

OUCH!

IN DEZE EDITIE...

- Overzicht
- Hoe Wachtwoordmanagers Werken
- Een Wachtwoordmanager Kiezen

Wachtwoordmanagers

Overzicht

Een van de belangrijkste maatregelen die je kan nemen om jezelf online te beschermen, is een uniek en sterk wachtwoord te voorzien voor iedere account die je gebruikt. Jammer genoeg hebben we zodanig veel accounts dat het herinneren van al deze wachtwoorden een haast onmogelijke opgave is. Om deze reden hergebruiken mensen hetzelfde wachtwoord. Als je hetzelfde wachtwoord hergebruikt voor andere accounts, loop je het risico dat eens er één account wordt gecompromitteerd, alle andere accounts met hetzelfde wachtwoord niet meer veilig zijn. Een wachtwoordmanager of een wachtwoordkluis biedt hierin een oplossing. Dit is een toepassing dat op een veilige manier jouw wachtwoorden bewaart, waardoor je makkelijk elke account van een uniek en sterk wachtwoord kunt voorzien. Met een wachtwoordmanager hoef je enkel het masterwachtwoord te onthouden in plaats van al jouw wachtwoorden.

Gast redacteur

Chris Christianson is een Informatiebeveiligingsconsultant uit Californië, met 20 jaar ervaring en verschillende technische certificeringen. Hij heeft op verschillende conferenties gesproken en meegeschreven aan talloze artikels. Je kan Chris bereiken via [@cchristianson](https://twitter.com/cchristianson) en <https://ismellpackets.com>.

Hoe Wachtwoordenmanagers Werken

Wachtwoordmanagers bewaren al jouw wachtwoorden in een database, dat ook wel een kluis wordt genoemd. De wachtwoordmanager versleutelt de inhoud van de kluis en beveiligt het met een masterwachtwoord dat enkel jij kent. Wanneer je een wachtwoord opvraagt, zoals die van jouw online bank of e-mailaccount, dan geef je het masterwachtwoord in om de kluis te ontgrendelen. In veel gevallen haalt de wachtwoordmanager jouw wachtwoord automatisch op en logt veilig voor je in. Dit maakt het eenvoudig om honderden unieke, sterke wachtwoorden te hebben, zonder dat je ze allemaal moet onthouden.

Sommige wachtwoordmanagers plaatsen de kluis op jouw computer of mobiel toestel, terwijl andere dit plaatsen in de Cloud. Daarenboven bieden de meeste wachtwoordmanagers de mogelijkheid om de kluis automatisch te synchroniseren tussen verschillende toestellen die je hebt geautoriseerd. Op die manier zullen wijzigingen die je doet vanaf jouw laptop worden gesynchroniseerd naar al jouw andere toestellen. Ongeacht waar de database is opgeslagen, dien je eerst de wachtwoordmanager toepassing te installeren op de computer of het mobiel toestel.

Wachtwoordmanagers

Als je de wachtwoordmanager voor de eerste keer instelt, dien je jouw accounts en wachtwoorden manueel in te voeren of importeren. Daarna kan de wachtwoordmanager detecteren wanneer je een nieuw onlineaccount registreert of een bestaand wachtwoord wijzigt en kan dit ook aanpassen in de kluis. Dit is mogelijk omdat de meeste wachtwoordmanagers nauw samenwerken met jouw web browser. Deze integratie laat het toe om automatisch in te loggen op websites.

Het is cruciaal dat het masterwachtwoord, die de inhoud van jouw wachtwoordmanager beveiligt, sterk en zeer moeilijk is om te raden. Net daarom raden we aan om een wachtzin te gebruiken, dit is een van de sterkst mogelijke type wachtwoorden die er zijn. Indien de wachtwoordmanager twee-staps-verificatie ondersteunt, voorzie dit dan voor jouw masterwachtwoord. Ten slotte, zorg je ervoor dat je jouw masterwachtwoord kunt onthouden. Als je het vergeet, heb je geen toegang meer tot de andere wachtwoorden.



Wachtwoordmanagers zijn een eenvoudig middel om jouw wachtwoorden op een veilige manier te bewaren en gebruiken.

Een Wachtwoordmanager Kiezen

Er zijn verschillende wachtwoordmanagers die je kan kiezen. In de Bronnen sectie geven we een link naar een recensie van wachtwoordmanagers. Wanneer je op zoek gaat naar een wachtwoordmanager, houd dan rekening met het volgende:

- Jouw wachtwoordmanager moet je eenvoudig kunnen gebruiken. Is de oplossing te complex of moeilijk, gebruik dan een andere die beter aansluit bij jouw stijl en ervaring.
- De wachtwoordmanager moet werken op ieder toestel waarop je wachtwoorden hebt. Synchronisatie van wachtwoordgegevens moet makkelijk zijn voor al jouw toestellen.
- Gebruik enkel bekende en vertrouwde wachtwoordmanagers. Wees voorzichtig met nieuwe producten die geen tot weinig recensies hebben. Cybercriminelen kunnen valse wachtwoordmanagers maken om zo jouw gegevens te stelen. Wees ook voorzichtig met leveranciers die melden dat de oplossing encryptiemethodes gebruikt die ze zelf hebben ontwikkeld.
- Vermijd ook managers die claimen dat masterwachtwoorden die je vergeet, makkelijk kunnen worden hersteld. Dit betekent dat ze jouw masterwachtwoord kennen, waardoor je extra risico loopt.
- Kijk of de verkoper actief updates en patches uitbrengt voor de wachtwoordmanager. Zorg er ook voor dat je altijd over de laatste versie beschikt.

Wachtwoordmanagers

- De wachtwoordmanager moet de mogelijkheid bieden om sterke wachtwoorden te genereren en de sterkte van het gekozen wachtwoord toont.
- De wachtwoordmanager moet ook andere gevoelige gegevens kunnen bewaren zoals antwoorden op beveiligingsvragen, kredietkaarten of frequent flyer nummers.

Wachtwoordmanagers zijn een veilige manier om al jouw wachtwoorden en andere gevoelige gegevens te bewaren. Net omdat ze zulke belangrijke informatie opslaan, dien je een sterk masterwachtwoord te kiezen dat niet eenvoudig te raden is, maar wel eenvoudig is om te onthouden.

Meer Weten?

Ga naar securingthehuman.sans.org/ouch/archives om je te abonneren op de maandelijkse OUCH! Security awareness nieuwsbrief, toegang te krijgen tot het OUCH! archief en kom meer te weten over SANS security awareness oplossingen.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Bronnen

Tweakers Password Managers Discussietopic: https://gathering.tweakers.net/forum/list_messages/1606030/

Top Password Managers of 2017: <https://www.pcmag.com/article2/0,2817,2407168,00.asp>

Passphrases: <https://securingthehuman.sans.org/ouch/2017#april2017>

Two-step Verification: <https://www.lockdownyourlogin.org/>

Lock Down Your Login: <https://securingthehuman.sans.org/ouch/2016#august2016>

SANS Security Tip of the Day: <https://www.sans.org/tip-of-the-day>

OUCH! Is een publicatie van SANS Securing The Human en wordt verdeeld onder de [Creative Commons BY-NC-ND 4.0 license](https://creativecommons.org/licenses/by-nc-nd/4.0/). Deze nieuwsbrief mag verder verdeeld worden en gebruikt worden in uw eigen security awareness programma, zolang u de inhoud niet wijzigt. Stuur een bericht naar ouch@securingthehuman.org voor meer informatie en voor vertalingen.

Redactie: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Vertaald door: Sven Jacobs, Tom Palmaers



securingthehuman.sans.org/blog



[/securethehuman](https://securethehuman)



[@securethehuman](https://twitter.com/securethehuman)



securingthehuman.sans.org/gplus