# WACHTWOORDMANAGERS

Thom Bloks

Het volgende verhaal gaat over het gebruik van wachtwoordmanagers.

Deze zijn belangrijke hulpmiddelen bij het beheren van het meest belangrijke en complexe op een computer namelijk de grote hoeveelheid wachtwoorden die we moeten gebruiken voor de diverse programma's en websites. Hierbij dus een handreiking.

| De 25 meest gebruikte wachtwoorden zijn: | |
|---|---|
| 123456 | 666666 |
| 123456789 | 18atcskd2w |
| qwerty | 7777777 |
| 12345678 | 1q2w3e4r |
| 111111 | 654321 |
| 1234567890 | 555555 |
| 1234567 | 3rjs1la7que |
| password | Google |
| 123123 | 1q2w3e4r5t |
| 987654321 | 123qwe |
| qwertyuiop | Zxcvbnm |
| mynoob | 1q2w3e |
| 12332 | |

Verder worden vaak gebruikt:

- namen van familieleden
- Namen van huisdieren; geboorte- of andere belangrijke data
- Namen van huisdieren
- Datums van geboorte of andere belangrijke gebeurtenissen in het leven

Deze informatie is betrekkelijk eenvoudig te achterhalen via sociale media en wat zoeken met behulp van Google/Bing.

# Nooit doen dus!!!

Wat doen we nog meer fout???

- Bijna iedereen gebruikt hetzelfde wachtwoord méér dan één keer!!!

Soms gebruiken we zelfs maar **één** wachtwoord voor alles waar een wachtwoord ingevuld moet worden.

U zult begrijpen dat wanneer dat ene wachtwoord bekend raakt bij de verkeerde personen de rapen gaar zijn?

Er zijn al vaker tips gegeven om er voor te zorgen dat onbevoegden niet bij uw data kunnen komen:

- Een sterk wachtwoord
- Daar waar mogelijk tweestapsverificatie gebruiken

Waar een sterk wachtwoord aan moet voldoen wordt zo meteen uitgelegd!

Voor zover de theorie; maar hoe moet dat nu in de praktijk? Het is immers bijna onmogelijk om meer dan drie ingewikkelde wachtwoorden te onthouden, laat staan 20 of meer want dat zou moeten voor iedere website die u bezoekt waar een wachtwoord ingevuld moet worden!!

In de praktijk zullen de meeste mensen ongeveer drie wachtwoorden hanteren die ze gemakkelijk kunnen onthouden maar zoals eerder gezegd brengt dat risico's met zich mee.

Er is niets op tegen om een redelijk simpel wachtwoord te gebruiken voor sites waar u alleen maar wat informatie opvraagt of waar u zich abonneert op een nieuwsbrief. Daar is niets aan verloren als dat wachtwoord bekend zou raken.

Voor sites waar u persoonlijke informatie moet achterlaten is het essentieel om een sterk wachtwoord te gebruiken.

Een sterk wachtwoord bestaat uit minimaal 6 tekens, bestaande uit hoofd- en kleine letters, cijfers en bijzondere tekens maar liever meer dan 6. Hoe langer het wachtwoord hoe moeilijker het te ontcijferen is.

Probeer zoveel mogelijk om logica in het wachtwoord te vermijden; ook dat maakt het moeilijker te ontcijferen.

Er zijn vele hulpmiddelen om wachtwoorden te maken en bewaren. Een van de beste gratis wachtwoordmanagers is LastPass. Dit programma gebruik ik zelf en ik zal er op de volgende pagina's wat meer van laten zien. Het neemt je een grote zorg uit handen in die zin dat je nooit meer zelf een wachtwoord hoeft te verzinnen. Het enige wachtwoord wat je nog moet onthouden is het wachtwoord van LastPass; maar let op: als je dat wachtwoord kwijt bent dan zit je zwaar in de penarie. Print dus een keer een lijst uit van je wachtwoorden en bewaar die op een veilige plek. Als alternatief zou je kunnen kijken naar KeePass.

LastPass is verkrijgbaar voor de volgende platformen.


Chrome


Edge


Windows


Explorer


Firefox

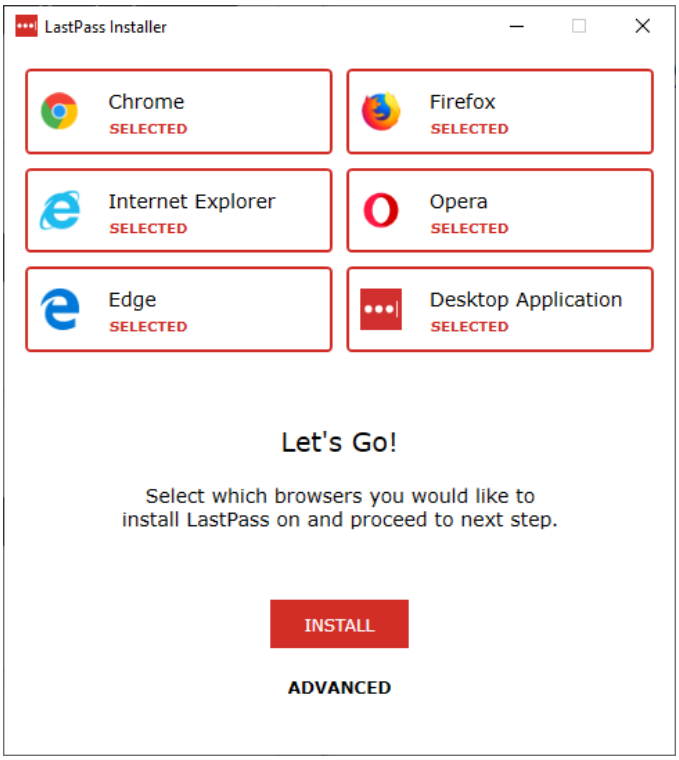

Opera


Zelfs voor Apple/Safari

Lastpass heeft ook Apps beschikbaar voor tablets en Mobiele apparaten.

De versie die u wenst is eenvoudig te downloaden vanaf:
**https://lastpass.com/misc_download2.php**

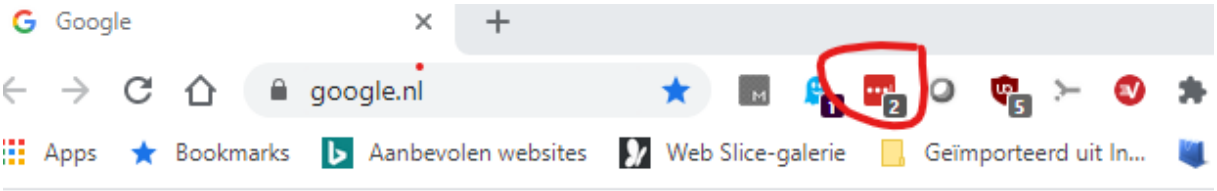
Wanneer u op installeren klikt, krijgt u het volgende venster te zien:



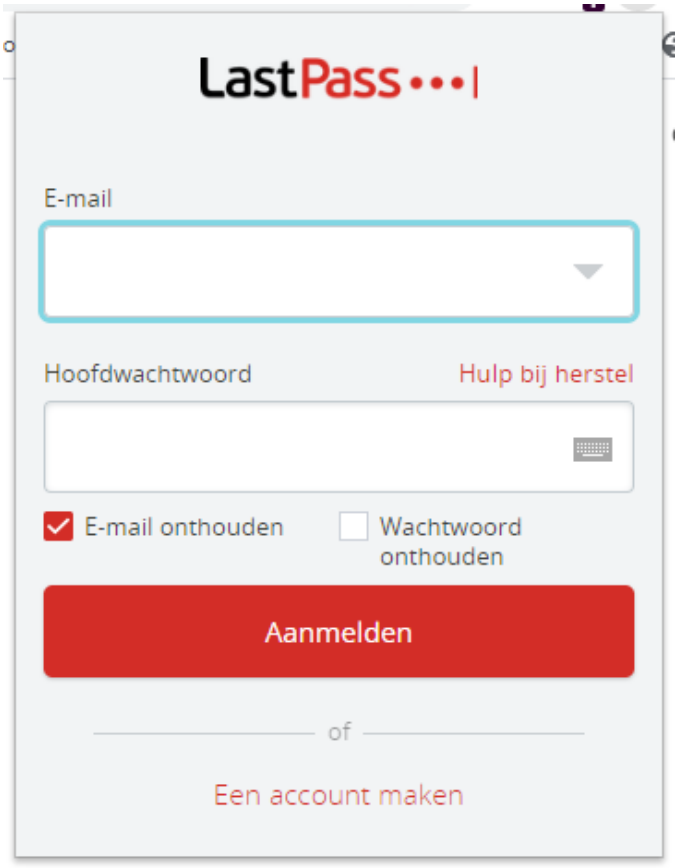

Het programma selecteert automatisch alle geïnstalleerde webbrowsers op uw systeem.

Bovenin aan de rechterkant van uw browser verschijnt een vakje met 3 puntjes. Zwart wanneer u NIET ingelogd bent bij Lastpass en rood wanneer u wel bent ingelogd.

In dit schermpje is het vakje met de witte puntjes rood omdat ik standaard ben ingelogd in LastPass .Als ik niet ben ingelogd is het vakje zwart en staat er geen cijfer bij.




Wanneer u op het zwarte vakje met drie witte puntjes klikt krijgt u het volgende venster te zien:

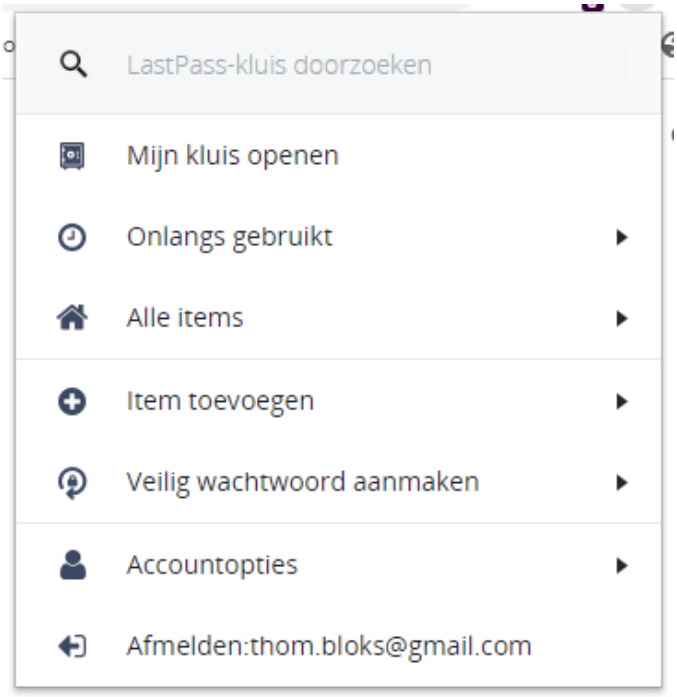



U vult uw emailadres in en een sterk wachtwoord van minimaal 11 tekens en klikt op Een account aanmaken en dat is het laatste wachtwoord dat u zelf moet verzinnen en onthouden.

U kunt er voor kiezen om uw emailadres en wachtwoord te laten onthouden.

Wanneer u de enige persoon bent die de computer gebruikt en hij staat op een vaste plek dan is daar niets op tegen maar wanneer het een laptop is dan is het natuurlijk niet verstandig het wachtwoord te laten onthouden want dan ligt alles nog steeds wijd open voor iedereen.

Een aantal mogelijkheden zal ik laten zien op de computer aan de hand van dit schemaatje:




In het bovenste vak kunt je invullen van welke toepassing of site in je kluis je het wachtwoord (automatisch) wilt laten invullen. Door te typen geeft het programma al suggesties.

Door op de tweede mogelijkheid van het rijtje te klikken open je je kluis met wachtwoorden en kun je op die manier de juiste site of toepassing selecteren.

Eigenlijk spreken alle mogelijkheden hier voor zichzelf maar een hele belangrijke is toch wel: “Veilig wachtwoord aanmaken”. Wanneer je hier op klikt doet het programma een suggestie voor een wachtwoord. Dit wordt volledig willekeurig gegenereerd aan de hand van criteria die je zelf in kunt stellen zoals lengte, toegestane tekens, enzovoorts.

Onder accountopties heb je ook de mogelijkheid om een veiligheidscheck uit te laten voeren. Hierbij wordt gekeken hoe veilig de wachtwoorden zijn die je in gebruik hebt.

Het behoort binnen het programma ook tot de mogelijkheden om een lijst te maken van alle wachtwoorden die je ingevoerd hebt in het programma. Wanneer je die in Excel importeert kun je de volgorde van de kolommen aanpassen aan je voorkeur en de lijst uitprinten zodat je een back-up hebt voor noodgevallen. Die moet je natuurlijk niet rond laten slingeren.

Het enige wachtwoord dat je voortaan nog maar hoeft te onthouden is je toegangswachtwoord tot Last Pass maar denk eraan dat je dat ene wachtwoord:

a. Veilig maakt
b. Nooit vergeet

Succes!!

## Proclamatie

Alle informatie in deze documentatie is uitsluitend bedoeld voor eigen gebruik. Wij hebben er èrg veel tijd en energie in gestoken om dit te maken! Respecteer onze intellectuele eigendomsrechten en geef niets hiervan door aan anderen, als kopie of in welke vorm dan ook!

Stichting SeniorWeb Mierlo