De maandelijkse Security Awareness nieuwsbrief voor jou!

Wachtwoordmanagers

Overzicht

Een van de belangrijkste stappen om jezelf te beschermen is het gebruik van een uniek, sterk wachtwoord voor elk account en app. Jammer genoeg is het bijna onmogelijk om al deze verschillende wachtwoorden te onthouden. Daarbij is het bijzonder tijdrovend om steeds de wachtwoorden in te typen, nieuwe wachtwoorden te maken, de antwoorden op beveiligingsvragen bij te houden en zo verder. Er is echter een oplossing die je leven niet alleen makkelijker maakt, maar ook veel veiliger - een wachtwoordmanager.

Hoe wachtwoordmanagers werken

Wachtwoordmanagers slaan al je wachtwoorden op in een database, een zogenoemde kluis. De wachtwoordmanager versleuteld de inhoud van de kluis en beveiligt deze met een hoofdwachtwoord dat jij alleen kent. Wanneer je jouw wachtwoorden nodig hebt, om bijvoorbeeld in te loggen in je online bank - of e-mail account, typ je gewoon je hoofdwachtwoord in om je kluis te openen. De wachtwoordmanager zal automatisch het juiste wachtwoord ophalen en je veilig inloggen op de website. Zodoende is het niet langer nodig dat je al je wachtwoorden onthoudt en handmatig inlogt op je accounts.

Daarbij bieden de meeste wachtwoordmanagers de mogelijkheid om automatisch te synchroniseren tussen verschillende apparaten. Op deze manier worden alle wijzigingen doorgevoerd op jouw apparaten wanneer je bijvoorbeeld een wachtwoord veranderd op je laptop. Tenslotte herkennen de meeste wachtwoordmanagers een poging om een nieuw online account te creëren of een bestaand wachtwoord te wijzigen en zullen ze de kluis automatisch voor je bijwerken.

Het is van essentieel belang dat het hoofdwachtwoord dat je kiest lang en uniek is. We raden zelfs aan van je hoofdwachtwoord een wachtwoordzin te maken-een lang wachtwoord dat bestaat uit meerdere woorden of zinnen. Wanneer je wachtwoordmanager tweestapsverificatie ondersteunt, gebruik dit dan ook voor je hoofdwachtwoord. Wees er zeker van dat je het hoofdwachtwoord kunt onthouden. Als je het vergeet kun je namelijk niet meer bij je andere wachtwoorden.

Een wachtwoordmanager kiezen

Er zijn veel wachtwoordmanagers waar je uit kunt kiezen. Onder het kopje Bronnen is een link opgenomen naar beoordelingen van wachtwoordmanagers. In de tussentijd kun je het volgende in ogenschouw nemen, terwijl je de beste manager zoekt voor jou:

Je wachtwoordmanager moet eenvoudig in gebruik zijn. Als de oplossing te ingewikkeld is, zoek dan een andere die beter aansluit bij jouw stijl en kennis.

De wachtwoordmanager moet werken op alle apparaten waar je wachtwoorden op gebruikt. Het zou ook eenvoudig mogelijk moeten zijn om de wachtwoorden te synchroniseren op alle apparaten.

Gebruik enkel bekende en vertrouwde wachtwoordmanagers. Wees voorzichtig met producten die pas op de markt zijn of weinig feedback hebben ontvangen vanuit de gemeenschap. Cyber criminelen kunnen nep wachtwoordmanagers maken om jouw informatie te stelen. Ben ook op je hoede wanneer een leverancier claimt een eigen versleutelingsmechanisme te hebben gemaakt.

Vermijd elke wachtwoordmanager die claimt je hoofdwachtwoord terug te kunnen halen. Dit betekent namelijk dat zij jouw hoofdwachtwoord kennen wat een enorm risico met zich meebrengt.

Welke oplossing je uiteindelijk ook kiest, overtuig je ervan dat de leverancier continu en actief blijft updaten en patchen en let op dat je altijd de meest recente versie gebruikt.

De wachtwoordmanager zou ook andere opties aan moeten bieden om gevoelige informatie op te slaan, zoals de antwoorden op beveiligingsvragen, credit card informatie en frequent flyer nummers.

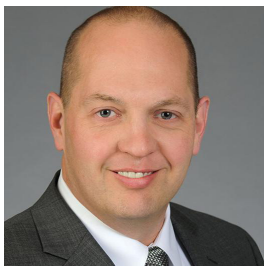
Overweeg het hoofdwachtwoord op te schrijven en te bewaren in een verzegelde envelop in een gesloten kist of een fysieke kluis.

Wachtwoordmanagers zijn een geweldige manier om wachtwoorden en andere gevoelige data op een veilige manier op te slaan, zoals bijvoorbeeld credit card nummers. Let er echter op dat je een uniek en sterk hoofdwachtwoord gebruikt en dat je altijd de laatste versie draait, eender welke oplossing je kiest.

Nederlandse versie

Vertaald door Tamara Brandt, eigenaar van Privara, een onafhankelijk adviesbureau op het gebied van privacy en informatiebeveiliging.

Gastredacteur



Russell Eubanks *is een leider op het gebied van informatiebeveiliging in Atlanta, met meer dan 20 jaar ervaring en heeft vele certificeringen. Hij werkt mee aan het SANS Internet Storm Center en draagt bij aan de Critical Security Controls. Russell is bereikbaar via @russeleubanks en https://www.securityeverafter.com.*

Bronnen

Wachtwoorden eenvoudig gemaakt: http://www.sans.org/u/Y10

Digitale erfenis: http://www.sans.org/u/10Uz

Beoordelingen van de beste wachtwoordmanagers: https://www.wired.com/story/best-password-managers/