Inhoud

Voorwoord

Onlangs zat er een mailtje in de mailbox dat sterk leek op een e-mail van de Rabobank. Het logo klopte wel, maar de tekst luidde als volgt:

Geachte klant,
Na meerdere meldingen in uw bankmail omgeving te hebben ontvangen willen wij u erop attenderen dat u een derde partij gemachtigd heeft om periodiek geld van uw rekening af te schrijven. Deze afschrijving vindt morgen voor het eerst via een Europees incasso plaats. U ontvangt dit bericht zodat u kunt controleren of de afschrijving terecht is.

Nu hebben we geen rekening bij de Rabobank, dus wisten we meteen dat dit een *phishing*-mailtje was. Een mailtje dat vist naar bankgegevens. Daarnaast is het in rommelig – slecht – Nederlands geschreven. Wat is *meldingen in uw bankmail omgeving*? Het klinkt quasi-officieel en zo hopen de boeven dat je erin trapt. Je moet op een link klikken en dan gebeurt er iets. Iets, ja, maar wat? Daar gaan we écht niet op klikken. Misschien besmetten we onze computers wel met een virus, een Trojaans paard of vragen ze me om mijn inloggegevens van de bank. Daarvan is bekend dat je die nooit – we herhalen: nooit! – moet geven. Ben je geen klant van de Rabo, dan weet je meteen dat dit een vals e-mailbericht is. Hoe kun je dat zien als je wel een Raborekening hebt? Meestal kun je dat bekijken als je naar het

e-mailadres van de afzender kijkt. Dat is in dit geval **w214715@usm.edu**. De link waarop ze willen dat je klikt gaat naar *x.co*, een nogal duister adres. Beide hebben niets van het Rabo-site-adres in zich.

En zo krijgen we, jij en ik, elke dag wel van dit soort kwaadaardige mailtjes binnen. Om jouw computer schoon en veilig te houden en je te beschermen tegen dit soort gespuis, hebben we dit boek geschreven. We gaan het hebben over dit soort valse mailtjes, over wachtwoorden, wachtwoordmanagers, tweestapsverificatie enzovoort. Allemaal niet echt ingewikkelde dingen, maar wel belangrijk als je veilig online wilt blijven. Het boek is voornamelijk praktisch, geen gedoe met complexe technologie.

We realiseren ons best dat je online nooit écht veilig kunt zijn. Als iemand je per se wil hacken, lukt dat een beveiligingsdienst of goede hacker altijd wel. Maar we gaan de kat niet op het spek binden door de voordeur naar onze computers wijd open te zetten.

Hans Frederiks en Ronald Smit, juli 2018

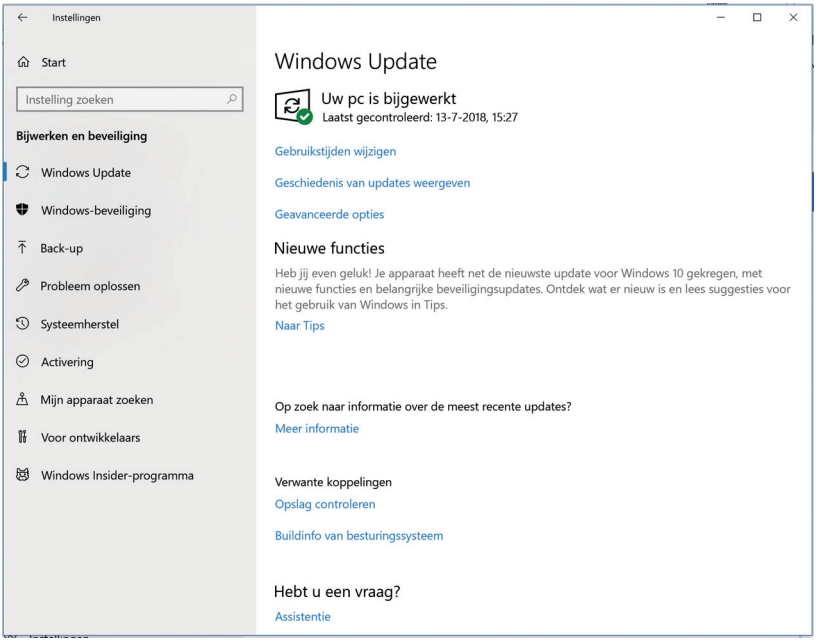
1

Niet paranoïde worden, maar blijf achterdochtig!

Dit boek bestaat uit een aantal hoofdstukken over specifieke onderwerpen: veilige wachtwoorden, tweestapsverificatie, updates van je apparaten, privacy, encryptie van je bestanden en beveiliging van je router en Wi-Fi-verbindingen. Waar het uiteindelijk om gaat is dat je eigen gegevens veilig zijn, dat je bestanden niet ineens gegijzeld worden. Of dat hackers niet bij je bankgegevens kunnen komen. Met jouw verbinding naar het internet sta je open voor die hackers, voor de overheid die misschien mee wil kijken met jouw internetgedrag. Je hoeft niet echt paranoïde te zijn of te worden, maar een gezonde dosis achterdocht kan geen kwaad.

Updates

Het besturingssysteem van het apparaat waar je op werkt – bijvoorbeeld een Windows-computer, een Macintosh, iPhone of Android-apparaat – is nooit echt honderd procent veilig. De makers van zo'n besturingssysteem hebben hun uiterste best gedaan om het veilig te maken, maar er zijn altijd 'hackers' die er zwakheden in vinden. Dat kan een 'goedwillende' hacker zijn die zo'n zwakheid meteen bij de makers van het besturingssysteem meldt. Het kan ook een kwaadwillende hacker zijn die ermee probeert jouw apparaat binnen te dringen. Als zo'n zwakheid wordt ontdekt zal de maker – Apple, Google, Microsoft – proberen die zwakheid te verhelpen. Het besturingssysteem krijgt een update.

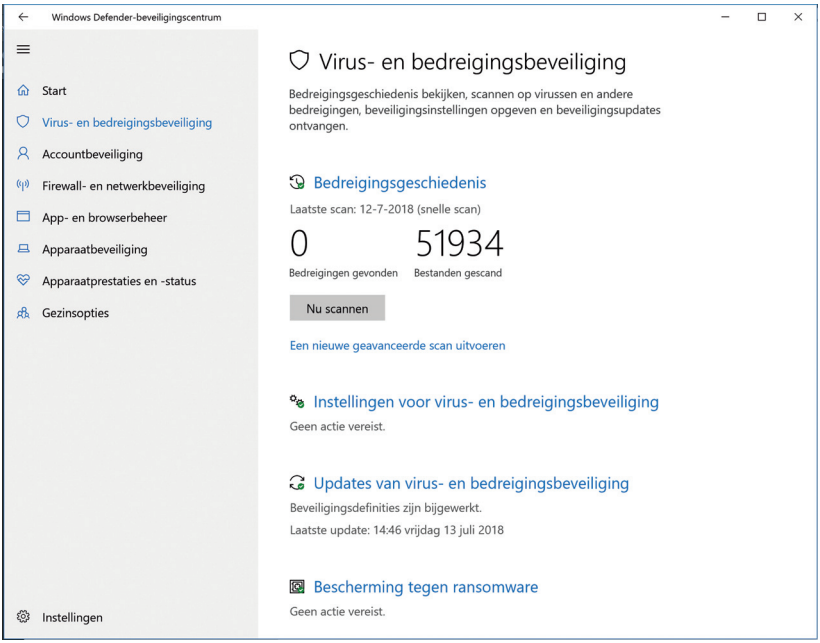


De Instellingen bij Windows 10 bij Windows Update.

Het is belangrijk om zo'n update meteen te installeren. Misschien heb je de neiging om een dergelijke update uit te stellen. Dat komt morgen wel, of overmorgen. Het is natuurlijk niet zo dat die kwaadwillende hacker meteen toeslaat en dan ook nog specifiek op jouw apparaat, maar je wilt niet dat je bestanden ineens gegijzeld zijn, omdat je die update niet hebt geïnstalleerd. Het kost misschien even tijd maar die updates zijn belangrijk. In hoofdstuk 5 van dit boek gaan we in op de verschillende manieren van updaten voor computer, telefoon en tablet.

Beveiligingsinstellingen

Moet je een virusscanner hebben op de Mac? Dat kan, maar hoeft afhankelijk van je gebruikersscenario niet per se. Voor Windows?



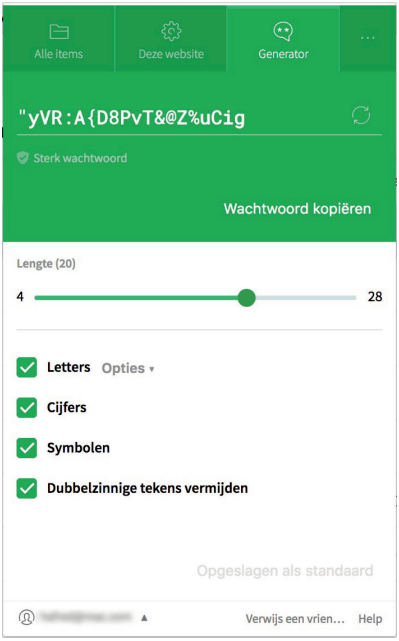
De Virus- en bedreigingsbeveiliging bij Windows 10.

Ja, daar staat er standaard al eentje aan: Windows Defender. En op een Android-apparaat? Dat ligt eraan of je je er veilig op gedraagt. Zet je een firewall aan op je computer? En ja, waarom doe je dat dan? Op een Windows 10-computer staat deze standaard aan, bij macOS niet. Je kunt je apparaten zo dichttimmeren dat je voor elke site die je bezoekt toestemming moet geven. Als je een site bezoekt, wordt er stevig heen en weer gecommuniceerd. Ha! Dit is die meneer/mevrouw die naar tuinstoelen zocht. Snel een advertentie zoeken van tuinstoelen. Dat is communicatie over en weer en als je software hebt die in de gaten houdt wat er allemaal naar binnen en buiten gaat, moet je misschien eerst toestemming geven of je die site wel mag bezoeken.

Wachtwoorden

Wachtwoorden… Wie heeft daar geen hekel aan? Het is niet voor niets dat er allerlei andere manieren worden bedacht om in te loggen op een apparaat, website of dienst. Inloggen met je vingerafdruk in de app van je bank. Inloggen met gezichtsherkenning op je telefoon, allemaal manieren om het inloggen eenvoudiger én veiliger te maken. Die kwaadwillende hackers zijn op zoek naar inlognamen en wachtwoorden om zo toch jouw bankrekening te kunnen plunderen. We zijn voorlopig niet van deze manier van inloggen af. Het is dus zaak om veilige wachtwoorden te gebruiken en voor elk apparaat, elke website of dienst een ander veilig wachtwoord te hebben.

Mensen hebben de neiging om eenvoudig te onthouden wachtwoorden te bedenken, wachtwoorden die je heel gemakkelijk kunt onthouden. En hebben ze een goed wachtwoord, dan gebruiken ze dat bij verschillende sites. Fout! Dus niet Fikkie12345 (naam van je huisdier met wat cijfers) maar een wachtwoord als *SC)8A57}.(-*&cGr!nHK*. En voor de volgende website gebruik je



Een veilig wachtwoord genereren met een wachtwoordmanager, in dit geval Dashlane.

"aZHAZJ_".]5[GH3raLR. Telkens een ander ingewikkeld wachtwoord dat voor een gewoon mens niet valt te onthouden. In het hoofdstuk over Wachtwoorden (hoofdstuk 2) behandelen we de wachtwoordmanager, de oplossing om voor elke site en dienst een uniek wachtwoord te gebruiken.

Tweestapsverificatie

Je kunt nog zulke prachtige en ingewikkelde wachtwoorden bedenken, als ze gestolen worden kan de dief ermee inloggen bij de site of dienst waar ze gestolen zijn. Als je hoort of leest dat zoiets gebeurd is bij een site die jij gebruikt, is het zaak om zo snel moge-

lijk je wachtwoord aan te passen. Misschien ben je net te laat en is er met jouw wachtwoord al ingelogd, heeft de dief jouw gegevens in kunnen zien en heeft het wachtwoord al zelf aangepast. Voor steeds meer sites en diensten kan tegenwoordig een extra beveiligingslaag aangebracht worden. Dat heet tweestapsverificatie.

Tweestapsverificatie bij je DigiD, via SMS of via een app op je telefoon. Dat is eenvoudig in te stellen en extra veilig.

Met tweestapsverificatie is naast het wachtwoord nog extra informatie nodig. Neem je bank, bijvoorbeeld ING. Je logt in met je inlognaam en wachtwoord, als je een overboeking doet moet er nog iets extra's ingevoerd worden. De aloude TAN-code was een voorbeeld van tweestapsverificatie, nu scan je een QR-code met jouw mobiele telefoon. Zonder die tweede stap kun je die betaling niet doen. Bij de bank is die tweede stap verplicht, maar bij Apple of Google heb je genoeg aan inlognaam en wachtwoord. Om die

accounts veiliger te maken kun je ook daar tweestapsverificatie instellen. Lees er alles over in hoofdstuk 3 en 4.

Privacy

Privacy is een hot item. Wat weten Google of Facebook over je? Of Microsoft? Leest Google je Gmail-berichten? Wat houdt Facebook precies over je bij? De berichten op WhatsApp zijn versleuteld, maar kan Facebook (tenslotte eigenaar van WhatsApp) ze misschien toch niet lezen? In de EU hebben we sinds mei dit jaar strenge privacywetgeving. Dat helpt natuurlijk voor het bewaren van die privacy, maar je zult zelf ook het een en ander moeten instellen.

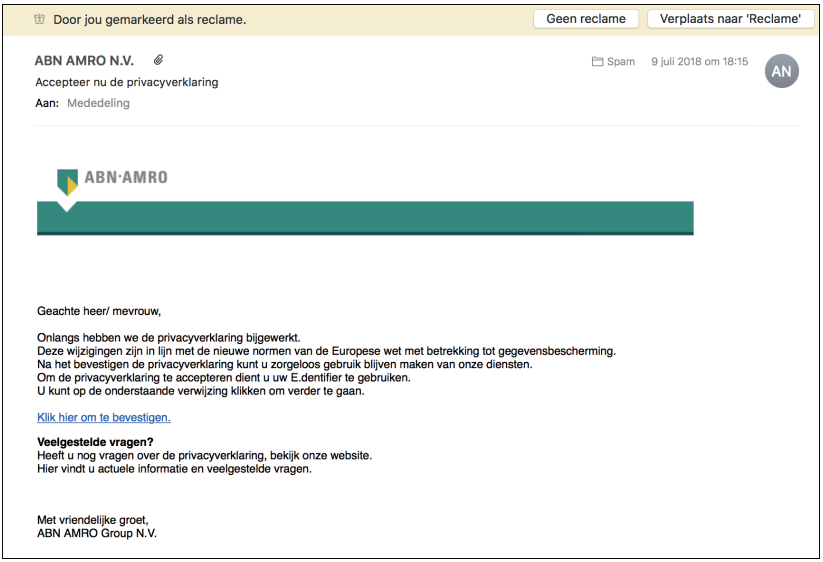
Je kunt bijvoorbeeld helemaal stoppen met Facebook, dan is je privacy vanaf dat moment veilig voor Facebook, maar dan mis je de onderdelen die wel leuk zijn van deze dienst. Je kunt Facebook ook zo instellen dat je zo weinig mogelijk informatie over jezelf prijs-

Het instellen van de privacy bij Facebook.

geeft. Datzelfde geldt voor instellingen bij Google, Microsoft en Apple. Hoe je dat doet lees je in hoofdstuk 9, dat privacy behandelt.

Phishing

Het internet is mooi, maar er liggen ook veel gevaren op de loer. Je klikt op een linkje in een e-mail en plotseling zijn al je bestanden gegijzeld. Of je maar even 500 euro in bitcoins wilt betalen voor het ontsluiten van je bestanden. In weer een ander mailtje vragen ze je je Rabobank-pas te recyclen en of je maar even je bankgegevens wilt invullen. En weer een ander mailtje heeft een virus op je computer geïnstalleerd, waarna je webcam meekijkt en al je toetsaanslagen worden opgeslagen. Onzin? Onmogelijk? Op een Windows-computer zonder update of virusbescherming is dit niet ondenkbaar.


Door jou gemarkeerd als reclame.

Geen reclame | Verplaats naar 'Reclame'

ABN AMRO N.V.

Spam 9 juli 2018 om 18:15

AN

Accepteer nu de privacyverklaring

Aan: Mededeling

ABN·AMRO

Geachte heer/ mevrouw,

Onlangs hebben we de privacyverklaring bijgewerkt.
Deze wijzigingen zijn in lijn met de nieuwe normen van de Europese wet met betrekking tot gegevensbescherming.
Na het bevestigen de privacyverklaring kunt u zorgeloos gebruik blijven maken van onze diensten.
Om de privacyverklaring te accepteren dient u uw E.dentifier te gebruiken.
U kunt op de onderstaande verwijzing klikken om verder te gaan.

Klik hier om te bevestigen.

Veelgestelde vragen?
Heeft u nog vragen over de privacyverklaring, bekijk onze website.
Hier vindt u actuele informatie en veelgestelde vragen.

Met vriendelijke groet,
ABN AMRO Group N.V.

Een phishingmail die je ABN AMRO-inloggegevens wil ontfutselen.

E-mails zijn een voortdurende bron van bedreiging en ellende. Je hebt natuurlijk de spam over middeltjes tegen nagelschimmel, mailtjes over Russische bruiden en Nigeriaanse geldbeloftes. Die zijn lastig, maar niet echt gevaarlijk. Zolang je geen trouwakte ondertekent, tenminste. De mailtjes met een verdachte link, dat zijn de gevaarlijke berichten. Een bericht van de Rabobank over een nieuwe pas schuif ik terzijde, ik heb geen rekening bij de Rabobank. Maar eentje van de ING? Die bekijk ik wat beter. Klopt het e-mailadres? Waar gaat de link naartoe? Zit er een verdachte bijlage in? Hoe je dat zelf kunt zonder meteen je computer te infecteren lees je in hoofdstuk 6.

Wi-Fi binnen en buiten de deur

Tegenwoordig gaan de meeste verbindingen via Wi-Fi en niet via een ethernetkabeltje. Wi-Fi, verbinding door de lucht. Als je kijkt hoeveel Wi-Fi-verbindingen er rondom je eigen huis zijn, weet je dat Wi-Fi de standaard is om je met het internet te verbinden. Hoe veilig is die verbinding? Kun je een verbinding maken met een ander netwerk uit de buurt, van iemand die zijn Wi-Fi niet goed heeft dichtgetimmerd? Hoe zit dat met je eigen netwerk? Heb je een gemakkelijk te kraken wachtwoord? Heb je de laatste firmware op je router geïnstalleerd? Die router van jouw internetprovider is de poort naar het internet. Naar buiten, maar ook naar binnen. Wat kun je daar aan- en uitzetten om het veiliger of onveiliger te maken?

En de Wi-Fi in openbare gelegenheden en op vakantie, in dat aardige koffiehuis of café? Wie kijkt er met je mee? Even een banktransactie in een café, omdat dat zo handig is? Dat kan, als je het veilig doet, met een VPN-verbinding. Over dit soort dingen gaat hoofdstuk 8 van dit boek.