# Praktische tips

## voor het gebruik van (mobiele) apparaten en netwerken

- Zijn je accounts wel eens gecompromitteerd (gehackt) geweest? Check het zelf op de website https://haveibeenpwned.com
- Gebruik nooit hetzelfde wachtwoord op meerdere plaatsen, zeker niet voor werk-gerelateerde accounts.
- Schakel altijd ‘twee factor authenticatie’ in waar mogelijk. Je hebt dan niet alleen een wachtwoord nodig, maar ook een code die je ontvangt op je mobiele telefoon wanneer je probeert in te loggen van een onbekend apparaat. Zo kunnen kwaadwillenden alsnog niet inloggen op je account wanneer je wachtwoord gestolen of gelekt is. Meer informatie voor het inschakelen van twee factor authenticatie vind je hier:
  Apple: https://support.apple.com/nl-nl/HT204915
  Google: https://www.google.nl/intl/nl/landing/2step/
  Instructies voor vele andere sites zijn te vinden op: https://www.turnon2fa.com/
- Zorg dat je altijd de laatste versie updates van je smartphone en computer geïnstalleerd hebt.
- Kijk uit met wat voor apparaten je aansluit op je (thuis-)netwerk. Verander altijd het standaard wachtwoord van bijvoorbeeld een netwerk/backup harde schijf (NAS) of beveiligingscamera nadat je deze geïnstalleerd hebt.
- Check of er onbewust zaken open staan op je thuisnetwerk. Dit kan je vanaf je eigen thuisnetwerk controleren op de volgende site:
  http://iotscanner.bullguard.com/
- Maak bij voorkeur geen gebruik van een openbaar WiFi-netwerk, maar gebruik de 3G/4G mobiele data verbinding van je telefoon.
- Zet je WiFi uit op het moment dat je het niet gebruikt.
- Maak nooit een backup van (gevoelige) werkbestanden op privé apparaten zoals USB-sticks of privé laptops of smartphones.
- Wees kritisch bij het installeren van apps op je smartphone. Kijk kritisch naar de rechten die de maker van de app vraagt op jouw apparaat.
  Een zaklamp-app die toestemming vraagt tot je locatie, contacten en microfoon is bijvoorbeeld niet erg logisch.
- Stop gevonden of gekregen USB-sticks nóóit zomaar in je eigen laptop. Meld bij de servicedesk of verantwoordelijke voor de informatiebeveiliging de vondst en laat de stick checken op de aanwezigheid van malware/virussen.

Maak vooral met veel plezier gebruik van de digitale mogelijkheden, maar wees bewust van de potentiële gevaren en bescherm jezelf daar dus tegen!