Perfect Day

10 Quick Wins Om veiliger te werken

01 Maak een noodplan
Wat ga je doen als je netwerk plat ligt of als je een datalek hebt? Wie moet je waarschuwen en wie moet het oplossen? Met een heldere taakverdeling in een goed uitgewerkt noodplan beperk je altijd schade.

02 Installeer goede antivirussoftware en een firewall
Goede anti-virus software lijkt een open deur, maar in de praktijk zien we anders. Schaf het aan, ook als je op een Mac werkt. Met goede antivirussoftware en een firewall beperk je de risico's snel en gemakkelijk.

03 Zorg dat alle software up-to-date is
Via bekende beveiligingsgaten is het makkelijk binnenkomen voor cybercriminelen. Vergeet niet om naast je telefoon en je computer ook je andere apparaten te updaten, zoals bijvoorbeeld de software van je router, je bluetooth speakers, jet netwerkprinters en andere slimme apparaten die met het internet verbonden zijn.

04 Maak en hanteer een wachtwoordbeleid met sterke wachtwoorden
Wachtwoorden van 10 of minder karakters zijn binnen een paar uur te kraken. Gebruik daarom sterke en unieke wachtwoorden, bijvoorbeeld een lange zin. 'Liesje leerde Lotje lopen' is 100.000 keer sterker dan een wachtwoord van 8 karakters.

05 Zet waar mogelijk 2 staps verificatie aan
2 staps verificatie is een authenticatie methode waarbij je twee stappen succesvol moet doorlopen om ergens toegang tot te krijgen. Zo kan iemand zelfs met jouw login en wachtwoord niet in je account omdat hij bijvoorbeeld een code van je telefoon nodig heeft.

06 Investeer in een goede back-up faciliteit
Back-ups zijn heel belangrijk en vaak het laatste redmiddel bij een cyber incident. Maak regelmatig en voldoende back-ups om ver genoeg in de tijd je bestanden terug te kunnen halen. Bewaar bijvoorbeeld 30 dagen een dagelijkse backup en bewaar vervolgens 12 maanden een maandelijkse backup. Zo kun je tot een jaar terug je bestanden terughalen. Zorg er ook voor dat de e-mails en de gegevens in de cloud, zoals in Dropbox, Gdrive en Onedrive, in de backups meegaan. Bewaar ook een kopie van de back-ups buiten je kantoor of werkplek en bewaar ook een kopie op een medium los van je netwerk en het internet.

07 Test het terugzetten van de back-ups
Wat belangrijk is maar vaak vergeten wordt is het testen van je back-up. Test minimaal een paar keer per jaar of de back-ups goed werken en ze alle bestanden bevatten.

08 Inventariseer welke apparaten er allemaal in je netwerk hangen
Maak een inventarisatie van alle apparaten die in je netwerk hangen. Vergeet niet je slimme thermostaat, bluetooth speakers, tablets en netwerkprinters.

09 Pas versleuteling op deze apparaten toe
Apparaatversleuteling is een extra bescherming voor alle gegevens die op een apparaat staan opgeslagen. Het zorgt ervoor dat de gegevens beschermd blijven en dat de harde schijf niet zomaar uitgelezen kan worden. Handig als een apparaat verloren gaat of gestolen is.

10 Verstuur gevoelige informatie op een veilige manier
Verzend je (gevoelige) persoonsgegevens via e-mail? Dat is volgens de AVG niet veilig. Gebruik hier een speciale applicatie voor of zet een wachtwoord op de bijlage of documenten en verstuur dit wachtwoord via een ander kanaal.