



**Neem geen
onnodig risico**

Verijdel het stelen van je wachtwoord.

Brussel, juli 2020

Hallo en welkom allemaal!



Een klassiek hackingscenario bij ondernemingen en kmo's.



Opgepast: hacking!

Een persoon met slechte bedoelingen heeft jouw wachtwoord gehackt.

We kunnen stellen dat deze persoon nu jouw sleutels in zijn bezit heeft. Hij kan vertrouwelijke informatie stelen, boodschappen versturen naar al je contacten, collega's en klanten. Hij kan met jouw profiel op de sociale netwerken inloggen en aankopen doen op jouw favoriete sites.

Om een wachtwoord te hacken of stelen

heeft een goed uitgeruste hacker slechts 1 minuut nodig



Een wachtwoord hacken... wasda?

Het hacken van een wachtwoord:

- Frauduleuze techniek
- Hacking

Doel:

- Persoonlijke informatie
- Gevoelige gegevens van de onderneming
- Bankgegevens

Hoe?

- Ontsleutelprogramma
- Persoonlijke aanval
- Via phishing

Het hacken van wachtwoorden is een frauduleuze techniek die erin bestaat **een wachtwoord te stelen om toegang te krijgen tot je professionele en privéaccounts.**

Het doel?

- Op zoek gaan naar **persoonlijke informatie** (ID, wachtwoorden, kredietkaartnummer).
- Toegang tot **gevoelige gegevens** binnen de onderneming.
- **Jou geld afhandig maken** door toegang te krijgen tot je bankgegevens.

Hoe?

- Een hacker gebruikt een **ontsleutelingprogramma** voor wachtwoorden.
- Een persoonlijke aanval, een kennis of een derde die rechtstreeks toegang heeft tot je wachtwoord.
- Een **phishing-e-mail** waardoor men je gegevens op frauduleuze manier heeft verkregen.



Bijna de helft van de Belgen gebruikt een zwak wachtwoord van **minder dan 8 karakters**.

Verontrustend! **1 Belg op 3 deelt zijn wachtwoord** met een derde, die hij al dan niet goed kent.

Een ander alarmerend cijfer voor ondernemingen en kmo's: **1 Belg op 4 heeft hetzelfde wachtwoord** voor zijn privé- en zijn professionele accounts.

15% van de Belgen gebruikt slechts 1 wachtwoord. (Safeonweb, Digitale Gezondheidsindex 2018)

Wachtwoorden onthouden is een hele klus. Gebruik daarvoor een online **wachtwoordkluis** of 'password manager'. Je vindt ze in alle soorten, gratis en betalend. Slechts 16% van de Belgen gebruikt een wachtwoordkluis. (Safeonweb, Digitale Gezondheidsindex 2018). Wachtwoordkluizen onthouden jouw wachtwoorden en beveilig je best met een sterk wachtwoord, het enige dat je moet onthouden.

39% van de Belgen maakt af en toe of vaak gebruik van **2FA (2 Factor Authenticatie, zie slide 8)**. (Safeonweb, Digitale Gezondheidsindex 2018).

123456, azerty, Star Wars of naam en geboortjaar zoals in JouwNaam1985 zijn de meest gebruikte wachtwoorden. Dat is geen goed idee: er bestaan namelijk programma's die dit soort wachtwoorden automatisch kraken of die elke mogelijke combinatie van karakters bliksemsnel uitproberen.



Afspraak op: <https://www.grc.com/haystack.htm>

In deze **(anonieme) test** moet je uiteraard niet jouw eigen wachtwoorden doorgeven!

Maar door op **enkele vragen** te antwoorden, zal je weten in hoeveel tijd een hacker je wachtwoord kan achterhalen.

- En, hoe snel ging het?
- Daag je collega's uit: wie heeft het **meest ingewikkelde wachtwoord**?

Je zal zien dat het misschien **niet zo sterk is** als je dacht. Maar geen paniek, je hebt nog tijd om het te veranderen...

En natuurlijk geef je je wachtwoorden NOOIT door.

Ga voor lang

Maak het de hackers niet te makkelijk

Hoe je wachtwoord veiliger maken?

De criteria:

- Lengte tussen 14 en 20 karakters
- Maak wachzinnen
- Spaties, hoofd- en kleine letters
- Cijfers en speciale tekens

[Dit leuke filmpje \('Longer is Stronger'\)](#) vat alles samen!



7

Maak je wachtwoord sterker

- Vorm een lang wachtwoord, tussen de **14 en 20 karakters**.
- Kies **wachzinnen**, makkelijk te onthouden en veiliger.
- Bewaar de **spaties**, zo typt het makkelijker.
- Gebruik **hoofd- en kleine letters**.
- Voeg **cijfers en symbolen** toe.

Een sterk wachtwoord is een lang wachtwoord. Vanaf 14 karakters zit je goed.

Sterk hoeft niet complex te zijn

Het is een wijdverbreid misverstand dat een sterk wachtwoord zo complex mogelijk moet zijn. Dat soort wachtwoorden is moeilijk te onthouden, moeilijk te typen en met de supersnelle computers van tegenwoordig kan een cyberaanvaller ze gemakkelijk kraken. De sleutel tot wachtwoorden is om ze **lang** te maken: **hoe meer tekens, hoe beter**. Dit worden passphrases ('wachzinnen') genoemd: een type sterk wachtwoord dat een korte zin of willekeurige woorden gebruikt. Bijvoorbeeld 'tijd voor sterke koffie!' of 'snelle-slak-kruip-t-zandbak'. Beide hebben meer dan twaalf karakters, zijn makkelijk te onthouden en eenvoudig te typen maar moeilijk te kraken. En wanneer gevraagd wordt om symbolen, cijfers of hoofdletters aan het wachtwoord toe te voegen, kun je dat eenvoudig doen.

Als je niet minimaal 12 karakters kan gebruiken, gebruik dan nog de 'oude' standaard van minimaal een hoofdletter, een klein letter, een cijfer en een speciaal teken.

Helaas zijn de meest gebruikte wachtwoorden nog steeds: 123456, 123456789, querty, password of 11111 (UK Cybersurvey, 2019).

Wees nog voorzichtiger

Blijf de hackers een lengte voor



Wat doe je tegen het hacken van je wachtwoord?

Goede reflexen:

- Verschillend voor privé en werk
- Verschillend per toepassing/per account
- Dubbele controle / Multi-factor authenticatie
- Voor belangrijke toepassingen/accounts: maak je wachtwoord nog langer/complexer en pas dubbele controle toe.
- Niet in de browser/niet in een file
- Verander min. 1x per jaar
- Vertrouwelijk
- Gebruik een wachtwoordmanager

8

Neem de juiste reflexen aan tegen het hacken van je wachtwoord

- Maak een onderscheid tussen je **professioneel** en je **privéwachtwoord**.
- Zorg voor **verschillende wachtwoorden** per toepassing/per account: gebruik voor elk account een ander wachtwoord. Internetcriminelen proberen een gestolen wachtwoord vaak uit op zoveel mogelijk verschillende internetdiensten. Krijgen criminelen je wachtwoord van één internetdienst in handen, dan hebben ze niet direct toegang tot je andere accounts.
- Geef de voorkeur aan een **dubbele controle**, bv. een **wachtwoord gecombineerd met een SMS-code** (dit noemt men '2 Factor Authenticatie' of 'Multi Factor Authenticatie, zie infra).
- Voor belangrijke toepassingen/accounts: maak je wachtwoord nog langer/complexer en pas dubbele controle (2FA) toe.
- Bewaar je wachtwoorden niet in je **browser, niet in een file op je pc**.
- Verander je wachtwoord **minimaal eenmaal per jaar**. Hergebruik geen oude wachtwoorden of delen hiervan. Verander bijvoorbeeld 'Hetpaardrijdmetderuiter2016' niet in 'Hetpaardrijdmetderuiter2017'.
- Geef je **wachtwoord niet door aan derden**.
- Gebruik een **wachtwoordmanager**. Daarin beheert je je wachtwoorden (je moet maar één wachtwoord onthouden, namelijk dat welk toegang geeft tot je 'wachtwoordkluis'. Voorbeelden: LastPass, OnePass, Dashlane, Keepass

Bron: Vrije Universiteit Brussel

Multi-Factor Authenticatie (MFA) is een authenticatie methode waarbij de onlinegebruiker minstens twee stappen (factoren) succesvol moet doorlopen om ergens toegang toe te krijgen.

De typische factoren zijn:

1. Iets wat je weet; deze factor is algemeen gekend: gebruikersnaam en wachtwoord.
2. Iets wat je bent; dit omvat alle biometrische gegevens zoals vingerafdruk, gezichtsherkenning of irisscan.
3. Iets wat je hebt; sleutelkaarten en hardware tokens zijn typische voorbeelden van deze factor. Het apparaat waarop de gebruiker werkt kan ook als factor gebruikt worden, het is dan enkel mogelijk in te loggen vanaf een 'vertrouwd apparaat'.
4. Locatie; in deze factor moet de gebruiker op een bepaalde locatie aanwezig zijn om toegang te kunnen krijgen. Dit kan een geografische of netwerkbepending zijn.

In een eerste stap voert de gebruiker gebruikersnaam en wachtwoord in. In de tweede stap dient de gebruiker een tweede actie uit te voeren. Dit kan het ingeven zijn van een tweede sleutel, bv. een ontvangen sms-code of een code ontvangen of aangemaakt

door een gekoppelde app op de gebruikerssmartphone, of het louter bevestigen van het inlogverzoek op zo'n gekoppelde app. Dit is een typische twee-factor authenticatie (2FA).

Waarom Multi-Factor Authenticatie?

Antivirus, firewall, encryptie en andere informatieveiligheidsinspanningen hebben geen enkel effect als een cybercrimineel zich kan voordoen als een legitieme gebruiker. Als een cybercrimineel inlogt met jouw gecompromitteerde inloggegevens, zal het systeem denken dat jij inlogt en deze cybercrimineel al de taken laten uitvoeren waartoe jij gemachtigd bent.

MFA verbetert de beveiliging van je inloggegevens en is een zeer belangrijk onderdeel van informatiebeveiliging geworden. Indien je wachtwoord gecompromitteerd wordt kan de cybercrimineel je wachtwoord niet direct misbruiken omdat deze ook de 2^{de} factor nodig heeft.

Tevens brengt dit conformiteit met de wetgeving dichterbij. Zo vereist de Algemene Verordening Gegevensbescherming (AVG) dat de bescherming van gevoelige persoonsgebonden data geoptimaliseerd wordt. MFA is een grote stap in deze richting.

Beperkingen van Multi-Factor Authenticatie

MFA is niet 100% veilig tegen cybercriminelen. Zo kunnen gebruikers nog altijd vallen voor phishing aanvallen waarbij de nietsvermoedende gebruiker naar een nagemaakte website gebracht wordt waar deze dan MFA-inlogt. De cybercrimineel heeft zo beide factoren verkregen en kan deze gebruiken om éénmalig zelf in te loggen. Ook kunnen SMS-berichten waarmee de 2^{de} factor wordt opgestuurd onderschept worden d.m.v. SIM-cloning (men maakt een duplicaat van je telefoon, waar dan copies van al je sms-berichten op toe komen).

Desondanks deze beperkingen blijft MFA de meest eenvoudige en zeer efficiënte beveiliging tegen misbruik van gecompromitteerde wachtwoorden, en MFA wordt dan ook meer aanschouwd als een minimale authenticatie beveiliging.

Bron: Vrije Universiteit Brussel

Verlies geen tijd

Waarschuw
onmiddellijk alle
betrokkenen



Hoe reageer je bij een aanval?

De middelen:

- Waarschuw de verantwoordelijke
- Contacteer dienst gehackte account
- Waarschuw contacten via ander kanaal
- Wijzig je wachtwoorden
- Voer antiviruscontrole uit

Hoe reageren wanneer je wachtwoord werd gehackt?

- Waarschuw de **verantwoordelijke** binnen je onderneming.
- Contacteer de **dienst** die je gehackte account beheert
- Waarschuw je **contacten** via een ander kanaal.
- Wijzig en versterk (=verleng) je **wachtwoorden**, overall trouwens: wijzig je wachtwoord als iemand (mogelijk) toegang heeft of toegang kan krijgen tot jouw account, bijvoorbeeld als je van anderen hoort dan ze vreemde berichtjes uit jouw naam krijgen. Verander je wachtwoord ook als de dienst waar je een account hebt te maken heeft met een datalek. Zo voorkom je dat degene die toegang heeft gekregen ook jouw accountgegevens kan misbruiken. Je kunt op de website www.haveibeenpwned.com controleren of jouw e-mailadres in een gelekte database voorkomt.
- Voer een **antiviruscontrole** uit op je computer.

Wachtwoorden: praat erover!

Wat is jouw mening?
Heb je opmerkingen?
Wat heb je
onthouden?
Je eerste actie?



10

Wat is jouw mening?
Heb je opmerkingen?
Wat heb je onthouden?
Wat zal de eerste actie zijn die je onderneemt na deze presentatie?



**CYBER SECURITY
COALITION**.be

**Een initiatief van
de Cyber Security Coalition**

Zijn doel? De IT-veiligheid in België opdrijven. Het brengt experts uit de academische wereld, de overheid en ondernemingen samen om cyber-crime beter te bestrijden.

www.cybersecuritycoalition.be



PASSWORD 7 123456 7
AZERTY 7 abc123 7

1 kleine lettertjes veilig voor 1 boze wolf
PASSWORD 3kl3v3rtbwl

Alle rechten voorbehouden © 2020 Cyber Security Coalition

Bedankt voor je aandacht!