

● Kort Goed ●

Rein de Jong

Zo af en toe inspireert mij een gedachte, ideetje of kort bericht, waarvan ik denk dat die inspiratie voor meer mensen waardevol kan zijn. Die gedachten en ideeën wil ik graag delen.



1. Windows- en MS-Office-versies

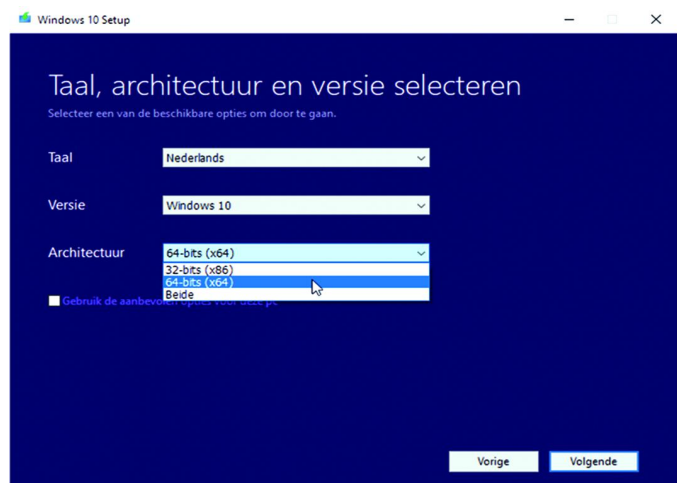
Bijna alle Windows- en Office-versies zijn van het internet op te halen. Het is verstandig om de door jou gebruikte versie(s) altijd op een USB-stick beschikbaar te hebben. Altijd fijn bij eventuele calamiteiten of voor een nieuwe installatie. Na het aanmaken kun je op een aangemaakte USB-stick meestal ook nog wat handige tools kwijt. Denk daarbij aan Total Commander, wachtwoordspuinders en diverse testprogramma's.

1.1. Het officiële distributiekanaal

Windows

Microsoft stelt op zijn website¹ altijd de meest recente Windows-versie beschikbaar. Vanaf die pagina kun je een Hulpprogramma, de Media Creation Tool (MCT) downloaden om daarmee een USB-stick, DVD en/of ISO te maken. De MCT stelt je in staat om een opstart/installatie-medium voor alle beschikbare talen en varianten in zowel een 32- als 64-bits uitvoering te vervaardigen.

Eén keer downloaden en dan handig voor gebruik op meerdere machines totdat de nieuwe halfjaarlijkse update verschijnt.



MS Office

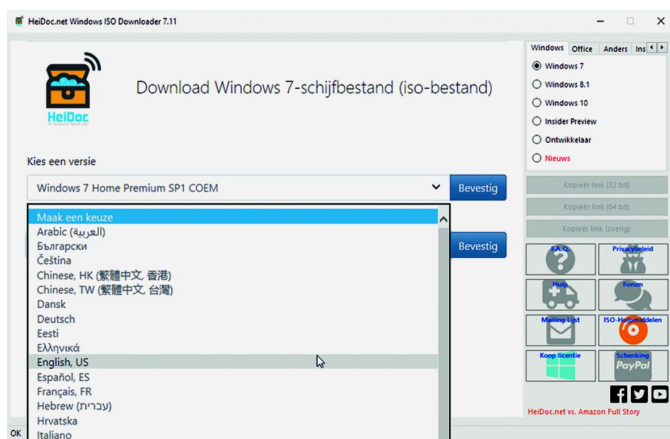
Office 365 kun je downloaden vanuit je Microsoft-account² bij Services en abonnementen. Heb je een andere Office-versie (vanaf 2010), dan kun je die ophalen op de webpagina met eerdere versies van Office³. Vul je productcode in en de download wordt voor je klaargezet.

TiP: Office 365 Home (€ 99,- /jr) kun je delen met vijf andere personen. Eenieder krijgt dan voor € 16,50 p.p./jr: Office, 1 TB OneDrive en 60 gratis belminuten voor Skype. Het enige wat je deelt is de rekening van € 99,-.

Windows Insider-versies

De insiderversies zijn bètaversies van Windows die je kunt ophalen⁴ nadat je bent aangemeld voor het Windows Insider-programma met een Microsoft-account. Het blijven bètaversies en zijn daarom niet geschikt voor productiedoeleinden en gevoelige data.

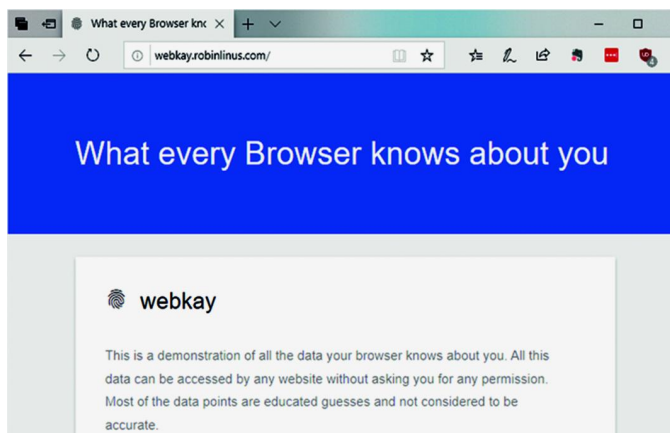
1.2. Het andere distributiekanaal



Alle Windows-versies (vanaf 7) en Office-versies (vanaf 2010) kunnen, in alle beschikbare talen, worden gedownload met de Microsoft Windows en Office ISO Download Tool⁵ van de Nederlander Jan Krohn. Deze ISO's komen direct van de Microsoft-servers en zijn veilig. Uiteraard heb je wel een productleutel nodig of hardware die al eerder onder Windows 10 is gebruikt.

TiP: Je kunt een nieuwe Windows 10-versie met elke legitieme Windows 7/8/8.1-sleutel installeren door die sleutel bij installatie of later bij activatie in te voeren.

2. Wat elke browser van je weet!



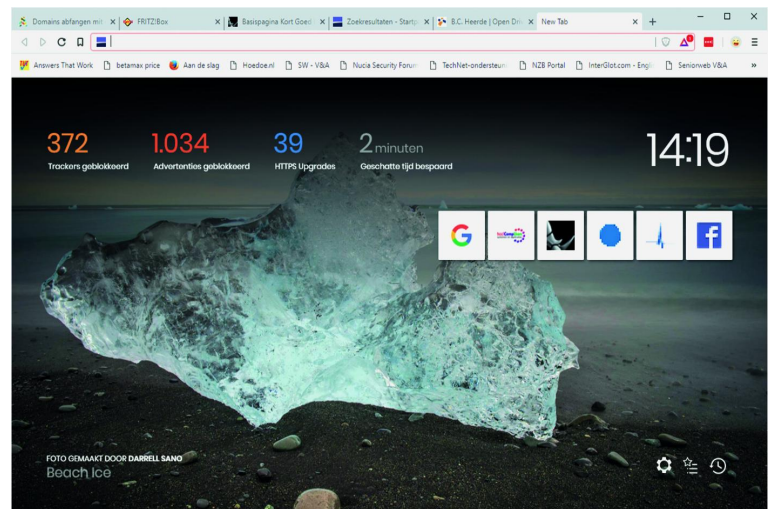
Mocht je denken anoniem op internet te kunnen surfen met standaard browsers, zoals Chrome, Edge, Firefox, Safari e.d., dan kom je bedrogen uit, alle extra instellingen en plug-ins ten spijt. Ook de incognito-modus <Ctrl+Shift+P> is niet zo verullend en maakt nog veel bekend over jou en de

gebruikte hardware; vaak wordt zelfs je locatie onthuld. Wil je weten wat? Surf dan naar de website van Robin Linus⁶: <http://webkey.robinlinus.com> (webkey=What Every Browser Knows About You). Een aanvulling op Webkey is Panopticlick⁷.

Voor een betere bescherming van je privacy kun je browsers ook uitbreiden met plug-ins, zoals:

- Edge: uBlock Origin, Ghostery,
- Chrome: ScriptSafe, Adblock Plus, HTTPS Everywhere en Canvas Blocker
- Firefox: NoScript, uBlock Origin, HTTPS Everywhere, Stop Fingerprinting en Windscribe

Wil je je hier maximaal tegen beschermen? Gebruik dan een VPN-server, zodat je IP-adres wordt gemaskeerd of surf volkomen anoniem met de TOR-browser. Alleen is die laatste vaak erg traag in het gebruik, maar wel de beste methode om volkomen anoniem te surfen.



Een goed alternatief is de razendsnelle browser Brave⁸, die ik zelf naast mijn Windows-pc's ook op mijn Android-telefoon gebruik. Brave is tevens beschikbaar voor Mac, Linux en iOS. In tegenstelling tot de eerder genoemde browsers is Brave bij installatie al goed ingesteld voor veiligheid en privacy!

3. Microsoft gaat Chrome helpen verbeteren



Je vraagt je af, wat is dit voor een vreemde titel?

Welnu: Microsoft heeft besloten om Chromium als basis voor hun Edge-browser te gaan gebruiken.

Chromium is het open-sourceproject dat de basis vormt van veel browsers, waaronder Chrome, Opera en Brave. Het gevolg daarvan is dat Microsoft zich uitdrukkelijk gaat bemoeien met Chromium. Daardoor zullen Chromium, en dus ook Chrome, en alle andere op Chromium gebaseerde browsers, alleen maar beter worden. Vooral op het gebied van de touch-bediening zou Microsoft veel kunnen bijdragen. De samenwerking betekent dat Edge-HTML, de laatste gesloten browser-engine, wordt verlaten. Dat is geweldig nieuws. De keerzijde is dat Google en Microsoft gaan samenwerken en zo een grotere controle over het internet krijgen.

4. Sim-swapping!



Het kapen van je mobiele nummer heet 'sim-swapping'. Helaas is er nog geen goed Nederlands woord voor. Misschien dat sim-kaping er dicht bij komt. Die kreet ben ik elders nog niet tegengekomen. Het komt er op neer dat een onbevoegde door het juist beantwoorden van een aantal beveiligingsvragen (o.a. geboortedatum, adres, rekeningnummer), jouw telefoonnummer kan omzetten naar een eigen sim-kaart. Zo wordt toegang gekregen tot een aantal diensten die aan jouw telefoonnummer zijn gekoppeld, waaronder de sim-verificatie.

Je merkt het zelf doordat je sim-kaart het niet meer doet. Waarschuw dan je provider en verder rest niets anders dan het zo snel mogelijk wijzigen van de getroffen wachtwoorden en het aanvragen van een nieuw telefoonnummer. Je kunt je extra beveiligen door een wachtwoord bij de telecomprovider te deponeren. Dat wachtwoord wordt dan gevraagd bij telefonische wijzigingen.

Ook dat is niet waterdicht doordat de medewerkers vanwege de lage salarissen gevoelig kunnen zijn voor omkoping. Beter zou het zijn wanneer de providers bij een telefonische aanpassing een sms-verificatie zouden verzenden in combinatie met een waarschuwing naar het mailadres dat bij de provider bekend is. Kan één van beide niet, dan is een brief per post op zijn plaats.

Daarnaast is het zaak om je telefoonnummer zoveel mogelijk te verwijderen van online-diensten. Gebruik in plaats van een tweestapsverificatie (2FA) per sms de authenticator-app van Authy⁹ die je op meerdere apparaten kunt gebruiken voor 2FA voor bijvoorbeeld LastPass, Twitter, Facebook, Microsoft of Google. Daarnaast is het wijs om je PIN-code en wachtwoord bij de telecomprovider te wijzigen.

Links:

Mijn eigen site	https://www.reindejong.nl/
1. Windows	http://bit.ly/r-win10
2. MS-account	http://bit.ly/r-ma
3. Office-versies	http://bit.ly/r-off
4. Windows Insider	http://bit.ly/r-wi
5. ISO-downloader	http://bit.ly/r-wodt
6. Browser test	http://bit.ly/r-bt
7. Panopticlick	http://bit.ly/r-pano
8. Brave	http://bit.ly/r-br
9. Authenticator App	http://bit.ly/r-authy
10. DiskPart	http://bit.ly/r-dp

4.1. Disk of Volume 'Read-only' maken!

Soms is het wenselijk om een hele schijf of partitie tegen schrijven te beveiligen. Dat doe je in het geval van data-herstel of als je sowieso niets op schijf wilt schrijven of wanneer je een usb-stick met waardevolle gegevens, zoals foto's, films of een presentatie, uitleent. Dit kan eenvoudig met het Windows-programma DiskPart¹⁰. Hoe doe je dat?

Open een Command prompt of PowerShell (*Win+X > PowerShell*). Tik in: *Diskpart <Enter>*; er wordt nu om Admin-rechten gevraagd en dan verschijnt het Diskpart-command-scherm.

```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\WINDOWS\system32> diskpart

Microsoft DiskPart version 10.0.17763.1

Copyright (C) Microsoft Corporation.
On computer:
DISKPART>
```

Tik nu de volgende commando's gevolgd door een <Enter>:

4.1.1 Een hele schijf (USB-disk) beschermen:

```
list disk
select disk x
X is het schijf die je 'read only' wenst te maken.
Kijk goed dat je de juiste selecteert.
Dat kun je controleren met het commando: detail disk
att disk set readonly
```

Ongedaan maken van de schrijfbeveiliging doe je met het commando:

```
att disk clear readonly
```

4.1.2. Een partitie beschermen

```
list volume
select volume x
X is het volumenummer dat je 'read only' wenst te maken.
Kijk goed dat je de juiste selecteert.
Dat kun je controleren met het commando: detail volume
att vol set readonly
```

Ongedaan maken van de schrijfbeveiliging doe je met de commando:

```
att vol set clear
```

