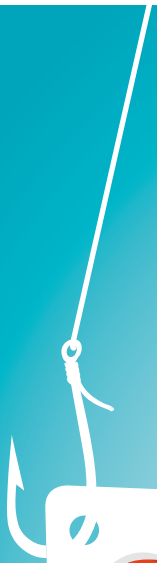


2 SURF BEWUST

Door alert te zijn bij het surfen op internet, is al een hoop ellende te voorkomen. Zo geef je fraudeurs geen kans en ben je criminelen die malware mailen, te slim af. In dit hoofdstuk onze tips.

consumentenbond

Het is belangrijk alert te zijn tijdens het surfen. Niet ieder mailtje is te vertrouwen. Dan hebben we het niet over ordinaire spam met reclame voor blauwe pillen. Die zijn vooral hinderlijk. Gevaarlijker zijn mailtjes met links naar malware, of lokformulieren om inloggegevens te stelen. Ook zijn er riskante websites die malware verspreiden.

2.1 Herken phishing

Phishingmails zijn ontworpen om de ontvangers om de tuin te leiden. Het begint met de afzender. Ze komen meestal van (zogenaamd) vertrouwenwekkende bedrijven en instellingen. Denk aan PostNL, Wehkamp, KPN, het Centraal Justitieel Incassobureau (CJIB) of de politie. Door het logo en de huisstijl te gebruiken, trachten de fraudeurs hun mails er echt uit te laten zien. Gelukkig zijn er bijna altijd wel aanwijzingen die ze verraden.

2.1a Onjuiste afzender

De afzender @icsmail.nl is niet correct

xavia.freemax.it/www.kpn.com/p

De afzender klopt. Toch is het phishing. Door de link te bekijken, wordt dat snel duidelijk

Eén van de hoofdkenmerken van een phishingmail is dat het mailadres van de afzender niet klopt. In het eerste voorbeeld eindigt het mailadres van de afzender op @icsmail.nl. Het correcte webadres van creditcardverstrekker ICS is icscards.nl. Het afzendadres is slim gekozen, want het lijkt op het echte mailadres. Het is niet zo dat een mail met een correcte afzender per definitie te vertrouwen is. Slimme hackers versturen phishingmails met een betrouwbaar uitziend verzendadres. In het tweede voorbeeld is een mail te zien met als afzender noreply@kpn.com. Het is phishing, ook al is het verzendadres correct.

© consumentenbond

2.1b Link klopt niet

In bijna alle phishingmails is een link te vinden die naar een namaaksite leidt. Daar staat een lokformulier klaar om gegevens in te vullen. Ook leiden ze soms naar een webpagina die malware probeert te installeren. Beweeg met de muis over een linkje om te kijken of die naar een correcte website leidt. Op de smartphone of tablet raak je de link lang aan. Er verschijnt dan een venster met het webadres. In de nepmail van KPN (zie de afbeelding onder par. 2.1a) leidt de link naar het webadres xavia.freemax.it. Foute boel dus. De fraudeurs hebben nog wel www.kpn.com achter het webadres geplakt om mensen op het verkeerde been te zetten. In de voorbeelden van KPN-phishing op de smartphone en tablet is te zien dat de link leidt naar een webadres dat begint met r1url.com; ook dat is incorrect.

Hoe herken je een betrouwbare link? Een webadres bestaat over het algemeen uit drie delen. Ze worden gescheiden door punten. Bij wijze van voorbeeld leggen we het uit aan de hand van de domeinnaam www.consumentenbond.nl. Daarin zien we drie onderdelen.

- *www* – Dit is het subdomein. Vaak wordt hier www gebruikt, maar dat hoeft niet. Wikipedia gebruikt subdomeinen voor de verschillende talen. Via nl.wikipedia.org kom je terecht op de Nederlandse versie, terwijl en.wikipedia.org naar de Engelstalige versie leidt. Sommige

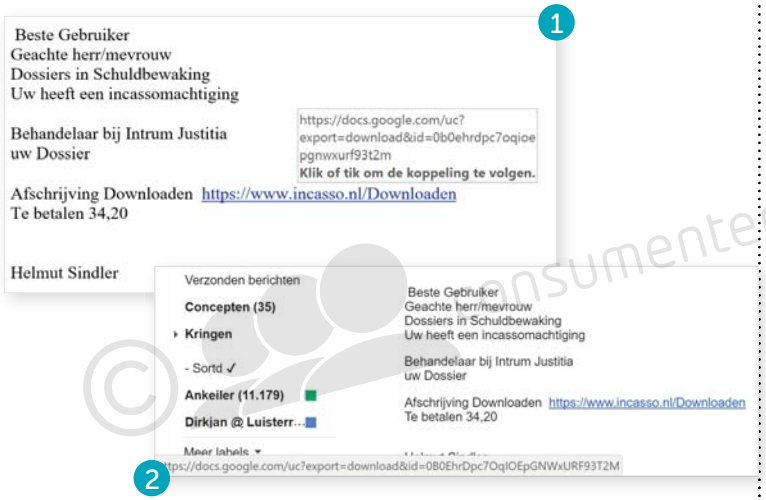
sites gebruiken de subdomeinen webshop, nieuwsbrieven of klantenservice. Zo zou je dus de fictieve domeinnamen webshop.consumentenbond.nl, nieuwsbrieven.consumentenbond.nl of klantenservice.consumentenbond.nl krijgen. Een domeinnaam kan meerdere subdomeinen bevatten. Denk aan nl.nieuwsbrieven.consumentenbond.nl om te verwijzen naar de Nederlandstalige versie van nieuwsbrieven, terwijl en.nieuwsbrieven.consumentenbond.nl naar de Engelse zou verwijzen.

- *consumentenbond* – Centraal in een webadres staat de naam van de organisatie. In vaktermen heet dit het secondleveldomein. Controleer altijd of dit goed is geschreven. Als er in een mail bijvoorbeeld www.deconsumentenbond.nl staat, is dat al reden tot twijfel. Deze naam moet altijd direct voor het topleveldomein staan (zie hieronder). Als de naam van de organisatie eerder in het webadres staat, klopt er iets niet. Een voorbeeld van een ondeugdelijk webadres is www.consumentenbond.website.nl. Daarbij is 'consumentenbond' het subdomein van website.nl. Je zit dus niet op de website van de Consumentenbond.
- *nl* – Dit wordt wel het topleveldomein genoemd. Nederlandse domeinen gebruiken .nl, terwijl in België .be wordt gebruikt. Internationaal is .com populair, maar ook .net of .org zijn gebruikelijk. Bijzonder zijn de topleveldomeinen die uit twee delen bestaan zoals .co.uk in het Verenigd Koninkrijk. Relatief nieuw zijn domeinnamen die eindigen op .eu of .biz.

Een domeinnaam kan maar één keer worden geregistreerd. Veel bedrijven registreren niet alleen de eigen bedrijfsnaam, maar ook namen die erop lijken. De Rabobank legt dus niet alleen rabobank.nl vast, maar ook derabobank.nl. Maar het is ondoenlijk om alle varianten vast te leggen. Daar maken criminelen gebruik van.
Dat het mogelijk is om een fout webadres te maskeren in een mail, maakt het extra lastig phishing te omzei-

© Consumentenbond

len. Iemand die een phishingmail verstuurt, kan de tekst rabobank.nl 'onder water' laten linken naar rabbobank.nl. Voordat je op een link klikt, moet je altijd controleren naar welk adres de link leidt.



1. In deze phishingmail lijkt de link te verwijzen naar incasso.nl. Op het eerste oog dus betrouwbaar. Maar wie met de cursor over het linkje gaat, ziet dat er wordt gelinkt naar een Google Docs-webadres.
2. Bij het gebruik van webmail verschijnt het echte linkadres niet in een soort pop-up, maar onderin de browser.

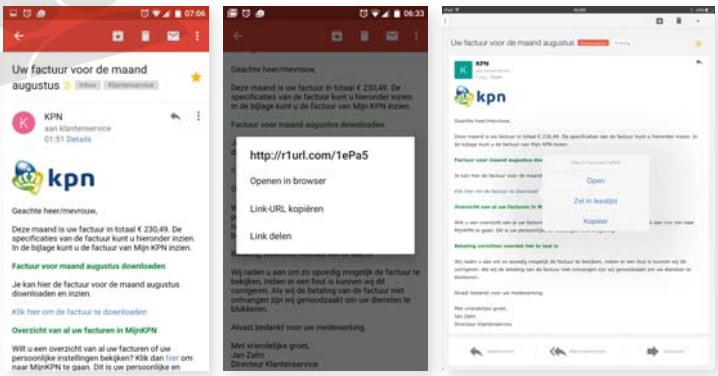
Let bij het beoordelen van een domeinnaam op deze zaken:

- *Is de spelling correct?* Wie een phishingmail ontvangt die naar consumenntenbond.nl verwijst, moet op zijn hoede zijn. Het is een onopvallende spelfout, maar de link zal hoogstwaarschijnlijk naar een onbetrouwbare website leiden. In phishingmails van banken wordt dit veel gebruikt. Er staat dan bijvoorbeeld een link naar rabbobank.nl.
- *Klopt de extensie?* Correct is consumentenbond.nl. Fout is consumentenbond.ru. Het is niet logisch dat een Ne-

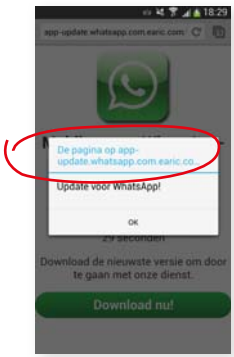
© consumentenbond

derlandse website de Russische extensie .ru gebruikt. Dit is reden voor alarmbellen.

- *Voor de domeinnaam mag extra tekst staan, maar alleen als deze van de rest is gescheiden door een punt*. Goed is dus login.consumentenbond.nl. Fout is login-consumentenbond.nl. In het laatste geval is 'login-consumentenbond' het secondleveldomein.
- *Achter de domeinnaam mag extra tekst staan, maar die moet zijn gescheiden door een of meer schuine strepen*. Ze staan direct achter .nl of .com. Een betrouwbaar webadres is consumentenbond.nl/nieuwsbrief/2016/11/04. Als er staat consumentenbond.nl.nieuwsbrief.webhostingxxs.org, is er iets mis.



Dit zijn KPN-phishingmails op iOS en Android. Op smartphones en tablets kun je het webadres van een link achterhalen door de tekst lang aan te raken



Valse systeemmelding

Phishing gaat niet altijd per mail. Een voorbeeld: tijdens het surfen op een Android-telefoon verschijnt er plots een schermpje met het verzoek WhatsApp te updaten. Het lijkt een systeemmelding, maar is feitelijk een advertentie. Wie erop ingaat, moet zijn telefoonnummer invullen en zit vast aan een duur sms-betaalabonnement. Vooral het webadres is verdacht: app-update.whatsapp.com.earic.com. De site earic.com heeft niets met WhatsApp te maken.

2.1c Onpersoonlijke aanhef

Criminelen hebben meestal alleen een mailadres, dus kunnen ze je niet persoonlijk aanspreken met voor- en achternaam. Dat is het volgende kenmerk van de phishingmail: een onpersoonlijke aanhef als 'beste klant'. In de KPN-mail op de vorige pagina is het duidelijk te zien: 'Geachte heer/mevrouw'. Ter vergelijking: in onderstaande afbeelding staat een echte mail van KPN, met een persoonlijke aanhef. Toch kan het bij een persoonlijke aanhef ook foute boel zijn. Zo werden in juni 2016 buitgemaakte gegevens van miljoenen LinkedIn-accounts gebruikt in een phishing-aanval. Om het nog lastiger te maken: sommige bedrijven sturen ook echte mail zonder persoonlijke aanhef.

Dit is geen phishing: alles klopt. Zowel de aanhef, de afzender als de link

2.1d Urgentie en dreiging

Urgentie uitstralen is een bekend drukmiddel om slachtoffers te laten reageren. Nepmails van banken dreigen met het blokkeren van de rekening, wat overigens ongeloofwaardig is. Ook de phishingmails van incassobureaus zijn dreigend van toon. Hetzelfde geldt voor de valse mails van het Centraal Justitieel Incassobureau (CJIB). Daarin krijgt de ontvanger meestal drie dagen de tijd om een nog uitstaande boete te betalen. Het CJIB verstuurt nooit een verzoek per mail om boetes te betalen.

Deze mail zet er flink druk achter: binnen drie dagen betalen

consumentenbond

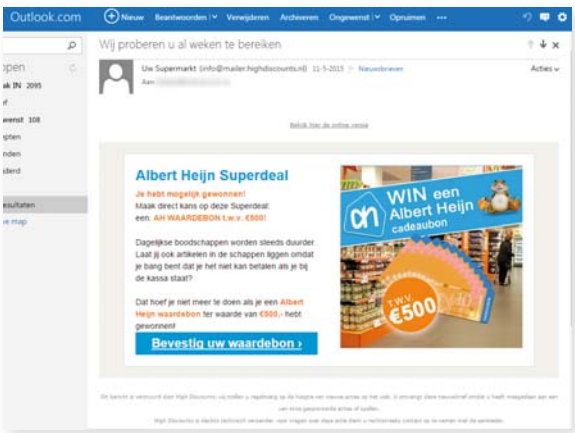
Check het rekeningnummer

Controleer of het IBAN-rekeningnummer correct is voordat u betaalt naar aanleiding van een mail. Daarmee ontdekt u snel dat het rekeningnummer in phishingmails uit naam van het CJIB niet klopt. Ook als een webwinkel een mail stuurt met het verzoek een bestelling te betalen, is het nuttig het rekeningnummer te controleren via een zoekopdracht bij Google. Als er criminelen achter zitten, is de kans groot dat u een vermelding aantreft. Staat het nummer correct vermeld op de (echte) site van de webwinkel, dan is het in orde.

© consumentenbond

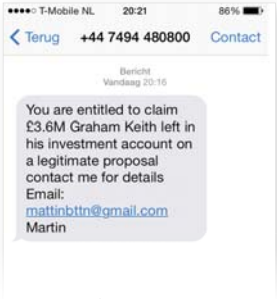
2.1e Onrealistische belofte

Er gaan veel mails rond waarin mooie prijzen worden beloofd. Vaak met namen van grote bedrijven om vertrouwen te wekken. In het voorbeeld zien we een nepmail van Albert Heijn waarin een waardebon van maar liefst €500 wordt beloofd. Om mee te doen wordt naar je naam, e-mailadres en telefoonnummer gevraagd. Daarna moet je een duur betaalnummer (90 cent per minuut) bellen en 300 (!) vragen beantwoorden. Reken op een forse telefoonrekening en geen waardebon. Bij veel van dit soort 'winacties' zit je ook vast aan een duur sms-abonnement.



Waardebon voor gratis boodschappen? Niet zo realistisch

Voorschotfraude (par. 1.3) komt ook voor op de mobiele telefoon. In de afbeelding hiernaast zien we een sms-bericht met de belofte van een erfenis van 3,6 miljoen pond. Klink aantrekkelijk, maar wie een bericht stuurt naar het genoemde e-mailadres krijgt gegarandeerd te maken met oplichting. Deze vorm van phishing gebeurt ook via WhatsApp.



Ook per sms komt voorschotfraude voor

2.1f Taalfouten

Het taalgebruik van de criminelen wordt beter, zoals te zien is in de nepmails van KPN en het CJIB. Maar we komen nog steeds voorbeelden tegen vol taalfouten. In de afgebeelde ING-mail wordt gesproken van 'malide functies'. Het mailtje adviseert 'uit beveiligingsmaatregelen' een nieuwe pas aan te vragen. Dat moet de 'malfunctie' oplossen waardoor betalingen 'dubbel worden verrekend'. Duidelijk, nietwaar?

2.1g Mail met bijlage

Ook mails van bedrijven waaraan een bijlage is toegevoegd, komen we veel tegen. Die bijlage bevat een kwaadaardig programma of besmet Office-document. Het kan bijvoorbeeld gaan over een onbetaalde rekening. In de afbeelding is een mail te zien over een boete. Hij lijkt behoorlijk echt, inclusief logo van de Rijksoverheid. Het CJIB mailt zogenaamd over schade

Open de bijlage

Nooit de bijlage openen!

© coachingintenbonne

veroorzaakt met de auto. In een bijlage zou een foto te zien zijn. Open zo'n bijlage nooit en bedenk dat het CJIB nooit mailt over dit soort zaken. De laatste tijd zijn phishingmails populair over een mislukte levering van een pakketje door bijvoorbeeld DHL of PostNL.

In opkomst zijn nepmails over gemiste pakketten

Kwaadaardig bestand herkennen

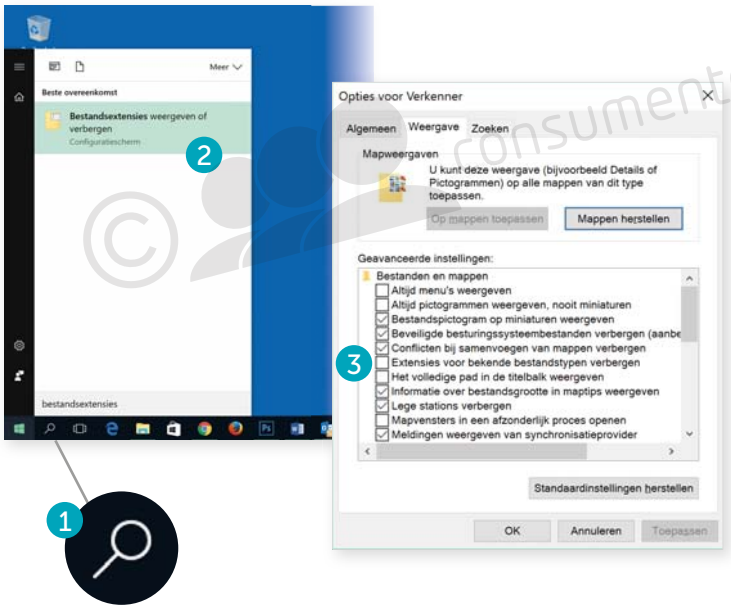
Het ene bestand is riskanter dan het andere. Wie een bestand met de extensie .txt toegestuurd krijgt, loopt weinig risico. Een .exe-bestand is wel riskant. Deze extensie wordt gebruikt door software. Het is een uitvoerbaar (exe staat voor *exe-cutable*) bestand en kan allerlei schade aanrichten. Voorbeelden van andere gevaarlijke bestandsformaten zijn .msi, .doc, .jar en .js. Het is ondoenlijk hier een complete lijst van te maken. Het advies is daarom: open een bijlage nooit direct. Sla het eerst op en laat de virusscanner daarna eerst het bestand controleren.

Om te maskeren dat het om een schadelijk bestand gaat, plaatsen sommige criminelen het in een zip-bestand. Een hinderlijke eigenschap van Windows is dat bestandsexten-

© consumentenbond

sies standaard niet worden getoond. Criminelen maken daar misbruik van door bijvoorbeeld het bestand factuur.pdf.exe toe te sturen. Met de standaardinstellingen ziet de gebruiker alleen factuur.pdf en denkt dat het om een betrouwbaar bestand gaat. Volg het 3-stappenplan hieronder om daar wat aan te doen.

Windows 10



Windows 7

In Windows 7 werkt het vergelijkbaar. Klik eerst op Start en typ daarna in het zoekvak 'bestandsextensies'. Vervolg met stap 2 uit bovenstaand stappenplan.

Windows 10

1. Gebruik in Windows 10 het zoekicoon in de taakbalk om 'bestandsextensies' te typen.
2. Klik op *Bestandsextensies weergeven of verbergen*.
3. Zorg dat er geen vinkje staat bij *Extensies voor bekende bestandstypen verbergen*.

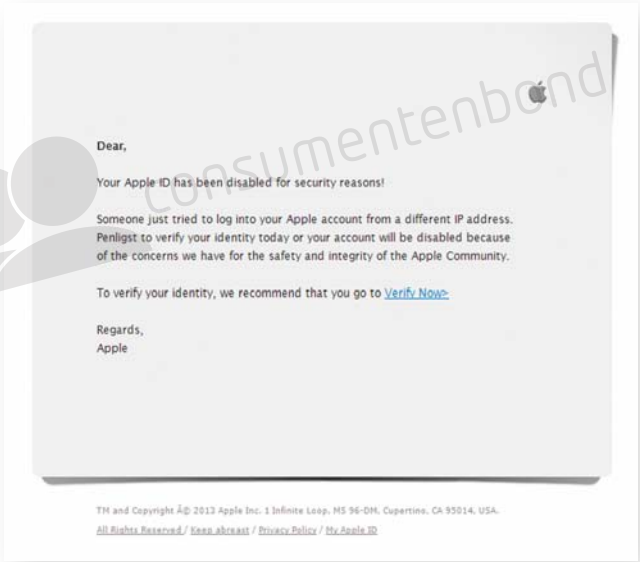
2.1h Account geblokkeerd

Regelmatig proberen phishingmails ons ervan te overtuigen dat we hoognodig ergens moeten inloggen, bijvoorbeeld bij een bank of internetdienst. Als je niet inlogt wordt het account verwijderd, klinkt het dreigend. Nep natuurlijk. In het voorbeeld op de volgende pagina zien we

© consumentenbond

een mail van Apple met de melding dat het account 'uit veiligheidsoverwegingen' geblokkeerd zal worden. Om alles weer in orde te maken, dient je identiteit geverifieerd te worden. De link leidt niet naar de site van Apple, maar naar criminelen. De mail is redelijk geloofwaardig. De vorm is in orde. Het taalgebruik is niet perfect. Verdachter nog is dat de aanhef alleen maar bestaat uit het woord 'Dear'.

Wantrouw mails met meldingen over een geblokkeerd account



© consumentenbond

TIP

Bij twijfel...

Bij twijfel of het gaat om phishing, is het verstandig op internet te zoeken. De sites van de Fraudehelpdesk (fraudehelpdesk.nl) en het tv-programma Opgelicht?! (https://opgelicht.avrotros.nl/alerts) maken melding van recente phishingaanvallen. Staat de mail er niet tussen en twijfelt u toch? Wacht het dan even af. Misschien dat er over een paar dagen wel een melding staat. Bovendien werken veel phishingwebadressen na een paar dagen niet meer. Ook wordt malware in een bijlage na een tijdje beter herkend door de virusscanner.

'Hallo, mag ik uw gegevens?'

Een aparte phishingcategorie vormen neptelefoontjes. Medewerkers van een bedrijf bellen op gegevens te achterhalen. Ze beweren bijvoorbeeld van de bank te zijn en vragen naar een pin- of TAN-code. Berucht zijn ook de neptelefoontjes van Microsoft met de melding dat er een probleem is met de computer. Of je even software wilt installeren om het op te lossen?

Apple niet langer veilig

Hoewel verreweg de meeste phishing is gericht op Windows-systemen, neemt het aantal phishingpogingen gericht op Apple-gebruikers toe. Recent bijvoorbeeld verschijnen op sommige websites pop-upvensters met de waarschuwing 'malicious adword attack'. Om dat op te lossen, moet je een telefoonnummer bellen van zogenaamd Apple. Die lost het 'probleem' op door software te installeren. De software neemt de computer op afstand over en gaat op zoek naar persoonlijke gegevens over bijvoorbeeld bankzaken. Het verraderlijke is dat Apple zelf ook een helpdesk heeft waarmee de computer op afstand overgenomen kan worden.

2.2 Uitkijken voor malware

Een besmetting met malware kan voor serieuze overlast zorgen, zelfs voor gegevensverlies. Besmetting gaat per mail of via een gehackte website. De meeste overlast is er de laatste tijd van malware die de computer gijzelt. Pas na het betalen van losgeld, geven de criminelen de computer weer vrij. Het betalen van het losgeld gaat vaak via bitcoins of andere anonieme betaalsystemen. In de meest eenvoudige variant blokkeert dit soort ransomware de toegang tot de computer. Door de kwaadaardige software te verwijderen, kunt u weer bij de bestanden. Geavanceerder is cryptoware die bestanden op de computer versleutelt.

© Consumentenbond

Alleen met de juiste sleutel is het mogelijk weer toegang te krijgen.
Ransomware zorgt wereldwijd voor miljoenen euro's aan schade. De FBI schatte het schadebedrag in Amerika gedurende het eerste kwartaal op 209 miljoen dollar.
Het gaat dan puur over de financiële schade. Het verlies van dierbare foto's is niet in geld uit te drukken. Om het probleem aan te pakken, is door onder meer de politie de site nomoreransom.org in het leven geroepen.
Is de computer eenmaal besmet, dan verschillen de symptomen en oplossingen voor 'gewone' ransomware en de cryptoware-variant.

© consumentenbond

2.2a Ransomware

Een besmetting met ransomware is in de regel meteen duidelijk. Toegang tot de computer is onmogelijk door een niet-wegklikbaar scherm na het opstarten van de pc. Op het scherm staan betaalinstructies om de computer weer te kunnen gebruiken. Vaak wordt de suggestie gewekt dat de blokkade is opgelegd door een overheidsinstantie, zoals de politie. Er kan (ten onrechte) worden gemeld dat er illegale software of pornografisch materiaal is aangetroffen. Soms wordt zelfs het beeld van de webcam getoond. Dit wekt de suggestie dat je in de gaten wordt gehouden.

Hoe te verwijderen?

1. De belangrijkste regel is: nooit betalen. De kans dat de computer wordt vrijgegeven is klein, in tegenstelling tot cryptoware.
2. Probeer de computer te herstellen met Windows-systeemherstel. Windows wordt daarmee teruggezet naar een eerder moment. Er gaan geen gegevens verloren.
3. Als dat niet werkt, probeer dan of de pc nog in veilige modus kan worden gestart. Als dat lukt, kun je de ransomware verwijderen met het gratis Malwarebytes Anti-Malware (malwarebytes.org). Let bij installatie op dat je het vinkje weghaalt bij 'start proefversie van Malwarebytes Anti-Malware Premium'.

4. Lukt het opstarten niet? Probeer het dan met Hitman-Pro.Kickstart (surfright.nl/kickstart). Dit programma download je op een andere pc en installeer je op een usb-stick. Door de geïnfecteerde pc daarna op te starten vanaf deze usb-stick, kan de pc worden geschoond van het virus.
5. Als dit ook niet lukt, rest er nog één optie: de pc herinstalleren. Dat is ook de enige manier om er 100% zeker van te zijn dat het virus weg is. Bedenk wel dat alle data op de computer zo wordt gewist.

2.2b Cryptoware

Als een computer besmet raakt met cryptoware, is dat niet meteen zichtbaar. In eerste instantie doet het virus zijn werk op de achtergrond. De computer werkt ogenschijnlijk net als anders, maar ongemerkt worden alle gegevens (foto's, muziek, Word-bestanden) versleuteld zodat ze niet meer geopend kunnen worden. Cryptoware kan ook bestanden op externe harde schijven en usb-sticks besmetten. Zelfs netwerkopslag die via Windows Verkenner met een schijfletter (zoals F: of G:) toegankelijk is, kan zo onbruikbaar raken.
Na versleuteling verschijnt de melding dat je honderden euro's moet betalen om weer bij de gegevens te kunnen. Meestal moet er betaald worden met Bitcoins. Om er extra druk achter te zetten, wordt gedreigd dat dit bedrag omhoog gaat als je niet snel betaalt.

Hoe te verwijderen?

Er zijn 4 mogelijkheden om de data terug te krijgen:

1. Als je geluk hebt, zijn de makers van de cryptoware opgepakt of heeft de politie ontsleutelingsgegevens weten te bemachtigen. Van Coinvault zijn de sleutels bekend en sinds kort is er een herstelprogramma voor Teslacrypt cryptoware-varianten. Kijk op nomoreransom.org voor een overzicht van alle ransomware die je zelf kunt ontsleutelen. Voor de meeste ransomware is er helaas geen oplossing.

© Consumentenbond

2. Een makkelijker methode is het terugplaatsen van een back-up van de bestanden. Dan moet zo'n (recente) back-up er natuurlijk wel zijn; eentje die niet is versleuteld door de cryptoware. Bedenk dat je de cryptoware wel moet verwijderen voordat je de bestanden terugplaatst, bijvoorbeeld door de computer opnieuw te installeren.
3. Geen back-up gemaakt? Dan is er een kleine kans dat Windows dit automatisch heeft gedaan via schaduwkopieën.
   a. Klik met rechts op een bestand of map.
   b. Selecteer *Eigenschappen* > tabblad 'Vorige versies'.
   c. Kijk of er een oudere versie staat die hersteld kan worden.
   d. Het is ook de moeite waard om dataherstelsoftware te proberen. Een aanrader is het gratis programma Recuva (piriform.com/recuva).
4. Het laatste redmiddel raden we sterk af, maar als het om erg belangrijke bestanden gaat kun je overwegen losgeld te betalen. Ervaringen tonen aan dat slachtoffers de sleutels vaak krijgen, maar er is geen garantie. Uiteraard houd je zo wel het verdienmodel van internetcriminelen in stand.

© consumentenbond

2.3 Oppassen met downloaden

Om besmetting te voorkomen is het zaak bij het downloaden van bestanden en software goed op te letten. We zagen eerder dit hoofdstuk al het voorbeeld van phishingmails met een bestand als bijlage. Wie zo'n bestand downloadt en opent, loopt grote kans besmet te raken met malware.
Ook bij het downloaden via websites is het oppassen geblazen. Obscure sites bieden dure softwarepakketten gratis aan, inclusief virus. Wat meer onschuldig zijn downloadsites met gratis software. Tijdens het installeren word je opgezadeld met toolbars en andere ongewenste programma's. Ze veroorzaken niet direct schade, maar zijn wel hinderlijk.