WWW.MINDYOURSTEP.INFO

Do's en Don'ts social media

je vuile was hang je ook niet buiten, waarom je gegevens dan wel?

De vraag

Veel mensen besteden meerdere uren per dag aan social media. Er wordt van alles gedeeld, van een bericht over weekendplannen en nieuw gekochte gadgets, tot een foto van een vliegticket of net behaald rijbewijs. Met deze berichten geef je (onbewust) veel informatie over jezelf vrij. En criminelen maken hier gretig gebruik van. Ze proberen via de informatie die in je profiel staat, je wachtwoorden te achterhalen of gebruiken deze informatie anderszins. Zo weten ze door een foto van je vliegticket dat je op vakantie bent en biedt dat kansen om ongestoord bij je thuis te kunnen inbreken. Je adres achterhalen ze door je naam, die op je vliegticket staat, of via andere informatie die je op social media hebt gedeeld. Belangrijk dus dat je bewust bent van wat je op social media plaats. Wat kun je beter wel en niet op social media delen?

De uitdaging

Het liefst maken we gebruik van social media voor gezellige en sociale doeleinden. Het delen van bijzondere momenten, en het gemakkelijk contact leggen met nieuwe of oude bekenden. Maar helaas zijn er ook criminelen online. Normaal gesproken laat je (vreemde) mensen toch ook niet in je tas kijken? Dit is immers privé. Waarom plaatsen we dan wel van alles op social media? Criminelen kunnen je (identiteit)gegevens die op je profiel te lezen zijn, voor criminele doeleinden gebruiken. Het is de uitdaging social media te gebruiken op een leuke en veilige manier, zonder dat je informatie weggeeft die criminelen kan helpen je identiteit te stelen.

De oplossing

Wees je daarom bewust van de zaken die je deelt op social media. We geven je graag een aantal tips over de Do's en Don'ts.

Do's

- Houd wat je deelt op social media, alleen voor vrienden zichtbaar.
- Gebruik maximale privé-instellingen.
- Zet je locatievoorziening voor Facebook uit, zo zien Facebook en anderen niet continu waar je bent.
- Maak gebruik van dubbele authenticatie voor het inloggen op social media, door naast het inloggen met een wachtwoord ook een via de sms verzonden code in te voeren.
- Kijk eens wat anderen op jouw social media pagina kunnen zien als ze wel en/of geen connectie van je zijn.
- Houd je netwerk klein.
- Je kunt niet overal bij zijn, en alle nieuwe updates als eerste lezen lukt ook niet. Gun jezelf meer momenten zonder telefoon.

Don'ts

- Plaats geen foto's met documenten waar persoonsgegevens op staan (identiteitskaart, vliegticket et cetera).
- Plaats geen onwaarheden. Het is ontzettend vermoeiend leugens vol te houden en je vrienden zien graag de 'echte' jij.
- Klik niet op verdachte content zoals een advertentie waarbij bijvoorbeeld €1.000,- aan shoptegoed wordt aangeboden, deze kan ransomware bevatten.
- Accepteer geen mensen die je niet kent.
- Zet niet op social media dat je op vakantie bent, zo maak je het inbrekers wel erg makkelijk.
- Zet geen contactgegevens op social media, zoals een telefoonnummer of e-mailadres.
- Plaats geen foto's of berichten online, die later een nadeel kunnen vormen. Foto's en berichten, blijven altijd (ergens) online staan.
- Maak bij het aanmaken van een account voor een App geen gebruik van 'Log in with Facebook', die voorkomt dat je je mail hoeft te gebruiken. Hiermee geef je Apps veel meer (persoons)informatie dan strikt noodzakelijk is.
- Geloof niet alles wat je leest. Iedereen kan nieuws plaatsen en regelmatig wordt nieuws maar vanuit één invalshoek belicht, of worden er feiten achterwege gelaten.

Meer weten?

Bezoek onze website www.mindyourstep.info voor meer tips en tricks op privacy- en informatieveiligheidsvlak.
Of neem direct contact op met Marijn Berndes via marijn@soulmade.nl of door te bellen naar 0162-430345.