Goede wachtwoorden 1

Optimaal en veilig online ondernemen

LEESWIJZER

Tegenwoordig hebben vrijwel alle bedrijven een computernetwerk. Hier wordt informatie over het bedrijf, het personeel en de klanten opgeslagen en uitgewisseld. Het is daarom van belang om de computers, netwerken en bedrijfsinformatie te beveiligen. Net als in de echte wereld kun je online vertrouwelijke informatie en privacy nooit 100% gegarandeerd beveiligen. Maar met een beetje gezond verstand en wat praktische handreikingen kom je wel een heel eind.

Verdeeld over 8 thema's krijg je informatie en opdrachten die je helpen om veilig online te ondernemen. Lees de concrete en praktische informatie, de praktijkervaringen van collega-ondernemers, doe de opdrachten en kies wat bij je past.

De 8 thema's zijn los van elkaar te lezen, maar vormen uiteindelijk één compleet webboek. Het webboek is in .pdf-formaat. Je kunt het webboek op je computer lezen en de opdrachten in .pdf maken. De ingevulde opdrachten kun je uitprinten (de informatie wordt bij de gratis versie van .pdf leesprogramma niet opgeslagen!). Maar als je het prettiger vindt, kun je het webboek of de geselecteerde thema's ook meteen uitprinten en de opdrachten met pen en papier uitwerken.

Dit zijn de thema's:

1 Goede wachtwoorden
2 Beveiliging van apparatuur en netwerk
3 Veilig gebruik sociale media
4 Cybercrime
5 Cookies
6 Privacy: beveiligen van klantgegevens en personeelsgegevens
7 Veilig werken in de cloud
8 Veilig online betalen

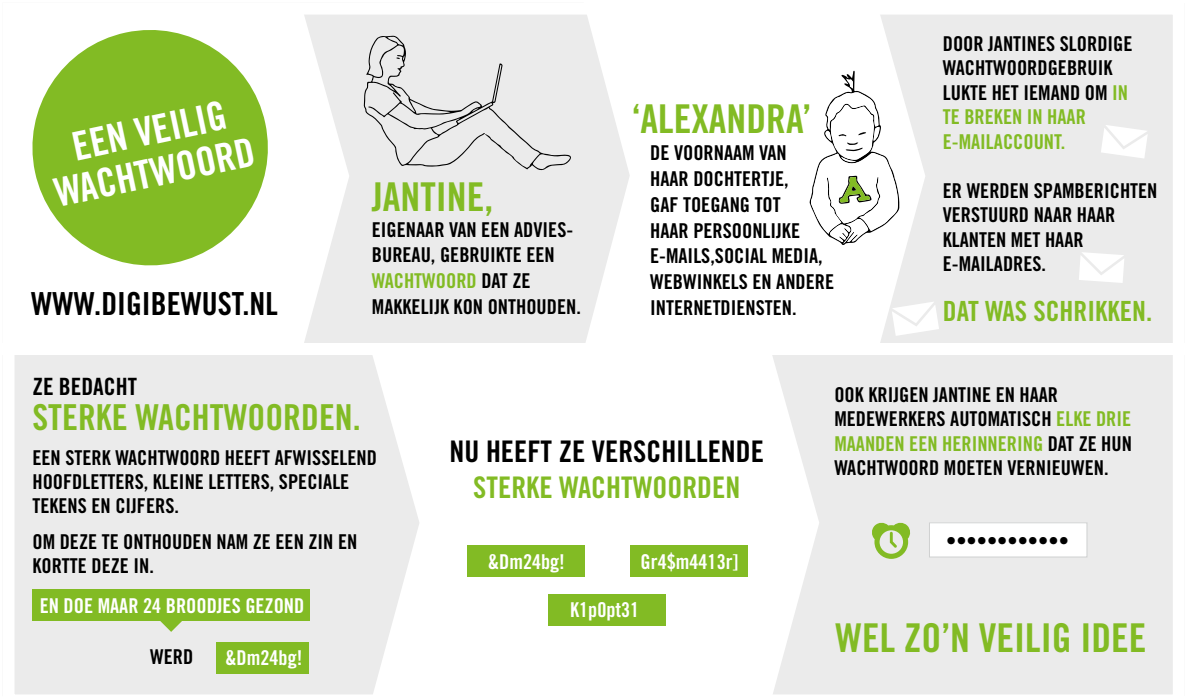
Het webboek en de themahoofdstukken zijn onderdeel van de cursus **digibewustondernemenin1minuut.nl**. Naast de informatie op onze website **Digibewust.nl** en de website **Beschermjebedrijf.nl** is het mogelijk om individuele ondersteuning te krijgen, je kunt hiervoor contact opnemen met:

Syntens Innovatieadvies

088-444 0 222 Iedere werkdag bereikbaar van 8.00 tot 20.00
Ook via e-mail en chat bereikbaar **http://www.syntens.nl/Contact.aspx**
of

MKB Servicedesk

088-652 0 020 gratis voor leden MKB- Nederland, er wordt gevraagd je lidnummer
0900-645 66 52 € 0,0,45 c/pm voor vragen van niet-leden
Ook bereikbaar via het contactformulier
http://www.mkbservicedesk.nl/vraag-mkb-servicedesk/9/marketing-desk.htm



Digitale informatie-uitwisseling wordt veelal beveiligd met een combinatie van een gebruikersnaam en een wachtwoord. Het aantal wachtwoorden dat je tegenwoordig moet onthouden is buitengewoon groot en de verwachting is dat dit alleen maar verder zal toenemen. Het is dus bijna onmogelijk om voor alle diensten unieke willekeurige tekenreeksen te verzinnen én te onthouden. En het wordt je nog lastiger gemaakt als de dienst waarvan je gebruikmaakt ook nog allerlei regels en beperkingen gaat opleggen met betrekking tot de samenstelling van het wachtwoord. Zo kun je bij de ene dienst maximaal zes cijfers gebruiken, bestaat de andere dienst uit een viercijferige pincode, en kun je soms wel en soms geen leestekens gebruiken. Kortom, je zult tot een aanvaardbaar compromis moeten komen van iets wat enerzijds makkelijk te onthouden is en anderzijds niet eenvoudig te achterhalen is.

WAAROM WORDEN WACHTWOORDEN GEKRAAKT?

Om jezelf te kunnen beschermen is het handig te weten waarom men interesse heeft in jouw gegevens. Criminelen stelen wachtwoorden op websites met een lage beveiliging en proberen datzelfde wachtwoord en dezelfde gebruikersnaam dan te gebruiken in een veiligere omgeving zoals op bankwebsites.

Persoonsgegevens zijn ook geliefd bij criminelen omdat je daarmee fraude kunt plegen terwijl je je achter de identiteit van een ander verschuilt.

HOE WORDEN WACHTWOORDEN GEKRAAKT?

I Wachtwoorden kunnen worden gekraakt met een script dat automatisch allerlei voorspelbare wachtwoorden uitprobeert. Vermijd daarom altijd:

- Woorden uit woordenboeken in welke taal dan ook.
- Woorden die achterwaarts zijn gespeld, algemeen verkeerd gespelde woorden en afkortingen.
- Tekens die in een voorspelbare volgorde staan of een herhaling van tekens, bijvoorbeeld **12345678, 222222, abcdefg** of letters die naast elkaar staan op het toetsenbord zoals **zxcvbn**.

II Bij identiteitsfraude wordt vaak meer gericht gezocht op bijvoorbeeld sociale media waar veel informatie over personen te achterhalen is. Vermijd dus wachtwoorden met persoonlijke informatie, zoals je naam, verjaardag, nummerbord, etc. Het is in elk geval niet raadzaam zaken als verzekeringsnummers, paspoort- of rijbewijsinformatie, burgerservicenummer, etc. op welke publiek zichtbare website dan ook te vermelden.

III Door in te breken bij een dienst waar je online gebruik van maakt. Je hebt vast weleens gelezen hoe klantgegevens van een bedrijf of instelling na een digitale inbraak op 'straat' zijn komen te liggen. Stel: er wordt digitaal ingebroken bij een onlinewinkel waar je recent iets besteld hebt; op deze wijze heeft men in één keer veel gegevens te pakken zoals je creditcardnummer, adresgegevens en dat in combinatie met je gebruikersnaam en wachtwoord.

WAT MAAKT WACHTWOORDEN STERKER?

- Hoe meer tekens een wachtwoord bevat hoe lastiger het wordt om het wachtwoord te kraken, gebruik daarom (waar mogelijk) minimaal acht tekens.
- Hoe meer variaties mogelijk zijn, hoe lastiger het wordt om het wachtwoord te kraken, probeer daarom zo veel mogelijk diversiteit in de gebruikte tekens aan te brengen (dus letters, hoofdletters, cijfers en leestekens).
- Naarmate je langer gebruikmaakt van een wachtwoord neemt de kans toe dat anderen het wachtwoord kennen of dat het wachtwoord gekraakt wordt, wachtwoorden worden dus sterker als ze maar voor korte tijd gebruikt worden en dan weer vervangen worden.
- Wachtwoorden worden zwakker als je ze voor al je internetdiensten gebruikt en sterker als je voor elke dienst een eigen wachtwoord gebruikt. Het is daarom raadzaam om voor diensten die extra risico met zich meebrengen indien ze achterhaald worden (financiële of privacygevoelige diensten) een volstrekt uniek wachtwoord te hanteren.

HOE KOM JE DAN WEL TOT EEN STERK WACHTWOORD DAT OOK NOG EENS EENVOUDIG TE ONTHOUDEN IS?

Er zijn veel verschillende methoden om tot een goed wachtwoord te komen. Hoewel je altijd enigszins afhankelijk bent van de wachtwoordregels die de aanbieder van de internetdienst hanteert. Een veel beproefde methode is de volgende:

STAP	Voorbeeld	Uitkomst	Jouw keuze
STAP 1 Kies een manier om te onthouden om welke internetdienst het gaat. Kies de eerste en de laatste letter van de dienst, of de eerste twee, of de eerste en de derde.	Kies bijvoorbeeld altijd de laatste twee letters vóór .com of .nl of .net. Dit betekent voor de dienst http://www.linked**in**.com dat je de letters in gebruikt.	in	http://www.youtube.com/ y o u t u b e Welke letters ga je kiezen? ☐☐
STAP 2 Maak STAP 1 persoonlijk door altijd een stapje vooruit in het alfabet te doen, of bepaalde letters te vervangen voor een cijfer/leesteken, of door een hoofdletter toe te passen.	Besluit bijvoorbeeld altijd: • bij de eerste letter vier stappen vooruit te doen in het alfabet >> **i** wordt **m** • en de tweede letter door een hoofdletter te vervangen >> **n** wordt **N**	mN	Hoe ga je het persoonlijk maken? ☐☐ Wordt: ☐☐
STAP 3 Kies een zin als ezelsbruggetje **Oom Jan heeft 2 katten op schoot.** Kies vervolgens bijvoorbeeld het eerste teken waaruit deze zin is opgebouwd.	Dit betekent voor deze zin: **O**om **J**an **h**eeft **2** **k**atten **o**p **s**choot >> OJh2kos	OJh2kos	Kies een zin met zes woorden: ☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐ ☐☐☐☐☐☐☐☐ Welke tekens ga je kiezen? ☐☐☐☐☐☐
STAP 4 Voor de extra veiligheid vervang je een van de letters door een leesteken.	mLOJh2kos Vervang bijvoorbeeld de laatste **s** door een **$**.	Het uiteindelijke wachtwoord voor LinkedIn is dus: mNOJh2ko$	Vervang een van de letters door een leesteken: ☐☐☐☐☐☐ Voeg het eindresultaat van STAP 2 en 4 samen in een wachtwoord met acht tekens: ☐☐☐☐☐☐☐☐

Dit ziet er misschien uit als een enorm ingewikkelde operatie, maar je zult zien dat binnen de kortste keren het wachtwoord vanwege het ezelsbruggetje in je hoofd zit en dat het relatief eenvoudig terug te redeneren is wat het wachtwoord is, mocht het je niet direct te binnen schieten.

Het is buitengewoon belangrijk om een lijst aan te leggen in je agenda van de diensten waar je gebruik van maakt (zonder wachtwoorden te vermelden!) en dat je elk kwartaal een uurtje de tijd neemt om je wachtwoorden te wijzigen.

WELKE ALTERNATIEVEN ZIJN ER?

Wachtwoorden opslaan in de browser

Je zult vast weleens de melding 'wachtwoord onthouden' of 'onthoud mijn wachtwoord' hebben gezien bij het inloggen op een website. Deze melding staat op de website zelf of wordt aangeboden door de browser die je gebruikt. Dit lijkt een handige optie, maar bedenk wel dat op het moment dat iemand jouw computer gebruikt of jouw laptop of tablet in verkeerde handen valt – na bijvoorbeeld verlies of diefstal – de weg naar jouw gegevens openstaat.
Ook wordt de software die nodig is om het wachtwoord voor je te onthouden en toe te passen (een zogenaamde cookie) juist door hackers gebruikt om toegang te krijgen tot jouw computer. De optie 'Wachtwoord onthouden' lijkt dus handig, maar brengt wel allerlei beveiligingsrisico's met zich mee.

Wachtwoordenkluis of wachtwoordenmanager

Zowel online als offline (bijvoorbeeld op een USB-stick) heb je de mogelijkheid om gebruik te maken van diensten waar je in een beveiligde omgeving wachtwoorden kunt opslaan. Dit wordt een wachtwoordenkluis of een wachtwoordenmanager genoemd. Voor beide opties valt iets te zeggen. Online kun je niet bij je wachtwoorden zonder internetverbinding of als de dienst om welke reden dan ook niet bereikbaar is. Offline (bijvoorbeeld op een USB-stick) kun je het apparaat waar je je wachtwoorden hebt opgeslagen, verliezen of beschadigen.
De wachtwoordenmanager of wachtwoordenkluis is uitsluitend toegankelijk met – je raadt het al – een wachtwoord.

OPENID

Met de komst van sociale media is het gemiddelde gebruik van het aantal wachtwoorden enorm toegenomen. Voor elk profiel en voor elke dienst moet er weer een wachtwoord ingevuld worden en gebruikers worden een beetje wachtwoord- en profielmoe. Daarom zijn er diverse initiatieven waarbij accounts en profielen van de verschillende diensten aan elkaar gekoppeld kunnen worden. Hierdoor kun je met één centraal profiel op verschillende plekken tegelijk inloggen. Als je bijvoorbeeld op de fotosite Flickr wilt inloggen, kun je dat doen met je Yahoo-, Facebook- of Google-gegevens, en is het niet nodig om een nieuw profiel aan te maken. Voorzichtigheid is uiteraard wel geboden! Log alleen in met de gegevens van een ander profiel als je zeker weet dat de website waar je je gegevens achterlaat een betrouwbare partij is.

INSTRUCTIES VOOR MEDEWERKERS

Wachtwoorden zijn ongelofelijk belangrijk. Ze vormen de sleutel tot de digitale kast waar alle vertrouwelijke gegevens in zitten, waar de concurrentiegevoelige prijsinformatie staat, of zelfs de sleutel naar het kassysteem. Je klant vertrouwt erop dat zijn informatie bij jou in goede handen is. Daarom is het uitermate

belangrijk helder te communiceren wat je van het personeel verwacht met betrekking tot het gebruik van wachtwoorden:

- Wachtwoorden moeten sterk zijn en dus opgebouwd zijn uit een grote diversiteit qua gebruikte tekens, dus letters, hoofdletters, cijfers en leestekens!
- Wachtwoorden moeten elk kwartaal gewijzigd worden.
- Men mag geen wachtwoorden gebruiken die gekoppeld zijn aan persoonlijke gegevens (trouwdata, namen van familieleden, huisdieren, etc.).
- Men mag geen wachtwoorden gebruiken die gelijk zijn aan wachtwoorden van persoonlijke internet-profielen.
- Wachtwoorden zijn strikt persoonlijk en mogen niet aan collega's of andere personen worden doorgegeven.
- Wachtwoorden moeten op websites, interne systemen, maar ook op apparatuur worden toegepast. Dus stel een wachtwoord in om laptops, mobiele telefoons, smartphones, tablets en andere apparatuur af te schermen van derden.

Colofon

Dit is een uitgave van het Digibewust. Digibewust wil het veilig en verantwoord gebruik van internet en van computer, mobiele telefoons en andere digitale middelen stimuleren. Digibewust is onderdeel van het programma Digivaardig & Digiveilig dat een samenwerkingsverband is tussen overheid, bedrijfsleven en maatschappelijke organisaties. Dit programma wordt ondersteund door het ministerie van Economische Zaken, de Europese Commissie en diverse bedrijven (KPN, UPC, NVB, IBM, SIDN en Ziggo, CA-ICT) en wordt uitgevoerd door ECP | Platform voor de Informatiesamenleving (**www.ecp.nl**).

Auteur Sandra Brandenburg | CapStock vormgeving | Het Redactiepakhuis

Mogelijk gemaakt door: