

De moeilijke balans tussen sociale media en cyber security

(naar een artikel bij Clickx van 5 februari 2021)

“Sociale media” is haast niet meer uit onze levens weg te denken. Het is de nieuwste vorm van communicatie geworden, en voor sommige mensen ook de enige.

We hebben allemaal onze eigen redenen om ons met sociale media bezig te houden. Of we er nu foto's van onze katten op delen, berichten mee sturen naar onze familie en vrienden, promotie op maken voor ... of op de hoogte willen blijven van al het nieuws dat zich over de wereld verspreidt, we kunnen haast niet meer zonder. Tegenover het gretige gebruik van sociale media staat wel het iets minder tastbare concept van cyberveiligheid, waar veel minder mensen mee bezig zijn, tot het echter te laat is. Hackers maken gebruik van allerlei technieken en slinkse listen om toegang te krijgen tot je sociale media en alle data die daarop te vinden is. Dat kan allerlei desastreuze gevolgen hebben voor jou en je omgeving, je bedrijf en je PC of laptop, maar ook voor je portefeuille.

De eenvoudigste oplossing om je veiligheid online te garanderen is natuurlijk om al je accounts bij sociale media-platformen te verwijderen. Dat is natuurlijk wat drastisch en ook een beetje onterecht, want deze platformen hebben ook hun voordelen.

ONBETROUWBARE PLATFORMEN

Sociale media hebben we in alle vormen en kleuren: Facebook, Twitter, Snapchat en Instagram, ...

Vermijd het klikken op advertenties

Voor veel van deze platformen is **elke klik die je maakt belangrijk**.

Een klik zorgt voor data, gegevens die geld opbrengen en informatie verstrekken: vandaar gepersonaliseerde advertenties.

Klik **NOOIT** op een url (webadres)

Vermijd gevoelige data

Elke info over familie – vrienden – vereniging ed. kan tot identiteitsdiefstal leiden. Hackers ontfutselen zo inloggegevens en dringen een netwerk binnen.

Denk eraan dat foto's die je plaatst GPS data kunnen bevatten. Deze gegevens zijn tot op 5 m nauwkeurig.

OOK:

GEEN telefoonnummers

Beperk de toegang tot je foto's: liefst 'enkel vrienden'

Een stevig **wachtwoord**

(gebruik wachtwoordmanagers – verander regelmatig van wachtwoord.)

Ruim sluimerende accounts op: afmelden – vermijden – afsluiten.

Stoute software (malicious malware)

Installeer UITSLUITEND APP's via de Google Play Store en Apple App Store

Het hele artikel vind je: [HIER](#)