Veelgestelde vragen over wachtwoorden

Heb je nog vragen over wachtwoorden? Je vindt hier een overzicht van veelgestelde vragen en antwoorden:

Wat is een veilig wachtwoord?

Hoe langer je wachtwoord, hoe veiliger. Gebruik een wacht'zin': die is langer dan een wachtwoord, dus ook veiliger én makkelijk te onthouden. Voeg in die zin hoofdletters, cijfers en leestekens toe, en je hebt een sterk wachtwoord.

Wat is een wachtzin?

Dat is een zin die je als wachtwoord gebruikt. Een zin is langer dan een wachtwoord, dus ook veiliger én makkelijk te onthouden. Voeg in die zin hoofdletters, cijfers en leestekens toe, en je hebt een sterk wachtwoord. Bijvoorbeeld: ‘BelgiëNaarHetEK16!’

Zijn cijfers, hoofdletters en symbolen nodig?

Cijfers, hoofdletters en symbolen maken je wachtwoord moeilijker te kraken. Zonder zijn er maar 26 mogelijkheden per karakter, waardoor het makkelijk wordt om een wachtwoord te ontcijferen. Met cijfers, hoofdletters en symbolen daarentegen, zijn er veel meer combinaties mogelijk.

Hoe gebruik ik cijfers, hoofdletters en symbolen?

Je kan ze overal in je wachtwoord of -zin gebruiken, ook in het midden van je wachtzin, bijv.: Hoera!2keerWeekend.

Hoe onthoud ik mijn wachtwoorden het gemakkelijkste?

Maak een wachtzin en gebruik herkenbare variaties die je zelf makkelijk kan onthouden, maar die voor anderen moeilijk te raden zijn.

Bijv.:

Voor je profiel op je lievelingsforum: 'Welkom,500Commentaren'

Voor je Twitter-profiel: 'Welkom,100Vrienden!'

Kan ik mijn wachtwoorden bijhouden op een veilige manier?

Heb je moeite om je wachtwoorden te onthouden en wil je ze ergens noteren? Dat kan zo:

- op je computer: gebruik een wachtwoordkluis, zoals Lastpass, Dashlane,1Password, enz. Sla wachtwoorden nooit je op in een Word-document, in je mail of in de notities van je smartphone.
- Op papier: berg dit veilig op, zeker niet in de buurt van je computer. Hang geen post-its aan je scherm of leg het niet op je bureau.

Heb ik altijd een ander wachtwoord nodig voor verschillende websites of applicaties?

Wachtwoorden hergebruiken is geen goed idee. Als je gegevens gehackt worden op 1 site, proberen de cybercriminelen diezelfde gegevens ook op andere sites. Gebruik voor je belangrijke accounts, zoals je e-mail en je Facebook-profiel, lange en totaal verschillende wachtwoorden. Kies bij voorkeur voor een wachtzin.

Wat doe ik met minder belangrijke accounts? Gebruik ik daar wel hetzelfde wachtwoord?

Wachtwoorden hergebruiken is altijd een slecht idee. Voor minder belangrijke accounts, waar je geen betalingsgegevens of persoonlijke gegevens hebt, kan je wel variaties op een wachtwoord gebruiken.

Bijv.:

een muziekforum: Welkom,500Muziek!

een voetbalforum: Welkom,100Voetbal!

Wanneer is een account belangrijk of minder belangrijk?

Beantwoord daarvoor de vraag: ‘Wat als mijn account wordt gehackt?’. Afhankelijk van de ernst van de gevolgen, is een account belangrijk of niet.

Belangrijke accounts waarvoor je beter een totaal verschillend wachtwoord gebruikt:

Mailbox

Die bevat vaak veel persoonlijke gegevens, zoals

een rijksregisternummer, adressen, contactenlijst, maar ook foto’s, werkdocumenten, doktersafspraken, enz. Kortom, gegevens over wie je bent. Bovendien bevat je mailbox ook informatie over je andere accounts. Vraag je voor een andere account een nieuw wachtwoord, dan ontvang je dat meestal via mail.

Socialemediaprofielen

Deze profielen linken je aan je vrienden en collega's. En die informatie kan misbruikt worden om in jouw naam iets te publiceren of om een virus naar je contacten te sturen.

Webshops

Je account in een webwinkel bevat soms een VISA- of Mastercard-nummer. Met die gegevens kan iemand in jouw naam aankopen doen.

Minder belangrijke accounts waarvoor je variaties van hetzelfde wachtwoord kan gebruiken:

Websites waar je niet betaalt, geen persoonlijke gegevens hebt en die je maar af en toe bezoekt, zijn minder belangrijk. Wordt zo een account gehackt, dan zijn de gevolgen voor jou en anderen beperkt.

Hoe kan ik me aanmelden in 2 stappen als extra beveiliging voor belangrijke accounts?

Voor je belangrijke accounts, kan je naast je wachtwoord een extra slot toevoegen. Dat kan door in te loggen in 2 stappen, bijvoorbeeld met een code die je via sms ontvangt.

Lees meer over hoe je kan inloggen in 2 stappen <link naar Pijler 3: Zorgeloos digitaal > Bescherm je privacy>

Hoe vaak verander ik mijn wachtwoorden?

Bij voorkeur verander je 1 keer per jaar de wachtwoorden van je privé-accounts. Voor professionele accounts doe je dat het best nog vaker, omdat die informatie nog gevoeliger kan zijn.

Als een website waar je een account hebt, wordt gehackt, verander onmiddellijk je wachtwoorden. Ga na of het probleem bij de website is opgelost, anders verander je je wachtwoord tevergeefs.

Wat als ik maar een beperkt aantal karakters kan gebruiken voor mijn wachtwoord?

Gebruik dan bijvoorbeeld dit trucje:

De wachtwoordzin: 'Zeg, oma drinkt 5-6 Jenevers:'

wordt dit wachtwoord: 'Z,od5-6J:'

Ik deel mijn wachtwoorden soms met familie, vrienden of collega’s. Is dit een goed idee?

Wachtwoorden delen is nooit een goed idee, of dat nu privé is of op het werk. Je weet nooit wat er gebeurt met je wachtwoord en misbruik is nooit veraf. Gebruik je een account waar je collega's ook toegang hebben? Gebruik dan een wachtwoordkluis om zo de wachtwoorden op een veilige manier te delen met alle collega’s. Vraag ook altijd aan je werkgever of er een beleid is om wachtwoorden te delen en/of je zulke programma’s kan en mag gebruiken