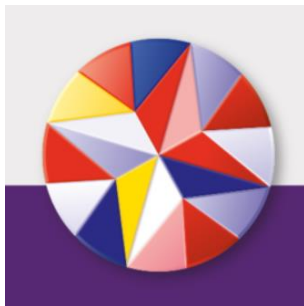


Veilig internetbankieren

Wil Veugelers 15 november 2018



- ☐ Veilig internetbankieren
 - ☐ Wat doet de bank
 - ☐ Wat kunt u zelf doen
- ☐ Valse e-mails
 - ☐ Wat is phishing
 - ☐ Herkennen van valse e-mails
- ☐ Veilig software downloaden
- ☐ Wat te doen bij misbruik



Wat doet de bank



- ☐ Beveiligde verbinding (met versleuteling) tussen klant en bank
- ☐ Monitoren transacties (zowel overboekingen als girale transacties met passen) op frauduleuze pogingen.
- ☐ Beschikbaar stellen van Rabo Scanner / Digipas (SNS) e.dentifier (ABNAMRO) voor identificatie van de klant.
- ☐ Gemaximaliseerde limieten voor overboekingen.
- ☐ Automatisch uitlog, wanneer geen gebruik gemaakt wordt van de bank omgeving.



Wat kunt u doen



- ☐ Houd uw beveiligingscodes geheim.
- ☐ Zorg ervoor dat uw bankpas nooit door een ander gebruikt wordt.
- ☐ Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken.
- ☐ Controleer uw bankrekening.
- ☐ Meld incidenten direct aan de bank en volg aanwijzingen van de bank op
- ☐ Zorg voor een veilig wifi-netwerk
- ☐ Controleer de website



Houd uw beveiligingscodes geheim



- ☐ Een beveiligingscode is niet alleen de pincode die u in combinatie met de bankpas gebruikt. Het zijn ook alle andere codes die u gebruikt om elektronische betalingen te doen en/of gebruik te maken van internet- en mobielbankieren.
- ☐ U mag deze beveiligingscodes alleen zelf gebruiken.
- ☐ Schrijf of sla de codes niet op.
- ☐ Zorg ervoor dat niemand kan meekijken als u uw beveiligingscodes intikt.
- ☐ Geef nooit een beveiligingscode door per telefoon of e-mail.



Houd uw beveiligingscodes geheim



**De bank en de bankmedewerkers
vragen u nooit om uw pincode of
inlogcodes!**

**Criminelen doen
dit wel.**



Zorg ervoor dat uw bankpas nooit door een ander gebruikt wordt.



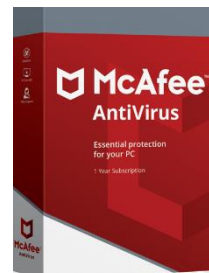
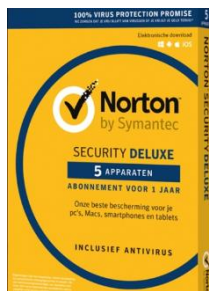
U bent verantwoordelijk voor uw pas, mocht een ander hiervan gebruik maken en betalingsopdrachten geven, dan bent u ook verantwoordelijk voor die opdracht.



Zorg voor een goede beveiliging van uw apparatuur.



- ❑ Houd uw browser en uw besturingssysteem up to date. Download en installeer altijd de laatste versies en schakel de auto-update functie in.
- ❑ Gebruik een anti-virusprogramma en houd dit programma up to date en actief.
- ❑ Scan regelmatig uw computer op virussen.



Controleer uw bankrekening.



- ☐ Controleer uw elektronische of papieren rekeninginformatie op transacties waarvoor u geen toestemming heeft gegeven.
- ☐ Als u alleen rekeninginformatie op papier ontvangt, controleer deze dan in ieder geval binnen twee weken na ontvangst.



Meld incidenten direct aan de bank



Neem in de volgende gevallen in elk geval direct met de bank contact op:

- ☐ U heeft uw bankpas niet meer in uw bezit of weet niet waar deze is.
- ☐ U weet of vermoedt dat iemand anders uw beveiligingscode kent of heeft gebruikt.
- ☐ U ziet dat er transacties op uw bankrekening hebben plaatsgevonden, waarvoor u geen toestemming heeft gegeven.
- ☐ U heeft uw mobiele apparaat met betaaltoepassing van de bank niet meer.



Zorg voor een veilig wifi-netwerk



Thuis:

Beveilig uw wifi-netwerk.

- ☐ Stel uw draadloze netwerk in op WPA2-beveiliging met AES-encryptie.
- ☐ WPA2 zorgt ervoor dat een wachtwoord nodig is om verbinding te maken.
Stel een zo lang mogelijk wachtwoord in, bij voorkeur meer dan 20 tekens.

Raadpleeg hiervoor de handleiding van uw router.



Zorg voor een veilig wifi-netwerk



Onderweg:



- ☐ Openbaar wifi-netwerk.

Openbaar wifi is voor iedereen toegankelijk.

Kwaadwillende kunnen:

- ☐ uw internetverkeer afluisteren
- ☐ Uw apparaat automatisch laten verbinden met een vals netwerk
- ☐ Beveiligd wifi-netwerk



Zorg voor een veilig wifi-netwerk

Afluisteren van internetverkeer:



- ☐ uw e-mails kunnen worden meegelezen waardoor uw privéleven op straat kan belanden;
- ☐ uw inloggegevens kunnen worden gestolen waardoor anderen uw accounts kunnen misbruiken en zich als u kunnen voordoen;
- ☐ uw surfgedrag kan worden geregistreerd waardoor partijen ongemerkt een persoonlijk profiel van u kunnen vastleggen.



Zorg voor een veilig wifi-netwerk



Verbinding met een vals netwerk:

- ☐ wanneer u ergens voor wilt inloggen kan een namaak-inlogpagina worden getoond die uw wachtwoord steelt;
- ☐ websites die u normaliter vertrouwt kunnen misleidend zijn;
- ☐ informatie of virussen bevatten;
- ☐ er kunnen valse updates voor apps worden aangeboden die in werkelijkheid een virus achterlaten.



Zorg voor een veilig wifi-netwerk



Conclusie:

Log bij een openbaar wifi-netwerk nooit in op websites waar u met uw persoonlijke gegevens gaat werken.



Zorg voor een veilig wifi-netwerk

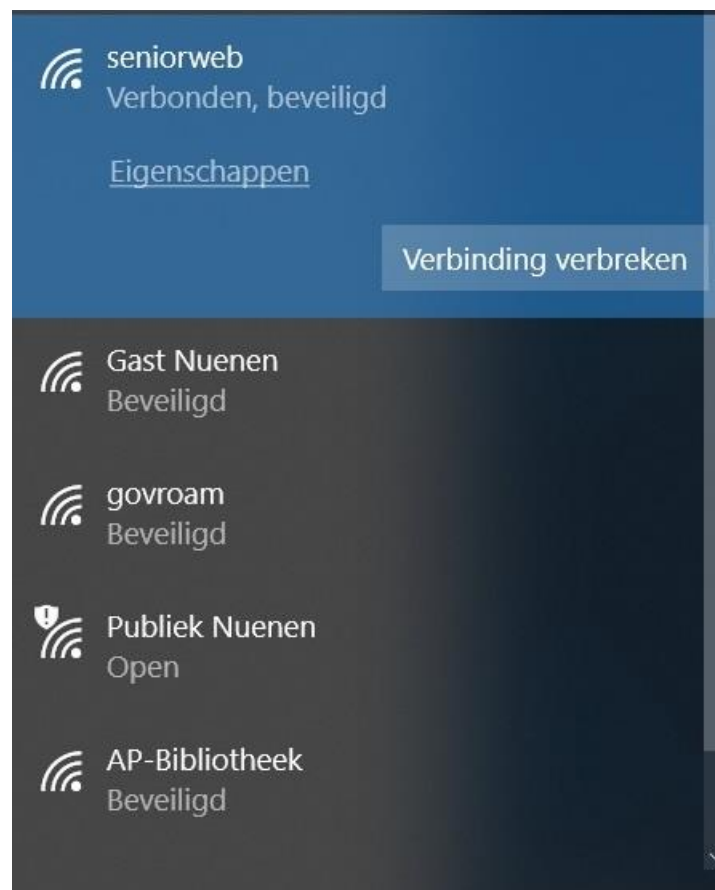
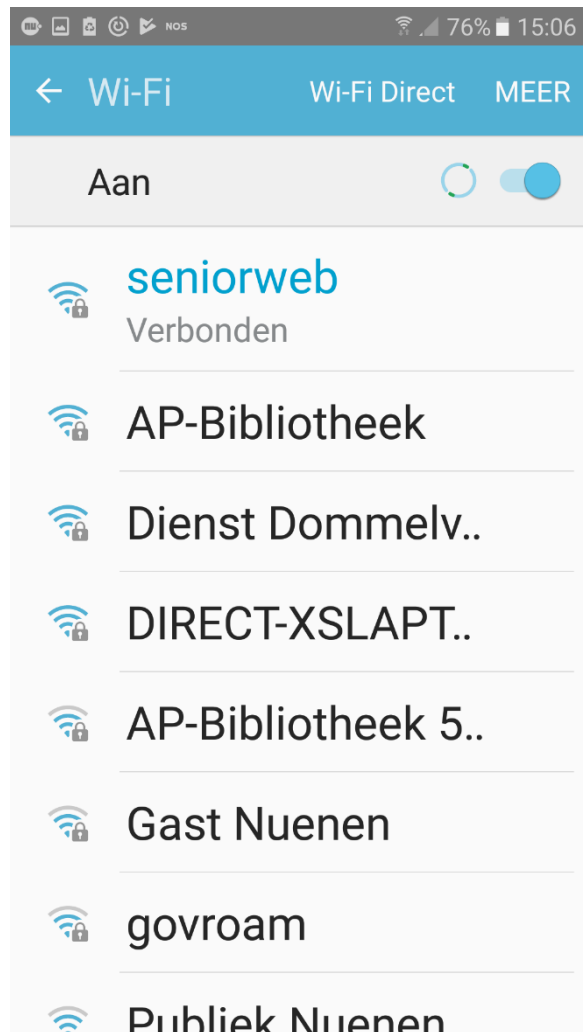


Beveiligd wifi-netwerk.

Uw apparaat kan met het hangslot-pictogram aangeven of een netwerk beveiligd is. Wanneer dat zo is, dan hebt u ook een wachtwoord nodig dat het plaatselijke personeel kan verzorgen. Deze beveiliging maakt de kans op afluisteren kleiner, maar het neemt het risico niet weg. Daarom blijft het raadzaam om uw eigen verbinding met de dienst die u gebruikt goed te controleren.



Zorg voor een veilig wifi-netwerk



Controleer de website



- ❑ Vul uw pasgegevens alleen in op de echte inlogpagina van de bank.
- ❑ De browser geeft een hangslotje weer en het webadres begint met https, waarbij de 's' staat voor 'secure'.
- ❑ Controleer het beveiligingscertificaat.

Dit certificaat geeft aan dat u een directe en beveiligde verbinding heeft met uw bank en uw browser.

- Klik met de linker muis op het hangslotje.
- Klik met de linker muis op Certificaat.
- Kijk of het certificaat nog geldig is.
- Kijk of het certificaat verleend is aan uw bank.
- Controleer het certificeringspad.



ABN AMRO Bank



ABN AMRO Bank N.V. [NL] | <https://www.abnamro.nl/nl/prive/index.html>

Certificaat [X]

Algemeen Details **Certificeringspad**

Certificaatinformatie

Doeleinden van dit certificaat:

- het garanderen van de identiteit van een externe computer
- het garanderen van uw identiteit aan een externe computer
- 1.3.6.1.4.1.8024.0.2.100.1.2

* Zie de verklaring van de certificeringsinstantie voor meer informatie

Verleend aan: www.abnamro.nl

Verleend door: QuoVadis EV SSL ICA G1

Geldig van 8-5-2017 **t/m** 8-5-2019

Verklaring van verlener

OK

Certificaat [X]

Algemeen Details **Certificeringspad**

Certificeringspad

QuoVadis Root CA 2
QuoVadis EV SSL ICA G1
www.abnamro.nl

Certificaat weergeven

Certificaatstatus:

Dit certificaat is in orde.

OK



ING BANK N.V. [NL] | <https://www.ing.nl/particulier/index.html>

Certificaat

Algemeen Details Certificeringspad

 **Certificaatinformatie**

Doeleinden van dit certificaat:

- het garanderen van de identiteit van een externe computer
- het garanderen van uw identiteit aan een externe computer
- 2.16.840.1.114028.10.1.2
- 2.23.140.1.1

* Zie de verklaring van de certificeringsinstantie voor meer informatie

Verleend aan: www.ing.nl

Verleend door: Entrust Certification Authority - L1M

Geldig van 24-3-2017 **t/m** 30-4-2019

Verklaring van verlener

OK

Certificaat

Algemeen Details Certificeringspad

Certificeringspad

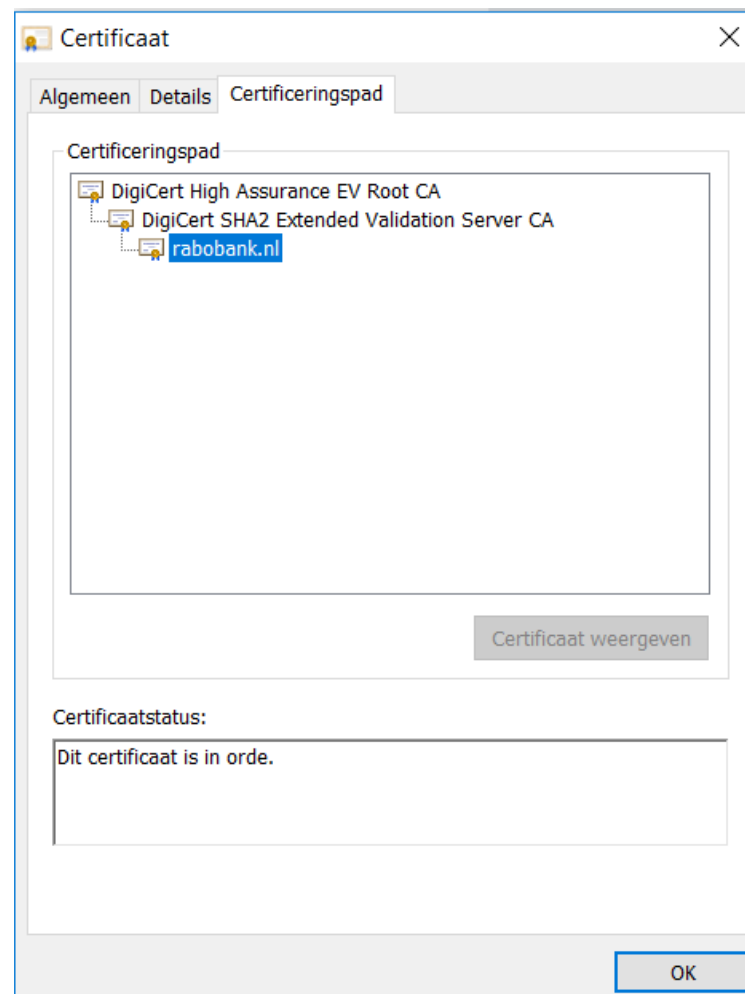
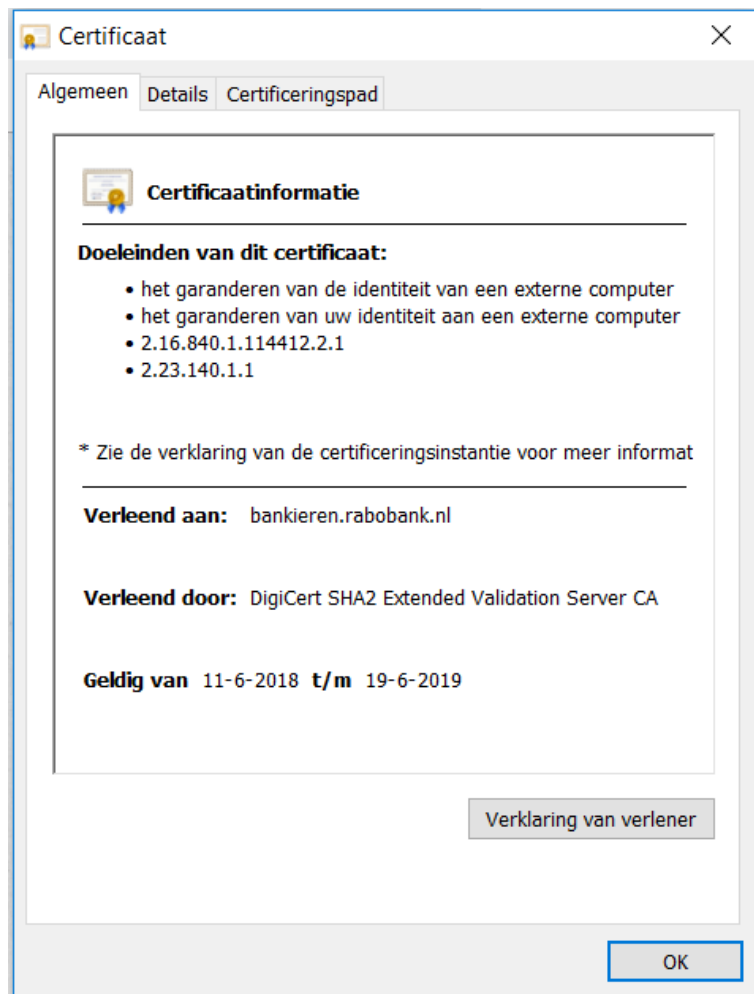
- Entrust
 - Entrust Root Certification Authority - G2
 - Entrust Certification Authority - L1M
 - www.ing.nl

Certificaat weergeven

Certificaatstatus:

Dit certificaat is in orde.

OK



Certificaat

AlgemeenDetailsCertificeringspad

**Certificaatinformatie**

Doeleinden van dit certificaat:

- het garanderen van de identiteit van een externe computer
- het garanderen van uw identiteit aan een externe computer
- 2.16.840.1.114412.2.1
- 2.23.140.1.1

* Zie de verklaring van de certificeringsinstantie voor meer informatie

Verleend aan: www.snsbank.nl

Verleend door: DigiCert SHA2 Extended Validation Server CA

Geldig van 12-7-2017 **t/m** 4-10-2019

Verklaring van verlener

OK

Certificaat

AlgemeenDetailsCertificeringspad

Certificeringspad

DigiCert High Assurance EV Root CA

- DigiCert SHA2 Extended Validation Server CA
 - www.snsbank.nl

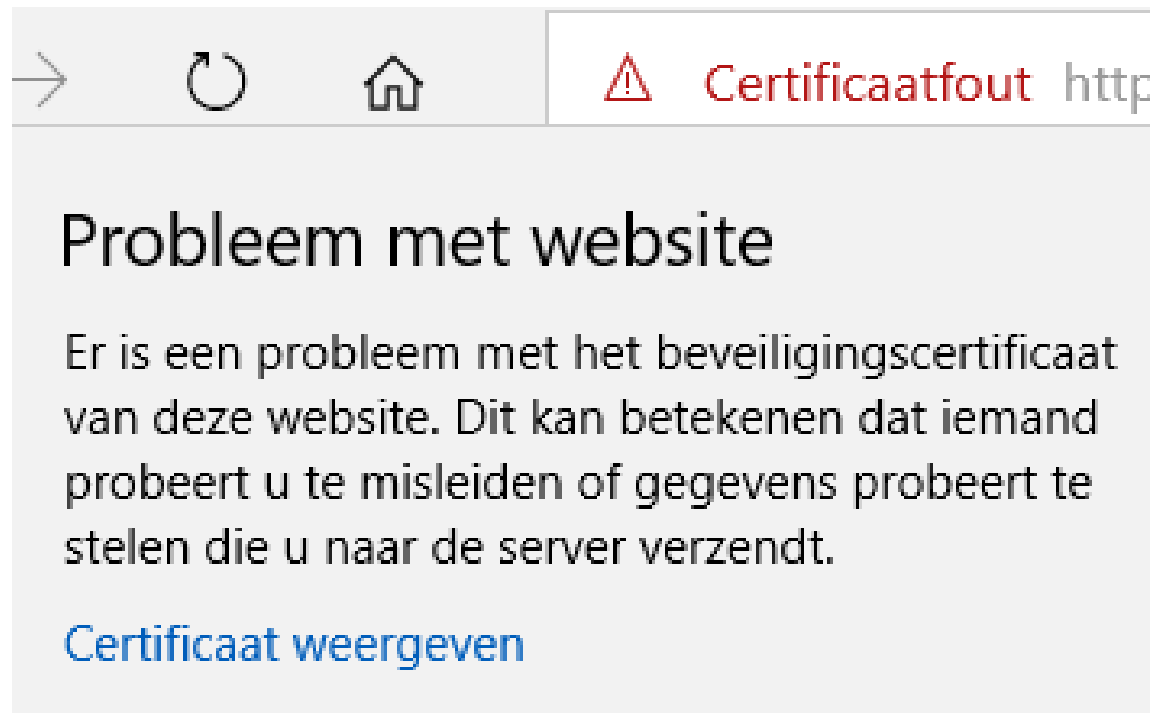
Certificaat weergeven

Certificaatstatus:

Dit certificaat is in orde.

OK

Certificatiefout



Voorbeelden foute websites



Foute website



Uw systeem is serieus beschadigd, er zijn (6) virussen gedecteerd!

4 November 2018

We hebben gedecteerd dat uw Windows voor 32,4% is beschadigd en (6) virussen bevat.

Als u deze virussen niet onmiddellijk verwijdert, zal het leiden tot beschadiging van systeembestanden, gegevens en applicaties.

Wat u moet doen (Stap voor stap):

Stap 1: Klik op **SYSTEEM OPSCHONEN** en download nu gratis PcCleaner!

Stap 2: Installeer en open de applicatie om het systeem te herstellen!

4 min. 25 sec.

SYSTEEM OPSCHONEN >>

Foute website



d1p5yllpswf3yq.cloudfront.net/dyna/loadie.html?osv=Windows%2010&trk=q.adtracking

→ ↻ 🏠 ⓘ d1p5yllpswf3yq.cloud

Wees hier voorzichtig

Uw verbinding met deze website is niet versleuteld. Hierdoor kan iemand eenvoudiger gevoelige informatie, zoals wachtwoorden, stelen.

Websitemachtigingen

U hebt nog geen machtigingen ingesteld voor deze site.

[Adobe Flash toestaan](#)

Deze website meldt het volgende...

Windows 10 heeft gedetecteerd dat uw Microsoft Windows-systeem momenteel verouderd is en beschadigd is.

Dit is er de oorzaak van dat uw systeembestanden automatisch worden verwijderd.

Volg de instructies onmiddellijk op om dit probleem op te lossen en om ervoor te zorgen dat uw systeem bijgewerkt blijft.

OK

Foute website



← → ↻ 🏠 <https://d2gcaq25bwmi6y.cloudfront.net/index.html?mid=3164&number=0800-022-3164>

Microsoft

Windows Windows Devices Apps+Games

Windows was blocked

Please stop or restart your computer



Call immediately
[0800-022-3164](tel:0800-022-3164)
Get the latest news on safety issues.

Instant help without waiting
call [0800-022-3164](tel:0800-022-3164) (Free of charge) and improve health. Of your computer

Be updated with windows
Our professionals will keep you up to date with the latest software

Kn...
Learn infor...

**** YOUR COMPUTER HAS BEEN BLOCKED.****

Please call us immediately at: [0800-022-3164](tel:0800-022-3164)
Do not ignore this critical alert.
Yes You close this page, your computer access will be disabled for Avoid further damage to our network. Our computer has alerted us That it was infected by a virus and a spyware. Information Following are stolen ...

Facebook Login
> Credit card details
> Login email account
> Photos stored on this computer.
You must contact us immediately so that our engineers can guide you through the removal process by phone. Please call us within 5 minutes to prevent your computer from being disabled.

Windows-beveiliging

Microsoft Edge

Server winfreesupport.club vraagt om uw gebruikersnaam en wachtwoord. De server geeft Microsoft has detected suspicious activity from your IP address. aan als serverbron.

OK Annuleren

Call Support Team : [0800-022-3164](tel:0800-022-3164) (Free of charge)

Valse e-mails



Valse e-mails



Uiteraard beschermt een goede virusscanner uw pc, maar toch is een heel groot deel van computer-criminaliteit niet gebaseerd op virussen, maar op eenvoudige psychologie. Bij phishing maakt de crimineel in de eerste plaats gebruik van menselijke zwakheden, zoals angst, nieuwsgierigheid en onoplettendheid. Hoe wapen jij je tegen de oplichters die eeuwenoude technieken van misleiding in een nieuw jasje hebben gestoken.



Wat is phishing

Phishing is “vissen” naar informatie. Methode om computergebruikers over te halen persoonlijke gegevens of financiële gegevens op te geven.



- ☐ Valse e-mails en berichten op sociale media waarbij u wordt doorverwezen naar een website die lijkt op bijv. de website van uw bank
- ☐ Contact zoeken via telefoon (babbeltruc)



Herkennen van valse e-mails



- ☐ Vaag of onduidelijk e-mailadres.
- ☐ U wordt gevraagd om op een link te klikken en/of persoonlijke gegevens door te geven.
- ☐ U wordt gevraagd om een bijlage te openen.
- ☐ De e-mail is niet aan u persoonlijk gericht, maar begint bijvoorbeeld met 'Beste klant' of 'Beste gebruiker'. Criminelen weten uw naam namelijk niet.
- ☐ Het bericht is in gebrekkig Nederlands geschreven.
- ☐ De boodschap speelt in op angstgevoelens. U moet bijvoorbeeld direct reageren anders wordt uw account stopgezet.
- ☐ De e-mail komt in uw spamfilter terecht.
- ☐ De link in de e-mail komt niet uit op de echte website.



Voorbeelden van valse e-mails



Valse e-mail



Rabobank

Beste meneer, mevrouw,

Ons geautomatiseerd systeem heeft zojuist gedetecteerd dat u nog gebruikt maakt van een verouderde betaalpas. Alle verouderde betaalpassen zullen komen te vervallen na 15 november 2018.

Vraag gratis een vernieuwde betaalpas aan voor:

Datum: 12 november 2018

Tijd: Tussen 00:00 en 24:00 uur

Vernieuwde betaalpas aanvragen

Klik [hier](#) om binnen 2 minuten een nieuwe betaalpas aan te vragen via Internet- of Mobiel Bankieren. Binnen 5 werkdagen heeft u uw nieuwe betaalpas geheel kosteloos in huis.

Met vriendelijke groet,

Robin 

Directeur Klantenservice



Valse e-mail



Van: WeTransfer
Verzonden: dinsdag 30 oktober 2018 17:40
Aan:
Onderwerp: Check Your New File that was sent to you

WeTransfer

**You have received a file via
WeTransfer**

3 Files, 20 MB in total · Will be deleted on 31 Oct 2018

[Download your Docs here](#)



Valse e-mail



Geachte relatie,

Uw account moet worden geverifieerd.

We vermoeden dat derden toegang hebben tot uw account en gegevens.

[Klik hier om uw account te verifiëren](#)

Wij willen u alvast bedanken voor uw medewerking.

Met vriendelijke groet,

MyVodafone Online Servicedesk



Valse e-mail



Van: klantenservice -
Aan: -
Datum: 8 november 2018 om 17:18
Onderwerp: felicitatie! het is je geluksdag

bol.com

bol.com

felicitatie

deze e-mail is alleen verzonden naar 10 geselecteerde klanten in uw regio.

Op deze manier willen we u bedanken dat u hier voor ons bent.

U bent een van de huidige klanten die een **IPHONE XS** wint

[Ga hierheen](#)



Valse e-mail



Van: CJIB - Ministerie van Veiligheid en Justitie <b[redacted]@cjiib.nl>
Verzonden: donderdag 8 november 2018 15:21
Aan: [redacted]
Onderwerp: EXT: Laatste aanmaning inzake verkeersovertreding



Betreft: Laatste aanmaning inzake Referentie: 98[redacted] KB

Geachte [redacted],

Bij deze willen we u meedelen dat u nog een bedrag heeft openstaan. De betalingstermijn is reeds overschreden.

Omschrijving: Overschrijding maximumsnelheid

Datum: [6 augustus 2018](#)

Locatie: A2 ter hoogte van Breukelen

Toegestane snelheid: 100 km/h

Gemeten snelheid: 114 km/h

Gecorrigeerde snelheid: 111 km/h

Openstaand bedrag: 86,00 Euro

Administratiekosten: 11,00 Euro

Aanmaningskosten: 37,00 Euro

Te betalen: 134,00 Euro

Wij sommen u het bedrag binnen 2 werkdagen te betalen volgens instructies.

Zie hiervoor bijgaand document of [klik hier](#).

Indien wij geen tijdige betaling ontvangen zullen verdere incassomaatregelen volgen.

Als uw betaling en deze herinnering elkaar gekruist hebben, kunt u deze brief als niet verzonden beschouwen.

Hoogachtend,

P [redacted]

DG CJIB - Ministerie van Veiligheid en Justitie

Valse e-mail



Subject: Persoonlijke uitnodiging voor het investeringsplan voor pr@pvge-nuenen.nl

Uitnodiging voor: pr@pvge-nuenen.nl

Hallo Pr.

U heeft een persoonlijke uitnodiging ontvangen voor een automatisch beleggingssysteem waarmee u minimaal EUR 7.850 per maand kunt verdienen!

Ga naar de website en ontdek het zelf:
<http://n.uitnodigingnl.ml/inv/uO4sRT35>

Dit automatische beleggingssysteem wisselt cryptogeld uit met behulp van geavanceerde kunstmatige intelligentie. Hiermee kunt u zeer grote hoeveelheden geld verdienen met minimale inspanning van uw kant!

Bekijk de video en ontdek wat er aan de hand is:
<http://n.uitnodigingnl.ml/inv/uO4sRT35>

Hoe zou u zich voelen als u elke dag wakker wordt en transfers naar uw account ziet voor 400 EUR? Zou het je toestaan om je dromen te vervullen en je passie te volgen? Zeker ja!

Ontdek de technologie van de 21ste eeuw die voor u werkt!

Gratis registratie:
<http://n.uitnodigingnl.ml/inv/uO4sRT35>

Registreer u vandaag nog en u zult er geen spijt van krijgen, dat garandeer ik!

Hoogachtend,
Alexander De backer



Valse e-mail



Meer voorbeelden op de website

[Fraudehelpdesk.nl](https://www.fraudehelpdesk.nl)



Veilig software downloaden



Veilig software downloaden



Zodra je programma's gaat downloaden van het internet is de kans groot dat er allerlei ongewenste software meekomt. Ineens heb je een andere werkbalk (toolbar), je hebt een andere zoekmachine of er staan allerlei onbekende pictogrammen op het bureaublad. Zelfs als je de computer goed beschermd hebt, met bijvoorbeeld een goede virusscanner, is de kans op ongewenste software nog steeds aanwezig.



Veilig software downloaden



Tips om ongewenste software te voorkomen:

- ☐ Ga voor een betrouwbare website
- ☐ Let op de vinkjes bij het installeren
- ☐ Uitvoeren of opslaan?



Ga voor een betrouwbare website



Ga altijd rechtstreeks naar de site van de aanbieder of ontwikkelaar van het programma. Het kan zijn dat de aanbieder je doorstuurt naar een andere website (een bekend voorbeeld is: download.com), maar je kunt er vanuit gaan dat die site ook betrouwbaar is.

Ga nooit downloaden van verzamelwebsites die meerdere programma's aanbieden.



Let op de vinkjes bij het installeren



Wees alert als je tijdens de installatie van een programma aangevinkte hokjes tegenkomt. Bedenk van tevoren goed of je die hokjes echt ook wilt. Meestal is er aangevinkt dat er een snelkoppeling op het bureaublad komt. Dit is nog tot daar aan toe, maar voor je het weet komt die toolbar ook mee of andere extra software. Kijk dus goed naar de vinkjes en klik ze gerust weg als je hier niet op zit te wachten. Het kan ook zijn dat er ongewenste software via een update van een bepaald programma binnenkomt. Wees hier dus ook alert op en klik niet klakkeloos op "updaten".



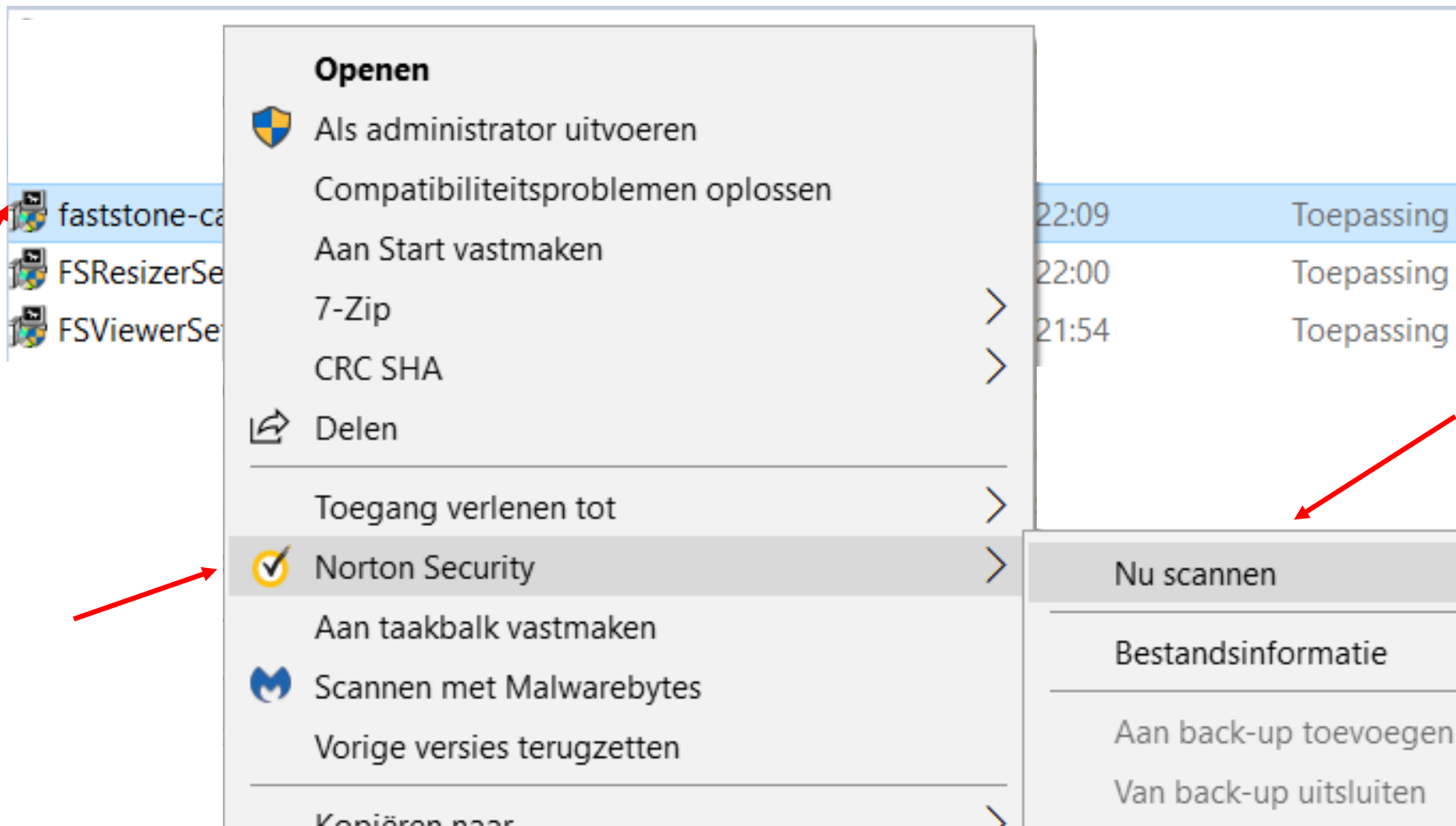
Uitvoeren of opslaan?



Vaak worden programma's aangeboden als exe-bestand. Met dit bestand kun je het programma op je computer installeren. Zodra je het programma gaat downloaden, krijg je de keuze: "uitvoeren" of "opslaan". Je kunt dan het beste kiezen voor "opslaan", omdat het programmabestand meestal in de map "Downloads" opgeslagen wordt. Nu kun je het programma voordat je het installeert nog scannen op virussen en spyware. Als je kiest voor "uitvoeren", wordt het programmabestand in een tijdelijke map opgeslagen en van daaruit geïnstalleerd. Je kunt het dan niet vooraf scannen.



Scannen op virussen



The screenshot shows a Windows file explorer window with a context menu open for a folder named 'faststone-ca'. The menu options include 'Openen', 'Als administrator uitvoeren', 'Compatibiliteitsproblemen oplossen', 'Aan Start vastmaken', '7-Zip', 'CRC SHA', 'Delen', 'Toegang verlenen tot', 'Norton Security', 'Aan taakbalk vastmaken', 'Scannen met Malwarebytes', 'Vorige versies terugzetten', and 'Kopiëren naar'. A red arrow points to the 'Norton Security' option. Another red arrow points to the 'Nu scannen' option in the sub-menu that appears when 'Norton Security' is selected. The sub-menu also includes 'Bestandsinformatie', 'Aan back-up toevoegen', and 'Van back-up uitsluiten'.

Time	Action
22:09	Toepassing
22:00	Toepassing
21:54	Toepassing



Programmabestand scannen



Handmatige scan ?



Geen bedreigingen gevonden

Resultatenoverzicht

[+] Totaalaantal gescande items:	1
[+] Totaalaantal gedetecteerde beveiligingsrisico's:	0
[+] Aantal opgeloste beveiligingsrisico's:	0
Totaalaantal beveiligingsrisico's dat aandacht vereist:	0

Als u denkt dat er nog steeds risico's aanwezig zijn, [klikt u hier](#).



[Resultaten exporteren](#)

Voltooien

Scannen op malware

 faststone-capture-8-4.exe

 FSResizerSetup38.exe

 FSViewerSetup64.exe

Openen



Als administrator uitvoeren

Compatibiliteitsproblemen oplossen

Aan Start vastmaken

7-Zip



CRC SHA



Delen

Toegang verlenen tot



Norton Security



Aan taakbalk vastmaken



Scannen met Malwarebytes

Vorige versies terugzetten

Toepassing

Toepassing

Toepassing

Programmabestand scannen



Malwarebytes Gratis 3.6.1

Malwarebytes | FREE

Licentie activeren Nu upgraden

Dashboard Scannen Scanplanning

Scannen Quarantaine Rapporten Instellingen

Sluiten X



Uw scan is voltooid.
Geen bedreigingen gedetecteerd!

Scantijd:	15 s
Gescande items:	1
Herkende dreigingen:	0

Overzicht exporteren Rapport bekijken

Geef criminelen geen kans

Voorkom dat hackers uw systeem infecteren en zich toegang verschaffen tot uw gegevens. Voer een upgrade uit naar premium.

Nu upgraden

Waarom Premium

Programmabestand scannen



← → ↻ 🏠 https://nl.malwarebytes.com/mwb-download/



Producten

Ondersteuning

Labs ▾

|

Malwarebytes gratis downloads

Elk computerbeveiligingsproduct van Malwarebytes dat u gratis kunt downloaden, inclusief de nieuwste hulpprogramma's voor het verwijderen van malware en spyware.



Voor thuis

Malwarebytes for Windows

Meerdere lagen malware vernietigende technologie, inclusief virusbeveiliging. Grondige verwijdering van malware en spyware. Gespecialiseerde ransomwarebescherming.

GRATIS VERSIE

Zie Prijzen voor premiumversie

Malwarebytes for Mac

Proactieve bescherming tegen malware, ransomware en andere gevaarlijke bedreigingen voor wat ieders favoriete computer aan het worden is. *Opmerking: Alleen Engels*

GRATIS VERSIE

Zie Prijzen voor premiumversie

Malwarebytes for Android

Proactieve bescherming tegen malware, ransomware en andere gevaarlijke bedreigingen voor wat ieders favoriete computer aan het worden is.



Wat te doen bij misbruik



Meld misbruik

Als u misbruik vermoedt is het van belang dat u bewijsmateriaal verzamelt en het misbruik meldt bij de juiste instanties. U kunt misbruik melden bij:

- ☐ de betreffende instantie

- ☐ het [Centraal Meldpunt Identiteitsfraude](#)

het CMI geeft ondersteuning en advies als u slachtoffer bent van identiteitsfraude.

- ☐ de politie: doe aangifte van misbruik



Dank voor uw aandacht.

SeniorWeb Nuenen

