Tips voor veilig wachtwoordgebruik en extra beveiliging door middel van 2FA (2 Factor Authenticatie)

Het doel van deze informatie is om de opdrachtgever te informeren over wachtwoordgebruik, om tips te geven en om te informeren. De informatie dekt niet alle mogelijkheden, beschrijft niet alle situaties en is dan ook niet volledig of als zodanig bedoeld. Deze hieronder verstrekte informatie dient dan ook als algemene richtlijnen beschouwd te worden waaraan geen rechten ontleend kunnen worden.

Een van de belangrijkste tip is om het wachtwoord dat u gebruikt voor het inloggen op het werk gebruikt ook alleen gebruikt voor inloggen op het werk. Hiermee voorkomt u dat wachtwoorden opgeslagen worden op plekken waarvan u geen weet heeft en dat het in de openbaarheid komt via gehackte databases van derden.

Als u vanaf een externe locatie inlogt op systemen en/of mail van uw werk, doe dat dan alleen via uw eigen notebook of PC of als dat niet kan via een PC die u 100% vertrouwd. Ook al is de beveiliging naar uw email en het werk versleuteld, dan nog is het redelijk eenvoudig om alles wat u intikt op de slaan en later uit te lezen.

Hoewel het geen kwaad kan om het wachtwoord regelmatig te wijzigen is een goed wachtwoord dat u alleen kent en dat alleen voor het werk gebruikt wordt beter dan een wachtwoord dat elke paar weken of maanden gewijzigd wordt.

In het algemeen hanteren wij de volgende instellingen:

1. Het wachtwoord moet minimaal uit 6 tekens bestaan
2. Het wachtwoord moet minimaal 3 tekens uit de volgende groepen bevatten: letters (a, b, c..), hoofdletters (A, B, C..), cijfers (1,2,3 ..) en vreemde tekens (!@#$..).
3. Het wachtwoord mag niet meer dan 3 achtereenvolgende tekens van uw eigen naam bevatten.
4. Het wachtwoord is één jaar geldig.
5. U kunt dit wachtwoord niet nog één keer gebruiken.

<u>Voorbeelden:</u>
Voorbeeld voor een gebruiker die Christa heet:

Fout i.v.m. minimale eisen: Christa en Chri$t@
Goed: Chr1$t@

Tip 1: **Gebruik woorden of zinnen.**
U kunt woorden gebruiken maar vervang de letters bijvoorbeeld door cijfers, wissel willekeurig hoofdletters en kleine letters af en gebruik een vreemd teken zoals een !, # of ().

<u>Voorbeelden:</u>

Kattekop	->	K@tt3Kop
Verfkwast	->	VerfKw@$t

Tip 2: **Verzin een zinnetje, of neem een spreekwoord, boek- of filmtitel en pak daar de eerste letter van. Zet er eventueel nog een vreemd teken of cijfer in of achter.**

<u>Voorbeelden:</u>

Once upon a time in the West	->	OuatitW!
Sonja Bakker, Zomerslank met Sonja	->	SBzsmS!
James Bond 007 in Casino Royal	->	JB0071cr
Als 3 honden vechten om een been	->	A3hvo1B

Tip 3. **Vervang letters door cijfers of symbolen.**
A ->@, B -> 8, E -> 3, S -> $, L -> 1, O -> 0, S -> 5

Over een jaar moet het wachtwoord weer gewijzigd worden, maar u kunt dit best weer gebruiken als u er iets aan veranderd. Bijvoorbeeld als u er een ander vreemd teken achter zet of een kleine letter in een hoofdletter veranderd. Op die manier is het wachtwoord voor u toch ***leesbaar*** terwijl het voor iemand die over u schouder meekijkt complete onzin lijkt. Doe dit wel willekeurig dus vervang niet elke A door een @.

Is uw wachtwoord al eens gehacked?
Er zijn niet alleen lijsten beschikbaar met de meest voorkomende wachtwoorden maar er zijn zelfs websites waarop u kunt kijken of uw combinatie van emailadres en wachtwoord al in omloop is. De kans is groot dat u bij controle een aantal websites zult vinden waar u op ingelogd heeft en die *gehacked* zijn.

https://haveibeenpwned.com/

https://www.avast.com/hackcheck

2 Factor Authenticatie (2FA)
Een extra beveiliging tegen ongewenst gebruik van uw login gegevens is 2FA. Na het intikken van uw naam en wachtwoord moet u via de smartphone, of op een andere fysieke manier bevestigen dat u daadwerkelijk de persoon bent die op dat moment wil inloggen. Voor mensen die veel vanaf externe locatie werken is dit een onmisbare extra beveiliging. Kosten ca. 3,00 per gebruiker per maand.

Hoe veilig is een wachtwoord dat u 6 tekens bestaat?
Ervan uitgaande dat u een willekeurig goed wachtwoord gebruikt dat niet in de top 10.000 voorkomt. In dat geval zijn er 72^6 = 139.314.069.504 mogelijkheden. Omdat wij na 5 pogingen de login minimaal 15 of zelfs 30 minuten blokkeren kan een hacker maar zo'n 35.000 pogingen per jaar doen en dat is 0,00002515% van de mogelijkheden. Als het proces dat probeert binnen te dringen tijdens de 'lockout' blijft proberen om het wachtwoord te kraken dan is de kans groot dat als het wachtwoord geraden wordt dit gebeurt op een moment dat er 'lockout' is en dat het dus nooit geraden wordt. Tenslotte is het ook voor de gebruiker niet mogelijk om in te loggen als er een 'lockout' is en zal deze zich – zeker als het vaker gebeurt – melden waarna er extra maatregelen genomen kunnen worden.

Hoe veilig is het beveiligen van documenten met wachtwoorden?
Het is waarschijnlijk beter dan niet beveiligen maar wachtwoorden op documenten zijn nagenoeg zinloos. Er bestaan speciale services die wachtwoorden op documenten kraken voor maar enkele tientallen EURO's.