WWW.MINDYOURSTEP.INFO

Wachtwoorden

waar moet een veilig wachtwoord eigenlijk aan voldoen?

De vraag

Tegenwoordig heb je voor bijna alles een gebruikersnaam en een wachtwoord nodig. Denk aan je e-mailaccount, social media, internetbankieren, en niet te vergeten al die webshops die je kunt bezoeken. We moeten inmiddels zoveel wachtwoorden onthouden dat we steeds vaker kiezen voor makkelijk te onthouden wachtwoorden. Om nog maar te zwijgen over het feit dat we ook vaak hetzelfde wachtwoord voor verschillende accounts gebruiken. Maar is dat wel zo veilig? Nee natuurlijk niet, want wie heeft er nou één sleutel voor zijn huis, kluis, auto én fiets? Stel nou dat iemand je fiets leent, dan heeft diegene dus ook toegang tot je huis, kluis én auto. Hetzelfde geldt dus voor je wachtwoorden.

De uitdaging

Om te voorkomen dat iemand anders met jouw gegevens toegang krijgt tot vertrouwelijke informatie is het daarom belangrijk om je wachtwoord zo veilig mogelijk te maken. Natuurlijk is er daarbij altijd het compromis tussen een veilig én een goed te onthouden wachtwoord. De sterkste, veiligste wachtwoorden zijn voor de meeste mensen niet te onthouden. Dus worden deze complexe, maar sterke wachtwoorden vaak op een post-it geschreven, die vervolgens op het computerscherm wordt geplakt of onder het toetsenbord wordt gelegd. Omgekeerd is een goed te onthouden wachtwoord vaak te makkelijk en dus zo te kraken, of simpelweg te raden. Maar waaraan moet een veilig wachtwoord eigenlijk voldoen? En belangijker nog, hoe onthoud je ze?

De oplossing

Om ervoor te zorgen dat je een veilig wachtwoord hebt dat goed te onthouden is, is het raadzaam om een wachtwoord te kiezen dat voldoet aan de volgende zaken:

- Zorg dat jouw wachtwoord minstens 8 tot 10 tekens bevat; hoe langer het wachtwoord is, hoe moelijker het is om het te raden.
- Zorg dat jouw wachtwoord bestaat uit een combinatie van hoofdletters, kleine letters, cijfers én speciale tekens.
- Zorg dat jouw wachtwoord geen voorspelbare combinaties bevat (zoals één enkel woord of 123).
- Gebruik geen persoonlijke gegevens als je achternaam, de naam van je kind of huisdier, je geboortedatum of lievelingseten; sommige van deze persoonlijke gegevens zijn namelijk gemakkelijk te achterhalen via bijvoorbeeld social media.
- Verander je wachtwoord meerdere keren per jaar.
- Verzin een ezelsbruggetje om je wachtwoord te onthouden.
- Lukt dat echt niet, schrijf ze dan op in een boekje wat je ergens thuis bewaard.
- Laat je browser of apps je wachtwoorden niet opslaan en sla ze zelf ook niet op je computer, tablet of telefoon op.

Zo zorg je ervoor dat jouw wachtwoord niet meer te kraken is.

Tenslotte; je wachtwoord kan nog zo sterk of veilig opgeborgen zijn, als je het op de verkeerde plek invult, kunnen mensen met je meelezen. Dus controleer altijd de adresbalk van je internetbrowser voordat je ergens inlogt. Een veilige internetpagina begint altijd met https in de adresbalk en/of wordt aangegeven met een slotje. Adresbalken zonder slotje zijn niet beveiligd en verhogen dus de kans op internetfraude. Een andere manier waarop hackers kunnen meekijken is wanneer je bent verbonden met een openbaar WiFi-netwerk. Log dus nooit in op je accounts wanneer je gebruik maakt van een openbaar WiFi-netwerk. Moet je toch echt inloggen? Zet dan je databundel van je telefoon aan.

Kortom, een veilig wachtwoord is zo simpel nog niet!

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak.
Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.