Hoe beveilig je online accounts met een sterk wachtwoord?

Bron: NU.nl
Gepubliceerd: 30 maart 2018 16:16

Om gebruik te maken van diensten op het internet als Facebook, Instagram, Spotify of Gmail moet je een account aanmaken. Daarbij hoort een goed en sterk wachtwoord. Hoe kun je het beste omgaan met al die verschillende accounts en wachtwoorden?

Van Facebook en andere sociale media tot webwinkels en accounts bij allerlei andere diensten: we slaan steeds meer informatie over onszelf bij andere bedrijven op. Het gaat vaak niet alleen om een gebruikersnaam en wachtwoord, maar ook om andere persoonlijke gegevens, zoals je achternaam, adres en geboortedatum.

Waarom heb ik een goed wachtwoord nodig?
Een goed wachtwoord is in feite de sleutel tot jouw schatkist van persoonlijke gegevens, accounts bij allerlei diensten en andere gevoelige informatie. Eenmaal binnen bij zo'n account kan een internetcrimineel deze gegevens misbruiken. Hij kan je persoonlijke gegevens bijvoorbeeld gebruiken voor identiteitsfraude of je account bij een webshop om - op jouw naam - producten te bestellen. Het is daarom belangrijk om je gegevens met een sterk wachtwoord zo goed mogelijk te beveiligen.

Wat is een goed wachtwoord?
De regel is: hoe langer en willekeuriger een wachtwoord, hoe sterker hij is. Een goed wachtwoord bestaat uit een willekeurige mix van hoofdletters, kleine letters, cijfers en bijzondere tekens. We raden aan om je wachtwoord minstens tien tekens lang te maken. Een alternatief is om vier willekeurige woorden te bedenken en die achter elkaar te plakken. Hierdoor ontstaat een zeer lang wachtwoord, dat iets makkelijker is om te onthouden. Een eenvoudig wachtwoord als 'welkom01' of 'wachtwoord' geeft kwaadwillenden vrij spel. Iemand die bij jouw account binnen wil komen, probeert eerst dit soort makkelijke en veelgebruikte wachtwoorden uit. Ook is het niet aan te raden om een wachtwoord te gebruiken dat is te herleiden tot de dienst, zoals 'Facebook01!' of 'F@c3B0oK!', of een woord dat is terug te vinden in het woordenboek. Hackers weten dat het makkelijk is om dit soort wachtwoorden te gebruiken. Ze proberen deze daarom als eerste uit als ze binnen willen komen.

Kan ik hetzelfde sterke wachtwoord gebruiken voor meerdere diensten?
Nee, het is niet aan te raden om een wachtwoord voor meerdere diensten tegelijk te gebruiken. Als een site wordt gehackt en je wachtwoord op straat komt te liggen, hebben de hackers immers ook het wachtwoord voor sites waar je deze code hebt hergebruikt. Internetcriminelen proberen een gestolen wachtwoord vaak uit op zoveel mogelijk verschillende internetdiensten, in de hoop dat hij ook op andere plekken wordt gebruikt. Door bij iedere site en app een ander wachtwoord te gebruiken, beperk je daarom de schade als één van je wachtwoorden wordt gestolen.

Moet ik mijn wachtwoord regelmatig veranderen?
Nee, dat is niet nodig. Als er geen aanleiding voor is om je wachtwoord aan te passen, hoef je dat ook niet te doen. Pas wanneer je denkt dat iemand (mogelijk) toegang heeft of toegang kan krijgen tot jouw account, is het raadzaam om actie te ondernemen. Een aanleiding om je wachtwoord aan te passen, is bijvoorbeeld dat je verdachte activiteit op je account ziet. Ook als een dienst waar je een account hebt is getroffen door een datalek, is het raadzaam om je wachtwoord zo snel mogelijk aan te passen. Je accountgegevens liggen dan namelijk op straat, waardoor kwaadwillenden ze kunnen gebruiken om bij je account in te breken. Door je

wachtwoord te veranderen, komt die niet meer overeen met het wachtwoord dat in de gelekte database staat.

Je kunt bij de dienst Have I Been Pwned? controleren of je e-mailadres in een gelekte database voorkomt. De politie heeft sinds 2017 een vergelijkbare dienst.

Hoe moet ik al die moeilijke wachtwoorden onthouden?
Een sterk wachtwoord bestaat zoals gezegd uit een willekeurige volgorde van tekens. Hoe langer het wachtwoord, hoe langer het duurt om hem te kraken. Het nadeel: moeilijke, complexe wachtwoorden zijn ook een stuk lastiger om te onthouden. Om al je wachtwoorden veilig op te slaan, kun je het best gebruikmaken van een wachtwoordmanager. Dit is een dienst waarmee je al jouw wachtwoorden opslaat en achter één ander wachtwoord. Op die manier hoef je alleen het wachtwoord te onthouden dat toegang geeft tot die dienst. De moeilijke en lange opgeslagen wachtwoorden kun je vervolgens vergeten.

Bekende en veelgebruikte wachtwoordmanagers zijn 1Password (betaald) en LastPass (gratis met premium-optie).

Hoe werkt een wachtwoordmanager?
Wachtwoordmanagers zijn op computers vaak browserextensies. Je hebt een knop rechts van je adresbalk staan, die je indrukt als je op een willekeurige website een account maakt of een nieuw wachtwoord instelt. De manager genereert een willekeurig wachtwoord dat automatisch wordt ingevuld en bewaard.
Als je bij het inloggen op een site op de wachtwoordmanagerknop drukt, worden je eerder gemaakte gebruikersnaam en wachtwoord automatisch ingevuld. Je hoeft ze daarom niet meer zelf te onthouden. Zolang je het wachtwoord hebt om bij de manager in te loggen, zit je goed. Veel wachtwoordbeheerders hebben ook een mobiele app, waar je bij kunt inloggen om op een telefoon wachtwoorden op te slaan of in te vullen. Bij het bezoeken van sites of apps kun je dan met een iPhone of iPad op de deel-knop drukken om de manager te openen. Heeft een app geen knop bij het invulscherm voor een wachtwoord, dan kun je de wachtwoordapp openen en het wachtwoord kopiëren. Op Android kunnen wachtwoordapps vaak boven op andere apps worden geopend, zodat je op die manier makkelijk kunt inloggen.

Kan ik mijn account nog extra beschermen?
Ja. Een goede manier om een extra beveiligingslaag aan je account toe te voegen, is door zogenoemde tweestapsverificatie. Dit zorgt ervoor dat er een extra code moet worden ingevuld bij het inloggen, die via een sms of app naar jouw mobiele telefoon wordt gestuurd. Omdat een hacker geen toegang heeft tot je telefoon, kan hij of zij niet zomaar binnendringen. Er zijn meerdere apps die je kunt gebruiken voor tweestapsverificaties, zoals bijvoorbeeld Google Authenticator (iOS / Android) en Authy. Deze apps genereren constant nieuwe cijfercodes die uniek zijn voor jouw mobiele apparaat, die je naast je wachtwoord invult. Veel grote sites en diensten bieden de mogelijkheid om tweestapsverificatie in te stellen. Je kunt de opstelling meestal vinden in de sectie 'Beveiliging' bij de instellingen van je account. De website Two Factor Auth heeft een overzicht van alle online diensten waarbij je tweestapsverificatie kunt activeren.