Cyber Fit

thuis en op het werk

Cyber awareness is niet alleen belangrijk op het werk, ook thuis is het van belang om zorgvuldig op de cyber veiligheid te letten. Juist nu thuiswerken zo gewoon is geworden zoeken criminelen naar de zwakste schakel van de medewerker om zo toegang te krijgen tot (bedrijfs-)systemen, e-mail accounts, login-gegevens en informatie.

Voorkom dat jij in je werk of privé slachtoffer wordt van een cyber-aanval. Neem de onderstaande informatie tot je en maak het kwaadwillenden zo moeilijk mogelijk om bij jouw persoonlijke gegevens en bedrijfsgegevens te komen.

Cyber fit, thuis en op het werk.

Email en telefoon

- Wantrouw e-mailberichten waarin je wordt gevraagd een **wachtwoord te wijzigen**. Helemaal wanneer je dit niet zelf hebt aangevraagd;
- Pas op voor berichten van **onbekende afzenders.** Als je het niet vertrouwt klik dan niet op links en open vooral geen bijlagen. Heb je toch iets geopend of op een link geklikt en vertrouw je het alsnog niet? Waarschuw dan jouw helpdesk, IT manager of IT security manager;
- Wees extra alert op verzoeken waarin je wordt gevraagd snel te beslissen of om **persoonlijke of gevoelige informatie** te delen of geld over te maken. Wees bewust van de waarde van informatie en overleg desnoods met een collega of leidinggevende. Durf 'nee' te zeggen tijdens een telefoongesprek.

Bescherm de computer

- Gebruik alleen **software uit een betrouwbare bron**. Apps uit de Apple App store en Google Play Store zijn meestal veilig;
- Controleer regelmatig of er updates en patches van software beschikbaar zijn en installeer deze meteen, ook op mobiele apparaten. Zet **automatische updates** aan;
- **Vergrendel de computer** wanneer je de werkplek verlaat;
- Stel jouw **virusscanner** ook zo in dat updates automatisch worden geïnstalleerd;
- Sluit **nooit privé apparatuur** (mobieltje, tablet, etc) aan op bedrijfssystemen, ook niet om op te laden. De oplaadkabel is vaak een datakabel en zo kan het ene apparaat het ander infecteren. Gebruik bij voorkeur een eigen oplader en kabel.

Wachtwoorden

- Gebruik **sterke wachtwoorden** en bij voorkeur een wachtwoordzin van tenminste 12 tekens en bij voorkeur langer. Korte wachtwoorden zijn al snel te kraken;
- Gebruik voor ieder systeem en elke website een **verschillend wachtwoord**;
- Gebruik **niet** een wachtwoord of wachtzin die eenvoudig **naar jou te herleiden** is;
- Een **wachtwoordmanager** kan je helpen om wachtwoorden te onthouden;
- Een gebruikersnaam en wachtwoord zijn strikt persoonlijk. Houd je wachtwoord altijd voor jezelf en **deel deze nooit met anderen**. Een helpdesk of IT manager zal jou nooit om jouw wachtwoord vragen;
- **Wijzig wachtwoorden** regelmatig, ten minste 1 keer per half jaar.

Datadragers

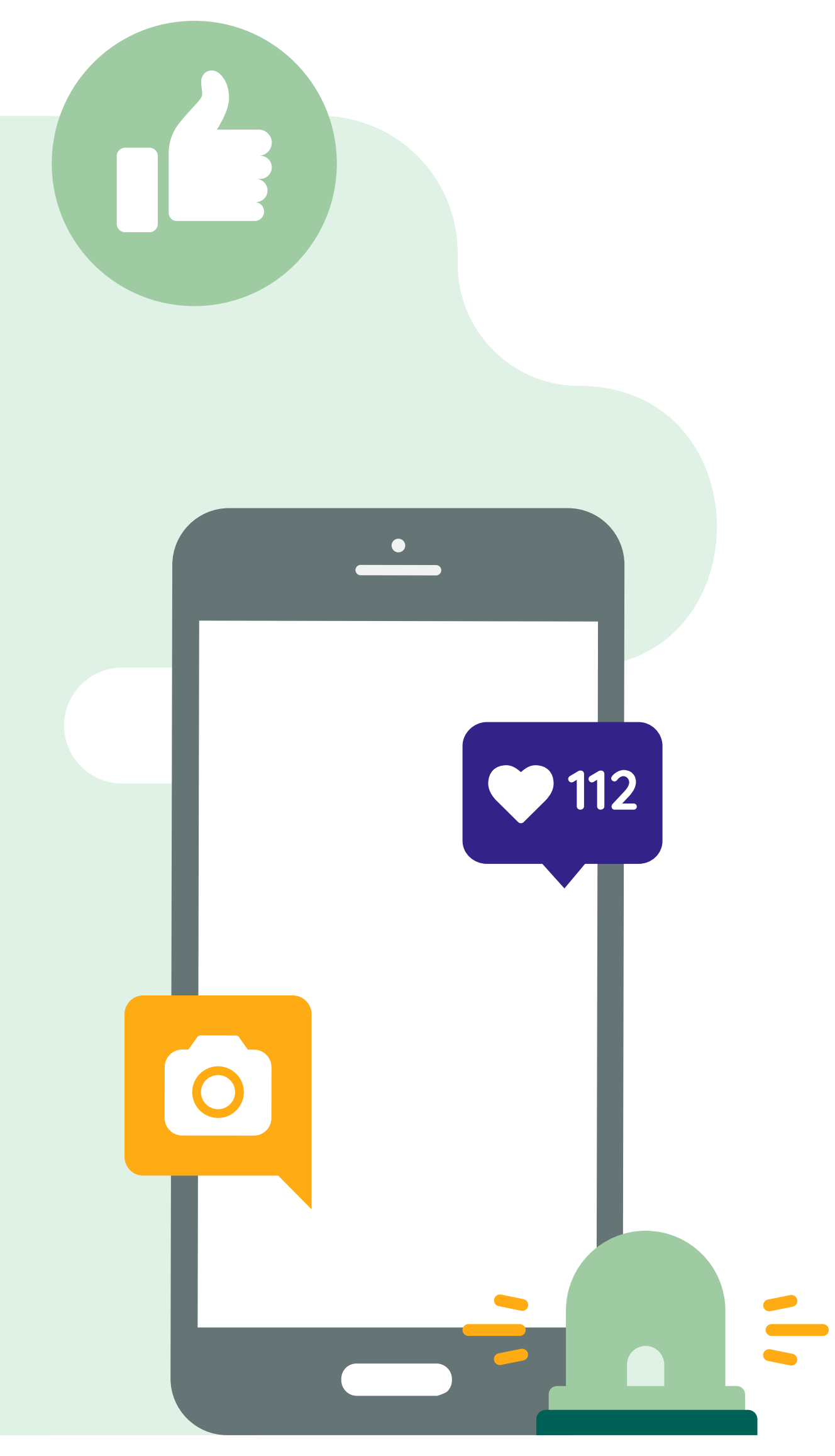
- **Voorkom diefstal of verlies**. Laat laptops, tablets, smartphones of datadragers (bijv. USB sticks) nooit onbeheerd achter;
- USB stick of datadrager toch uit het oog verloren? Dan is deze onbetrouwbaar en bij het terugvinden moet deze worden **gecontroleerd of vernietigd**;
- **Open gevonden datadragers** (waaronder CD-Roms en DVD's) **niet** om te kijken wat erop staat. Bedwing de nieuwsgierigheid;
- Gebruik datadragers alleen **om data van A naar B over te zetten** en wis deze na gebruik.

WiFi en Internet

- Maak bij voorkeur **geen gebruik van openbare WiFi netwerken** (zoals McDonalds, Wifi in de trein etc.), maar gebruik 3G/4G of 5G op jouw mobiele apparaat;
- Schakel WiFi liever helemaal uit als je buiten de deur bent. Wil je toch van openbare WiFi gebruik maken, gebruik dan een **betaalde en aanbevolen VPN oplossing**. Kijk op www.vpndiensten.nl voor een overzicht.

Social Media

- **Deel geen vertrouwelijke informatie**, zelfs niet met vrienden;
- **Plaats geen vertrouwelijke informatie op social media**. Ook als je de zichtbaarheid van jouw profiel hebt beperkt tot alleen vrienden kunnen delen van jouw profiel nog steeds zichtbaar zijn voor anderen. Reacties van vrienden op jouw bericht kunnen jouw bericht alsnog openbaar maken;
- Wat je op Internet plaatst **blijft voor altijd online**, zelfs wanneer je informatie zoals tekst en foto's verwijdert, kan het al door anderen zijn gekopieerd en verspreid;
- **Plaats geen ongepaste, onjuiste of illegale zaken** op het Internet. Plaats ook zeker geen foto's van de werkomgeving, materieel en van collega's;
- Aanvallers gebruiken vaak nep-accounts om vriendschappen aan te gaan en zo informatie te verzamelen. **Denk goed na alvorens online vriendschapsverzoeken te accepteren** van mensen die je niet kent of waarvan je niet weet hoe ze bij jou zijn gekomen. Durf ook hier vragen te stellen en "nee" te zeggen.



COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Z-CERT Stationsplein 121, 3818 LE Amersfoort **www.z-cert.nl**