EEN VEILIG WACHTWOORD

AAN DE SLAG MET DIGITALE VAARDIGHEDEN
TRAINING: EEN VEILIG WACHTWOORD

DIGIVAARDIG IN DE ZORG

EEN VEILIG WACHTWOORD

Een goed wachtwoord is een begin van veilig social media gebruik. In dit werkblad wordt besproken hoe je een veilig wachtwoord maakt voor jouw social mediaprofielen.

Social media is vooral leuk. Maar het kent ook wat gevaren. Deze zijn te voorkomen door je gezonde verstand en een goed wachtwoord te gebruiken.

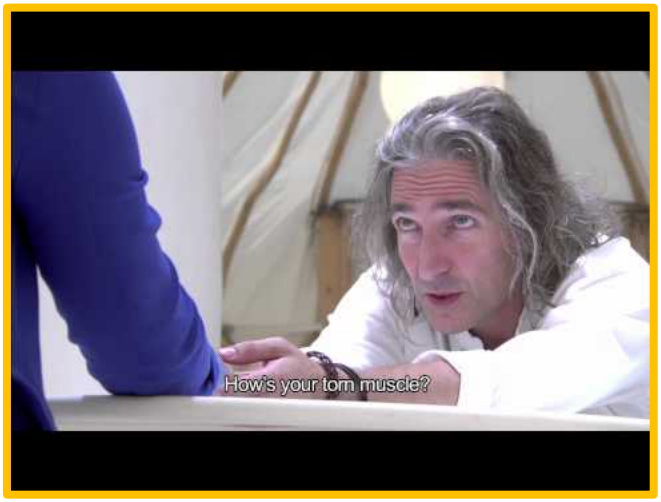
Opdracht 1

Kun je benoemen wat een risico is als je geen goed wachtwoord voor je Facebook-account hebt?

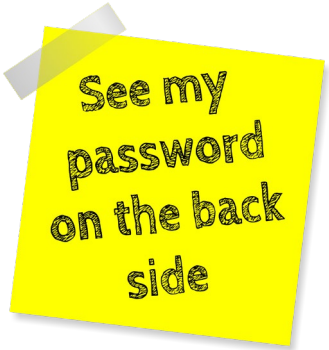
Natuurlijk moet je oppassen

In dit inmiddels legendarische filmpje zie je hoe gewone mensen verrast worden door een “waarzegger” die alles van ze lijkt te kunnen zien ….

Of zoek op YouTube naar
‘Amazing mind reader reveals his 'gift'



Het zweet breekt je nu al uit? Nogmaals, je hebt veel zelf in de hand. Als je maar weet wat je kan doen. Laten we dus maar snel verder gaan.



Wachtwoord

Online veiligheid begint met jouw wachtwoorden.
Voor het beschermen van de computer die je gebruikt.
Voor het beschermen van je smartphone en tablet.
En voor al je social media-accounts en de websites die je bezoekt.

En dan niet zoals hiernaast, op een briefje met alle wachtwoorden van jou en je collega’s dat op kantoor hangt (we hebben het echt gezien!). Maar persoonlijke sterke wachtwoorden (onthoudt “sterke”) die voor verschillende platformen verschillend zijn en regelmatig veranderen.

Opdracht 2

Wat is het risico als je hetzelfde wachtwoord gebruikt voor je Facebook en voor het EPD (elektronische patiënt dossier)?

Om toegang te krijgen tot de computer van het ziekenhuis moet je regelmatig je wachtwoord veranderen. Wel zo veilig! Je krijgt vanzelf een melding van het systeem dat het weer tijd is om je wachtwoord te wijzigen.

Opdracht 3

Hoe help jij jezelf herinneren dat het weer tijd is om je social media wachtwoorden te wijzigen?

Om het risico te verkleinen dat je gehackt wordt gebruikt het ziekenhuis Twee-Staps-Verificatie.
Meer informatie hierover vind je in het werkblad Basisvaardigheden In- en uitloggen.

Wil je je social media ook extra beschermen met Twee-Staps-Verificatie? Kijk dan op https://veiliginternetten.nl/themes/situatie/wat-tweestapsverificatie/

"Wachtwoorden? Lastig!"

Je moet ze verzinnen en je moet ze onthouden. En ze moeten ook nog "sterk" zijn. Daarom nemen we vaak de naam van ons huisdier, of onze partner of kinderen en voegen er cijfers aan toe, zoals 1234, 4321 of je trouwdatum of geboortedatum. Helaas, dat ligt wel erg voor de hand.
Die wachtwoorden zijn heel snel te kraken.

Stappenplan

Een sterk, goed en betrouwbaar wachtwoord is makkelijker te maken dan je denkt. Hieronder vind je daarvoor de stappen die door beveiligings-experts worden aangeraden.

1. verzin een zin

Die zin mag niet te kort zijn. Gebruik minimaal 8 woorden. Je wachtwoord voor Facebook kan bijvoorbeeld zijn:

Dit wachtwoord heb ik op 1 september bedacht voor Facebook

2. Vervang letters door cijfers

Van de i kan je een 1 maken, van de B een 8, of de kleine letter b een 6 en van de o een 0.
De datum in de wachtzin kan je vervangen door het nummer van de maand te noemen.
1 september wordt dan 19

Dit wachtwoord heb ik op 19 bedacht voor Facebook

3. Gebruik van ieder woord de eerste letter
Je wachtzin wordt dan een wachtwoord, veel minder lang, maar toch te onthouden.
De voorbeeldzin voor Facebook wordt dan:

Dwhio19bvF

4. Bedenk welke letter een hoofdletter moet zijn
Dat kan iedere derde letter zijn.

DwHiO19bVF

Of alleen de eerste en de laatste. Maar dat is minder sterk.

Dwhio19bvF

5. Gebruik "speciale tekens"
Dat zijn bijvoorbeeld deze: ! @ # $ % ^ & * ( ) + = ? > < _ -
Je wachtwoord kan er dan zo uit zien:

@DwHiO19BvF-

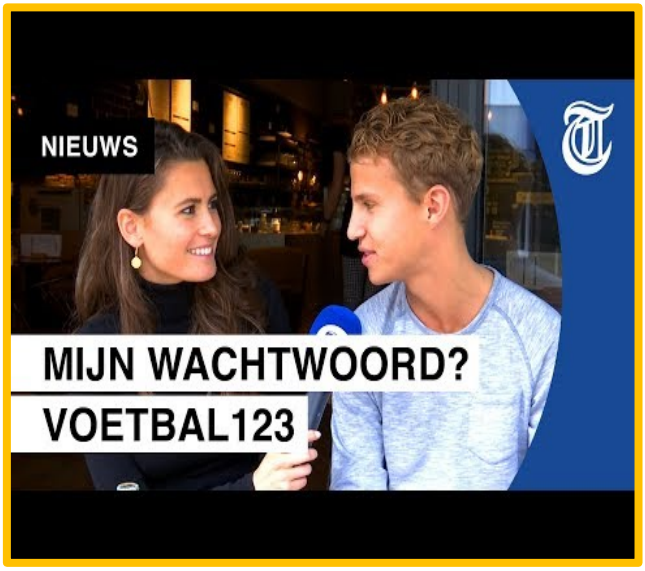
6. Controleer je wachtwoord
Natuurlijk wil je weten of je wachtwoord sterk genoeg is. Zowel je oude als je nieuwe wachtwoord kan je controleren op deze site: https://veiliginternetten.nl/wachtwoord-check/

Opdracht 4

Volg de voorgaande stappen en controleer je wachtwoord.
Hoe komt jouw wachtwoord uit de test?

Verstandig omgaan met je wachtwoord

Nu je een goed wachtwoord hebt is het belangrijk dat je het kunt onthouden maar met niemand deelt. Bekijk dit filmpje maar eens over hoe het dus niet moet. Het filmpje is op YouTube te vinden als je zoekt op 'bizar iedereen geeft wachtwoord'.



Twee-staps-verificatie

Wil je je social media-accounts echt goed beveiligen dan hebben de meeste kanalen een mogelijkheid om twee-staps-verificatie in te stellen. Je krijgt dan nadat je je gebruikersnaam en wachtwoord invult bijvoorbeeld een sms met een code die je in moet vullen. Zo weet je helemaal zeker dat alleen jij toegang hebt tot jouw social media.

Nog wat laatste tips:

Bron: https://veiliginternetten.nl/themes/basisbeveiliging/situatie/mijn-wachtwoord-sterk-genoeg/?type=q

1. Geef je wachtwoord aan niemand
2. Laat niemand meekijken als je je wachtwoord intypt
3. Gebruik verschillende wachtwoorden voor verschillende diensten
4. Wissel je wachtwoorden
5. Laat je wachtwoord niet rondslingeren in de buurt van je computer, op je bureau of in je agenda
6. Sla je wachtwoorden niet onbeveiligd op je computer op. Versleutel het bestand of neem een wachtwoordmanager
7. Laat je wachtwoorden niet in de e-mail staan
8. Geef je wachtwoord nooit aan bedrijven die er om vragen
9. Verander je wachtwoord als een website is gehackt
10. Sla wachtwoorden niet op in de browser
11. En zorg uiteraard voor een beveiligde computer, smartphone of tablet.

Dit werkblad is gemaakt door: Hans Versteegh, Welzijn 3.0 (www.welzijn30.nl) en bewerkt door Tessa Hoonhorst in opdracht van Digivaardig in de Zorg. Heb je opmerkingen of vragen over dit lesmateriaal? Mail dan naar info@digivaardigindezorg.nl.