



## Sterke wachtwoorden maken en gebruiken



Uw wachtwoorden zijn de sleutels die u gebruikt om uw computer en online accounts te ontgrendelen. Hoe sterker het wachtwoord, des te beter is de beveiliging tegen aanvallen door hackers en dieven die uw gegevens zouden kunnen gebruiken voor het openen van nieuwe creditcardrekeningen, het afsluiten van een hypotheek of zelfs het online chatten onder uw naam - en u zou er pas achterkomen als het al te laat is. Het is niet moeilijk sterke wachtwoorden te maken. Met een klein beetje inspanning van uw kant en een aantal trucjes uit dit artikel kunt u de beveiliging van uw computer verbeteren.

### Op deze pagina

1. Controlelijst voor sterke wachtwoorden
2. Een sterk en gemakkelijk te onthouden wachtwoord in vier stappen
3. Uw wachtwoorden geheim houden
4. Uw wachtwoorden ophalen en wijzigen
5. Als uw wachtwoord wordt gestolen

### 1 Controlelijst voor sterke wachtwoorden

Een goed, sterk wachtwoord moet aan de volgende drie criteria voldoen:

- 1 **Meer dan acht tekens** lang. Korte wachtwoorden zijn gemakkelijker te kraken dan lange wachtwoorden.
- 2 Combineer **letters, cijfers en symbolen**, maar:
  - **Geen opeenvolgende** of herhalende combinaties, zoals '12345678', '222222', 'abcdefg' of aangrenzende letters op het toetsenbord
  - **Geen gewone woorden waarbij de letters vervangen zijn** door cijfers of symbolen, zoals 'M1cr0\$0ft' of 'W@chtw00rd'. Helaas kennen hackers deze trucjes ook.
- 3 **Voor u gemakkelijk te onthouden**, maar door anderen moeilijk te raden. Vermijd ook het volgende:
  - **Niet uw aanmeldingsnaam**, de naam van uw partner of uw geboortedatum.
  - **Geen woorden uit het woordenboek**, uit welke taal dan ook. Hackers gebruiken geraffineerde hulpmiddelen die snel wachtwoorden kunnen raden die gebaseerd zijn op woorden uit het woordenboek, uit een groot aantal talen, en die achterstevoren zijn gespeeld.
  - **Niet moeilijk te onthouden**. Als u toevallige combinaties van letters, cijfers en symbolen gebruikt die u alleen onthoudt als u ze opschrijft, kan het gebeuren dat u deze verkeerd invoert of dat deze door anderen worden gevonden en gebruikt.



Meet de sterkte van uw wachtwoorden met de [wachtwoordcontrole](#).

[http://www.microsoft.com/netherlands/thuisgebruikers/beveiliging/privacy/password\\_checker.msp](http://www.microsoft.com/netherlands/thuisgebruikers/beveiliging/privacy/password_checker.msp)



## Een sterk en gemakkelijk te onthouden wachtwoord in vier stappen

Een manier om een sterk en gemakkelijk te onthouden wachtwoord te maken, is het verzinnen van een 'wachtzin'. Hier is een manier om in vier stappen een wachtwoord te maken dat op een wachtzin is gebaseerd:

- 1 **Bedenk een zin** die u kunt onthouden, zoals "Mijn zoon André is drie jaar ouder dan mijn dochter Anna". Dit is dan uw wachtzin.
- 2 **Neem de eerste letter** van elk woord uit de zin om een nieuw woord te maken. In ons voorbeeld krijgt u: 'mzaidjodmda'.
- 3 **Maak hiermee een mix** van hoofdletters, kleine letters en cijfers. Voorbeeld: 'MzAi3jodmdA'
- 4 **Vervang tot slot enkele tekens door speciale tekens** die op letters lijken, om het wachtwoord nog sterker te maken. Deze trucjes leiden in dit voorbeeld uiteindelijk tot het volgende wachtwoord: 'Mz@i3jodmd@'.

Als u twijfelt of u de wachtzin kunt onthouden, neem dan eerst een gewone zin als uw wachtzin, zoals "Je kunt een oude hond geen nieuwe trucjes leren", en voeg minstens één cijfer of symbool aan het wachtwoord toe. Zo kan 'jkeohgntl' worden omgezet in 'JkeOHgnTL' of zelfs in 'Jke@HgnT1'.

## Uw wachtwoorden geheim houden

**Spring voorzichtig met uw wachtwoorden en wachtzinnen om.**

- **Geef ze niet aan** vrienden of familieleden (in het bijzonder kinderen) die ze weer aan andere, onbetrouwbare personen zouden kunnen doorgeven
- **Bewaar opgeschreven wachtwoorden niet** in uw bureau. Het briefje waarop u de wachtwoorden voor uw eigen gemak hebt genoteerd kan dieven die het vinden eenvoudig toegang verschaffen tot uw computer.
- **Verstrek nooit uw wachtwoord via e-mail**, zelfs als het verzoek van een betrouwbaar bedrijf of persoon komt. Bij **phishing** kan frauduleuze e-mail gebruikt worden om u ertoe te verleiden uw gebruikersnamen en wachtwoorden prijs te geven, zodat criminelen toegang kunnen krijgen tot uw accounts, uw identiteit kunnen stelen, enzovoort.

**Wijzig wachtwoorden regelmatig.** Idealiter moet u elke paar maanden nieuwe, sterke wachtwoorden voor uw accounts maken. Dit laat hackers in het ongewisse als ze een website in de gaten houden die u regelmatig bezoekt.

**Gebruik niet dezelfde wachtwoorden voor meerdere accounts.** U moet elke keer dat u een nieuwe account opent een nieuw, sterk wachtwoord maken.

**Schakel de optie 'Wachtwoord opslaan' niet in.** Als u een dialoogvenster te zien krijgt waarin u wordt gevraagd of uw computer het wachtwoord moet opslaan, kies dan **Nee**. Met deze optie kan iedereen die van uw computer gebruikmaakt, uw opgeslagen wachtwoorden voor deze accounts gebruiken.

## Uw wachtwoorden ophalen en wijzigen

### Online accounts

Websites kennen een verscheidenheid aan regels waarmee wordt bepaald hoe u toegang krijgt tot uw account en hoe u uw wachtwoord kunt wijzigen. Zoek op de startpagina van de site naar een koppeling (zoals 'uw account') waarmee u naar een bepaalde locatie op de site kunt gaan waar het wachtwoord- en accountbeheer zich bevinden



## Computerwachtwoorden

Normaal gesproken vindt u informatie over het maken van, het wijzigen van en het toegang krijgen tot gebruikersaccounts die met een wachtwoord zijn beveiligd, en over het verplicht invoeren van een wachtwoord na het opstarten van de computer, in de Help-bestanden van uw besturingssysteem of op de website van de fabrikant van het besturingssysteem. Als u bijvoorbeeld Microsoft Windows XP gebruikt, kunt u via [de Hulp en ondersteuningspagina voor Windows XP](#) meer informatie vinden.

## Als uw wachtwoord wordt gestolen

Zorg ervoor dat u al uw maandelijkse bankafschriften goed controleert. Sterke, makkelijk te onthouden wachtwoorden kunnen u beschermen tegen fraude en identiteitsdiefstal, maar ze bieden geen garanties. Als ondanks alles uw wachtwoord toch wordt gestolen, meld dit dan zo snel mogelijk aan het bevoegd gezag. Zie voor meer informatie het artikel [Wat te doen als slachtoffer bent van fraude met uw creditcard](#) over wat u moet doen als u denkt dat uw identiteit is gestolen of dat u het slachtoffer bent geworden van een soortgelijke fraude.

CMVG B.V.  
Rechtzaad 15  
4703 RC Roosendaal

Tel : 0165 785253  
Mobiel : 06 53769491  
E-mail : [info@cmvg.nl](mailto:info@cmvg.nl)  
Web : [www.cmvg.nl](http://www.cmvg.nl)

KvK NR : 20144131  
ING Bank : 676019560  
BTW NR : NL 8198.55.091.B01