

An abstract graphic featuring three blue circles of varying sizes, each composed of concentric rings in different shades of blue. Two thin blue lines intersect at a point between the top two circles, extending towards the top-left and bottom-right corners of the page. A third blue circle is partially visible in the bottom-right corner.

Veilig internet en e-mail

Gerrit Tiemens
9-2-2020

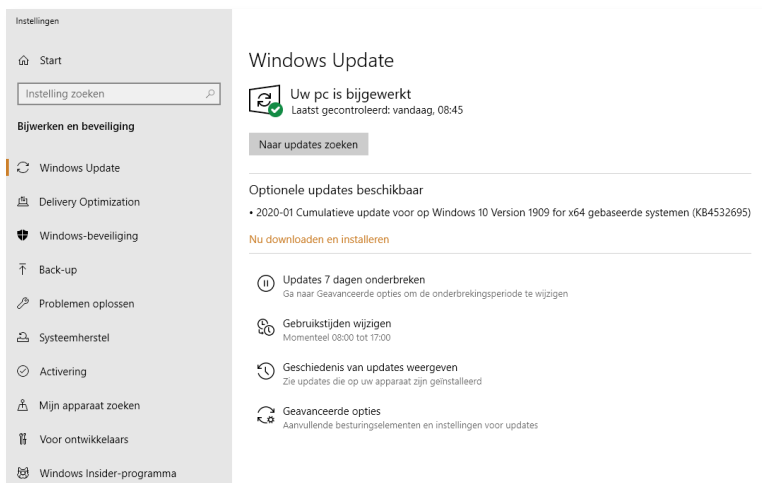
Inhoud

1. Het belang van updates installeren.....	3
2. Firewall	3
3. Antivirusprogramma	4
4. Adblock Plus	5
5. Cookies	5
5.1 Cookies beheren.....	5
5.1.a FireFox	5
5.2 CCleaner	6
6. Browser finger printing.....	6
7. Gebruik geen administrator account	7
8. Andere browsers	9
8.1 Browser in the box (BitBox).....	9
8.2 Tor Browser	9
9. Hostfile	10
10. Alternatieven voor Google	11
11. SpywareBlaster.....	11
12. Malware.....	11
12.a Ransomware.....	12
13. Phishing	12
13.1 Phising via e-mail.....	13
13.2 Phishing via de telefoon	14
14. Wachtwoorden.....	14
15. Tot slot:.....	15

1. Het belang van updates installeren

Updates worden automatisch geïnstalleerd en daar hoeft je niets voor te doen. Het is zelfs niet uit te schakelen in Windows 10.

Windows 10 biedt je echter wel de keuze om te bepalen wanneer en hoe je de meest recente updates wilt ontvangen om je apparaat soepel en veilig te laten werken. Als je je opties wilt beheren en beschikbare updates wilt bekijken, selecteer je Controleren op Windows-updates. Of selecteer de Startknop en ga vervolgens naar Instellingen > Bijwerken en beveiliging > Windows Update.



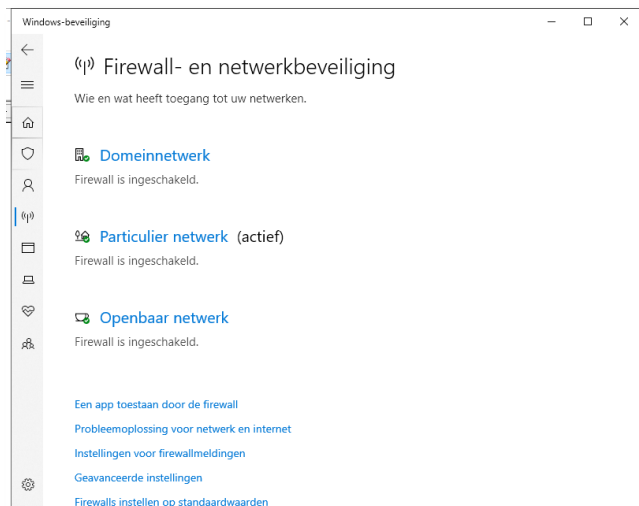
Mocht je problemen ondervinden met updates, zie <https://support.microsoft.com/nl-nl/help/4089834/windows-10-troubleshoot-problems-updating>.

2. Firewall

Een firewall is software of hardware die informatie die van internet of een netwerk binnenkomt, controleert en deze informatie vervolgens blokkeert of naar jouw computer doorlaat, al naar gelang jouw firewallinstellingen.

Je kunt een firewall gebruiken als je wilt voorkomen dat hackers of schadelijke software (zoals worms) via een netwerk of internet toegang tot jouw computer krijgen. Het gebruik van een firewall kan er daarnaast toe bijdragen dat het verzenden van schadelijke software vanaf jouw computer naar andere computers wordt geblokkeerd.

Een firewall is niet hetzelfde als een antivirusprogramma. Om jouw computer goed te beveiligen heb je naast een firewall software nodig die jouw computer beveiligt tegen virussen en schadelijke software.



Standaard staat de firewall van Windows aan. Het programma maakt onderdeel uit van Windows Defender.

Meer info over Windows Defender:

- <https://www.seniorweb.nl/artikel/defender-de-ingebouwde-virusscanner-in-windows-10>
- <https://nl.safetynet.com/best-antivirus/windows-defender/>

Meer info over firewall:

- <https://www.kaspersky.nl/resource-center/definitions/firewall>

3. Antivirusprogramma

Antivirussoftware is software die probeert om computervirussen te identificeren, tegen te houden en te verwijderen.

Normaal gesproken is één virusscanner voldoende om jouw computer te beveiligen. Windows bevat een ingebouwde virusscanner.

Daarnaast bestaat de mogelijkheid om een online scan laten uitvoeren. Deze kun je gebruiken naast jouw eigen virusscanner als extra check of als second opinion. Als je een bepaald bestand niet vertrouwt maar toch geen melding krijgt van jouw eigen virusscanner kun je de online virusscanner gebruiken. Je kunt het ook gebruiken als je een viruswaarschuwing krijgt die niet terecht lijkt.

Het is zeker aan te raden om eens in de zoveel tijd jouw computer te laten scannen door zo'n online virusscanner.

Gratis online virusscanners:

- <http://housecall.trendmicro.com/nl/>
- <http://www.pandasecurity.com/activescan/index/>
- <https://www.eset.com/nl/thuis/online-scanner/>
- <https://www.f-secure.com/nl/home/free-tools/online-scanner>

4. Adblock Plus

Adblock Plus blokkeert irritante advertenties op het web. Het blokkeert ook andere zaken, zoals tracking.

Meer info over Adblock Plus:

- <https://adblockplus.org/nl/about>

Downloaden:

- <https://adblockplus.org/>

5. Cookies

Een cookie is een klein tekstbestand dat tijdens jouw bezoek aan een website op jouw computer wordt geplaatst. In dit tekstbestand wordt informatie opgeslagen. Deze informatie kan op een later bezoek weer worden herkend door deze website. Sommige cookies zijn noodzakelijk. Omdat de website het anders niet doet. Er zijn ook cookies die handig zijn voor de bezoeker. Bijvoorbeeld omdat hij onthoudt in welke taal je de website wilt lezen.

In cookies kunnen ook persoonlijk identificeerbare gegevens worden opgeslagen. Persoonlijk identificeerbare gegevens zijn gegevens die kunnen worden gebruikt om je te identificeren en met je contact op te nemen, zoals jouw naam, e-mailadres, huis- of werkadres, of jouw telefoonnummer. Een website heeft echter alleen toegang tot de persoonlijk identificeerbare gegevens die je opgeeft. Jouw e-mailadres kan bijvoorbeeld alleen door een website worden bepaald als je het opgeeft. Een website heeft evenmin toegang tot andere gegevens op jouw computer.

Een cookie die op jouw computer is opgeslagen, kan alleen worden gelezen door de website waardoor de cookie is gemaakt.

Er zijn weliswaar geen veiligheidsproblemen met het gebruik van cookies, maar cookies kunnen wel een aantasting van de privacy van webgebruikers vormen. Het cookiemechanisme kan bijvoorbeeld door websites gebruikt worden om te traceren welke 'wandeling' een gebruiker maakt door zijn pagina's, zogenaamde tracking cookies. Sporen van een gebruiker kunnen precies gevolgd worden.

Meer info over cookies:

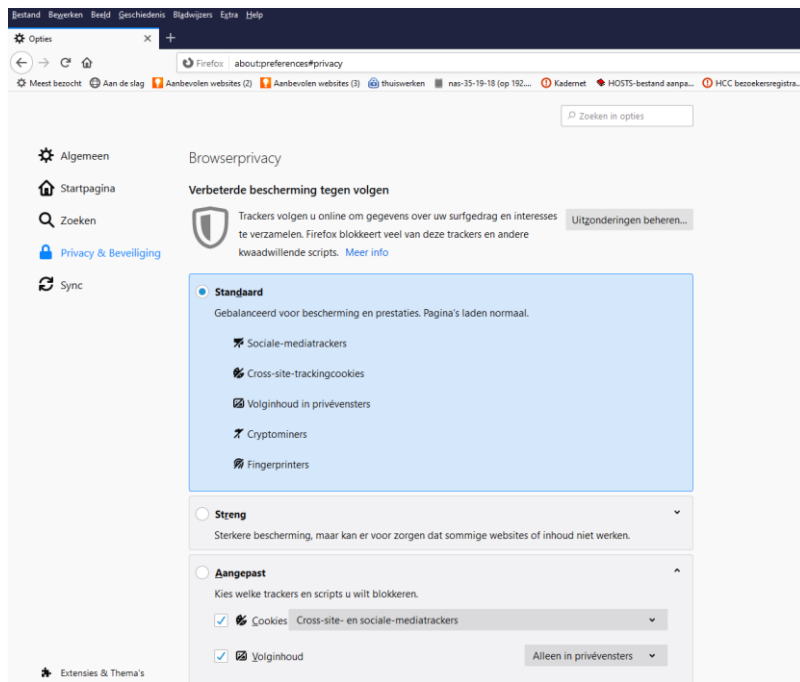
- <https://www.consumentenbond.nl/internet-privacy/wat-zijn-cookies>
- <https://www.consuwijzer.nl/telecom-post/internet/privacy/uitleg-cookies>

5.1 Cookies beheren

Binnen elke browser is het mogelijk om cookies te beheren. Een voorbeeld hieronder van Firefox.

5.1.a FireFox

Ga naar Menu openen (☰) → Opties → Privacy & Beveiliging



5.2 CCleaner

Met dit programma kunnen in één keer op eenvoudige wijze allerlei gegevens verwijderd worden van de geïnstalleerde browsers, zoals cookies en de cache.

Meer info over CCleaner:

- <https://www.seniorweb.nl/artikel/36928/computer-opschonen-met-ccleaner;>
- <https://nl.wikipedia.org/wiki/CCleaner>

Meer info over cache:

- <https://www.browserchecker.nl/cache-bestanden-verwijderen>
- <https://www.seniorweb.nl/tip/wat-is-cache>

6. Browser finger printing

Websites kunnen je volgen via trackingcookies. Die kun je uitzetten in de browser. Maar ook zonder cookies kunnen websites je herkennen. Hoe werkt het en wat kun je ertegen doen?

Device fingerprinting is een techniek die gebruikmaakt van een simpel gegeven. Computers verschillen - altijd - van elkaar. Denk aan verschillen in besturingssysteem, browserversie, schermresolutie en nog veel meer gegevens.

Die combinatie kan een unieke vingerafdruk opleveren waar de bezoeker aan te herkennen is. Die vingerafdruk wordt gebruikt om fraude of misbruik van de website te voorkomen, maar ook om gericht te adverteren.

Je kunt voor Chrome en Firefox ook een losse extensie installeren die canvas fingerprinting herkent en tegengaat, d.i. Canvas Defender.

- Canvas Defender voor Firefox (<https://addons.mozilla.org/nl/firefox/addon/no-canvas-fingerprinting/>)
- Canvas Defender voor Chrome (<https://chrome.google.com/webstore/detail/canvas-defender/obdbgnebcljmgkoljcdddaopadkifnpm>)

Meer info over browser finger printing:

- <https://www.consumentenbond.nl/internet-privacy/browser-fingerprinting>
- <https://computerworld.nl/security/101760-zo-verberg-je-je-voor-browser-fingerprinting>

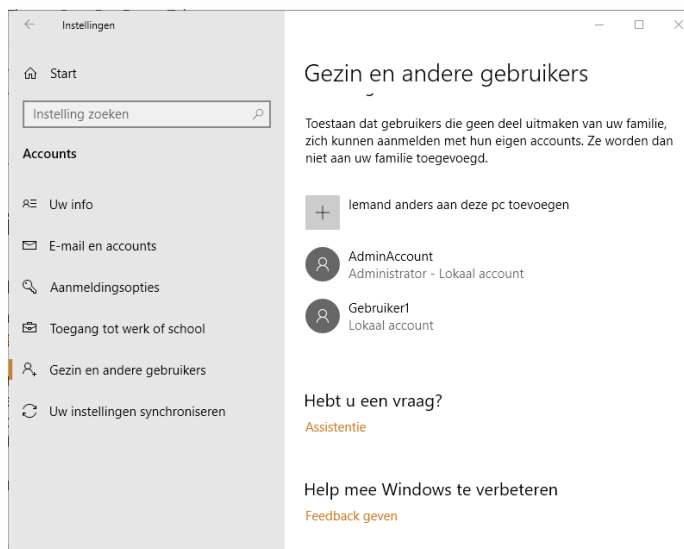
7. Gebruik geen administrator account

De impact van negen van de tien kwetsbaarheden in Windows is te beperken of zelfs te voorkomen als je niet zijn ingelogd of niet de rechten hebt als administrator.

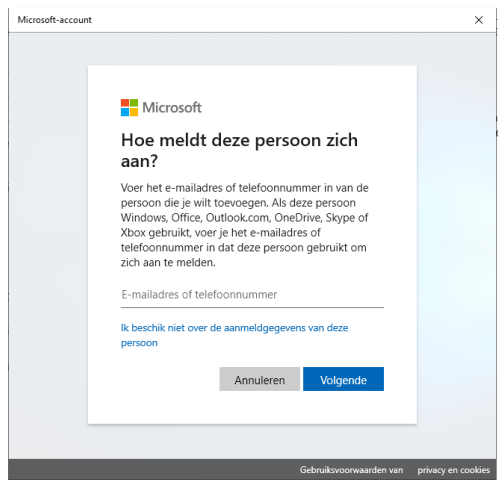
Er zijn twee typen accounts. Elk type geeft je een verschillend niveau van beheer op jouw computer:

- Standaardaccounts zijn voor dagelijkse computerwerkzaamheden.
- Administratoraccounts bieden de uitgebreidste rechten voor de computer. Gebruik deze accounts alleen wanneer dit nodig is.

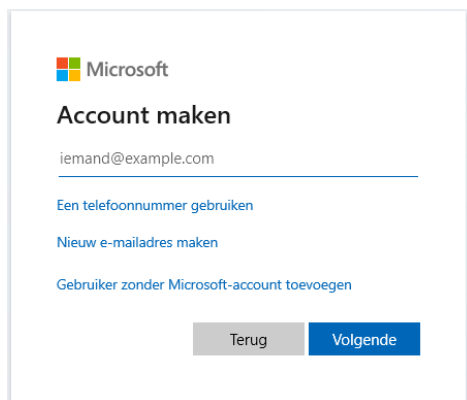
Nieuw account aanmaken, ga naar Instellingen → Accounts → Gezin en andere gebruikers → Iemand anders aan deze pc toevoegen.



Kies vervolgens voor *Ik beschik niet over de aanmeldgegevens van deze persoon*.



Kies *Gebruiker zonder Microsoft-account toevoegen*.



Voer in Gebruikersnaam en wachtwoord.

Een account maken voor deze pc

Als u een wachtwoord wilt gebruiken, kies dan iets dat u gemakkelijk kunt onthouden maar voor anderen moeilijk te raden is.

Wie gaat deze pc gebruiken?

Geef uw gebruikersnaam op.

Zorg dat het veilig is.

Meer info over accounts:

- https://www.schoonepc.nl/windows10/werken_met_gebruikersaccounts.html

8. Andere browsers

8.1 Browser in the box (BitBox)

Eenvoudig veilig surfen. Als je in een veilige omgeving wilt surfen of internetbankieren is de Browser in the Box een goede optie.

Omdat de tool in een virtuele omgeving creëert, ben je beschermd tegen virussen en hackers. In deze omgeving ben je op geen enkele manier beperkt, dus bijvoorbeeld Flash werkt ook in de omgeving.

Downloaden:

- https://www.chip.de/downloads/BitBox-Browser-in-the-Box-Firefox-Edition_48987303.html
- <https://www.pcwelt.de/downloads/Browser-in-the-Box-BitBox-3405376.html>

8.2 Tor Browser

De Tor Browser is een browser die verkeer via het Tor-netwerk anonimiseert, zodat gebruikers hun identiteit beter kunnen maskeren.

Meer info over Tor browser:

- <https://computerworld.nl/algemeen/105936-zo-werkt-de-tor-browser>
- <https://www.torproject.org/>

Zie het verschil bij bezoek www.watismijnipadres.nl!

IP-adres via TOR browser:



Ip-adres andere browsers:

IP adres informatie

Wat is een IP adres? Wat is IPv6? Wat is een MAC adres? Wat is DHCP?

Wat is mijn IP adres?

Mijn IP adres is: **212.187.90.95**

Mijn hostname is: c90095-upc-c.chello.nl
Mijn internet provider is: Ziggo

Wanneer je problemen hebt met je internetverbinding, neem dan contact op met jouw internet provider. De internet provider die wij automatisch voor je hebben gedetecteerd op basis van onze gegevens is Ziggo. Mocht dit niet juist zijn, dan is de kans groot dat je provider Ziggo of KPN is. Gezamenlijk zijn deze 2 partijen goed voor zo'n 85% van de Nederlandse breedbandmarkt.

Maak je gebruik van een proxyserver, dan zal het IP adres van de proxyserver vermeld staan achter 'mijn ip adres is'.

Wat is mijn locatie?

Breedtegraad: 51.958900 (51°57'32.04" N)
Lengtegraad: 5.970300 (5°58'13.08" E)



Het gebruik van Tor browser is legaal, maar mijdt het zogenaamde Dark Web!

9. Hostfile

Een HOSTS file of HOSTS bestand is een tekstbestand die door het besturingssysteem wordt gebruikt om hostnamen aan IP adressen te koppelen. Dit bestand vind je in de map C:\Windows\System32\Drivers\Etc.

```
hosts - Kladblok
Bestand Bewerken Opmaak Beeld Help
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10        x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         localhost
#       ::1               localhost
#
# 127.0.0.1       www.gtiemens.nl
```

Een voorbeeld: 127.0.0.1 www.gtiemens.nl

Deze regel zorgt ervoor dat "www.gtiemens.nl" doorgestuurd wordt naar 127.0.0.1. 127.0.0.1 is de "localhost", wat inhoudt dat deze website doorgestuurd wordt naar jouw eigen computer. Dit zal

resulteren in een "Pagina die niet kan worden weergegeven". Op deze wijze kunnen veel slechte of ongewenste sites geblokkeerd worden.

Meer info over hosts:

- <http://plazilla.com/page/4295006394/wat-is-je-hosts-file>
- https://www.schoonepc.nl/nieuwsbrief/hosts-bestand_aanpassen.html

10. Alternatieven voor Google

Er zijn veel zoekmachines die het meestal niet zo nauw nemen met de privacy of niet fijn werken. Dat geldt niet voor:

- DuckDuckGo (<https://duckduckgo.com/>)
- Startpage (<https://www.startpage.com/>)

11. SpywareBlaster

SpywareBlaster voorkomt de installatie van spyware en andere ongewenste software. Verder kan met dit programma een back-up van het HOSTS-bestand (zie verder onder 9) worden gemaakt.

Meer info over SpywareBlaster:

- <https://nl.wikipedia.org/wiki/SpywareBlaster>
- <https://computertotaal.nl/overige-elektronica/spywareblaster-in-3-stappen-malwarevrij-62334>

12. Malware

Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen. Het woord is een samentrekking van het Engelse malicious software. Malware veronderstelt kwade opzet (bron: Wikipedia).

Typen malware:

- Adware - infecteert de computer met reclamesoftware en laat vaak pop-ups verschijnen.
- Bootsectorvirus - infecteert het opstartgedeelte op een harde schijf of diskette.
- Backdoor - is in een programma geplaatst om toegang tot een systeem of programma te krijgen.
- Computervirus - infecteert bestanden en richt vaak schade aan.
- Computerworm - verspreidt zich direct over het netwerk en richt vaak schade aan.
- Dialer - verbindt de modem met een duur telefoonnummer.
- IRC-bot - verbindt de geïnfecteerde computer met een netwerk van waaruit de computer bestuurd kan worden.
- Keylogger - kan de toetsaanslagen of de muisbewegingen en wat er op het scherm getoond wordt registreren.

-
- Ransomware - blokkeert de computer of de gegevens die erop staan en vraagt vervolgens geld van de gebruiker om de blokkade op te heffen (zie verder onder 12.a).
 - Rootkit - geeft een computerkraker toegang tot de computer.
 - Spyware - geeft gegevens van de gebruiker door aan derden.
 - Rogueware of scareware - tracht de gebruiker ertoe te bewegen geld te betalen voor het verwijderen van onechte bedreigingen en waarschuwingen.
 - Trojaans paard - doet zich voor als iets anders dan het daadwerkelijk is en richt dan schade aan of functioneert als spyware.

Meer info over malware:

- <https://opgelicht.avrotros.nl/hulp/vraag-antwoord/artikel/wat-is-malware/>
- <https://www.vpngids.nl/veilig-internet/malware/>

12.a Ransomware

Ransomware is kwaadaardige software die een apparaat infecteert en de bestanden op die computer in gijzeling neemt.

Ransomware verspreidt zich net als ieder ander virus. Je opent – per ongeluk of in onwetendheid – een geïnfecteerd bestand. De ransomware wordt hiermee op het besturingssysteem van de computer geïnstalleerd.

Besmetting van bestanden op een computer kan gebeuren door een bijlage in een e-mail te openen of tijdens het surfen op internet. De ransomware kan ook verstopt zijn in advertenties. Je hoeft dan niet eens op een advertentie te klikken om besmet te raken. Het openen van een pagina is soms al voldoende voor een besmetting!

Doorgaans zijn er twee type gijzelsoftware: crypto-ransomware en locker-ransomware. Bij crypto-ransomware worden waardevolle documenten op je apparaat vergrendeld zodat je er niet bij kan. Bij locker-ransomware worden er geen documenten vergrendeld, maar kun je als slachtoffer je computer helemaal niet meer in.

Algemeen advies: betaal géén losgeld!!

Meer info over ransomware:

- <https://www.vpngids.nl/veilig-internet/malware/wat-is-ransomware/>
- <https://www.politie.nl/themas/ransomware.html>
- <https://www.nomoreransom.org/nl/index.html>

13. Phishing

Phishing (naar analogie van phreaking, is het afgeleid van fishing: "vissen", "hengelen") is een vorm van internetfraude. Het bestaat uit het oplichten van mensen door ze te lokken naar een valse (bank)website, die een kopie is van de echte website, om ze daar – nietsvermoedend – te laten inloggen met hun inlognaam en wachtwoord of hun creditcardnummer. Hierdoor krijgt de fraudeur

de beschikking over deze gegevens met alle gevolgen van dien. De fraudeur doet zich hierbij voor als een vertrouwde instantie, zoals een bank.

13.1 Phishing via e-mail

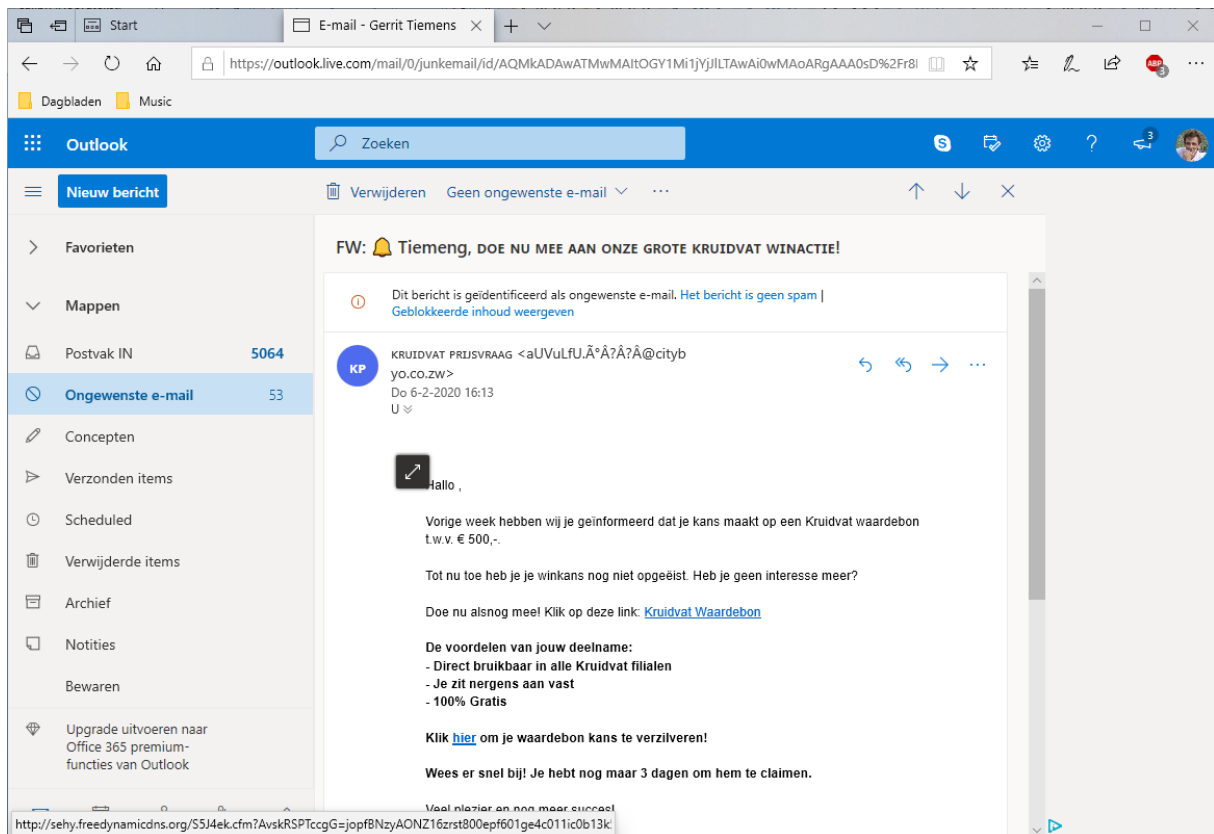
De meeste vormen van phishing vinden plaats via e-mail. Je wordt hierbij met een e-mail naar deze valse website gelokt. De mail bevat een link naar een (valse) website met het verzoek om zogenaamd "de inloggegevens te controleren" (bron: Wikipedia).

Hoe herken je een phishing e-mail?

- Controleer het adres van de afzender. De naam van de afzender mag dan precies hetzelfde zijn als die van je bank of webwinkel, maar vaak is het gebruikte e-mailadres vaag of een afgeleide versie van een echte bedrijfsnaam of de naam van een instantie.
- Kijk goed naar de domeinnaam waarvan je de e-mail hebt ontvangen. De domeinnaam is te herkennen aan alles wat achter het @-teken in het e-mailadres staat.
- Controleer of het e-mailadres ook echt overeenkomt met het websiteadres. Een veel gebruikte manier om valse e-mails te verspreiden is namelijk het vervangen van bepaalde letters uit de domeinnaam door cijfers.
- Het verschil tussen een legitiem en vals e-mailadres kan soms moeilijk te onderscheiden zijn. In het volgende voorbeeld is 1 (cijfer) vervangen door een l (letter). Vergelijk mail@31008mailers.nl en mail@3l008mailers.nl.

Controle:

- Kijk hoe het e-mailadres is opgebouwd.
- Ga met de muis op de link staan (niet klikken!!) in de mail en kijk links onder wat de link is.



13.2 Phishing via de telefoon

Phishing kan ook via de telefoon plaatsvinden. Je wordt dan gebeld door een zogenaamde medewerker van de bank of Microsoft. Echter: Microsoft, banken of andere instanties zullen je nooit bellen en je ook niet vragen om handelingen te verrichten op je pc!

Meer info over phishing:

- <https://www.veiligbankieren.nl/online-fraude/phishing/>
- <https://www.digitaltrustcenter.nl/hoe-herken-ik-een-phishing-e-mail>

14. Wachtwoorden

Om je online diensten goed beveiligd te houden, is het van belang dat je verschillende wachtwoorden hebt voor de diensten die je gebruikt.

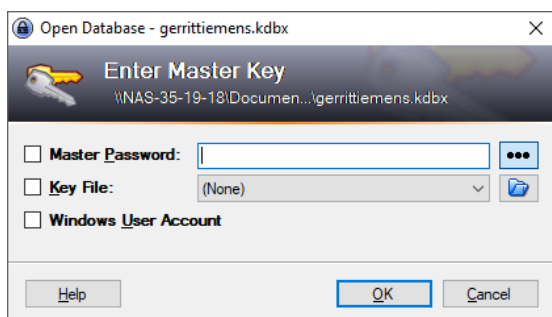
Om wachtwoorden aan te maken, kun je gebruik maken van een online wachtwoord generator, bijvoorbeeld <https://www.lastpass.com/nl/password-generator>. Hiermee maak je sterke wachtwoorden aan.



Meer info over wachtwoorden:

- <https://radar.avrotros.nl/hulp-tips/hulpartikelen/item/6-voorwaarden-voor-veilige-wachtwoorden/>

Wachtwoorden kun je vastleggen in een zogenaamde wachtwoordmanager. Een ervan is Keepass. Deze is gratis.



Meer info over wachtwoorden:

- <https://radar.avrotros.nl/hulp-tips/hulpartikelen/item/6-voorwaarden-voor-veilige-wachtwoorden/>

Meer info over Keepass:

- <https://www.consumentenbond.nl/internet-privacy/keepass-wachtwoordkluis>

15. Tot slot:

Handige links:

- <https://veiliginternetten.nl/>

-
- https://www.seniorweb.nl/online-veiligheid?utm_source=bing&utm_medium=cpc&utm_campaign=Veiligheid&utm_term=veilig%20internetten&utm_content=Veilig%20internetten
 - <https://www.consumentenbond.nl/veilig-internetten>
 - <https://www.mijnonlineidentiteit.nl/veilig-internetten-tips/>