestuurd heeft? Zal iemand hem geloven? En Sanne dan, gaat ze hem nu haten? Hij weet nu zeker dat hij gehackt is, maar hoe? En waarom heeft hij daar niets van gemerkt?

Hij pakt zijn mobiel en verandert meteen zijn belangrijkste wachtwoorden. Na school fietst hij zo snel als hij kan naar huis en haalt zijn laptop op. Daarna fietst hij door naar Rickey. Als Sanne maar niet opendoet. Elke keer als hij haar ziet, wordt hij verlegen, maar nu heeft hij ook nog een goede reden om door de grond te zakken.

Met kloppend hart belt André aan. Het eerste wat hij ziet, zijn lange blonde lokken. Een seconde later kijkt hij in het verbaasde gezicht van Sanne.

'Wat kom je hier doen?' zegt ze op een hatelijke toon. 'Je denkt toch niet dat na alles wat gebeurd is, je nog steeds welkom bent in dit huis? Ik heb het Rickey al

verteld en hij is heel teleurgesteld in jou. Ik ook trouwens. Ik had nooit gedacht dat je tot zoiets in staat bent!' Met een klap smijt Sanne de deur dicht.

André heeft geen tijd om na te denken wat hij het beste kan doen. In een flits van een seconde drukt hij op de bel.

Een paar tellen later doet Sanne opnieuw open. 'Wat ben je van plan, de hele dag hier hangen en op de bel drukken? Volgens mij heb ik duidelijk gezegd dat je niet meer welkom bent. Je weet zelf wel waarom.'

'Ik weet waarom, maar het is niet waar. Ik heb al die nare berichten niet gestuurd. Dat heeft iemand anders gedaan. Iemand heeft mijn account gehackt, ik weet niet hoe. Daarom wil ik met je broer spreken, misschien kan hij achterhalen hoe dat precies gebeurd is.'

Sanne kijkt hem achterdochtig aan: 'Is dat waar of is dat weer een verhaal dat je verzint?'

'Geloof me, het is waar. Kom anders kijken wat je broer zegt, dan weet je zeker dat ik niet lieg.' André kijkt haar met smekende ogen aan. Hij weet niet wat hij moet doen als hij gehackt is. Hij kent alleen maar Rickey die daar veel verstand van heeft.

Sanne doet de deur langzaam open. 'Oké, loop door naar de kamer van Rickey. Maar als je liegt, is dat de laatste keer dat je hier een stap naar binnen zet.' Ze loopt met hem mee. André voelt dat ze hem niet meer

vertrouwt. Dat doet pijn. Haar afwijzing vindt hij nog het ergste van alles.

Als Sanne de deur van de kamer opent, kijkt Rickey hem verbaasd aan.

'Jij hier?'

André haalt diep adem. Hij moet deze gênante situatie nog een keer uitleggen.

Gek genoeg lijkt Rickey hem meteen te geloven. 'Geef me even je laptop om te zien hoe dat gebeurd is,' zegt hij. Hij strekt zijn hand uit.

André overhandigt hem onmiddellijk zijn laptop, blij dat hij niet eerst allerlei moeilijke vragen moet beantwoorden.

'Wat is het wachtwoord van je laptop?'.

André twijfelt wat hij moet zeggen. Sanne is nog steeds in de kamer en zijn wachtwoord is Sanne12.

Rickey lijkt zijn geduld te verliezen: 'Wat, weet je je wachtwoord niet?'

'Jawel,' mompelt André. 'Mag ik het zelf intypen?'

'Huh, vertrouw je me niet?' vraagt Rickey. 'Ik mag je hele laptop ondersteboven keren op zoek naar een virus, maar ik mag je wachtwoord niet weten? Volgens mij ben je een beetje vergeten wat voor werk ik doe. Als je wachtwoord niet zo lang is, dan run ik een programma waarmee

ik het binnen enkele seconden kan kraken. Alleen als je een heel lang wachtwoord hebt, wordt het lastig, maar de meeste mensen houden niet van lange wachtwoorden.'

'Sanne12,' mompelt André.

'Wat bedoel je met Sanne12?'

'Dat is mijn wachtwoord.'

André hoopt dat Sanne het niet gehoord heeft, maar hij vreest het ergste, want ze staat redelijk in de buurt.

Opeens hoort hij haar stem: 'Wat, ben ik je wachtwoord? Hoezo?'

Zijn hersenen werken op volle toeren. *Verzin iets, verzin een leugen, je kunt onmogelijk zeggen dat je verliefd op haar bent en dat je daarom haar naam als wachtwoord gebruikt.*

'Uuh, mijn vorige vriendinnetje heette Sanne, we hebben elkaar op de camping ontmoet. We zien elkaar niet meer, maar ik heb mijn wachtwoord niet meer veranderd.'

'Interessante uitleg,' zegt Rickey. 'Ik moet er niet aan denken om elke dag de naam van mijn ex als wachtwoord in te typen.' Zijn stem klinkt alsof hij hem totaal niet gelooft.

'Ik ga weer,' zegt Sanne. 'Ik moet naar hockey. Ik hoor wel hoe het afgelopen is.'

Voordat ze de deur sluit, werpt ze André een verwijtende blik. Een teken dat ze zijn versie van het verhaal nog

niet gelooft.

‘Sanne dus,’ zegt Rickey nadat zijn zus weg is. ‘Ik heb het idee dat ik die ken.’

André wordt zo rood als een tomaat, maar besluit open kaart te spelen. ‘Je kent haar inderdaad, maar laat dat alsjeblieft tussen ons blijven. Iedereen denkt dat ik knettergek ben geworden om zulke berichten te sturen en je zus vertrouwt me ook voor geen meter meer. Maar ik zag die berichten vandaag pas op school. Ik heb een vermoeden wie ze geschreven heeft, maar niet hoe hij mijn computer heeft overgenomen.’

‘Nog vreemde mailtjes ontvangen?’

‘Meer dan genoeg. DarkHacker13 bombardeert me met phishingmails. Maar daar heb ik niet op geklikt.’

‘Heb je anders op een vreemd mailtje van een bekende geklikt?’

André denkt na. ‘Ja, Joeri stuurde me een domme mail, een soort grap.’

Rickey gaat naar de prullenbak en bekijkt de verwijderde e-mail van Joeri. ‘Hm, een zip-bestand, daar kun je heel gemakkelijk een virus in stoppen. Ik ga het even door een aantal virusscanners halen, kijken wat erin zit.’

Hij googelt op VirusTotal. ‘Als je een bestandje niet vertrouwt, kun je dat zelf met dit online programma

gratis checken. Dan kijken meer dan zestig antivirusprogramma's tegelijkertijd of ze iets verdachts vinden,' zegt Rickey, terwijl hij dat doet.

Even later verschijnt er een waarschuwing op zijn scherm.

'Bingo, twintig van die programma's merken dit als foute boel aan.'

'Waarom reageerde mijn antivirusprogramma niet en herkent de rest het ook niet?' vraagt André.

'Omdat ze dat gisteren nog niet herkenden. Er verschijnen elke dag duizenden nieuwe virussen, dat is bijna niet bij te houden. De nieuwste worden soms een paar uur later, soms een dag later en soms pas nog veel later herkend. De hackers zijn dus meteen binnen en hebben meestal volledige toegang tot iemands laptop. Ze schakelen dan het antivirusprogramma uit, zodat het de verdachte bestanden even later niet kan opruimen. Ik ga kijken waarom je antivirusprogramma nog steeds niet reageert.'

Een paar seconden later weet Rickey het al: 'Zoals ik al dacht: de hacker heeft je antivirusprogramma uitgeschakeld om onopgemerkt in je laptop te blijven. Hoe wist je dat je gehackt was?'

'Omdat ik al die berichten niet heb verstuurd. En omdat Joeri beweerde dat hij me geen mail heeft gestuurd.'

‘Aha, dan heeft de hacker eerst zijn computer gehackt om jou een berichtje met een virus te sturen. Slimme aanpak, werkt bij de meeste mensen. Iedereen klikt tenslotte op berichtjes van vrienden en kennissen. Eigenlijk mag je online niemand vertrouwen, niet eens je beste vrienden. Je weet simpelweg niet of ze gehackt zijn of niet. Dus als je een vreemd mailtje van een bekende ontvangt, voortaan niet zomaar erop klikken. Stuur eerst een WhatsApp om te vragen of hij je echt iets gestuurd heeft.’

‘Jeetje, wat een achterdochtig gedoe.’

‘Ja, maar beter achterdochtig dan zomaar op een zipbestand klikken. Je ziet zelf de gevolgen.’

‘Dus als Sanne je een e-mail stuurt, lees je die niet?’

‘Jawel, maar als ik de tekst verdacht vind, dan ga ik niet op de bijlage klikken. Ik scan het even met VirusTotal of ik stuur haar een berichtje. Ik weet niet hoe goed mijn zus met haar wachtwoorden omgaat en of ze niet op een verdacht linkje geklikt heeft.’

‘En wat doen we nu?’

‘We gaan de groetjes doen aan DarkHacker13, daarna het virus verwijderen en al je wachtwoorden resetten.’

‘De groetjes doen?’

‘Ja, het is wel leuk om hem te laten zien dat hij snel ontdekt is. Wat wordt je boodschap?’

André denkt even na. Dan zegt hij: ‘De boodschap

wordt: Je kunt me niet meer stoppen, HackShield gaat door.’

7. POLITIE

André draait zich voor de zoveelste keer in zijn bed om. Zijn laptop is niet meer gehackt, maar hoe gaat hij zijn reputatie herstellen? De gedachte alleen al dat zijn klasgenoten inmiddels de pest aan hem hebben, laat hem niet los.

Rickey heeft hem weer een paar wijze lessen gegeven hoe hij een volgende hack-poging kan voorkomen.

'Weet je waarom je waarschijnlijk gemakkelijk te hacken was?' vroeg hij.

André had geen idee.

'Gewoon omdat je een aantal updates niet hebt gedaan. Veel mensen klikken ze weg of stellen ze uit, maar al die niet geinstalleerde updates zijn open ramen en deuren voor de digitale inbrekers. Doe ze dicht en dan wordt het een stuk moeilijker om binnen te komen.'

'Geldt dat ook voor mijn mobiel?'

Rickey grijnsde: 'Natuurlijk, steeds meer hackers richten zich op mobieltjes, omdat daar tegenwoordig net zo veel te halen valt als in laptops. En doe me een lol: sla nooit je wachtwoorden op in een tekstbestandje, want ik zag dat je dat doet. Als een hacker binnenkomt omdat je op een fout linkje klikt of een besmette website bezoekt, dan

heeft hij meteen toegang tot je wachtwoorden. Sommige mensen maken er ook nog mooie documenten van en noemen ze “Mijn wachtwoorden”. Lekker handig.’

Natuurlijk had André geprotesteerd dat hij niet zo veel verschillende lange wachtwoorden kon onthouden, maar Rickey keek hem alleen maar streng aan. ‘Er zijn genoeg manieren waarop dat kan en als je geen zin hebt om al die wachtwoorden te onthouden, dan kun je daar een gratis programma voor gebruiken.’

‘En dat moet dan wel veilig zijn?’ merkte André op.

Rickey haalde zijn schouders op: ‘Niets is onhackbaar, maar deze programma’s versleutelen je wachtwoorden en bij een hack zijn die onleesbaar. Het is in elk geval honderd keer veiliger en makkelijker dan hoe de meeste mensen op dit moment met wachtwoorden omgaan.’

André installeerde meteen zo’n programma. Het werkte verbazingwekkend simpel. ‘Iets voor mijn nieuwe vlog,’ dacht hij. Maar toen kromp zijn hart ineen: zo’n nieuwe vlog gaat niemand serieus nemen na alles wat er gebeurd was. Waarschijnlijk zou hij door iedereen in de commentaren uitgescholden worden. Als hij eerst ging vertellen dat hij gehackt was, dan zouden ze waarschijnlijk denken dat hij een smoes verzon of een nieuwe leugen.

In zijn bed blijft André draaien. Hoe lost hij dat allemaal op? Hij moet het oplossen, anders gaat niemand

HackShield gebruiken als het klaar is.

Onuitgeslapen en voor het eerst met grote tegenzin gaat André naar school. Hij ziet alweer hoe klasgenoten hem de rug toekeren. Vermoedelijk roddelen ze ook over hem, want hij ziet een aantal naar hem wijzen. Dat doet hem denken aan Sanne, hoe lang zij gepest werd toen haar naaktfoto rondgestuurd werd. Dat lijkt nu af te nemen, ze hebben een volgende zondebok gevonden.

Twee politieagenten staan op het schoolplein. Huh, wat doet de politie hier? denkt André. Ze lopen zijn kant op. Hij begint een steeds onbehaaglijker gevoel te krijgen. Ze zullen hem toch niet arresteren? En voor wat dan? Hij kan niets bedenken.

Veel meer tijd om na te denken, is er niet. De agenten stoppen naast hem. 'Je gaat met ons mee,' zeggen ze. Ze brengen hem naar een politieauto. Iedereen kijkt hen na. Ook dat nog, denkt André. Wat denken ze dat ik gedaan heb?

Op het politiebureau ziet hij tot zijn verbazing Sanne. Ze wordt net door een agente naar een verhoorkamer gebracht. 'Waarom houden jullie ons aan, we hebben niets gedaan!' roept André verontwaardigd. Hij probeert achter Sanne aan te lopen. Eén van de politieagenten

duwt hem de andere kant op. ‘We zullen wel zien of jullie niets gedaan hebben en wie dan wel met de cijfers in Magister geknoeid heeft.’

‘Heeft iemand Magister gehackt?’ vraagt André verbaasd.

‘Ja, en je bent toevallig met een werkstuk over hackers bezig en van je klas hoorde ik ook verhalen over een hackersplatform. Maar dat mag je straks uitleggen.’

‘Dit heeft er echt niets mee te maken!’ schreeuwt André verontwaardigd. ‘Dat platform is juist tegen hackers. Ik probeer iedereen te leren hoe je jezelf tegen hackers kunt beschermen.’

‘Maar je leert wel skills als je je in dit onderwerp verdiept, niet waar?’ zegt de agent op een spottende toon.

‘Denken jullie echt dat ik Magister heb gehackt? Waarom zou ik?’

‘Misschien om jezelf alleen maar tienen te geven? En de mensen aan wie je een hekel hebt, allemaal onvoldoendes. Aan Joeri bijvoorbeeld. Of zegt die naam je niets?’

André kijkt hem sprakeloos aan.

8. VERDACHTE

‘Ik heb er echt niets mee te maken,’ zegt André. ‘Als ik Magister zou hacken, dan moeten er toch sporen te vinden zijn op mijn laptop?’

‘We hebben jouw laptop al bij je ouders thuis opgehaald en nu zijn we die op sporen aan het onderzoeken. Maar als we geen sporen vinden, zegt dat nog niets. We zijn al best veel hackers tegengekomen die perfect wisten hoe ze hun sporen konden uitwissen.’

‘Oké, maar waarom ik? Alle leerlingen kunnen in principe verdachte zijn.’

‘Er waren maar twee leerlingen die opeens alleen tienen hadden, Sanne en jij. Heb je daar een verklaring voor?’

‘Hoe moet ik dat weten? Ik heb het in elk geval niet gedaan. Waarom zou ik mezelf alleen maar tienen geven? Ik ben niet achterlijk om te snappen dat dit heel verdacht is.’

‘Misschien heeft je vriendinnetje het gedaan? Haar broer werkt als ethische hacker, dus hij kan ook een handje geholpen hebben.’

‘Sanne is mijn vriendinnetje niet,’ zegt André. Hij voelt een steek in zijn hart, want hij wil niets liever. Maar na

alles wat gebeurd is, is Sanne juist mijlenver van hem verwijderd geraakt. Zou zij ook denken dat hij Magister gehackt heeft?

De politieagent onderbreekt zijn gedachten: ‘Ik luister wat je ons te vertellen hebt.’

‘De enige aan wie ik kan denken is DarkHacker13,’ zegt André. Daarna vertelt hij op welke manieren deze hacker zijn leven zuur maakte en waarom.

De politieagent luistert aandachtig, terwijl een andere agent aantekeningen maakt. ‘En je kunt ons verder niets over DarkHacker13 vertellen?’

‘Niet echt. Ik weet dat Rickey, de broer van Sanne, hem probeerde te traceren. Hij had toen niet veel tijd om verder te zoeken, maar hij zei dat DarkHacker13 zichzelf ook zo noemt op allerlei hackersforums. Kunnen jullie zo iemand opsporen, alleen op basis van een nickname?’

‘Ook ervaren hackers maken wel eens fouten en zijn te traceren, hoewel dat lastig is omdat ze software gebruiken die hun digitale sporen wist,’ zegt de agent. ‘Maar laten we niet vergeten wie hier de vragen stelt. Ik wil heel graag weten wat je zelf over de verschillende hackmethodes hebt geleerd.’

‘Bijna niets,’ reageert André. ‘Ik verzamel kennis hoe jongeren zich tegen kwaadwillende hackers kunnen beschermen en niet hoe ze zelf zouden kunnen hacken.’

‘Dat klinkt heel goed,’ zegt de politieagent die aantekeningen maakt. ‘Ik hoop voor je dat je hier niets mee te maken hebt en dat je je plan doorzet. Er komen hier elke dag slachtoffers van cybercrime binnen. We willen graag iedereen helpen en alle boeven oppakken, maar dat kunnen we niet.’

‘Waarom niet?’

‘Omdat we daar niet genoeg mensen voor hebben. Het aantal slachtoffers is gewoon te groot geworden. En soms weten we dat het heel lastig wordt om de hackers te pakken, vooral als ze in een ander land zitten.’

‘DarkHacker13 stuurt zijn berichten in het Nederlands.’

‘Daar gaan we naar kijken. We gaan je nu terug naar school brengen.’

9. EEN MAAND LATER

‘Yes! Gelukt!’ André klapt zijn laptop dicht en kijkt tevreden. Het boek met tips tegen hackers is af. En ook het HackShield-platform is klaar om te lanceren. André heeft met behulp van Rickey en een paar van zijn vrienden een heel gaaf spel gemaakt waarin de spelers een kwaadaardige hacker moeten opsporen.

Zijn blije gevoel verandert langzamerhand in angst als hij nadenkt over de lancering. Zullen ze hem wel geloven dat hij ze niet in de maling neemt, maar dat hij heel veel vrije tijd heeft besteed aan dit project? Eigenlijk al zijn vrije tijd. Hij heeft de afgelopen tijd niet eens een uurtje gegamed, terwijl hij daarvoor redelijk verslaafd was.

Hij belt Rickey op: ‘Ik ben klaar, maar ik durf het niet.’

Aan de andere kant van de lijn klinkt een kuch: ‘Wat heb je te verliezen? Op school kijken ze je nog steeds met de nek aan en dat gaat niet veranderen als je niets doet.’

‘Ja, maar het begint nu juist rustiger te worden, ze wijzen me niet allemaal aan. Als ik het nu lanceer, dan begint het waarschijnlijk weer opnieuw en krijg ik alleen maar haat-berichten. Wat moet ik doen, Rickey? Ik wil geen afgang.’

‘Het wordt ook geen afgang, want HackShield is heel tof geworden. Ze zien vanzelf dat het een spannend spel is en dat je ze niet in de maling neemt. En de tips uit je boek gaan ze zeker gebruiken. Maar goed, slaap er nog een nachtje over. De ochtend is wijzer dan de avond, zeggen ze.’

‘Ja, zeggen ze,’ mompelt André. Hij heeft niet het gevoel dat hij de volgende dag zo veel beter zal weten wat te doen.

Tijdens het ontbijt checkt André de berichten op zijn mobiel. Plots gaat de telefoon.

‘Met rechercheur Nick Ooms. Spreek ik met André?’

‘Ja, dat ben ik,’ zegt André en zijn hart gaat sneller kloppen. ‘Er is toch niet weer wat gebeurd, hè?’

‘Nee, gelukkig niet. Ik bel alleen maar om te zeggen dat we dankzij jouw aanwijzingen op het juiste spoor terechtkwamen. DarkHacker13 is vannacht opgepakt en hij heeft het hacken van Magister bekend en ook het hacken van jouw laptop. Hij kon ook moeilijk ontkennen, want we hebben al zijn apparatuur in beslag genomen en daar stond meer dan genoeg bewijs op.’

‘Wat goed!’ roept André. Hij voelt zijn hartslag tot rust komen. Eindelijk goed nieuws, eindelijk gerechtigheid.

‘Er is nog iets wat ik je wil vertellen,’ zegt de agent.

‘Dankzij jouw tip hebben we een zeer zware cybercrimineel te pakken. DarkHacker13 was één van zijn nicknames, maar hij gebruikte meerdere namen op het internet. Hij heeft grote banken aangevallen met zijn botnet van duizenden besmette computers. En hij heeft recentelijk een bekende webshop afgeperst. We vinden het eigenlijk heel tof dat een jongen zoals jij het tegen zo’n hacker durft op te nemen. Als veel burgers de politie tips geven, kunnen we veel meer criminelen oppakken. Wil je misschien samen met ons de persconferentie geven en vertellen waarom je dat gedaan hebt? Dan kan je meteen je platform aankondigen om de jongeren te leren vechten tegen hackers.’

Wauw, André weet niet wat hij moet zeggen. Zo’n persconferentie klinkt als een prachtige kans om HackShield bekend te maken, maar durft hij dat aan? Een persconferentie betekent dat hij straks in de krant staat en misschien zelfs op tv komt. Hoe zullen zijn klasgenoten reageren? Wat als heel veel mensen via social media zich er mee gaan bemoeien als iemand iets negatiefs over hem zegt?

‘Als je tijd nodig hebt om na te denken, dan is dat prima,’ zegt de agent aan de andere kant van de lijn. ‘Ik begrijp wel dat ik je hiermee overval.’

Nou, in elk geval niet zo erg als op het schoolplein toen jullie een vermoeden hadden dat ik misschien de hacker was, denkt André. Maar uiteraard zegt hij dat niet. Zijn hersenen draaien op volle toeren. Zo'n persconferentie is echt een mooie kans om zijn kant van het verhaal te vertellen. De politie kan tenslotte bevestigen dat hij gehackt was en dat de hacker ook de cijfers in Magister heeft veranderd.

'Oké, ik doe het,' zegt André.

10. HACKSHIELD

De volgende dag is de persconferentie groot nieuws. ‘Jongen neemt het op tegen gevaarlijke cybercrimineel,’ kopt de Volkskrant. ‘Politie pakt cybercrimineel dankzij tip 14-jarige gehackte jongen,’ schrijft NRC Handelsblad. En op het Journaal laten ze beelden zien van het HackShield platform dat André samen met Rickey en zijn vrienden gemaakt heeft.
‘Tof platform voor jongeren tegen hackers,’ bericht RTL.

Sanne zit met open mond te kijken naar de tv, vooral als ze haar naam hoort vallen. André vertelt vol enthousiasme dat Sanne hem geïnspireerd heeft om dat te doen en dat zij ook een groot gedeelte van het succes is, omdat ze hem in contact bracht met haar broer die hem heel veel leerde.

‘Wat heb je vooral geleerd toen je gehackt werd?’ vraagt de presentator.

Sanne ziet dat André niet zo lang naar woorden hoeft te zoeken. Zo kent ze hem helemaal niet, meestal is hij heel verlegen, maar op tv heeft hij een goed antwoord op elke vraag.

‘Ik heb vooral geleerd dat de meeste mensen per toeval gehackt worden, simpelweg omdat ze het de hackers niet moeilijk maken. Eigenlijk is het niet zo moeilijk om jezelf beter te beschermen, maar we weten vaak niet hoe, omdat we dat niet op school leren.’

‘En je ouders dan? Vertellen die daar niets over?’

‘Mijn ouders weten het zelf niet,’ lacht André. ‘Ik moest ze laatst uitleggen hoe ze sterke wachtwoorden kunnen verzinnen en onthouden, en waarom een wachtwoord zoals Winter18 binnen enkele seconden gehackt is.’

‘Je hebt inmiddels veel geleerd. Als je de kijker drie tips mag geven om zich digitaal beter te beschermen, welke drie tips kies je dan?’

‘Dan kies ik voor de drie digitale deuren die de meeste mensen open laten staan, waardoor de cyberdieven binnenkomen. De eerste deur zit goed dicht, maar elke keer kloppen phishingmails erop om binnen te komen. Kijk eerst goed door het spionnetje voordat je open doet. Check de afzender en de link of de bijlage voordat je iets openklikt.

De tweede deur is simpel dicht te doen: negeer geen updates van programma’s, want die beschermen je automatisch tegen hackers.

En de derde deur laten veel mensen open: ze gebruiken hetzelfde wachtwoord voor meerdere websites. Als

een hacker ergens binnenkomt, kan hij al hun accounts overnemen. Verzin dus voor alles een lang wachtwoord en maak ze allemaal verschillend. Hoe je dat doet, kun je op HackShield vinden.'

Jeetje, wat vertelt hij dat vloeiend en overtuigend, denkt Sanne. Ze vindt het knap dat André niet van al die camera's en het publiek schrikt.

Het platform is meteen een groot succes. De jongeren spelen massaal de game en proberen DarkHacker13 in de gevangenis te krijgen. Dat hadden ze op het laatste moment als hoogste level aan het spel toegevoegd. André verzon een sterk wachtwoord met een geheime boodschap: #IkhouvanSanne13! Dat moeten de spelers zien te raden.

Hij is benieuwd of het Sanne lukt om het wachtwoord te ontcijferen.

Dezelfde avond krijgt hij een Whatsapp-berichtje. 'Mooi wachtwoord!' Ik heb net je gratis e-book met de tips gedownload en gelijk zelf een heel sterk wachtwoord gemaakt. Meer dan twintig karakters, dus absoluut onhackbaar. Je bent de enige die het mag weten als je het voor jezelf houdt. **#Wil_je_met_me_daten13?**'

André glimlacht. 'Heb je in het e-book ook gelezen dat een verificatiecode je wachtwoord nog sterker maakt? De

code is **YES**.’

Wil je de game spelen gebaseerd op dit boek? Ga dan naar
www.joinhackshield.nl
en probeer te winnen van
DARKHACKER13.


Of wil je eerst lezen
wat voor e-book
André heeft gemaakt
met behulp van
Rickey?

What the h@ck!

Tip vooraf: mocht je vinden dat je ouders dit boek harder nodig hebben dan jij, geef het dan eerst aan je ouders om te lezen.

Vorig jaar waren zo'n drie miljoen Nederlanders slachtoffer van cybercrime. Dat is de snelst groeiende vorm van criminaliteit.

Ben je zelf interessant genoeg voor hackers?
A. Ja B. Nee C. Misschien

Het antwoord is ja. Maar hoe interessant hangt van je eigen beveiliging af. Vergelijk de hackers met de gewone inbrekers. Ze lopen langs de huizen en kijken waar ze gemakkelijk naar binnen kunnen komen.

Wat doe je tegen de gewone inbrekers als je weggaat?
A. Deur op slot? B. Ramen dicht? C. Licht aan? D. Een waakhond?

Natuurlijk kun je het licht aan laten, maar dat is energie-

verspilling.

Sommige mensen nemen een waakhond. Een poedel bijvoorbeeld. Die geven de inbrekerswat hondenkoekjes en dan zijn ze van die waakhond af.

De meeste mensen doen de deur op slot en de ramen dicht, en dat is meestal voldoende. De inbreker kijkt dan liever even verder, op zoek naar mensen die dat niet gedaan hebben. De hackers werken op dezelfde manier. Weet je welke digitale ramen en deuren je open hebt gelaten?

Waarom zijn computers en mobieltjes gemakkelijk te hacken?

Dat komt door fouten van de programmeurs die de software maken. Daar maken de hackers gebruik van. Een antivirusprogramma onderschept ongeveer 100.000 mogelijke besmettingen per uur, maar dat is niet voldoende. Soms zijn de hackers sneller. Iedere 3,75 seconden verschijnt er nieuwe kwaadaardige software.

> Op sommige websites zie je tegenwoordig pop-ups die je waarschuwen dat je een virus op je computer hebt. Of ze beloven je om je computer sneller te maken. Als je klikt, wordt je laptop soms gehackt. Dat geldt ook voor je mobiele telefoon. Beveiliger G DATA registreert bijna negenduizend nieuwe bedreigingen voor Android telefoons per dag.

Cybercriminelen maken graag gebruik van foto's en filmpjes van beroemdheden om computers en mobiele telefoons over te nemen. Als je op zoek bent naar informatie over een bekend iemand, kun je zomaar op de verkeerde link klikken en dan is het gebeurd. Kim

Kardashian, Doutzen Kroes en Adéle verspreiden dus ongewild virussen. Lil' Kleine, Max Verstappen en Armin van Buuren ook.
Om te voorkomen dat je computer of mobiele telefoon op deze manier overgenomen wordt, moet je altijd de updates uitvoeren en een goed antivirus programma hebben.

Maak geregeld een backup. Zo raak je niet alles kwijt als je gehackt wordt. Het beste is om een backup op een externe harde schrijf te maken, die niet gekoppeld is aan je computer.

> In Nederland worden elke dag gemiddeld 118 per mobiele telefoons gestolen. Slechts één op de vijf jongeren heeft zijn smartphone goed beschermd. Hoe je je telefoon onbruikbaar maakt voor dieven, kun je lezen op de site:
> **www.maakhetzeniettemakkelijk.nl**

Heb je je mobiele nummer ingevuld op een foute site? Meld je dan meteen af voor ongewenste (sms) betaaldiensten via **Payinfo.nl**.

Trap je in een nep-mail?

Phishingmails hebben soms grote gevolgen. Een Britse crimineel ontsnapte uit de gevangenis door het personeel een phishingmail te sturen dat hij moest worden vrijgelaten. De 28-jarige Brit gebruikte een naar binnen gesmokkelde smartphone om de e-mail op te stellen. Daarin deed hij zich voor als een griffier van de rechtbank en gaf het personeel van de gevangenis instructies voor zijn vrijlating. De fraudeur bleek een website te hebben geregistreerd die erg op die van de rechtbank leek. Vervolgens verstuurde hij de e-mail vanaf deze website en

werd vrijgelaten.

Ook voetbalclubs trappen in phishingmails. Het Italiaanse Lazio Roma betaalde 8,5 miljoen euro aan Feyenoord voor de voetballer Stefan de Vrij. Nadat Feyenoord bij Lazio klaagde dat ze nog twee miljoen moesten ontvangen, bleek dat Lazio in een nep-mail was getrapt. Criminelen hadden een nepmail opgezet die precies leek alsof het van Feyenoord kwam. De directie van Lazio trapte erin en maakte twee miljoen euro over naar criminelen.

Zeer slechte phishingmails bestaan nog, maar ze worden steeds zeldzamer. Ik kreeg er eentje van Ziggo.

Ziggo Mail.com <lefort.harry@t-online.de>
Wed 11/14/2018
You
Lieve verbonden, dank u voor het helpen
ons beschermen uw account door te online :
Ziggo-Mail
Dank u voor uw vertrouwen
Klantenservice

Boven aan de mail staat Ziggo Mail.com. Iedereen klikt zo'n slechte mail snel weg, maar stel dat het een zeer overtuigend geschreven mail was, zonder typfouten? Die

zie je steeds vaker. De enige redding is om de vrij betrouwbaar klinkende Ziggo Mail.com niet te vertrouwen, maar op de afzender te klikken om te kijken wie er achter dat adres schuilt. In dit geval is het lefort.harry@t-online.de. Welkom Harry, je moet nog veel Nederlands leren voordat je Nederlandse computers kunt hacken. Vooral blijven oefenen.

Even later ontvang ik een bestelbevestiging van Bol.com dat het bedrag van 21,98 euro van mijn rekening wordt afgeschreven. Ik heb helemaal geen bestelling geplaatst! "Klik op de link om de bestelling te annuleren," staat er. Eén zo'n klik en je computer kan overgenomen worden door hackers. Zweef altijd met je muis boven de link voordat je klikt, dan zie je dat de link helemaal niet naar de site van bol.com gaat, maar naar een onbekende site waar een virus op je wacht.
Sommige e-mailadressen lijken op elkaar.

Welke van die drie is goed?
A. nieuwsbrief@mail.ing.nl
B. nieuwsbrief@maillogin-ing.nl
C. nieuwsbrief@mijning-nieuwsbrief.nl

nieuwsbrief@mail.ing.nl is goed. Het deel achter het @-teken moet eindigen op de domeinnaam. De tekst voor

de domeinnaam moet gescheiden zijn met een punt.

Een goed uitziend e-mailadres geeft geen garantie, want hackers kunnen e-mailadressen namaken. Maar meestal doen ze de moeite niet, simpelweg omdat ze weten dat de meeste mensen niet op de afzender klikken.

Een paar recente voorbeelden:

Een mail van bol.com met de tekst: 'Win een Bol.com pakket en een 200 euro cadeaukaart!' Als je op de afzender klikt op je computer of op je mobiel, zie je v@ptgay.tacticpvc.com verschijnen. Dat klinkt niet bepaald als bol.com.

Een bericht van Netflix: 'Krijg nu gratis Netflix toegang voor drie maanden!'
De afzender is: ci43ijq@insiightly.org.uk

'Een feestelijke mededeling in verband met jubileum IKEA'. Afzender: reply@exur.carbontaekwondo.com

ING heeft de app voor mobiel bankieren verbeterd. De link leidt naar een zeer goed nagebouwde website van de bank. Maar let op de naam in de zoekmachine: healav. men. Dat klinkt heel anders dan ING. Zo zie je maar, onder de hackers heb je ook best veel prutsers. Want ze kunnen ook een site zoals www.verbeterdeING-app.nl registreren. Dat klinkt al een stuk beter.

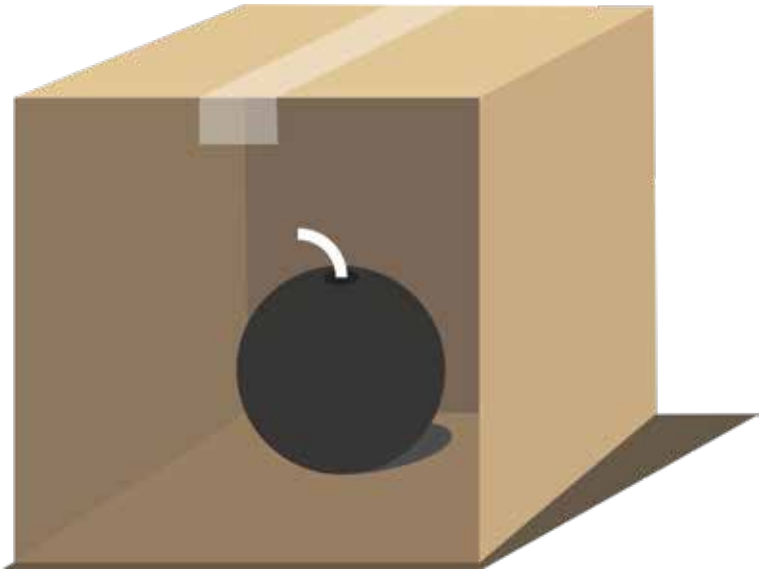
Waar je ook op moet letten, is of de echte site eindigt op bijvoorbeeld **nl**, **com**, **eu**, **be** of **nu**. Soms is slechts één van deze van het echte bedrijf en kunnen de andere domeinnamen door hackers gekocht zijn.

Hackers maken vaak sites na die op de echte lijken. Stel je wilt de tips over veilig internetten lezen op de Belgische site `Safeonweb`.

Welke van de 2 is de goede site?
A. www.safeonweb.be/tips B. www.safeonweb.tips.be/safeonweb

Extra tekst vóór de domeinnaam moet gescheiden zijn met een punt. Extra tekst achter de domeinnaam moet gescheiden zijn door een schuine streep (/).

Valse webadressen zijn bijvoorbeeld **login-consumentenbond.nl** (geen punt voor de domeinnaam) en **abnamro.nl.nieuwsbrief2016.nl** (geen streep achter de domeinnaam).
Bij twijfel: google het bedrijf, dan kom je vanzelf op de goede site.



Online bestellen

Je hebt iets besteld. Je ontvangt een bericht dat er geprobeerd is om je pakketje af te leveren, maar er was niemand aanwezig. Je kunt je pakket afhalen bij een PostNL Pakketpunt.

Wat doe je?
A. Klikken op de link in de mail om te zien waar je het pakketje kunt ophalen B. Even zweven boven de link om te kijken naar welke site deze gaat C. Klikken op de afzender om te checken wie de afzender is

Bij antwoord A ben je waarschijnlijk gehackt. Dit was helemaal niet een mail van een bezorgbedrijf, maar van de hackers. Met dat soort mails zijn er al duizenden Nederlanders gehackt. In veel gevallen werden hun computers versleuteld en waren ze alles kwijt.

Hoe wisten ze dat je op een pakje zat te wachten? Dat wisten ze niet. Ze sturen dit mailtje naar miljoenen mensen tegelijk. Er zijn altijd mensen die precies die dag een pakje verwachten. Daarom sturen ze de phishingmails namens alle bekende bedrijven: de kans dat iemand klant is, is heel groot.

Antwoorden B en C zijn goed. Klik altijd even op de afzender om te checken of die klopt of zweef met je cursor over het linkje om te zien of het naar de site van PostNL leidt. Zelf de site googelen en dan inloggen, is altijd veiliger dan via een link.

Als je op je mobiel wilt checken of een e-mail betrouwbaar is, kun je het beste op de afzender klikken. Meestal zie je maffe e-mailadressen verschijnen. Soms zien ze er goed uit. Dan kun je een tweede check uitvoeren: de link heel lang vasthouden om te kijken waar die naartoe gaat. Persoonlijk durf ik dat niet, want het is ook mogelijk om te snel los te laten en dan ga je wel naar de besmette site. Als je dat wilt uitproberen, oefen even met een link die je

wel vertrouwt.

> Als je accounts maakt bij online bestellen, gebruik niet hetzelfde wachtwoord. Momenteel zijn hackers heel succesvol bij webshops, omdat veel mensen overal hetzelfde wachtwoord voor gebruiken. Gehackte accounts van onder meer Wehkamp, Zalando en Bol.com worden massaal doorverkocht aan criminelen.

De hackers die de accountgegevens doorverkopen, maken misbruik van grote datalekken. Ze bieden ook accounts voor New York Pizza, MediaMarkt, Ziggo Sport en Marktplaats aan. Het gaat om duizenden gestolen mailadressen en wachtwoorden. Met de gegevens worden dure spullen op jouw naam besteld. De criminelen kiezen voor de optie 'achteraf betalen'. De dure artikelen worden opgehaald bij afhaalpunten en daarna doorverkocht.

In plaats van je standaard wachtwoord kun je een lange zin gebruiken. Daarna kun je die vergeten, want zo vaak bestel je waarschijnlijk niet bij dezelfde site. Als je een jaar later weer iets wilt bestellen, dan klik je op 'wachtwoord vergeten'. Sterke wachtwoorden zijn bijvoorbeeld zinnen zoals 'Vandaag ga ik een nieuwe koptelefoon bestellen'

of ‘Vandaag bestel ik een jas’. En natuurlijk kun je ook een cijfer en een uitroepteken toevoegen, want veel sites eisen dat.

> De apps van de banken zijn goed beveiligd, maar criminelen maken ze na. Dus pas op als je iets op bijvoorbeeld Marktplaats verkoopt en iemand komt het persoonlijk ophalen. Je kunt vaak meekijken hoe de koper geld naar je rekening overmaakt met zijn bank-app. Maar de app is soms vals, ook al is die vrijwel niet te onderscheiden van de echte bank-app. Er wordt geen cent overgemaakt en de koper is verdwenen met je spullen. Als de koper met een bank-app betaalt, moet je nog voordat hij weggaat checken of je de betaling ontvangen hebt.

Ook bij betaal-apps zoals Tikkie moet je oppassen. Sanne Kok betaalde 1 cent via Tikkie om haar account te bevestigen op verzoek van een koper op Marktplaats en raakte bijna 10.000 euro kwijt. De crimineel stuurde haar het linkje **`https://tlkkie.nl`**. De echte app van Tikkie is tikkie.me en eindigt dus niet op nl . Als je goed kijkt, zie je dat ook de i vervangen is door een l. Op een klein

scherm vallen dat soort dingen nauwelijks op. De link naar Tikkie gaat naar een inlogpagina van de bank die perfect nagemaakt is. Is **`https://www.ABNAMR0.nl`** goed of fout? Veel mensen vinden het er goed eruit zien. Ze letten op het groene slotje en beseffen niet dat het de boeven geen moeite kost om dat na te maken. In dit geval was het ook geen goede site, ze hebben de O vervangen door het cijfer 0. Bij ING doen ze iets soortgelijks. Is lNG goed? Nee, want ze hebben hier hoofdletter I vervangen door een kleine letter l (l van lelie dus).

Op het moment dat je inlogt op het valse inlogscherm, haalt de crimineel je bankrekening leeg.

Hoe verzin je en onthoud je sterke wachtwoorden?

Een op de drie kinderen gebruikt altijd hetzelfde wachtwoord. Wie kwaad wil, heeft dus in veel gevallen in één keer toegang tot alle accounts. Slechts een kwart van de kinderen verandert zijn wachtwoord regelmatig. Dat blijkt uit onderzoek van **www.alertonline.nl**

Volwassenen gebruiken trouwens ook vaak slechte wachtwoorden en zijn gemakkelijk te hacken. Soms per ongeluk. Zo heeft de Britse Susan (9) een reis naar Disneyland Parijs geboekt, terwijl haar vader lag te slapen. Ze slaagde erin zijn wachtwoord voor betaaldienst PayPal te raden en daarmee 1.100 euro uit te geven aan vluchten, hotel en entreekaartjes voor Disneyland.

Susan wist niet precies wat ze deed, maar volgens Google stelen hackers bijna 250.000 wachtwoorden per week. Ook de wachtwoorden van meer dan drie miljoen Nederlanders zijn al in handen van kwaadwillenden. De gegevens zijn afkomstig uit honderden gehackte websites

Vaak worden wachtwoorden geraden met automatische hack-programma's, omdat ze te kort zijn of te simpel.

Een wachtwoord met zes karakters, bestaande uit kleine letters, heeft bijna 309 miljoen combinaties.

Hoe lang duurt het om zo'n wachtwoord met een moderne computer te raden?
A. minder dan 7 seconden B. 4 dagen C. 30 dagen

En hoe lang duurt het als je dit wachtwoord verlengt naar 12 karakters?
A. 28 dagen B. 67 maanden C. 66 jaar

De antwoorden A en C zijn juist.
De lengte van een wachtwoord is een ontzettend belangrijk wapen tegen hackers. Als je een wachtwoord iets langer maakt, wordt het al vele malen sterker. Het verschil tussen 7 seconden en 66 jaar is enorm. Dat komt omdat er met twee keer meer letters ontzettend veel meer variaties op het wachtwoord mogelijk zijn. De hackers vinden het lastig te raden welke de goede combinatie is.

Als je tweestaps-verificatie aanzet, wordt het onmogelijk om je accounts te hacken. Hoe je dat doet, lees je hier: **https://veiliginternetten.nl/themes/situatie/wat-tweestapsverificatie/**

De zoekmachine voor gelekte wachtwoorden **`https://haveibeenpwned.com`** is enorm populair. Je kunt je e-mailadres invoeren en dan krijg je een melding welke bedrijven je wachtwoord gelekt hebben. Elke maand zijn er nieuwe datalekken.

Hoeveel gelekte accountgegevens bevat de website `Have I Been Pwned`?
A. 500.000 B. 5 miljoen C. 5 miljard

C is juist. Meer dan 5 miljard gelekte accounts van mensen uit de hele wereld. Veel mensen gebruiken hetzelfde wachtwoord en zo kunnen ook hun andere accounts overgenomen worden.

Uit een onderzoek blijkt dat slimme mensen net zulke slechte wachtwoorden hebben als de minder slimme mensen. Ook bekende mensen houden van simpel. Facebook-baas Mark Zuckerberg gebruikte het wachtwoord Dadada voor verschillende social media-accounts. Dat bleek toen zijn accounts werden gehackt.

Slechtste wacht-woorden	Hoe lang om hem te kraken (volgens Random-ize)	Hoe lang om hem te kraken (volgens BetterBuys)
123456	minder dan een seconde	0.25 milliseconden
123456789	minder dan een seconde	0.25 milliseconden
qwerty	minder dan een seconde	0.25 milliseconden
12345678	minder dan een seconde	0.25 milliseconden
111111	minder dan een seconde	0.25 milliseconden
1234567890	3 seconden	0.25 milliseconden
1234567	minder dan een seconde	0.25 milliseconden
password	1 minuut, 13 seconde	0.25 milliseconden
123123	minder dan een seconde	0.25 milliseconden
987654321	minder dan een seconde	0.25 milliseconden
qwertyuiop	13 uur, 48 minuten	4 maanden, 4 dagen, 7 uur
mynoob	minder dan een seconde	24 seconden
123321	minder dan een seconde	0.25 milliseconden
666666	minder dan een seconde	0.25 milliseconden
18atcskd2w	14 dagen, 21 uur	8 jaar, 9 maanden, 3 weken, 6 dagen, 8 uur
777777	minder dan een seconde	0.25 milliseconden
1q2w3e4r	16 minuten, 33 seconde	0.25 milliseconden
654321	minder dan een seconde	0.25 milliseconden
555555	minder dan een seconde	0.25 milliseconden
3rjs1la7qe	14 dagen, 21 uur	8 jaar, 9 maanden, 3 weken, 6 dagen, 8 uur
google	minder dan een seconde	0.25 milliseconden
1q2w3e4r5t	14 dagen, 21 uur	8 jaar, 9 maanden, 3 weken, 6 dagen, 8 uur
123qwe	minder dan een seconde	0.25 milliseconden
zxcvbnm	2 seconde	0.25 milliseconden
1q2w3e	minder dan een seconde	0.25 milliseconden

Hoe snel is het wachtwoord 12345678 gekraakt? Het duurt net zo lang als 1 keer niezen. Gebruik dus geen logische reeksen. Ook alle woorden uit het woordenboek zijn simpel te hacken. De hackers hebben al die woorden in automatische hack-programma's ingevoerd.

Welk wachtwoord is sterker?
A. School4! B. Ikhebeenhekelaanschool

Een wachtwoord als School4! voldoet aan de eisen voor een veilig wachtwoord (hoofdletter, cijfer en een teken). Toch is het simpel te hacken. Een wachtwoord zoals Ikhebeenhekelaanschool is vele malen sterker, ook al heb je geen cijfers en vreemde tekens gebruikt. Dat komt doordat het zo lang is. Dan moeten de hackers miljarden mogelijke combinaties raden en dat duurt meer dan 100 jaar. Als je na 100 jaar nog steeds leeft, moet je dat wachtwoord natuurlijk wel vervangen. Hoe? Dat is niet zo moeilijk, het nieuwe wachtwoord wordt: Vroegerhad-ikeenhekelaanschool.

Je kunt grappige en gekke zinnen verzinnen, des te makkelijker onthoud je ze. Bijvoorbeeld: 'Mijn kat bijt een hond','Ik ben de slimste van de klas' of 'Ik kan mijn wachtwoorden niet onthouden'. Als zo'n zin te lang wordt,

mag je die natuurlijk wel een beetje inkorten. Gebruik bijvoorbeeld de eerste letters van ieder woord in de zin en plak deze achter elkaar. Als het te kort wordt, dan gebruik je het laatste woord voluit. Ikamwnonthouden staat voor Ik kan al mijn wachtwoorden niet onthouden. Probeer op minimaal twaalf karakters uit te komen, want als je wachtzin korter is, dan kan die makkelijker gehackt worden.

Je kunt ook een wachtwoordmanager gebruiken, bijvoorbeeld LastPass Free (**https://www.lastpass.com/nl)**. Dat is een slimme kluis die al je wachtwoorden bewaart, automatisch invult op de websites waar je wilt inloggen en ook nieuwe ingewikkelde wachtwoorden voor je kan verzinnen en onthouden. Je hoeft slechts één heel lang wachtwoord zelf te onthouden. Zo'n wachtwoord-manager is veilig, want alle wachtwoorden zijn versleuteld opgeslagen. De versleuteling is bijna onmogelijk te kraken. Daarnaast kun je tweetraps-verificatie instellen. Dan krijg je een extra code op je mobiel. Zelfs als de hackers je wachtwoord geraden hebben, hebben ze je mobiel nodig om in te loggen.

Heb je een Google of iCloud-account? Schrijf je inlogge-gevens op papier en bewaar dat papiertje op een veilige plek voor het geval dat al je apparaten gestolen worden.

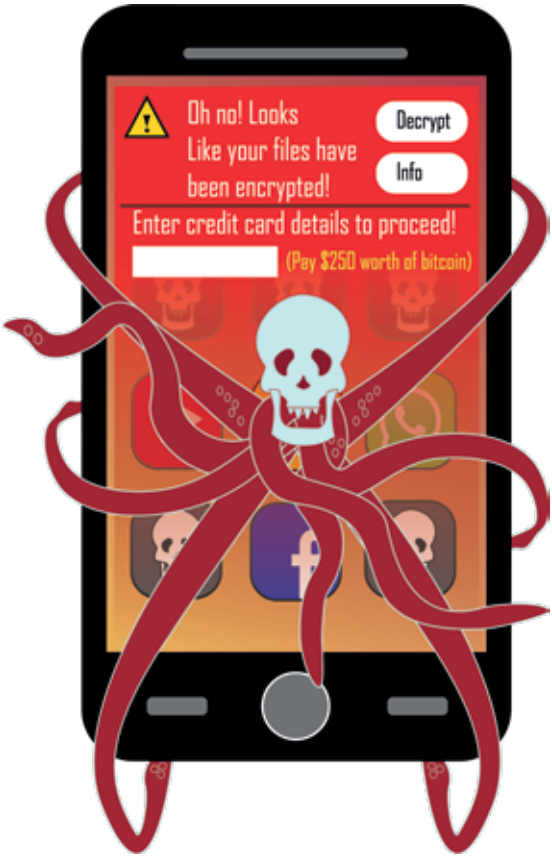
Hacken voor de politie

Veel bedrijven betalen aan ethische hackers die kwetsbaarheden in programma's opsporen, maar niet misbruiken. Google betaalde in slechts één jaar tijd drie miljoen dollar aan ethische hackers voor het ontdekken van beveiligingsfouten in hun systemen. Je kunt ook een goed zakcentje bijverdienen als je grote bedrijven hackt en dat meldt. Dat kan bij alle bedrijven die op hun site de

woorden ‘responsible disclosure’ vermelden. Als je een ernstige fout ontdekt, kun je soms 100.000 dollar beloning krijgen.

Veel jongeren hacken voor de lol. Ddos-aanvallen blijken vaak online-kattekwaad van tieners. Wereldwijd gaat het om zo’n 30.000 aanvallen per dag. Het kost de bedrijven heel veel geld. Sommige jongeren begrijpen niet hoe groot de gevolgen zijn. Je kunt er een strafblad voor krijgen. Omdat dit je verdere leven kan verpesten, straft het Openbaar Ministerie ook op een alternatieve manier. Jongeren die hacken en waarbij de gevolgen niet uit de hand lopen, moeten als straf na schooltijd of tijdens vakanties bij een ict-bedrijf werken. Daar leren ze hun computertalent op een goede manier gebruiken. Dit project heet HackRight.

Als je goed kunt hacken, kun je ook bij de politie solliciteren. Ze zijn op zoek naar hackers en als je voor de politie hackt, doe je niets strafbaars. Dan help je juist om boeven op te sporen. De komende jaren zoekt de politie veel hackers, maar ook ontwikkelaars van computersystemen. Kijk op it.kombijdepolitie.nl voor meer informatie.



Kwaadaardige apps

Bijna iedereen downloadt apps, maar vrijwel niemand leest de voorwaarden. De gratis apps zijn niet gratis. Je betaalt met je privacy. Ze willen bijvoorbeeld toegang tot al je contactgegevens en ze slaan alles van je vrienden op. Soms willen ze toegang tot je microfoon en tot je foto's.

Ze willen je ook de hele dag volgen. Daar geef je allemaal toestemming voor als je op 'accept' klikt zonder de voorwaarden te lezen. Die voorwaarden zijn supersaai om te lezen, maar wat je kunt doen, is meteen na het installeren van de app naar de instellingen gaan en achteraf alles afvinken, bijvoorbeeld toegang tot je contacten, tot je locatie en de rest. De app blijft gewoon werken, maar kan niet meer je hele mobiel leegtrekken.

De Britse zender Channel 4 deed onderzoek naar de apps die we op onze mobiele telefoons hebben.

Hoe vaak sturen 30 bekende apps die veel mensen op hun mobiel hebben staan, gegevens door naar de adverteerders en naar de makers?
A. 350.000 keer per dag B. 350.000 keer per week C. 350.000 keer per maand

Een smartphone met 30 bekende apps stuurt tot 350.000 keer per dag gegevens naar de adverteerders en naar de makers. Dat kan van alles zijn: van je locatie tot je contactgegevens.

Hoe vaak maakt een telefoon die ongebruikt op tafel ligt verbinding met servers in verschillende landen?
A. 30.000 keer per uur B. 30.000 keer per dag C. 30.000 keer per week

In nog geen uur tijd maakte de mobiel op tafel 30.000 keer een verbinding.

De gemiddelde gebruiker van een Android smartphone of tablet heeft 33 apps geïnstalleerd. In de officiële Google Play store vind je ook duizenden kwaadaardige apps. Ze worden niet altijd op tijd ontdekt. Zo hebben ruim één miljoen mensen een kwaadaardige versie van WhatsApp gedownload voordat deze werd verwijderd. Je krijgt bij dat soort apps geen waarschuwing dat ze mogelijk je telefoon kunnen overnemen. Ze zijn vaak ook lastig te herkennen. Alleen de naam van de app wijkt af: 'Update WhatsApp' in plaats van 'WhatsApp'. De imitatie-app maakte gebruik van hetzelfde app-icoontje. De app gebruikte daarnaast WhatsApp Inc. als naam van ontwikkelaar, net als het origineel. Het enige verschil was een onzichtbare spatie.

De app Gooligan bleek 13.000 Google-accounts per dag te stelen. Er zijn ook apps die je meer Instagram-volgers beloven, maar stiekem stelen ze je gebruikersnaam en

wachtwoord. Dit soort apps zijn honderdduizenden keren gedownload. Dat zijn apps met namen als ‘Instagram Followers’ en ‘Real Followers for Instagram’.

Wat doet een update?

Updates verschijnen vaak op een een moment dat je niet uitkomt. Veel mensen vinden ze irritant en klikken ze weg of klikken op ‘later, later, later’.

Wat doe je zelf als een programma om een update vraagt, terwijl je met iets anders bezig bent?
A. Wegklikken B. Meteen uitvoeren C. Aangeven dat ik dat later wil uitvoeren

Vergelijk de updates met de ramen en de deuren van je huis. Laat je die open als je weggaat?
Natuurlijk niet, want je wilt niet dat inbrekers binnenkomen en je computer stelen. Maar de inbrekers kunnen ook op afstand alles van je computer stelen als je de updates niet gedaan hebt.

> Hoe weten de digitale inbrekers precies jouw laptop of mobiele telefoon te vinden? Meestal is dat puur toeval. Ze scannen de digitale 'poortjes' van miljoenen computers tegelijkertijd en kijken welke niet dicht zijn. Ze komen bijvoorbeeld binnen via een besmette advertentie op een normale website. Je hoeft niet eens op de advertentie te klikken.

Als je de updates hebt gedaan, zoekt zo'n kwaadaardige advertentie naar een open deurtje, maar dat is er niet. Dan gaan de hackers door naar het volgende slachtoffer, naar iemand die de updates niet heeft geïnstalleerd.

Kijk je wel eens naar de Formule 1? Dan zie je dat er wel eens auto's crashen. Als je de updates niet doet, heb je grote kans dat je computer ook gaat crashen en dat je alles kwijt bent. Echt alles.

Als je te traag update, heb je misschien mazzel en gebeurt er niets, maar goed is het niet. Als Max Verstappen te langzaam is bij een bocht, dan verliest hij waarschijnlijk ook de wedstrijd. De winnaar rijdt snel en neemt geen onnodige risico's. Dat doet een update voor je, zorgt ervoor dat de meeste risico's uitgeschakeld worden. Eigenlijk is dat 1 van de snelste manieren om je tegen de hackers te beschermen.

De gevaren van social media

Op Facebook Messenger circuleren geregeld berichten met een virus. De filmpjes komen van bekenden. In de tekst staat bijvoorbeeld ‘Ik kijk naar jou’, ‘Je hebt jezelf laten opnemen’ of in het Engels ‘This video belongs to you’. Daarbij staat een link die je door lijkt te sturen naar YouTube. Klik niet, maar waarschuw de afzender van het

bericht dat hij of zij gehackt is.

Je (gehackte) vriend kan je ook een bijlage sturen. Aan een bijlage kun je niet altijd zien dat het een virus bevat, maar vaak kun je dat wel vermoeden. 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.

Bestanden zoals .exe. js .lnk .wsf .scr .jar zijn gevaarlijk. Ze bevatten vaak 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. Dat is mogelijk een poging om je te hacken.

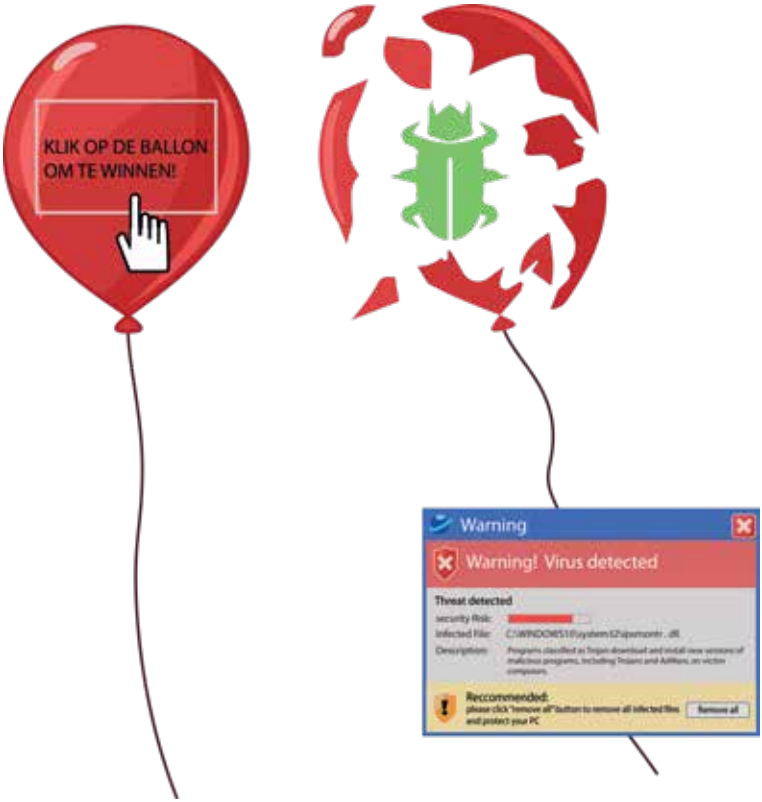
> Helaas zijn de extensies (zoals .exe) in Windows standaard verborgen. Schakel de extensies in, zodat je ziet om wat voor bestand het gaat. Typ Windowstoets + R, typ in het venster 'control folders' en druk op Enter. In het tabblad Weergave verwijder je het vinkje voor 'Extensies voor bekende bestandstypen verbergen'.

Op social media moet je ook oppassen voor nepprofielen en nepnieuws. Twitter heeft in de afgelopen maanden

meer dan een miljoen accounts per dag verwijderd. Twitter is strenger gaan optreden tegen mensen die het platform misbruiken. Daarbij gaat het onder meer om de verspreiding van nepnieuws en misleidende informatie.

Hoeveel nepaccounts heeft Facebook in 3 maanden tijd verwijderd?
A. 5 miljoen B. 64 miljoen C. 583 miljoen

Facebook heeft 583 miljoen nep-accounts verwijderd in slechts drie maanden tijd. En ook meer dan 800 miljoen spamberichten en miljoenen haatberichten. De meeste worden automatisch offline gehaald omdat ze door mensen gerapporteerd worden. Dat gebeurt door middel van programma's die nepprofielen herkennen. Maar er is ook controle op de inhoud door menselijke moderatoren. Het Nederlandse team ontvangt ongeveer achtduizend meldingen per dag van ongepaste berichten.



Winacties

‘Gefeliciteerd, u bent de winnaar van een iPhone 8. Claim uw prijs nu!’ Op het internet barst het van dat soort winacties en ze zijn vrijwel altijd nep. Soms moet je een paar gemakkelijke vragen beantwoorden om iets te winnen. Een andere keer mag je dure producten testen en daarna

houden. Trap er niet in, want het enige wat er gebeurt is dat louche bedrijven je gegevens bemachtigen en voor spam gebruiken. Of ze laten je een duur betaalnummer bellen. In het slechtste geval ben je gehackt. Een virus kan zich prima in een plaatje met ballonnen verstoppen.

> Cybercriminelen hebben ook WhatsApp ontdekt voor het versturen van aanbiedingen. Wil je een waardebon van 250 euro winnen? Het lijkt alsof vrienden of bekenden deze leuke aanbiedingen doorsturen. Wie het linkje aanklikt en zijn gegevens invult om de waardebon te claimen, stuurt zijn gegevens door naar cybercriminelen.

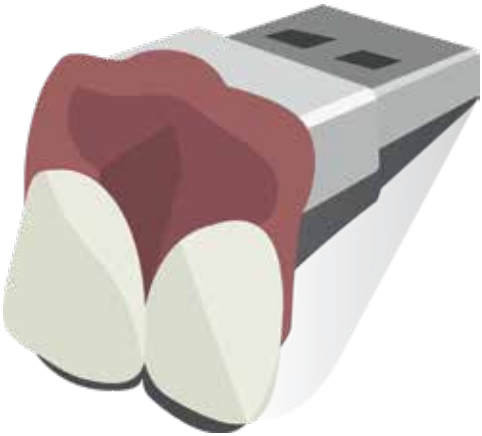
Heel wat pretparkliefhebbers trapten in een vals bericht dat van de Efteling leek te komen. De Efteling zou jarig zijn en 500 gezinnen gelukkig willen maken met gratis tickets. In dit geval was de val behoorlijk misleidend opgezet. De URL die in het bericht verscheen **`http://www.efṭeling.com`** leek heel erg op de echte URL: **`https://www.efteling.com`**. Toch waren er twee belangrijke verschillen: een betrouwbare URL gebruikt https in de plaats van http. Als je goed kijkt, zie je een puntje onder de letter t verschijnen (ṭ).

Google altijd zelf het bedrijf, op hun website staan alle winacties.

Je hoeft niet altijd iets te winnen, soms vind je zomaar iets op straat of op school. Bijvoorbeeld een usb-stick.

Wat doe je daarmee?
A. In de computer steken om te kijken van wie het is B. Kapotmaken

Het beste is kapotmaken. Steek het nooit in je laptop, want sommige usb-sticks zijn voorgeprogrammeerd en geven commando's aan je laptop. Zo'n commando kan zijn om alles te kopiëren en naar de hackers te sturen.



Geldezels

Fraudeurs zijn voortdurend op zoek naar ‘geldezels’ om gestolen geld door te sluizen. Dat doen ze ook via Instagram, Snapchat en WhatsApp. Ze vertellen de jongeren dat ze snel geld kunnen verdienen door hun pinpas te lenen of te verkopen voor enkele legale transacties. De pinpas wordt echter gebruikt om gestolen geld door te sluizen. Bij minderjarigen kunnen de ouders voor de schade opdraaien. Bekijk dit confronterende filmpje over deze en andere vormen van cybercrime: **https://www.youtube.com/watch?v=4JqfChAKSfE**

Valse websites

1 op de 5 webshops is nep. Deze webshops eindigen vaak op .nl en verkopen vooral sportschoenen, kleding en bekende merken. Als je bijvoorbeeld op Nike schoenen zoekt of bekende kledingmerken, heb je grote kans dat je op een foute website terechtkomt, zoals 2017nikeairmax.nl. Sommige van die nep-webshops adverteren op Instagram en Facebook. Dan denken mensen dat die te

vertrouwen zijn.

> Vaak zien de websites er goed uit. Soms zijn ze ook voorzien van een slotje. Maar een slotje op zich zegt niet zo veel, de verbinding is wel beveiligd, maar wat heb je eraan om op een veilige manier een verbinding met een hacker te maken? Je raakt in alle gevallen je geld kwijt als je op zo'n site bestelt.

Veel van die domeinnamen scoren hoog op Google. Jarenlang waren ze van betrouwbare bedrijven, maar die hadden ze niet meer nodig. Toen hebben hackers ze opgekocht. Zo krijg je wel vreemde combinaties, want een Chinese hacker weet helemaal niet wat Sinterklaas is, maar diverse sites over Sinterklaas zijn niet meer verlengd en kunnen soms voor slechts 1 euro geregistreerd worden. Een van de vele sites was sinterklaasinommen.nl. Blijkbaar was Sinterklaas een keer in de plaats Ommen op bezoek en had de website daarna niet meer nodig. De hackers wel. Als je daar iets bestelt, ga je voor Sinterklaas spelen.

Naast de vele valse websites, zijn er ook duizenden gehackte sites. De eigenaren weten niet dat hun site

gehackt is en misbruikt wordt om de bezoekers te besmetten. Dat kan via een valse advertentie of je krijgt een waarschuwing dat je je webbrowser of Flash Player moet updaten om de website te kunnen bekijken. In werkelijkheid downloadt je een kwaadaardig programma. Dat is in het verleden ook gebeurd met bekende sites zoals nu.nl, marktplaats.nl en sbs6.nl. Als je een pop-up met een advertentie ziet, klik niet op 'Nee' of 'x' om te sluiten. Hiermee kun je al kwaadaardige software installeren. Veilig wegklikken kan via de toetscombinatie Alt+F4.

Laat je altijd digitale sporen na?

Bij alles wat we doen op het internet laten we een digitale voetafdruk achter. Dat kan een reactie zijn op Instagram, een Whatsapp-gesprek of een nieuw account. Cookies verzamelen veel informatie over je. Wat best grappig is: google op 'Hoe verwijder ik cookies op een Apple pc?' en de hoogst scorende site zegt: 'Accepteer cookies om dat te lezen'.

Als je niet wilt dat de websites van alles over je verzamelen, van je locatie tot je e-mailadres, kun je dat gratis blokkeren door het installeren van een ad-blocker.

Op **https://www.consumentenbond.nl/internet-privacy/adblockers-faq** staat hoe je dat doet. Je kunt zelf aangeven voor welke sites je een uitzondering wilt maken.

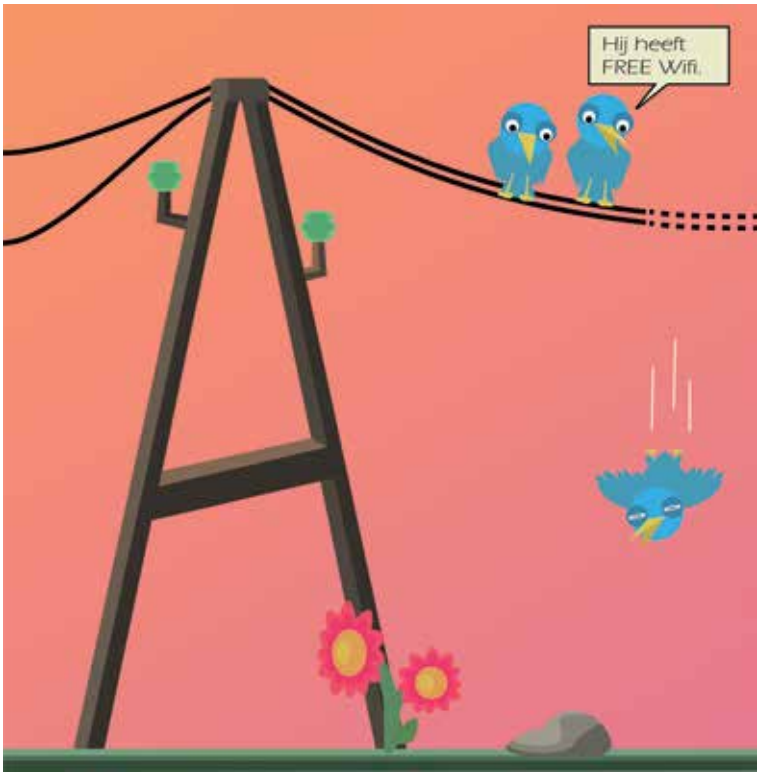
Bij online winkelen kun je er vaak niet omheen om persoonlijke gegevens in te vullen. Je kunt wel checken (**https://www.consumentenbond.nl/online-kopen/keurmerken-webwinkels**) of de winkel betrouwbaar is.

Je hoeft niet alles naar waarheid in te vullen als je ergens voor het eerst inlogt. Er worden heel veel betrouwbare websites gehackt en dan zien de hackers wat je ingevuld hebt. Soms blijken zelfs prijswinnende websites niet goed om te gaan met de gegevens van de bezoekers. Beter-spellen.nl won de prijs 'Populairste educatieve website', maar lekte de accountgegevens van ongeveer 150.000 bezoekers, zoals e-mailadressen, geboortedata en namen. Deze gegevens waren niet bij alle accounts ingevuld; bij een derde van de 150.000 accounts was geen e-mailadres opgegeven.

Als je wilt weten wat sites over je openbaar laten zien, kun je je naam tussen aanhalingstekens googelen. Je kunt ze vragen om alle informatie die ze over je hebben te

wissen. Dat mogen ze niet weigeren, want dan overtreden ze de privacy-wet (AVG). Je kunt ook Google vragen om je hele zoekgeschiedenis te verwijderen. Dat is vrij simpel, gewoon aanvinken in de instellingen.

Er zijn ook online tools zoals Disconnect.me en DoNotTrackMe die ervoor zorgen dat software die bijhoudt wat je online allemaal doet wordt geblokkeerd. Check (**https://www.consumentenbond.nl/internet-privacy/privacy-op-twitter-en-instagram**) de privacy-instellingen van sociale media die je gebruikt, zoals Instagram, Facebook en Twitter. Controleer je online privacy met deze scan: **https://www.consumentenbond.nl/internet-privacy/keuzehulp-privacyscan**.



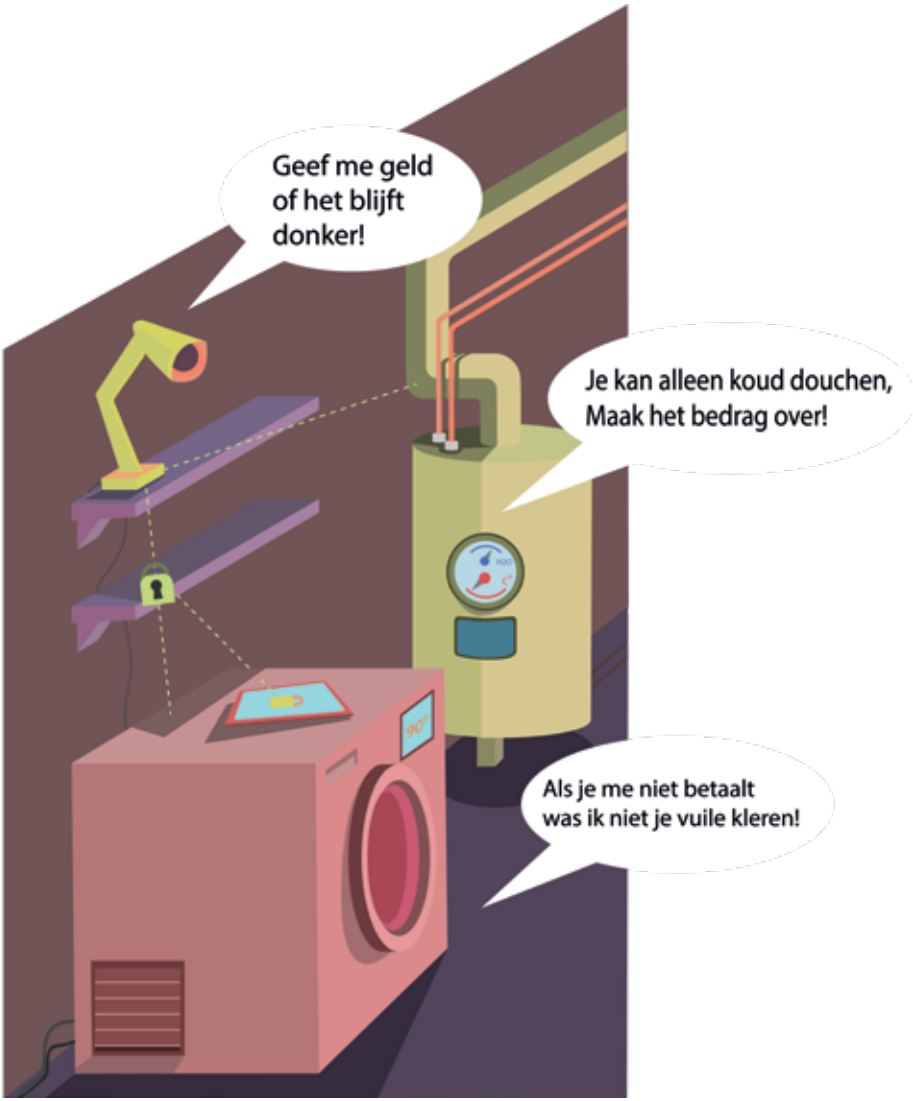
Wifi

Hacken via openbare wifi netwerken is heel gemakkelijk. De hackers kunnen zelf namen verzinnen die goed klinken, bijvoorbeeld ‘Free Wifi McDonalds’ of ‘Gratis Wifi KPN’. Als je inlogt, kan de hacker je inloggegevens stelen en ook je mobiel of je laptop overnemen. Bij nep-wifi krijg je vaak een inlogscherm en word je gevraagd om iets te

installeren, bijvoorbeeld een app of een certificaat. De inlogpagina lijkt net echt, maar alles wordt automatisch doorgestuurd naar de hackers.

Met een VPN (virtual private network) kun je veilig en anoniem op gratis wifi-netwerken internetten. ProtonVPN heeft een gratis versie. Van de betaalde VPN-diensten zijn de gemakkelijkste en veiligste opties Private Internet Access (**https://nld.privateinternetaccess.com/)**, NordVPN (**https://nordvpn.com/nl/**) en Freedome (**https://www.f-secure.com/nl_NL/web/home_nl/freedome**). Ze kosten een paar euro per maand.

Op veel plekken heb je niet alleen gratis wifi, maar ook openbare computers: bijvoorbeeld in bibliotheken, in hotels en op vliegvelden. Cybercriminelen kunnen achter je inloggegevens komen als ze een virus op zo'n openbare computer installeren.



Internet of Things

Alle slimme apparaten zijn tegenwoordig verbonden met het internet: slimme tv's, slimme thermostaten, slimme koelkasten, slimme camera's… En ze zijn allemaal op een simpele manier te hacken. Hoe? Omdat veel mensen het standaard wachtwoord niet veranderd hebben. Ook de thermometer die in een aquarium in een casino was geïnstalleerd, werd gehackt. En via die thermometer kregen de hackers toegang tot het netwerk van het bedrijf en konden de gegevens van veel klanten stelen.

Er zijn ook gevallen bekend waarbij hackers via snoepautomaten en slimme lantaarnpalen het computernetwerk van een universiteit hebben platgelegd.

> Als je een slim apparaat koopt, moet je meteen het standaard wachtwoord veranderen. Sommige mensen kopen een beveiligingscamera, maar doen dat niet. Via het standaard wachtwoord kunnen de hackers duizenden van die beveiligingscamera's tegelijkertijd overnemen. Ze kunnen de camera in plaats van naar buiten naar binnen laten draaien en je thuis filmen. Ze kunnen met duizenden gehackte camera's ook websites platleggen.

Ook het wachtwoord van een smart tv moet je eenmalig veranderen.

Sexting

1 op de 5 jongeren verstuurt weleens sexy foto's via Whatsapp, e-mail of social media. Meer dan de helft van de jongeren heeft zijn of haar webcam niet afgedekt en kan door een hacker ongewild gefilmd worden (onderzoek

SmartStudentDeals).

Als je een sexy foto wilt sturen, zorg dan dat je niet herkenbaar bent. Vermeld je naam niet, laat je hoofd niet zien en zet er als hashtag bij #foryoureyesonly. Stuur nooit foto's aan mensen die je alleen van het internet kent. Soms blijkt een knappe jongen een zestigjarige man te zijn.

Laat je niet onder druk zetten. Als iemand verliefd is op jou en vraagt om naaktfoto's, durf ook nee te zeggen. De liefde van de ander neemt daardoor echt niet af.

> Chat niet met je eigen naam, maar gebruik een nickname. Gebruik ook niet je eigen naam in je gmail als je die aan onbekenden geeft. Maak anders een nieuwe gmail aan. Vertel niet waar je op school zit of waar je woont. Accepteer niet iedereen als vriend.

Controleer als je een vriendschapsverzoek ontvangt wat voor vrienden diegene heeft. Wanneer een jongen alleen maar jonge meisjes als 'vriend' heeft toegevoegd, is dat verdacht.

Als je iemand die je online hebt leren kennen wilt bellen,

doe dat dan eerst zonder nummerherkenning. Blijf altijd goed nadenken en luister naar je gevoel. Als je het niet vertrouwt, stop er dan gewoon mee. Spreek bij een eerste date nooit alleen thuis af. Spreek af op een plek waar andere mensen zijn, bijvoorbeeld in een café. Vertel je ouders of een vriend(in) waar je bent, met wie en tot hoe laat.

> Staat er iets vervelends over jou online? Maak screenshots en zorg ervoor dat de url in beeld is. Ga naar de politie en vraag daar een oriënterend gesprek aan. Meld diegene bij de website waar het contact is ontstaan. Misschien zijn er al meer klachten en kunnen zij informatie doorgeven aan de politie.

De politie adviseert om bij sextortion (afpersing waarbij ze vaak om naaktfoto's vragen) zo snel mogelijk aangifte te doen en geen geld te betalen aan de afpersers. Als ze je foto of filmpje verspreiden, zijn ze strafbaar. Meestal blijft het bij bedreigingen en doen ze het niet.

Als je in de problemen komt, neem contact op met HelpWanted.nl of Meldknop.nl. Daar helpen ze je aan oplossingen. Je kunt ook kijken op **www.qpido.nl** en

chatten met mensen die je kunnen helpen.
Vraaghetdepolitie.nl is een website van de politie, speciaal voor jongeren. Daarin worden heel veel vragen op een simpele manier en met leuke filmpjes beantwoord. Wil je direct een antwoord van de politie op je vragen? Check de data op de chatagenda van **vraaghetdepolitie.nl**. In privéchat-sessies kunnen jongeren hun verhaal doen en krijgen ze direct antwoord of advies. Bellen kan ook: 0900-8844.

Praat erover met een volwassene die jij vertrouwt. Bijvoorbeeld met je ouders, je mentor, de vertrouwenspersoon van school, je trainer of misschien je lievelingstante.

Als je een naaktfoto of -filmpje van iemand krijgt, denk dan na voordat je iets doorstuurt. Realiseer je wat voor impact doorsturen kan hebben op het slachtoffer. Verwijder naaktfoto's en -filmpjes die je binnenkrijgt.
Heel veel waargebeurde verhalen van jongeren over naaktfoto's vind je in het boek **Sexy selfies**
https://www.bol.com/nl/p/sexy-selfies/9200000046267474/

Doe-het-zelf tips bij ransom-ware (gijzelingssoftware

Zet de automatische backup zo snel mogelijk uit. Ga naar NoMoreRansom (**https://www.nomoreransom.org/nl/index.html**) om te kijken of je een gratis sleutel kunt krijgen om je bestanden terug te krijgen.
Pas als alle besmettingen zijn verwijderd met een anti-virusprogramma, kunt je de automatische backup weer aanzetten.
Op de site Veilig Internetten vind je veel tips en kun je je computer gratis laten schoonmaken: **https://veiliginternetten.nl/maakjecomputerschoon/**

Over hoe dit boek ontstond en iets over mij :

Nadat ik het boek 'Komt een vrouw bij de h@cker' schreef, werd ik uitgenodigd voor lezingen over privacy en cybercrime aan alle mogelijke bedrijven en overheidsinstellingen. Dat doe ik nog steeds met veel plezier en de reacties zijn altijd verbaasd en geschrokken. Veel mensen vragen: 'Mooi dat ik vandaag geleerd heb hoe ik mezelf tegen hackers kan beschermen, maar hoe vertel ik dat aan mijn kinderen? Ze zijn vaak online en zien de gevaren niet.' Zo ontstond het idee voor 'What the hack!'

Gamebedrijf Flavour las de eerste versie van het boek en was zo enthousiast dat ze besloten hebben om de game HackShield op het boek te baseren. Speel het gratis op https://www.flavour.nl/hackshield en test hoe cybersmart je bent geworden.

Wil je een keer een leuk en spannend event op het

gebied van privacy en cybercrime organiseren? Nodig me dan uit samen met een ethische hacker. We laten op een interactieve manier zien welke digitale deuren wijd open staan en hoe je die dicht kunt doen.

Je kunt me altijd mailen via mijn site www.mariagenova.nl

Groetjes,