5 tips om cyberveilig te zijn

Voor particulieren en bedrijven

#1 | Het instellen van tweefactorauthenticatie

Tweefactorauthenticatie betekent dat er **twee stappen** gezet moeten worden om in te loggen op een account. Je kunt het zien als dat je niet één maar **twee verschillende sleutels** gebruikt om een slot te openen.

Door te kiezen voor **tweefactorauthenticatie** maak je het voor een hacker lastiger om in te loggen op jouw accounts. Je **wachtwoord** is de **eerste stap** die je zet om in te loggen op een account. Hoe sterker je wachtwoord, hoe veiliger dit is.

Vervolgens moet je een tweede stap zetten om in te kunnen loggen. Dit kan op verschillende manieren. De meest gangbare is dat je via een authenticatorapp of via een sms een code ontvangt die je invoert, waarna je ingelogd bent.

Voor organisaties is het raadzaam tweefactorauthenticatie door te voeren in de organisatie. Een systeem kan bijvoorbeeld erg kwetsbaar zijn wanneer medewerkers inloggen vanuit thuis op het bedrijfsnetwerk, leveranciers toegang krijgen tot jouw systemen of er gebruikers met hogere rechten worden toegevoegd aan een systeem.

#2 | Goede wachtwoorden kiezen

Een **goed wachtwoord** is de basis van een goede beveiliging. Dit geldt voor het gebruik van wachtwoorden bij privé accounts van medewerkers en bedrijfsaccounts. Een paar tips:

Gebruik een wachtwoordzin

Het woord wachtwoordzin zegt het al, maar we hebben het letterlijk over **zinnen** die je inzet als wachtwoord. Het voordeel van een wachtwoordzin is dat deze **lang** is, waardoor dit **moeilijk** te **kraken** is. Hierbij is het raadzaam om volstrekt willekeurige woorden te gebruiken met een combinatie van speciale teksten en cijfers.

Gebruik voor elk account een ander wachtwoord

In de meest ideale situatie gebruik je voor **elk account** een **ander wachtwoord**. Dat is in de praktijk best wel ingewikkeld omdat je veel wachtwoorden moet onthouden. Toch is voor elk account een ander wachtwoord de **veiligste manier**. Heb je hetzelfde wachtwoord voor meerdere accounts, dan ben je vele malen kwetsbaarder. Als de hackers je wachtwoord hebben, kunnen ze immers meerdere accounts hacken.

Onthoud alle wachtwoorden met behulp van een wachtwoordmanager

Het is verstandig om je wachtwoorden op te slaan via een **wachtwoordmanager**. Dit is een soort **digitale kluis** waarin je jouw wachtwoorden opslaat. Hierdoor kun je makkelijk bij jouw gegevens terwijl je zeker weet dat de gegevens veilig worden opgeslagen. Je hoeft dus maar 1 wachtwoord te onthouden.

Ook bieden partijen die wachtwoordmanagers aanbieden meestal een optie waarbij ze helpen om sterke wachtwoorden te genereren.

Checken of wachtwoorden zijn betrokken bij een datalek

Je kunt eenvoudig checken of wachtwoorden zijn betrokken bij een datalek. Bij een datalek hacken cybercriminelen bedrijven en stelen de wachtwoorden van hun klanten. Als jouw wachtwoord is gelekt, dan is het belangrijk om de accounts waarbij je dat wachtwoord gebruikt direct te veranderen.

Dit check je eenvoudig via de site **haveibeenpwned.com.**

#3 | Klik nooit op een link die je niet vertrouwt

Pas op wanneer je mails of appjes krijgt met linkjes die niet te vertrouwen zijn. Dit noemen we ook wel **phishing**.

Wanneer je op de **link klinkt** word je naar een site gestuurd waar wordt gevraagd naar **vertrouwelijke gegevens**.

Of er wordt **software geïnstalleerd** op je computer die het mogelijk maakt om mee te kijken op je computer.

Je vindt hier een aantal handige tips:

Volg je gevoel:

Twijfel je of een mail veilig is, **klik dan zeker niet op een link**. Je kunt beter te voorzichtig zijn dan impulsief handelen in dit geval.

Check het webadres of het mailadres.

Check het **e-mailadres** waarmee de **mail** is **verzonden**. Dit geldt ook voor het webadres waar de link naar verwijst.

Vaak zijn het kleine dingen zoals een cijfer wat is toegevoegd wat maakt dat je ziet dat het mailadres of een site niet te vertrouwen is.

Vragen om persoonlijke gegevens

Wordt er om **persoonlijke gegevens** gevraagd, wees dan op je **hoede**. Een bank of verzekeringsmaatschappij zal niet vlot naar je persoonlijke gegevens vragen via de mail.

Vreemd taalgebruik

Let op **onregelmatigheden** in **taalgebruik**. Dit kan een signaal zijn dat het niet goed zit.

Pas op met linkjes als bitly en tinyurl.

Pas op met linkjes zoals bitly of tinyurl. Dit zijn zogenaamde URL verkorters. Je kunt **niet zien wat er achter deze link zit**.

Ga naar de browser

Wil je zeker weten dat je goed zit. Ga naar het account waar je in wilt loggen via het webadres wat je kent. Dus betaal je via de Rabobank, dan ga je naar de site van de Rabobank en dan betaal je vanaf daar. Nog beter dan dit: log in via de app op jouw telefoon. Dan hoef je niet op de link te klikken.

Zeker weten of een linkje veilig is?

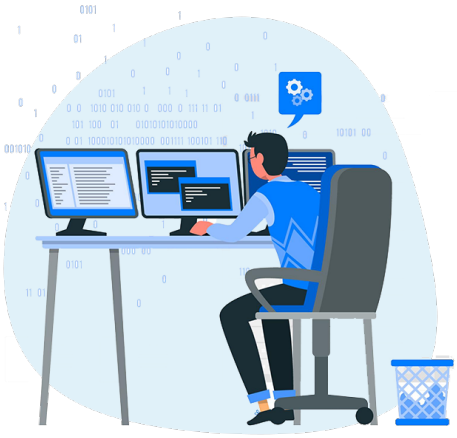
Ga naar checkjelinkje.nl

#4 | Back-up van je gegevens

Zowel particulier als zakelijk is een **goede back-up** noodzakelijk. Zorg ervoor dat alle gegevens ergens anders staan opgeslagen dan op je computer. Bijvoorbeeld op een USB-stick die niet is aangesloten op het internet.

Maar cloud back-ups zijn ook een veilige optie en altijd bereikbaar. In dit geval kun je, als je gehackt bent, al je gegevens herstellen.

Voor organisaties is het **veiligstellen** van **data groter** en **omvangrijker**.



Mocht je slachtoffer worden van een cybercrime aanval, zoals ransomware dan is het cruciaal om een **goede back-up van data** te hebben die te benaderen is vanaf een andere plek.

Uiteraard is het nog verstandiger om een mogelijke cybercrime aanval te voorkomen. Een **goed back-upplan** is een onderdeel wat hierbij hoort.

Als je dit goed hebt ingeregeld en je wordt getroffen met ransomware, dan hoef je **geen losgeld te betalen** omdat je zelf de data nog hebt.

5 | Updaten van software, apps en gegevens.

Gebruik altijd de **nieuwste versies** van alle software, apps op telefoons en computers.

Doorgaans worden updates door fabrikanten en ontwikkelaars uitgevoerd om **software** te **verbeteren**.

Wanneer er een **kwetsbaarheid** in de **software** zit of er een betere beveiliging wordt ontwikkeld, dan wordt dit aangeboden via een update.

Daarom is het updaten van software zo belangrijk.

Binnen organisaties is het van belang dat het **updaten van software** in een plan gegoten wordt. Dit geldt voor het updaten van alle systemen en apparaten zoals de smartphones, de routers en de website.