de Correspondent

Oproep

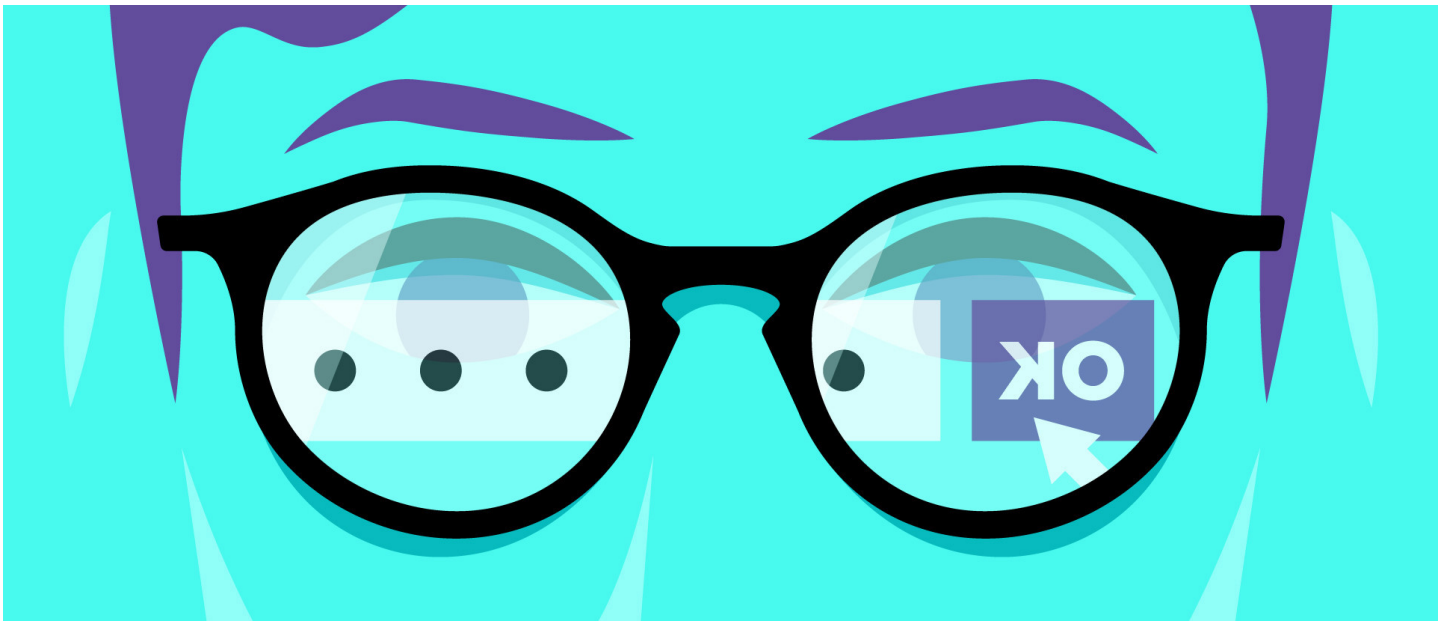
11.01.2017 • *Leestijd 3 minuten*

Vandaag nemen we een cruciale stap in de bescherming van onze data en digitale levens. We nemen onze wachtwoorden onder handen.

Neem jij vandaag een wachtwoordmanager om je beter te beschermen? #privacyweek

Correspondent Veiligheidsindustrie

Dimitri **TOKMETZIS**



Illustratie: Leon Postma (redactioneel ontwerper bij De Correspondent)

Wachtwoorden zijn de sleutels tot je privéleven. Gek dat we daar vaak zo slordig mee omgaan.

Want voor wachtwoorden zijn een paar zaken essentieel om ze veilig te maken:

- Ze moeten niet te raden zijn - door een slimme hacker of razendsnelle software. Dit is bijvoorbeeld een goed wachtwoord: ny?E4R5h#.NqPsK. Of dit:a@6[nXy-XW(<rsE;
- Gebruik ook nooit hetzelfde wachtwoord voor verschillende diensten, want als een van die sites wordt gehackt, heb je een probleem;
- Jij moet dus, als je aan bovenstaande voorwaarden wilt voldoen, heel veel hele moeilijke wachtwoorden onthouden.

Dat is simpelweg ondoenlijk.

Hoe zorg je dan toch dat je wachtwoorden veilig zijn?

Er bestaan verschillende diensten die je helpen om zeer goede wachtwoorden te verzinnen en, belangrijker nog, die voor je te beheren. Deze diensten zorgen ervoor dat je voor iedere app of dienst een ander wachtwoord gebruikt. Met andere woorden: dat aan bovenstaande voorwaarden wordt voldaan.

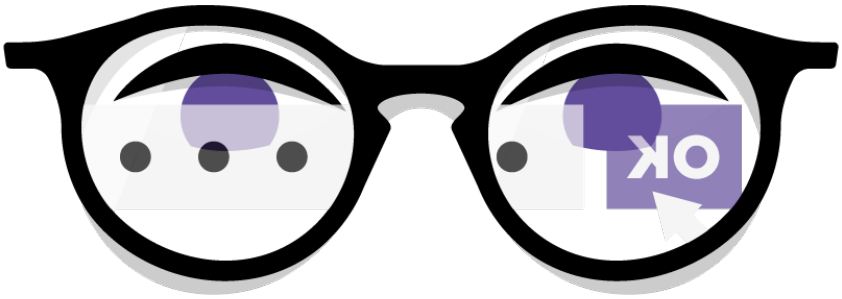
Eén zo'n dienst die wij zelf veel gebruiken, is LastPass. Je downloadt een plug-in voor je browser (of een app voor je smartphone). Je neemt een hoofdwachtwoord - een dat je kunt onthouden, maar dat voor anderen onmogelijk te raden is.

LastPass maakt voor al je diensten een goed wachtwoord aan en bewaart deze wachtwoorden in een online kluis.

Een online kluis?
Is dat niet gevaarlijk?

Een beetje. LastPass is vorig jaar een keer gehackt en een onderzoeker heeft een aantal zwakheden in de software van LastPass gevonden. Desondanks maakten wij ons geen zorgen omdat we tweefactorauthenticatie gebruikten. Als je LastPass start en toegang wilt tot je kluis vanaf een andere computer, moet je bijvoorbeeld een code invoeren die je per sms of via Google Authenticator hebt gekregen. Net zoals bij bankieren. Daarnaast zijn de wachtwoorden bij LastPass heel goed versleuteld en heeft het bedrijf transparant en

adequaat op de hack en kritiek gereageerd.



Wil je liever een ander programma gebruiken, dan is 1Password een optie of KeePassX. KeePassX is gratis. Voor 1Password en LastPass moet je betalen.

En om echt zeker te zijn, raden wij je aan om voor de belangrijkste en meest fraudegevoelige diensten die je gebruikt, gewoon een zeer uniek wachtwoord te kiezen. Dat zijn er meestal niet meer dan vijf. Bijvoorbeeld voor je bankaccount, je DigiD, je mail. Kies in dat geval een zin die je makkelijk kunt onthouden, iets in de trant van Gerard.Joling.is.eigenlijk.kaal!

Waarom moeten we gezamenlijk actie ondernemen?

Ten eerste omdat wachtwoorden écht essentieel zijn. Je zou wel kunnen zeggen: de eerste digitale verdedigingslinie in de strijd tegen onbevoegden op zoek naar jouw data. Uit onderzoek van Google bleek dan ook dat het managen van wachtwoorden voor security-experts absolute topprioriteit heeft. Net als tweefactorauthenticatie.

Het is heel makkelijk, je moet er alleen even wat tijd voor uittrekken. Wij schatten in dat je in drie uur je wachtwoordmanager op orde hebt, je wachtwoorden hebt veranderd en tweefactorauthenticatie hebt geregeld. En als je toch bezig bent, stel dan meteen tweefactorauthenticatie in voor je mail- en socialemedia-accounts.

In drie uur heb je je wachtwoordmanager op orde, wachtwoorden veranderd en tweefactorauthenticatie geregeld

Ten tweede, goede beveiliging werkt aanstekelijk. Zorg er bijvoorbeeld voor dat je kinderen of je ouders goed met wachtwoorden leren omgaan. Je kunt LastPass ook met je geliefde en kinderen gebruiken, zodat je gezamenlijke diensten goed beschermd zijn.

Zie je een collega zijn wachtwoorden op een post-it schrijven en op zijn beeldscherm plakken? Zeg er wat van. Mailt een collega een wachtwoord? Gooi dat mailtje in ieder geval weg, maar beter nog, mail het niet, maar schrijf zo'n wachtwoord even op en gooi daarna het briefje weg (en nee, niet bij het oud papier, maar in kleine stukjes, liefst met koffieprut erover).

Zorg ervoor dat ook andere apparatuur wordt beveiligd, dus zet een wachtwoord op je computer en zeker ook op je telefoon. En spreek anderen erop aan als zij dat niet doen. En denk er altijd aan om standaardwachtwoorden op apparatuur - bijvoorbeeld je router, of een IP-camera - te veranderen. Die wachtwoorden zijn vaak publiek bekend. Een nieuw wachtwoord kan voorkomen dat je apparaten worden gehackt.

En verder?

Besef dat je privéleven grotendeels gedigitaliseerd is en dat je veel gevoelige gegevens continu bij je draagt. Gedraag je daarnaar. Je gebruikt ook niet maar één sleutel voor al je sloten, en je laat je voordeur niet zomaar openstaan. Net zo logisch is het dat je je computers goed moet beveiligen. Zo houd je jezelf en de ander veilig en je privéleven meer privé.

Doe je mee?