Tip 10 – Ook in je vrije tijd bescherm je informatie

Scherm niet alleen op het werk informatie af. Ook in je privésfeer moet je persoonlijke en bedrijfsgevoelige informatie beschermen. Wees dus voorzichtig met wat je thuis, in de vereniging, aan de toog of op sociale media vertelt.

Hou hierbij zeker rekening met de volgende aandachtspunten:

- **Eens op het internet, altijd op het internet**. Totale verwijdering op het internet heb je vaak niet meer in eigen handen. Denk dus 2x na vooraleer je foto's deelt, posts maakt of documenten openbaar maakt.

- **Persoonlijke toestellen**. Iedereen die toegang heeft tot jouw toestel (bv. familieleden), heeft ook toegang tot mogelijks vertrouwelijke informatie! Zorg voor een pincode, fingerprint of andere beveiliging.

Cybercriminelen zullen niet twijfelen om je gegevens te gebruiken om phishingmails of andere malwareberichten te sturen om je te overtuigen je logingegevens, bankgegevens, pincodes of andere private gegevens door te geven.

Denk ook aan :

- Regelmatig melden o.a. facebook, instagram en google, dat zij hun gebruiksvoorwaarden (policy) hebben aangepast. Controleer dan opnieuw de beveiligingsinstellingen van deze toepassingen. Beperk de zichtbaarheid van je privégegevens of laat ze achterwege!

- Maak ook regelmatig backups van je informatie, documenten, foto's of andere belangrijke bestanden en bescherm je zo tegen ransomware waarbij jouw gegevens onverwacht versleuteld worden en waarvoor losgeld moet betaald worden aan de cybercriminelen om ze terug te kunnen raadplegen.