consumentenbond

4

Minigids

€3 • 2017

VEILIG ONLINE

Slim op ’t web

Wees hackers een stap voor

Wachtwoordstress
Zo onthoud je je wachtwoorden

oprecht consumentenbond

MIJNENVELD

Als je het nieuws op digitaal vlak een beetje volgt dan lijkt internet wel een mijnenveld. Overal liggen hackers op de loer om ons geld af te troggelen, bijvoorbeeld met nepmailtjes, met nepartikelen op Marktplaats of achter je rug om via gaten in lekke software.

Zeker, het internet is geen speeltuin en als je niet oppast kun je behoorlijk het schip in gaan. Sommige nepmails zien er bedrieglijk echt uit, en wat er dan kan gebeuren kun je lezen op pagina 6. Ik ben er ook een paar keer bijna ingetuind.

Maar het goede nieuws is: als je weet waar je op moet letten en als je je apparaten en je accounts voldoende dichttimmert, kun je een hele hoop ellende voorkomen. Dat lijkt misschien allemaal heel ingewikkeld, maar dat valt reuze mee.

In deze minigids leggen we uit hoe je je wapent tegen hackers, zowel op je computer, tablet als op mobiel. Je kunt lezen wat bekende Nederlanders doen om hun veiligheid online te beschermen (met tips van onze expert Ronald Kamp). En mis ook niet het verhaal van de moedige Michaja (pagina 28), die achter haar oplichter aanging en hem ontmaskerde. Ik wens je veel leesplezier met deze minigids.

VINCENT VAN AMERONGEN
Hoofdredacteur Digitaalgids
vvamerongen@consumentenbond.nl

COLOFON

De Minigids Veilig Online is een uitgave van de Consumentenbond (mei 2017)

Hoofdredactie Vincent van Amerongen
Redactie Vincent van Amerongen, Esther Derks, Ronald Kamp, Rob Schleiffert
Uitgever Dieneke Hengeveld
Ontwerp, art directie en vormgeving Sanna Terpstra (ontwerp), Miranda van Agthoven (art directie en vormgeving), Twin Media bv
Beeld Hollandse Hoogte, Mieke Meesen, Shutterstock, Koen Verheijden, Maarten van der Wal, Wikimedia Commons
Marketing Mirjam Bijleveld, Bart Brouwer, Jessica Tanke, Jantine Zuidervaart
Druk Senefelder Misset, Doetinchem

CONSUMENTENBOND
Service & Advies
070 - 445 45 45
Internet consumentenbond.nl
Contactformulier
consumentenbond.nl/contact

Volg ons op
twitter.com/consumentenbond

Praat mee op
facebook.com/consumentenbond

Bekijk onze filmpjes op YouTube
youtube.com/consumentenbond

Ook actief op Google+
google.com/+consumentenbond

Consumentenbond Kiosk-App
Lees onze uitgaven digitaal

INHOUD

TIPS & ADVIES

BN'ER IN BEELD

INTERVIEW

Maar 17% van de Nederlanders gebruikt een adblocker, tegen 11% wereldwijd. 38% meer vrouwen dan mannen geven als hoofdreden voor een adblocker op dat ze willen voorkomen dat foute advertenties de pc besmetten.

(BRON: PAGEFAIR)

Bedrog

Drie Amsterdammers hebben in januari 2017 2500 mensen opgelicht. Ze boden op Marktplaats mobieltjes aan zonder die te leveren. Kopers moesten via WhatsApp een kopie van hun legitimatiebewijs opsturen. Daarmee deden de verdachten zich op Martkplaats voor als 'nieuwe' kopers.

➜ Lees ook het interview op pagina 28.

Jongeren lopen driemaal zoveel risico op cybercrime als ouderen

JONGEREN LOPEN MEESTE RISICO

Uit onderzoek van het CBS blijkt dat jongeren tussen 15 en 24 jaar vaker slachtoffer zijn van cybercrime dan ouderen. 16% van de jongeren kreeg ermee te maken, dat is ruim drie keer zo veel als bij de 65-plussers (5%). Jongeren zijn relatief vaak slachtoffer van cyberpesten, koop- en verkoopfraude en hacken. Bij identiteitsfraude zijn ze juist minder vaak slachtoffer.

Emma Watson gehackt

Tientallen privéfoto's van Emma Watson zijn na een hack op internet beland. Het zou niet om intieme foto's gaan. De actrice neemt juridische stappen. Eerder kwamen naaktfoto's van beroemdheden op straat te liggen, onder meer van Jennifer Lawrence en Ariana Grande. Eén van de gebruikte trucs is het versturen van phishingmails, om zo gebruikersnamen en wachtwoorden te achterhalen.

RANSOMWARE

De eerste maanden van 2017 heeft de politie 75.000 slachtoffers geholpen waarvan hun bestanden op slot waren gezet door ransomware (gijzelsoftware). In juli 2016 lanceerde de Nederlandse politie samen met Europol en enkele beveiligingsbedrijven de website www.nomoreransom.org. Op deze website zijn hulpmiddelen te vinden om versleutelde bestanden te ontsleutelen. **➜ Lees ook het interview op pagina 6.**

BAAS OVER EIGEN DATA

De Consumentenbond is de komende jaren volop bezig met het thema 'Baas over eigen data'. Drie vragen aan campagneleider Inge Piek.

1. Wat is het probleem?
'Bedrijven verzamelen veel meer persoonlijke gegevens dan nodig. Ze gebruiken soms ook je postcode om je te kunnen weigeren voor een telefoonabonnement of energiecontract.'

2. Wat is jullie doel?
'We willen dat bedrijven alleen gegevens vragen en gebruiken die nodig zijn om een goede dienst te leveren, en verder niets.'

3. Wat gaan jullie doen?
'Op basis van de tientallen klachten op ons meldpunt 'Dupe van je data' onderzoeken we nu bedrijven die je kredietwaardigheid beoordelen en energieleveranciers die daarvan gebruikmaken.'

INFO & TIPS
CONSUMENTENBOND.NL/PRIVACYTIPS

(BRON: CBS)

11% van de Nederlanders was in 2016 de dupe van cybercrime. Hacken en koop- en verkoopfraude komen het meest voor.

ÉÉN KLIK, BESTANDEN OP SLOT

'Hoe had ik zo onoplettend kunnen zijn!'

Kathelijn kon ineens niet meer bij haar bestanden.

IK VOELDE ME ZO naïef!

Kathelijn (37) klikte op een foute link waardoor haar bestanden werden versleuteld. Nu is ze al haar data kwijt.

TIP
Voorkomen is beter dan genezen: maak een back-up van je bestanden.

‘Normaal gesproken ben ik alert op e-mails met onbekende afzenders of vreemde verzoeken. Toch ben ik er op een onbewaakt moment ingetrapt. Als coach werk ik vanaf verschillende locaties. Mijn laptop is als het ware mijn bedrijf, die neem ik overal mee naartoe. Al mijn gegevens staan erop en met collega-coaches werk ik samen via Dropbox (een dienst waarbij je online bestanden kunt opslaan en delen – red.).

Trillende vingers

Op die bewuste dag zat ik op een plek waar internet vaak traag is. Terwijl ik me voorbereidde op een coachgesprek, zat ik ondertussen te wachten op een pakje van Post.nl. Er kwamen nog wat telefoontjes tussendoor en te midden van alle drukte zag ik in mijn mailbox een bericht van Post.nl verschijnen. In een reflex opende ik de mail en klikte op de link om te zien waar mijn pakje zich bevond.

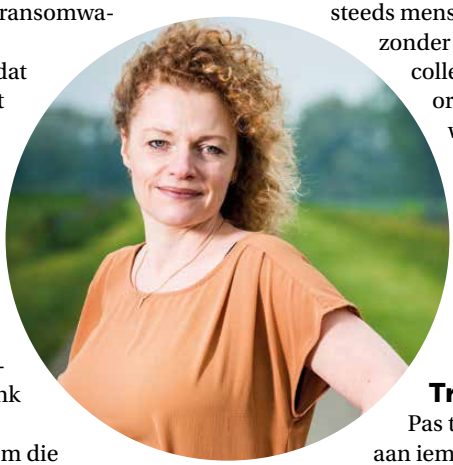
Het internet liep vast, maar dat was die dag al vaker gebeurd, dus klapte ik mijn laptop dicht en ging aan de slag met mijn cliënt.

Na de sessie deed het internet het nog steeds niet. Ik klikte nog vijf keer op de link, totdat ik een bezorgde app ontving van een collega. Er was iets vreemds aan

[BRON: SYMANTEC]

de hand met mijn bestanden in Dropbox. Ze konden niet meer worden geopend.

Met trillende vingers probeerde ik een bestand op mijn laptop te openen, maar in plaats van mijn eigen tekstbestand verscheen er een bericht dat mijn laptop was vergrendeld met ransomware (een kwaadaardig softwareprogramma dat alle bestanden op slot zet – red.). Internetcriminelen hadden mijn computer gehackt! Via een link zou ik kunnen zien hoeveel losgeld ik moest betalen om weer bij mijn gegevens te kunnen komen. Op die link heb ik niet geklikt. Ik peinsde er niet over om die criminelen geld te geven.



Alles kwijt

Ik voelde me zo naïef! Hoe had ik zo onoplettend kunnen zijn! Doordat ik allerlei dingen tegelijk aan het doen was, had ik niet goed opgelet en nu was ik al mijn data kwijt. In paniek belde ik de man die mijn website onderhoudt. Er was volgens hem nog geen digitale sleutel ontwikkeld om het hackersprogramma te ontgrendelen.

'Pas later besefte ik hoever de hackers in mijn persoonlijke leven waren doorgedrongen.'

Daar gaat mijn bedrijf, dacht ik. Mijn boekhouding, mijn klanthistorie! Gelukkig besefte ik al snel dat ik nog steeds mensen kon coachen, ook zonder laptop. En via mijn collega's kon ik veel originele bestanden weer opvragen. Daarnaast stond er veel data in mijn mailbox en had mijn boekhouder een vrij recente back-up van mijn boekhouding.

Trouwfoto's

Pas toen ik een tijdje later aan iemand foto's wilde laten zien van mijn overleden moeder, besefte ik hoever de hackers in mijn persoonlijke leven waren doorgedrongen. Ze hadden zelfs mijn privébestanden van mij afgenomen! Mijn moeder is zes jaar geleden overleden, waardoor die foto's extra dierbaar zijn. Het gaat de criminelen enkel om geld, maar het is wel mijn leven! Het maakte me boos en verdrietig. Gelukkig bleek mijn zus dezelfde foto's te hebben, dus met een omweg heb ik ze weer terug.

Mijn trouwfoto's ben ik wel echt kwijt. We hebben er in die tijd een paar laten afdrukken, maar van de rest van de foto's had ik geen back-up.

Het was een harde les voor mij. Ik heb meteen een externe harde schijf gekocht en maak nu heel trouw iedere maand een back-up van al mijn bestanden.

BESTANDEN OP SLOT, WAT NU?

Er zijn vier mogelijkheden om je bestanden terug te krijgen:

POLL

Ben jij ook bang dat je slachtoffer wordt van ransomware? Ga naar consumentenbond.nl/community/poll-gijzelsoftware

1 Zelf ontsleutelen
Als je geluk hebt, zijn de makers van de ransomware opgepakt of heeft de politie ontsleutelingsgegevens weten te bemachtigen. Kijk op nomoreransom.org voor een overzicht van alle ransomware die je zelf kunt ontsleutelen. Voor de meeste ransomware is er helaas geen oplossing.

In één jaar tijd is de hoogte van het losgeld dat wordt geëist, verdrievoudigd van $294 naar $1077.

[BRON: SYMANTEC]

2 Back-up terugzetten
Makkelijker is het om een back-up van je bestanden terug te zetten. Die back-up moet je dan natuurlijk wel vooraf hebben gemaakt! Bedenk dat de ransomware eerst moet zijn verwijderd voordat je de bestanden terugplaatst, bijvoorbeeld door Windows opnieuw te installeren.

3 Windows back-up terugzetten
Geen back-up gemaakt? Dan is er een kleine kans dat Windows een automatische back-up heeft gemaakt. Rechtsklik op een bestand of map > Eigenschappen > tabblad 'Vorige versies'. Kijk of er een oudere versie staat die hersteld kan worden.

4 Losgeld betalen
Zijn de bestanden erg belangrijk voor je, dan kun je overwegen losgeld te betalen. Ervaringen tonen aan dat slachtoffers de sleutels vaak krijgen, maar er is geen garantie.

HOE HERKEN JE EEN NEPMAIL? LEES HET ARTIKEL OP PAGINA 34.

Sleutel

Het heeft me uiteindelijk twee dagen gekost om veel bestanden weer terug te krijgen. Van sommige bestanden kom ik er pas achter dat ik ze echt kwijt ben als ik ze nodig heb. Op dat moment baal ik weer even dat ik erin ben getrapt.

Inmiddels is het een half jaar geleden dat mijn laptop werd gehackt. Stilletjes hoop ik dat er binnenkort een sleutel wordt ontwikkeld waarmee ik mijn laptop alsnog kan ontgrendelen.' ●

In software worden regelmatig lekken ontdekt die kunnen worden misbruikt. Daarom is het belangrijk dat Windows en andere programma's up-to-date blijven. Lees de 5 tips.

Software updaten

TIP #1

CHECK DE WINDOWSUPDATES

Windows staat standaard ingesteld op het automatisch downloaden van nieuwe updates en het installeren hiervan. Je kunt zelf ook de instelling controleren.
Windows 7: Klik op *Start* > Typ in het zoekvak '*Windows Update*' > Klik op *Windows Update*.
Windows 10: klik linksonder op het vergrootglas > Typ '*Windows Update*' > Klik op '*Instellingen voor Windows Update*' en controleer of er in het scherm staat '*Beschikbare downloads worden automatisch gedownload en geïnstalleerd*'.

Java en Flash zijn technieken die kunnen worden misbruikt, dus die kun je beter uitzetten.

TIP #2

SCHAKEL JAVA EN FLASH UIT

Sommige websites en programma's gebruiken de kwetsbare technieken Java en Flash. Die worden veel misbruikt en kun je beter standaard uitzetten.

Java wordt nog maar gebruikt door weinig websites. Schakel het uit (*Configuratiescherm* > *Java* > tabblad *Security* > vink het vakje '*Enable Java content in the webbrowser*' uit) of verwijder het helemaal (*Configuratiescherm* > *Programma's en onderdelen*).

Flash is soms nog wel nodig. Zorg in elk geval dat Flash-elementen in webpagina's alleen afspelen met je toestemming. Bekijk op consumentenbond.nl/flash hoe je dat doet, of gebruik een adblocker.

WEETJE

Vrouwen stellen updates vaker uit dan mannen (62% tegen 49% doet dit weleens)

TIP #3

GEBRUIK EEN UPDATETOOL

De **Kaspersky Software Updater** (http://free.kaspersky.com/nl) is een handig programma om te controleren of er verouderde software op je pc staat. Dit programma kan ook updates voor deze programma's laten installeren.
Hoe? Bekijk onze video: consumentenbond.nl/videokasperskyupdater

NINITE

Op Ninite.com staat veel nuttige software die je veilig kunt downloaden.

TIP #4

VERWIJDER ONGEBRUIKTE EN KWETSBARE SOFTWARE

Elk programma op je pc is een mogelijke toegangspoort voor hackers. Verwijder daarom software die je niet (meer) gebruikt. Dat doe je zo: **Windows 7:** *Start* > *Configuratiescherm* > *Een programma verwijderen* > kies het programma uit de lijst, rechtsklik op *Verwijderen*.

Windows 10: *Start* > *Instellingen* > *Systeem* > *Apps en onderdelen* > kies het programma uit de lijst, klik op *Verwijderen*. > *Verwijderen*.

Tip: in **Adobe Reader** worden vaak lekken ontdekt. Vervang die door een andere gratis pdf-lezer, zoals Foxit Reader (foxitsoftware.com) of Sumatra PDF reader (sumatrapdfreader.org).

TIP #5

SCAN DE PC MET SCANCIRCLE

De Kaspersky Software Updater is een prima tool, maar vindt niet alle verouderde software. Daarom raden we aan om daarnaast ook af en toe een scan te doen op www.scancircle.com/nl. Deze online tool werkt prima en doet een uitgebreide scan. Het ziet er wel rommelig uit en je moet nog zelf de software updaten. Download de software met de knop 'Direct scannen', druk op Uitvoeren en je krijgt een webpagina met resultaten. Links, onder 'Software', zie je bij 'Software updates' welke programma's moeten worden bijgewerkt.

MAC-TIP

Zijn er updates? Open de App Store en klik op Updates op de knoppenbalk

HOE ZIT HET MET DE MAC?

Het installeren van updates voor MacOS en andere software voor de Mac doe je via de App Store. Bij programma's die niet via de App Store worden aangeboden, moet je zelf controleren of er updates zijn. Dat kan meestal door linksboven te klikken op de programmanaam en dan op 'Over dit programma'. Sommige programma's updaten zichzelf, zoals Firefox en het mailprogramma Thunderbird.

7 DO'S & DON'TS

Veilig software downloaden

WEL
Kiezen voor aangepaste installatie. Met de standaardinstallatie kan er ongewenste software meekomen zoals werkbalken in de browser. Let goed op elk vinkje dat langskomt.

WEL
Download de software via Ninite. Ninite is een verzamelsite met veel software. Daar kun je software met een gerust hart downloaden.

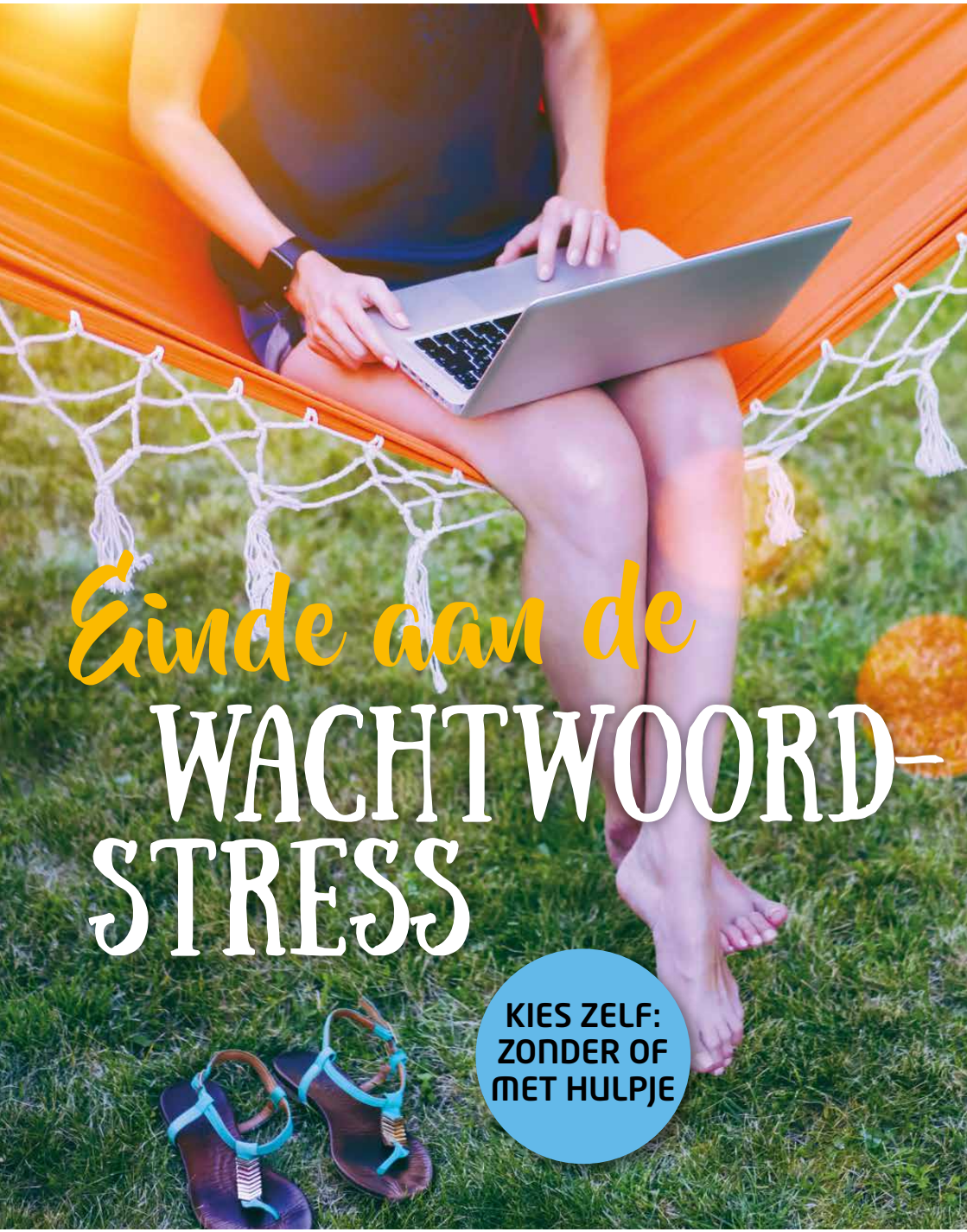
WEL
Download Unchecky. Dit hulpje waarschuwt als er bij het installeren van software ook foute **software meekomt. unchecky.com.**

NIET
Klikken op de grootste downloadknop. Veel sites misleiden je met grote knoppen die naar andere software en websites leiden. Zweef met de cursor boven de knop en kijk waar de link heengaat.

NIET
Online 'probleemoplossers' downloaden. Soms duikt ineens een foutmelding op dat je pc fouten of virussen bevat. Vaak is dat een websiteplaatje vermomd als foutmelding. Klik je, dan installeer je juist foute software. Niet doen dus!

NIET
Downloaden via Google. Het bovenste resultaat in Google is vaak een nepversie. Download software direct van de site van de maker zelf.

NIET
Gratis muziek, films of songteksten. Juist dan kom je vaak uit bij schimmige sites met een reële kans dat je troep binnenhaalt.



Einde aan de WACHTWOORD-STRESS

KIES ZELF: ZONDER OF MET HULPJE

WACHTWOORDEN IN DE BROWSER?
Misschien denk je: de browser vraagt toch ook al 'wachtwoord onthouden?' Dat lijkt ideaal, maar is beperkt en vaak helemaal niet veilig. Gebruik dus liever een wachtwoordmanager.

Het is bijna ondoenlijk voor elke site een ander, goed wachtwoord te bedenken én te onthouden. Maar met tools en trucjes kom je een heel eind.

Ga er maar aan staan. Maar liefst 22 wachtwoorden moeten we gemiddeld onthouden, blijkt uit onderzoek. En die moeten ook nog eens makkelijk te onthouden zijn door jouzelf, maar niet te raden of te kraken door anderen. Dat is niet te doen, toch? Logisch dat veel mensen dan toch maar kiezen voor Loes123 of Jan1960.

Gelukkig zijn er vrij eenvoudige oplossingen die je helpen om toch goede wachtwoorden te maken. De eerste is technisch: gebruik een wachtwoordmanager. Wil je dat niet of heb je een goed geheugen: verzin dan met onze truc sterke wachtwoorden die je wél kunt onthouden.

OPTIE #1

ZELF BEDENKEN

Wachtwoorden bedenken die voor jou makkelijk te onthouden zijn maar voor anderen niet te raden, hoe doe je dat? De truc: gebruik één sterk wachtwoord en plak daar steeds iets anders aan vast. We leggen het uit:
1. Verzin een sterk **basiswachtwoord**. Dat hoeft echt niet uit allemaal gekke tekens te bestaan. Hoe langer het woord, hoe minder rare tekens nodig zijn. Dat doe je met een wachtzin als 'IkHeb100Fietspompen' of '131KilometerIsTeSnel'. Die is ook beter te onthouden. Zorg dat je geen persoonlijke info in het wachtwoord stopt die makkelijk is op te zoeken, zoals je geboortedatum.
2. Gebruik de **naam van de website** voor het tweede deel: Bijvoorbeeld de tweede en voorlaatste letter van de website. Bij Facebook wordt dat ao. Nog beter: schuif de letters een plek op in het alfabet. Ao wordt dan bp.
3. Plak deel 1 en 2 aan elkaar: Voor Facebook wordt het: IkHeb100Fietspompenao.
Zo heb je één wachtwoord met talloze variaties.

OOK TIPS VOOR STERKE WACHTWOORDEN?
DEEL ZE OP CONSUMENTENBOND.NL/COMMUNITY/WACHTWOORDTIPS

LASTPASS

1. Ga naar **lastpass.com/download**. Klik op **Download**.
2. Klik op het installatiebestand en volg de instructies.
3. Kies **Maak een nieuw account**.
4. Vul je mailadres in en kies een ijzersterk hoofdwachtwoord. Dit is het enige wachtwoord dat je straks nog hoeft te onthouden. Zorg dat je dit wachtwoord niet vergeet!
5. Open de internetbrowser. De browser vraagt of hij de LastPass-uitbreiding mag installeren en inschakelen. Als dat klaar is, zie je rechtsboven in de browser het LastPass-icoontje, een rode knop met drie witte bolletjes.
6. Vanaf nu kijkt LastPass mee en helpt het je bij het inloggen. Hij vraagt standaard een keer in de twee weken om het hoofdwachtwoord, maar dat kun je aanpassen.

LastPass •••|

OPTIE #2

WACHTWOORD-MANAGER

Een hulpje dat al je wachtwoorden voor je onthoudt en ze invult op het moment dat je ze nodig hebt. Wie wil dat niet? Het mooie is: zo'n hulpje bestaat en is nog gratis ook.
Het werkt als volgt. Je downloadt een programmaatje (extensie) voor je internetbrowser. Als je dan op een nieuwe website, zeg bol.com, een wachtwoord moet invullen, onthoudt hij dat – of hij verzint zelf een sterk wachtwoord voor je. De volgende keer op bol.com vult hij dat wachtwoord voor je in. Zelf hoef je vanaf nu alleen nog maar het wachtwoord van de wachtwoordmanager te onthouden.
Uit onze laatste test kwam LastPass als de beste gratis optie uit de bus. Hij werkt op de pc, Mac en mobiel.

MEER WETEN OVER WACHTWOORDMANAGERS?
CONSUMENTENBOND.NL/WACHTWOORDMANAGERS

GEBRUIK TWEETRAPSAUTHENTICATIE
Bij veel websites, maar ook bij e-mail en WhatsApp, kun je instellen dat je na het invullen van je wachtwoord nog een extra beveiliging moet gebruiken, vaak een code die je via sms of app op je telefoon krijgt. Doe dit vooral! Het maakt hacken praktisch onmogelijk, en je ziet het meteen als een hacker probeert in te loggen.

ONTDEK DE DIGITAALGIDS MET 35% KORTING

Met de slimme tips en trucs uit de Digitaalgids maak je optimaal gebruik van je pc, tablet of smartphone.

Ga naar **consumentenbond.nl/digitaalgids**

NU 6 X VOOR €22,75

consumentenbond.nl/digitaalgids

BN'ER IN BEELD

Presentatrice en actrice, woont in Amsterdam met dochter Jacky (8)

EXPERT RONALD KAMP 'Een dubbele back-up van gegevens is verstandig. Zo heb je altijd een reservekopie, wat er ook gebeurt. Linkjes in mails check je het beste door er met je muis boven te zweven (pc) of het linkje ingedrukt te houden (mobiel). Goed dat je zoekt naar reviews. Reviews op de site van het bedrijf kunnen nep zijn, kijk dus ook op andere sites.'

MARIT VAN BOHEMEN (45) OVER HAAR DIGITALE VEILIGHEID

Welke digitale apparaten gebruikt u? 'Een mobiele telefoon, een tablet, een Macbook en een Windows-pc.'

Windows is gevoeliger voor virussen en hackers dan Apple. Heeft u daar ooit last van gehad? 'Ja, ik heb ooit op mijn pc een mail met een virus aangeklikt. Die nepmails lijken soms zo echt. Ik kan begrijpen dat je er op een onbewaakt moment op klikt. Mijn pc is toen gecrasht. Al mijn werk stond erop en ik had geen back-up! Een computerexpert heeft een deel van mijn harde schijf kunnen redden, maar ik ben ook veel kwijtgeraakt. Zoals foto's van een periode uit mijn leven en schrijfwerk. Daar baal ik enorm van. Ik heb de harde schijf bewaard in de hoop dat er in de toekomst een oplossing komt om hem te ontgrendelen. Gelukkig ben ik nog nooit gehackt. Het lijkt mij heel naar als bijvoorbeeld je Twitter-account wordt gehackt en dat onbekenden onder jouw naam dingen de wereld in schrijven.'

Maakt u nu wel regelmatig een back-up? 'Ja, na die ervaring maak ik regelmatig een back-up van al mijn gegevens en bewaar ik mijn data in de cloud. Mail van bedrijven en organisaties check ik voortaan door op de afzender te klikken. Daaraan kun je vaak al zien of het nep is.'

Hoe gaat u om met uw wachtwoorden? 'Voor accounts die ik niet vaak gebruik maak ik regelmatig nieuwe wachtwoorden aan. Ik kan ze niet allemaal onthouden en opschrijven is ook niet slim. Voor de accounts die ik regelmatig gebruik heb ik ingewikkelde wachtwoorden bedacht. Die wijzig ik nauwelijks.'

Bent u ooit opgelicht op internet? 'Ja, ik heb online een lamp gekocht die nooit is aangekomen. Via Marktplaats belandde ik op de site van een bedrijf. Het zag er allemaal professioneel uit. Toen ik echter belde en mailde waar mijn bestelling bleef, kreeg ik geen gehoor. Ik let nu extra goed op als ik iets via internet koop. Zo kijk ik bijvoorbeeld of er positieve reviews zijn van klanten. Pas wanneer je een virus krijgt of wordt opgelicht, besef je de risico's die je op internet kunt lopen.'

TEKST: ESTHER DERKS FOTO: MIEKE MEESEN

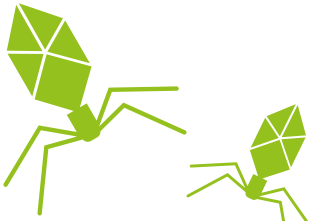
VIRUSSCANNER gratis of betaald?

KIES UIT DEZE 4 OPTIES

Een virusscanner is nog altijd onmisbaar op de Windows-pc. Heb je genoeg aan de ingebouwde scanner of moet je nog iets installeren? En moet je daarvoor betalen?

Een virus op de computer is de nachtmerrie van elke computergebruiker. Zo'n kwaadaardig programmaatje kan de computer laten vastlopen, persoonsgegevens doorspelen of – op dit moment een ware plaag – bestanden op slot zetten en pas na betaling vrijgeven (dat heet ransomware; lees het artikel op pagina 6).

Natuurlijk is voorkomen beter dan genezen. Maar gaat het toch mis, dan is het wel zo prettig als je een virusscanner hebt die aanslaat bij ongewenste indringers. Maar ja, welke moet je dan kiezen? We zetten de opties op een rij.



OPTIE 1

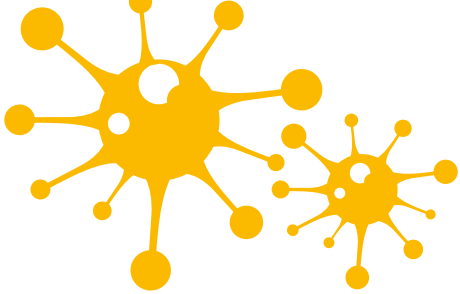
De ingebouwde virusscanner

Bij Windows 8 en 10 krijg je van Microsoft standaard het programma Windows Defender. Dat houdt ook virussen tegen, dus is dat niet voldoende? Laten we zeggen: het is een stuk beter dan niks. Maar er zijn zeker scanners, gratis en betaald, die meer virussen tegenhouden. Voor Mac-gebruikers hebben we goed nieuws: de ingebouwde beveiliging van Apple-computers is wél goed genoeg.

Windows Defender is een stuk beter dan niks, maar er zijn scanners die veel meer virussen weten tegen te houden.

NIET VERLENGEN!

Heb je een betaalde virusscanner en verloopt het jaarabonnement binnenkort? Ga dan niet zomaar in op het standaard verlengingsaanbod. Vaak is het voordeliger de software opnieuw te kopen. Koop je rechtstreeks van de fabrikant, schakel dan 'automatisch verlengen' uit. Als je het hebt gekocht met je creditcard, staat dat vaak standaard aangevinkt.



OPTIE 2

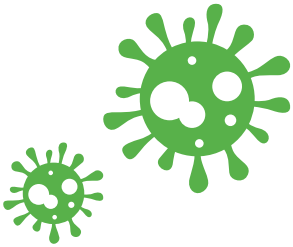
Een gratis virusscanner

Waarom betalen als het ook gratis kan? Veel mensen hebben op hun computer een gratis virusscanner van een van de '3 A's': AVG, Avast of Avira. En sinds kort is er ook het gratis Sophos Home. Uit onze test blijkt dat sommige gratis virusscanners het heel aardig doen. Die van AVG en Avira geven we zelfs het predikaat 'beste koop' (toegegeven: een beetje gek voor iets dat gratis is). Maar, voor niets gaat de zon op: de makers willen graag dat je de betaalversie koopt. Ten eerste moet je op de website goed zoeken naar de gratis versie. En daarna krijg je met regelmaat reclame voor de betaalversie. Irritant is ook dat ze je browser aanpassen met een andere startpagina of een prijsvergelijker. Dat kun je wel weer ongedaan maken, maar toch. O ja, ze verzamelen ook nog eens (geanonimiseerd) veel informatie over je surfgedrag. Dat je het weet.

OPTIE 3

De gratis scanner van de internetprovider

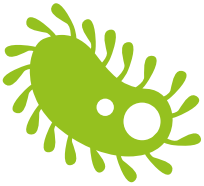
Bij grote internetproviders als KPN en Ziggo kun je een gratis virusscanner nemen. KPN noemt het 'KPN Veilig' en Ziggo 'Internetbeveiliging Basis', maar het is gewoon het pakket van F-Secure, en dat hebben we ook getest. Conclusie: het werkt even goed als de beste gratis scanners, maar minder goed dan de beste betaalde.

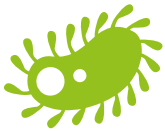


IS HET EEN VIRUS OF NIET? DOE DE CHECK OP VIRUSTOTAL.COM

Vertrouw je een bestand of website niet? Stuur het bestand naar virustotal.com. Deze site checkt of het malware bevat, waarbij tientallen (online) scanners worden geraadpleegd. Let op, Virustotal geeft alleen aan of er malware is aangetroffen, niet of bijvoorbeeld een programma goed functioneert of een website malafide is. De gevaarlijkste virussen worden hier nagenoeg altijd opgemerkt, maar de site scant slechts en verwijdert een virus niet.

Elk jaar blijkt uit onze test weer dat de beste scores worden gehaald door betaalde software





OPTIE 4

Een betaalde virusscanner

Is er dan wel een reden om toch geld uit te geven aan een virusscanner? Zeker. Elk jaar blijkt uit onze test weer dat de beste scores worden gehaald door betaalde software. Maar: niet elk pakket dat geld kost is goed. Sommige grote namen scoren slechter dan de gratis software – soms zelfs nog slechter dan wat er al in Windows zit.

Heel duur hoeft een virusscanner trouwens niet te zijn. De testwinnaar kost een paar tientjes per jaar. En als je een beetje zoekt, vind je vaak ook nog een actie met 50% korting.

BESTE KOOP

AVG ANTIVIRUS FREE
Dit pakket weet gijzelsoftware verrassend goed te weren en scoort mede daardoor vrij goed op bescherming tegen kwaadaardige software. In sommige browsers past AVG ongevraagd de zoekmachine en startpagina aan.

AVIRA FREE ANTIVIRUS
beschermt de pc beter dan Windows Defender en sommige betaalde pakketten. Het is net wat prettiger in het gebruik dan AVG. Schakel wel tijdens de installatie de volstrekt onnodige SafePrice-browseraanvulling uit.

BESPAARTIP: PAKKET ZONDER FIREWALL

Bij veel virusscanners kun je kiezen tussen alleen een virusscanner kopen of een duurder 'internet security'-pakket. De belangrijkste extra daarin is de firewall. Een firewall is een soort douanier die al het inkomende en uitgaande verkeer checkt op verdachte kenmerken. Maar uit onze test blijkt dat die firewalls meestal niet beter zijn dan de firewall die al in Windows zit. Door alleen een virusscanner te kopen, bespaar je zo twee tientjes per jaar.

MEER WETEN? GA NAAR CONSUMENTENBOND.NL/VIRUSSCANNER VOOR MEER INFORMATIE EN BEVEILIGINGSTIPS

JAN DE HOOP (63) OVER ZIJN ONLINE VEILIGHEID

Welke digitale apparaten gebruikt u? 'Dat zijn er heel wat. Zoals een iMac, een iPhone, een iPad, het muzieksysteem Sonos en mijn digitale videocamera voor het maken van mijn vlog op YouTube.'

Als bekende Nederlander heeft u een groot netwerk. Hoe gaat u om met uw online veiligheid? 'Op Twitter heb ik bijna 180.000 volgers. Dat vind ik best een verantwoordelijkheid. Om te voorkomen dat mensen mijn account hacken, heb ik een extra wachtwoord aan mijn account gekoppeld via mijn mobiele telefoon.'

Heeft u ooit rare dingen meegemaakt op Twitter? 'Ik heb mazzel met mijn volgers. Een enkele keer ontstaat er discussie. Zoals de keer dat ik het niet vond kunnen dat een ambtenaar geen homostellen wilde trouwen. Gelukkig gaat zo'n discussie met een zeker respect. Er zijn nooit scheldpartijen. Bij sommige collega's van mij is dat wel anders.'

Hoe gaat u om met uw wachtwoorden? 'Op al mijn online apparaten zit een wachtwoord. Dit zijn ingewikkelde woorden. Ik wijzig ze nooit, al weet ik dat het beter is om dat wel te doen. Ik zou ze anders gewoonweg nooit kunnen onthouden. Mocht een apparaat worden gestolen, dan kan ik via een ander apparaat zien waar het zich bevindt.
En met een paar knoppen kan ik op afstand de inhoud van mijn iPhone wissen. Op mijn iPhone staan nogal wat nummers van bekende collega's. Die mogen niet in verkeerde handen vallen.'

Maakt u wel eens een back-up? 'In huis hebben we een apparaat dat automatisch een back-up maakt van alle veranderingen op de computer. Gelukkig ben ik niet in het bezit van filmpjes waarin andere mensen over me heen plassen.'

Bent u ooit slachtoffer geweest van digitale oplichting? 'Gelukkig niet. Ik klik ook nooit zomaar op een mail met onbekende afzender. Ik vind het wel een beetje dom als mensen zoiets openen. Daarbij heb ik de mazzel dat het op Apple-computers minder snel misgaat dan op Windows-computers.'

TEKST: ESTHER DERKS FOTO: KOEN VERHEIJDEN

Presentator van het RTL ontbijt-nieuws, woont in Radio Kootwijk met vriend Coen Lievaart (55), boxer Bob en hun kippen

EXPERT RONALD KAMP 'Prima dat Jan een lokale back-up heeft. Om geen gegevens te verliezen bij inbraak of brand, is het slim om ook nog een kopie elders te bewaren. Verder is het bij wachtwoorden vooral belangrijk dat ze sterk zijn en voor elk account verschillend. Dat is belangrijker dan ze steeds wijzigen. Heel goed om een extra inlog-wachtwoord in te stellen. Zo maak je het hackers een stuk lastiger. '

Wat moet je doen om veilig te zijn op internet? Dit zijn onze tien belangrijkste tips.

Veilig op internet

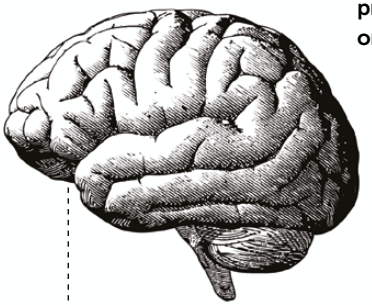
10 TI

1 SOFTWARE UP-TO-DATE

Hackers maken misbruik van mazen in software om je pc of telefoon binnen te dringen. Het kost weinig moeite om al je software bijgewerkt te houden. ➜ Lees het artikel op pagina 10.

3 ADBLOCKER

Adblockers blokkeren advertenties en volgcookies en dat is niet alleen goed voor je privacy, maar ook voor je veiligheid. Advertenties kunnen namelijk kwaadaardige software bevatten. Onze favorieten zijn uBlock Origin (alleen te installeren vanuit de internetbrowser) en de 'zelflerende' Privacy Badger van de Amerikaanse privacyorganisatie EFF (eff.org/privacybadger).



2 GEZOND VERSTAND

Klinkt als een open deur, maar o zo belangrijk: als iets te mooi lijkt om waar te zijn, is het dat meestal ook.

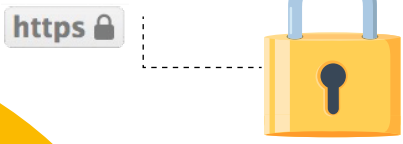
4 ANTIVIRUS-SOFTWARE

Niet zo belangrijk als goed opletten, maar als extra verdedigingslinie onmisbaar. Welke virusscanner moet je kiezen? ➜ Lees het op pagina 20.

TIP TOP-10

5 CHECK HET SLOTJE

Als je op een website gegevens achterlaat of moet inloggen, controleer dan altijd of het webadres met https begint en of er een slotje naast het webadres staat.



6 WACHTWOORDEN

Gebruik sterke wachtwoorden en/of gebruik een wachtwoordmanager. Spreekt voor zich. Hoe je dat doet? ➜ Lees het artikel op pagina 14.

7 TWEESTAPS-VERIFICATIE

Naast een sterk wachtwoord kun je bij veel webdiensten een extra controleslag laten uitvoeren, meestal met een code in een sms'je. Doe dit in elk geval bij cruciale diensten als Google, webmail, WhatsApp, Facebook, bankaccounts en DigiD.

8 NIET KLIKKEN

Klik niet zomaar op linkjes en bijlagen in mails. Criminelen sturen nepmails om je bankinloggegevens te kapen of je pc te gijzelen. ➜ Lees het artikel over phishing op pagina 34.

9 MAAK BACK-UPS

De laatste jaren is gijzelsoftware (ransomware) sterk in opkomst – zie ook het artikel op pagina 6. De gevaarlijkste variant versleutelt je bestanden. Kopieer je bestanden daarom regelmatig, zowel naar een externe harde schijf (koppel hem los als je hem niet gebruikt!) en naar een online-opslagdienst zoals Dropbox of Google Drive.

In Windows zit al back-upsoftware ingebouwd. Ga naar: *Instellingen* > *Bijwerken en beveiliging* > *Back-up*. Apples MacOS heeft een goedwerkende ingebouwde back-up functie.

10 NEPVIRUSMELDINGEN

Negeer spontane meldingen dat je pc virussen zou bevatten. Dat zijn vaak vensters in websites die eruitzien als een Windows-melding. Twijfel je? Open je virusscanner en kijk of er echt een melding is.

OPGELICHT OP MARKT-PLAATS

IK KON HET NIET loslaten

Michaja: 'Ik geef niet snel op en startte mijn eigen onderzoek'.

Michaja (40) werd opgelicht op Marktplaats. Ze liet het er echter niet bij zitten en ontmaskerde uiteindelijk zelf haar oplichter.

In 2015 ontving de politie 35.500 meldingen van internetoplichting

'Op Marktplaats vond ik de hoge laarzen waar ik al heel lang naar op zoek was. Binnen een uur kreeg ik reactie van de verkoopster en met een bedrag van €25 gingen we beiden akkoord.

De verzendkosten bedroegen €6,95. De verkoopster bood aan daarvan de helft te betalen. Dat vond ik aardig van haar en ik maakte het geld over via internetbankieren. Op mijn vraag of ze een Track & Trace nummer had, kreeg ik echter geen reactie. Zelfs niet nadat de leveringstijd van twee dagen was verstreken.

Ongerust keek ik of er nog andere advertenties van haar op Marktplaats stonden. Ze bleek ook een make-upset aan te bieden en ik reageerde daarop via een ander account, onder een andere naam, om te kijken of ze dan wel zou reageren. Nog steeds uitgaande van het goede, bedacht ik dat ze misschien erg druk was geweest.

Waarheid

Binnen een half uur reageerde ze al op mijn vraag over de make-up en vervolgens kreeg ik steeds vlot antwoord op verdere vragen. Ondertussen reageerde ze nog altijd niet op mijn vraag waar de laarzen bleven.
Ik stelde voor de make-up persoonlijk bij haar op te komen halen, zodat ik haar zou

10 TIPS VOOR MARKTPLAATS

1 Als iets te mooi lijkt om waar te zijn, dan is dat meestal ook zo.
2 Bekijk hoe lang de verkoper actief is op Marktplaats en check zijn andere advertenties.
3 Bel de verkoper, vraag naam en adres.
4 Google de gegevens van de verkoper
5 Check ook of de verkoper bekend is bij de politie: politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html
6 Wees alert bij kopers en verkopers in het buitenland. Gebruik geen anonieme betaalmethoden als Western Union.
7 Ophalen is veiliger. Het is verdacht als ophalen niet mogelijk is.
8 Als opsturen praktischer is, betaal dan liefst met PayPal. Je krijgt in veel gevallen het bedrag dan terug als de bestelling niet wordt geleverd.
9 Let extra op bij elektronica en tickets.
10 Stuur nooit een kopie van je identiteitsbewijs. Ook niet als de andere partij zelf eerst een kopie stuurt.

kunnen confronteren. Misschien bleek het allemaal een misverstand te zijn. Maar afspreken was geen optie voor haar, ze had echt geen tijd. Langzaam begon de waarheid tot me door te dringen. Ze zou me toch niet echt hebben opgelicht? Toen ik haar vervolgens zei dat ik naast de make-up ook graag de laarzen wilde hebben die ik bij haar had gekocht, viel het hele gesprek van haar kant stil. Wat ik ook stuurde, ze reageerde niet meer. Ik was woedend.

Vertrouwen

Mijn omgeving zei dat ik het moest laten gaan, maar ik kon het niet loslaten. Ik wilde niet dat iemand op die manier misbruik maakte van mijn vertrouwen.

Via mijn eigen account stelde ik haar een ultimatum. Als ze niet binnen een paar uur zou reageren, zou ik aangifte doen van oplichting. Een reactie bleef uit, dus deed ik digitaal aangifte bij de politie. Via Marktplaats kreeg ik vervolgens bericht dat ze haar account hadden gesloten op basis van meerdere meldingen. De politie stuurde mij een standaard ontvangstbevestiging dat ze geen strafrechtelijke procedure in werking gingen stellen, omdat ze prioriteit moesten stellen aan andere werkzaamheden. Gefrustreerd belde ik mijn bank, maar ook die kon mij niet helpen.

Via de bank

Daarmee was voor mij de zaak echter nog niet gesloten. Ik geef niet snel op en startte mijn eigen onderzoek. Op een website over oplichting kreeg ik de tip om een 0900-nummer te bellen waarmee ik met het rekeningnummer en de naam van de verkoopster de vestiging van haar bank kon achterhalen. En dat lukte! Helaas bestaat dit telefoonnummer inmiddels niet meer.

Ik belde haar bank met een verhaal dat ik via Marktplaats een aankoop had gedaan en per ongeluk geld had overgemaakt naar de verkeerde verkoper, doordat ik zat te twijfelen tussen twee aanbieders van hetzelfde product. Ik legde uit dat ik geen internet meer had en haar dus geen bericht kon sturen. Haar telefoonnummer mochten ze mij niet geven. De bankmedewerker zei dat hij contact op zou nemen met de verkoopster. Daar moet de verkoopster van zijn geschrokken, want de volgende dag stond het geld weer op mijn rekening! Wat was ik opgelucht!

Ik ben hierdoor voorzichtiger geworden met spullen kopen op internet. Gelukkig gaan mijn aankopen op Marktplaats meestal goed. Toch probeer ik voortaan zoveel mogelijk persoonlijk langs te gaan bij mensen om het product op te halen. Ook betaal ik het liefst contant, want dat is uiteindelijk toch het veiligst.' ●

TIP

Stuur nooit een kopie van je identiteitsbewijs

Apps die het leven leuker maken

Shoppen en betalen, uit eten of je sportprestaties bijhouden? Er zijn talloze apps die je hierbij helpen. Het boek De beste gratis apps bevat onze topselectie van zo'n 150 apps.

consumentenbond.nl/debestegratisapps

Leden €20,50, niet-leden €25. De verzending is gratis. Ook verkrijgbaar als voordelig e-book.

MARLAYNE SAHUPALA (45) OVER HAAR DIGITALE VEILIGHEID

Welke digitale apparaten gebruikt u? 'Een iPhone, Macbook en een iPad.'

Als bekende Nederlander heeft u een groot netwerk. Hoe gaat u om met uw online veiligheid? 'Ik zou wel wat beter op mijn veiligheid mogen letten, want ik blijf op mijn eigen computers vaak gewoon ingelogd. Puur uit gemakzucht, dan hoef ik niet iedere keer opnieuw in te loggen. In verkeerde handen kunnen mensen op die manier bij veel van mijn gegevens. Ik klik ook altijd op 'onthoud wachtwoord' [in de browser – red.]. Op mijn werkmail log ik heel bewust uit, daar staat al mijn SBS-mail in en ik vind het belangrijk dat dat goed beschermd is.'

Heeft u ooit rare dingen meegemaakt op social media? 'Ik gebruik Twitter, Instagram en Facebook. Soms schrijft iemand weleens iets raars, maar gelukkig zijn mijn accounts nooit gehackt. Wel verscheen er een keer onder mijn naam een nepaccount op Facebook. Dat was wel vervelend. Toen ik er melding van maakte, werd het gelukkig snel verwijderd.'

Hoe gaat u om met uw wachtwoorden? 'Ik wijzig zo nu en dan mijn wachtwoorden. Voor mijn werkmail krijg ik automatisch iedere drie maanden een melding dat ik hem weer moet veranderen. Anders zou ik het waarschijnlijk toch vaak vergeten.'

Maakt u weleens een back-up? 'Van de inhoud van mijn iPhone en laptop heb ik een back-up in iCloud. Ook heb ik thuis een externe hardeschijf waar regelmatig back-ups op worden gemaakt. Ik vind het een fijn gevoel dat mijn data ergens veilig is opgeslagen.'

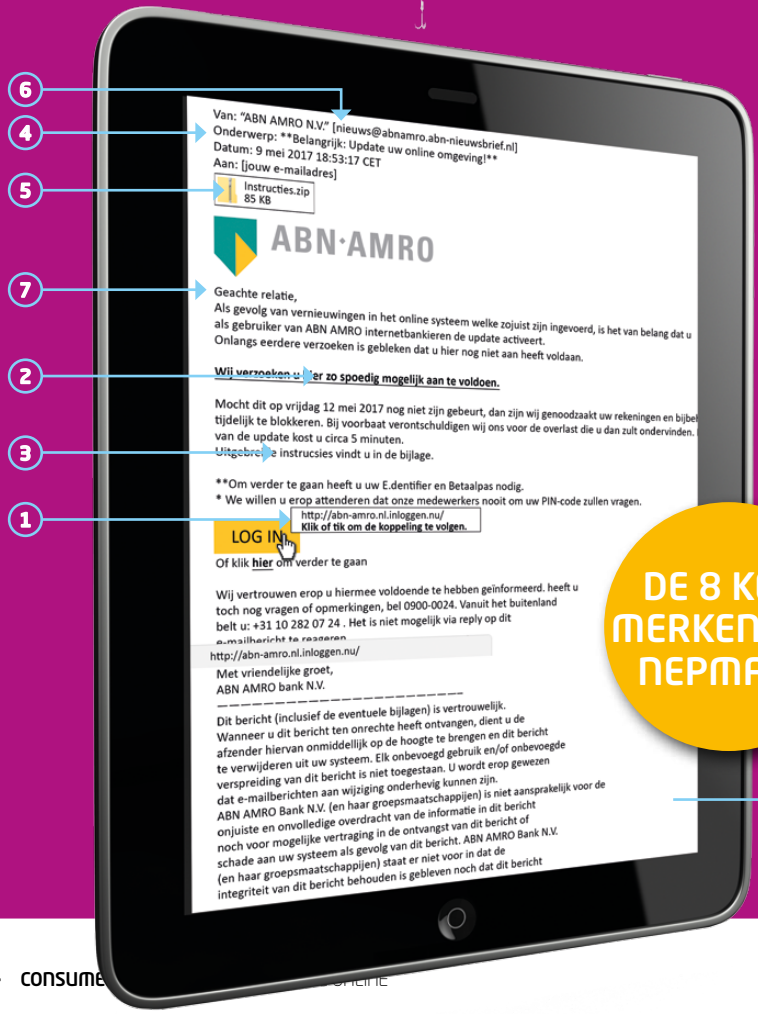
Bent u ooit slachtoffer geweest van digitale oplichting? 'Gelukkig niet. Ik heb sinds kort Marktplaats 'ontdekt' en vind het hartstikke leuk. Mijn moeder ging verhuizen en wilde van veel spullen af. Marktplaats bleek daarvoor ideaal. Ik ben meteen mijn zolder op die manier gaan opruimen. Al vind ik het niet prettig als mensen bij mij aan de deur komen. Ik wacht eerst tot het geld op mijn rekening staat en stuur het dan netjes op.'

TEKST: ESTHER DERKS FOTO: MIEKE MEESEN

Zangeres en SBS 6 presentatrice, woont in Hilversum met man Danny (56) en dochter Charlee (8)

EXPERT RONALD KAMP 'Met Apple-producten loop je minder risico op foute software. Wachtwoorden opslaan in de browser is niet zo'n goed idee, behalve bij Safari en Firefox, daar kun je een hoofdwachtwoord instellen. Een back-up online én op een externe schijf is verstandig. En op Marktplaats kun je inderdaad beter wachten tot het geld binnen is.'

Zó herken je een PHISHINGMAIL



DE 8 KENMERKEN VAN NEPMAILS

8 kenmerk 8 zit niet in deze mail

Met deze acht tips vis je de foute nepmails er moeiteloos uit.

MARKETINGMAILS LIJKEN VAAK OP PHISHING

Veel bedrijven laten hun nieuwsbrieven en reclamemails versturen door marketingbureaus. Dan staat er bijvoorbeeld als afzender kpn.client.mailplus.nl. Dat lijkt dus hartstikke nep, maar is het niet. Doe de quiz.

1 De foute link

Zweef altijd eerst met het muispijltje boven een link. Linksonder op het scherm verschijnt het webadres waarnaar de link gaat. Op je mobiel: laat je vinger rusten op de link. Het webadres verschijnt vervolgens in een venstertje. Oplichters kiezen vaak een link die sterk lijkt op het echte webadres. Een goed webadres bestaat uit de naam van het bedrijf met .nl of .com er direct achter, zoals kpn.com. Extra tekst vóór de bedrijfsnaam moet gescheiden zijn met een punt. Nepvarianten zijn login-kpn.com of kpn.nieuwsbrief.nl.

2 Gevoel van urgentie

Oplichters doen er alles aan om te voorkomen dat je de mail zomaar weg klikt. Daarom wordt er vaak op hoge toon gewaarschuwd: 'reageer binnen 24 uur, anders word je bankrekening geblokkeerd!'

3 Taalfouten

Het gros van de phishingmails bevat nog altijd taal- en/of typfouten.

Oplichters kiezen vaak een link die lijkt op het echte webadres, zoals login-kpn.com of kpn.nieuwsbrief.nl

PHISHINGMAIL ONTVANGEN?

Deel deze dan hier! consumentenbond.nl/community/phishingmails

4 Verdachte onderwerpen

Extra aandacht verdienen mails met onderwerpen als bankzaken, incasso's, (verkeers)boetes, vorderingen, facturen, (gemiste) pakketleveringen, printerscans en autoschademeldingen.

5 Kwaadaardige bijlage

Veel mailbijlagen van phishingmails bevatten malware. Dat is kwaadaardige software. Bestanden met extensie .zip, .exe of .js zijn verdacht als ze in een bijlage staan. Vervelend is dat Windows die extensies standaard verbergt. Let bij het openen van een Word-document vanuit je mail op of Word vraagt of hij macro's mag inschakelen. Niet doen.

6 Vreemde afzender

Een vreemd mailadres als afzender is vaak een aanwijzing voor phishing. Het deel achter het @-teken moet eindigen op de domeinnaam. Goed: nieuwsbrief@mail.ing.nl. Fout: nieuwsbrief@emaillogin-ing.nl. Let op: een goed uitziend mailadres geeft geen garanties.

DE 6 BELANGRIJKSTE SOORTEN PHISHING

PHISHINGMAIL VAN DE BANK

De 'klassieke' phishingmail, zogenaamd afkomstig van je bank. Op het eerste gezicht is er niets raars te zien, tot je het foute linkje ontdekt naar een nagemaakte bankpagina. Soms wordt er foute software op je pc gezet die je betaalopdrachten aanpast.

TELEFONISCHE PHISHING

Wie kent hem niet? De nepmedewerker van Microsoft die beweert dat je computer problemen heeft. Laat je hem meekijken op je pc, dan maakt hij je bang met onschuldige foutmeldingen of blokkeert hij je bestanden. En dan is het betalen geblazen.

GIJZELSOFTWARE

Steeds meer nepmails hebben een kwaadaardig bestand als bijlage die zogenoemde ransomware installeert – software die je persoonlijke bestanden versleutelt. Ineens staan al je foto's en documenten op slot, en moet je betalen om ze terug te krijgen. Zie ook het artikel op pagina 6.

7 Onpersoonlijke aanhef
Pas op bij een aanhef als 'Geachte klant'. Ook een persoonlijke aanhef is trouwens geen garantie voor een bonafide mail.

8 Fout rekeningnummer
Niet in onze voorbeeldmail: het foute rekeningnummer. Controleer nummers in mails op de echte website van het bedrijf. Gelukkig gaan banken, mede dankzij ons aandringen, bij overboekingen checken of een naam echt bij het rekeningnummer hoort.

De banken gaan, mede dankzij ons aandringen, checken of een naam bij het rekeningnummer hoort.

BIJ TWIJFEL KIJK OP INTERNET

Twijfel je of een e-mail echt is, kijk dan of je de mail tegenkomt op fraudehelpdesk.nl of opgelicht.avrotros.nl. Zo niet, check het dan een dag later nogmaals.

HERKEN JIJ DE PHISHINGMAIL?
DOE DE TEST OP DOE DE TEST OP CONSUMENTENBOND.NL/ PHISHINGQUIZ.

WINACTIES
Op Facebook zie je vaak winacties die nep zijn, met teksten als 'Ontvang uw prijs'. Je hoeft alleen nog maar te klikken op een link of een nummer te bellen. Uiteindelijk beland je in een eindeloze telefonische quiz op een duur betaalnummer of zit je vast aan een duur sms-abonnement.

DATINGSITES
Verliefde mensen denken vaak niet meer helder, dat weten oplichters ook. Daarvan maken ze misbruik via datingsites en via Facebook. Het eind van het liedje is dat je 'geliefde' door een noodsituatie ineens tijdelijk zonder geld zit. Driemaal raden op wie hij of zij een beroep doet.

BEKENDE WIL GELD
De noodkreet van een bekende via Facebook, Twitter of WhatsApp. Of je geld wilt overmaken, bijvoorbeeld omdat hij of zij in het buitenland bestolen is. In werkelijkheid is zijn of haar account gehackt of is er een nieuw account aangemaakt met zijn of haar naam.

Beveilig je toestel met een pincode, wachtwoord of vingerafdruk. Kies liever geen patroon dat je met je vingers tekent, want dat is makkelijker te raden.

Veilig op de mobiel

Apps updaten

Het beste is om je mobiel zo in te stellen dat updates voor apps automatisch worden geïnstalleerd.
iOS: Instellingen > iTunes en App Stores > zet een vinkje bij Updates.
Android: open de Google Play Store-app > tik op menuknop (3 streepjes) > Instellingen > Apps automatisch updaten.

TIP: Elke app kan een lek bevatten. Verwijder daarom apps die je niet meer gebruikt.

NIEUWE TELEFOON? NIET TE OUD

Zoek je een nieuwe telefoon? Koop een (niet te oud) toestel waarvan je kunt verwachten dat het minimaal nog een paar jaar (veiligheids)updates krijgt. Als je deze updates niet meer krijgt, worden ook veiligheidslekken niet meer hersteld. Koop een iPhone 5S of hoger of een Android-toestel met versie 6 of hoger. Op consumentenbond.nl/smartphone zie je welke telefoons een recente versie hebben.

Heb je Android 4.3 of ouder? Gebruik dan niet de standaardbrowser

Hou je mobiel up-to-date

Als er een nieuwe versie beschikbaar is, krijg je automatisch een melding met de vraag of je die wilt downloaden en installeren. Check:
iOS: Instellingen > Algemeen > Software-update.
Android: Instellingen > Over de telefoon > Systeemupdates > hier verschijnt een melding als er een update beschikbaar is. Voor de zekerheid kun je via 'Controleren op updates' een extra check uitvoeren.

ANTIDIEFSTALTIP

Is je mobiel gestolen? Dan is het fijn als je hem op afstand kunt lokaliseren en kunt wissen. Zo zet je die functie aan:
iOS: Instellingen > iCloud > Zoek mijn iPhone > zet schuifje op Aan.
Android: via Mijn account (myaccount.google.com), onder Inloggen en beveiliging > Zoek mijn telefoon. Bij oudere telefoons moet je op de telefoon ook nog iets aanzetten.

GEEF APPS NIET TE VEEL RECHTEN

Veel apps willen in je telefoon kijken, zoals toegang tot je camera, adresboek en microfoon. Soms is dat totaal niet nodig, denk aan een zaklamp-app die je microfoon wil aanzetten. Zo regel je de rechten van elke app:

iOS: Instellingen > Privacy > tik op het onderdeel (bv. camera) en zet de schuifjes uit bij apps die geen toegang mogen.
Android: Instellingen > Apps > tik op het tandwieltje > App-machtigingen. Nu kun je per onderdeel regelen welke apps toegang krijgen.

Elke app kan een lek bevatten die hackers kunnen misbruiken. Verwijder daarom apps van je toestel als je ze al een tijd niet meer gebruikt.

Bescherm jezelf

Phishing, inbreuk op je online privacy, oplichting op Marktplaats. Zomaar een greep uit wat je kan gebeuren. Voel jij je nog veilig op internet? De Consumentenbond maakt zich hard voor een veilige online omgeving. Zonder invloed van bedrijven en de overheid. Steun ons in deze strijd.

Maak 2 maanden gratis kennis. Blijf je na die 2 maanden lid, dan betaal je €7,25 per maand. Opzeggen kan per maand.

consumentenbond.nl/lidworden