



SOCIAL MEDIA VEILIGHEID & WACHTWOORD



AAN DE SLAG MET DIGITALE VAARDIGHEDEN
TRAINING: **SOCIAL MEDIA**





SOCIAL MEDIA EN VEILIGHEID

Ben ik wel veilig als ik social media gebruik?

Kan niemand mijn gegevens stelen?

Of mijn foto misbruiken?

Online veiligheid, en vooral het gevoel dat het onveilig is, maakt dat we soms erg onzeker zijn.

Of maar gewoon in het diepe duiken, "We zien wel." Terwijl je zelf veel kan doen om ellende te voorkomen.

Jouw cliënt

Daarom is het erg verstandig hier bij stil te staan. Voor jezelf maar ook zeker voor jouw cliënt.

Als begeleider ben jij vaak degene die helpt er voor te zorgen dat jouw cliënt niet via de computer of smartphone in de problemen raakt. De vragen aan het begin, hierboven, kan je ook vanuit hem of haar stellen.

Hopelijk is dat voor jou geen argument om er niet aan te beginnen. Je ontzegt je cliënt dan ook de positieve kanten van social media en internet. We hopen dat je hierna weet wat je te doen staat en dat je de goede maatregelen neemt. Dan komt het vast wel goed.

Wat zijn de gevaren?

In de werkbladen die gaan over veiligheid gaan we het hebben over de volgende "gevaren van het internet" waar jij in de begeleiding van je cliënt mee te maken kunt krijgen en waar je op moet letten:

- Wachtwoorden
- Je online identiteit
- Wat je kan doen als het mis gaat
- Grooming
- Sexting
- Cyberpesten
- Hacken
- Phising
- Wat je online deelt
- Online netwerken

Natuurlijk moet je oppassen

In dit inmiddels legendarische filmpje zie je hoe gewone mensen verrast worden door een "waarzegger" die alles van ze schijnt te kunnen zien

<https://youtu.be/F7pYHN9iC9I>

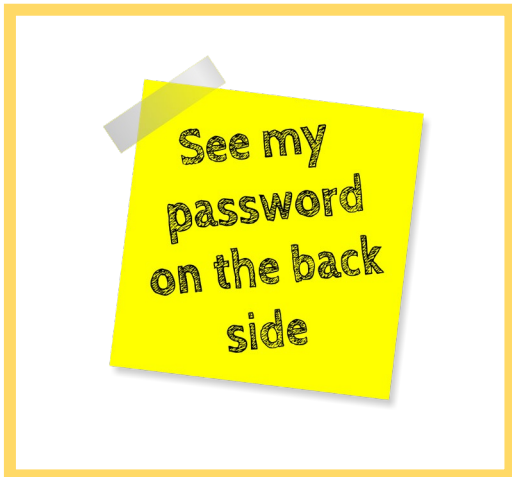
Of zoek op YouTube naar
'Amazing mind reader reveals his 'gift'



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.

AAN DE SLAG MET DIGITALE VAARDIGHEDEN
TRAINING: SOCIAL MEDIA





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.

"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.

Pak pen en papier en schrijf mee met de volgende stappen. Je ziet je sterke wachtwoord dan vanzelf ontstaan. Of print de laatste pagina van deze module uit en schrijf daarop mee.

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

Hier doen we even een tussen-check. Tel het aantal tekens waaruit het wachtwoord nu bestaat. In dit geval zijn het er 10. Sterke wachtwoorden hebben minimaal 8 tekens. Hoe meer hoe beter. Daarom moest je oorspronkelijke zin lang genoeg zijn.

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-

Check je wachtwoord

Natuurlijk wil je wel 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/>

Hoe komt ons voorbeeld wachtwoord uit de test?



Hoe ga je verstandig met je wachtwoorden om?

Je moet je wachtwoorden natuurlijk wel goed bewaren en onderhouden. Met deze tips zit je goed:

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

En zorg uiteraard voor een beveiligde computer, smartphone of tablet.

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

AAN DE SLAG MET DIGITALE VAARDIGHEDEN

TRAINING: SOCIAL MEDIA



Nu jij! Maak al je wachtwoorden sterk en veilig.

Hoe veilig zijn jouw wachtwoorden? Doe de check. En verzin tenminste één nieuwe.

Test het wachtwoord dat je gebruikt om in te loggen op je werk via de site onderaan deze pagina. Bij punt 6. Goed of niet? En het wachtwoord voor je meest gebruikte social media account? Ga zo al je wachtwoorden langs.

Verzin als het niet sterk genoeg is volgens het stappenplan een nieuw wachtwoord.

1. Verzin een zin (minimaal 8 woorden)

.....

2. Vervang letters door cijfers

.....

3. Gebruik van ieder woord alleen de eerste letter

.....

Doe de tussencheck, heb je minimaal 8 tekens gebruikt?

4. Bedenk waar de hoofdletters moeten komen

.....

5. Voeg speciale tekens toe

.....

6. Doe de sterkte-check op : <https://veiliginternetten.nl/wachtwoord-check/>

Snap je het? Leg het nu uit aan cliënten die op Social Media zitten!

Tip:

Print het blad met dit stappenplan uit. Of schrijf het over, voor ieder wachtwoord dat je gaat veranderen.