Corona is een goudmijn voor de hackers, omdat iedereen geïnteresseerd is in het onderwerp. Alle cybersecurity bedrijven signaleren massale aanvallen op thuiswerkers.

We hebben enkele tips voor je op een rij gezet:

- Hackers proberen wachtwoorden te ontfutselen. Gebruik nooit dezelfde wachtwoorden en maak ze zo lang mogelijk, mocht je hem vergeten kan je via de wachtwoord manager je wachtwoord zo weer herstellen.
- Installeer thuis altijd de updates van programma's die om een update vragen. Hackers maken gebruik van de kwetsbaarheden van programma's die geen update hebben ontvangen. Dit geldt vooral voor je eigen apparatuur. ICT zorgt ervoor dat bedrijfsprogramma's zo goed mogelijk up-to-date zijn
- Fraudeurs benaderen thuiswerkers en doen zich voor als de IT-helpdesk. Ze willen een probleem oplossen. Als je ze je inloggegevens doorgeeft, kunnen ze heel veel schade aanrichten.
- Cybercriminelen sturen je een 'corona update' mail namens je organisatie of namens de RIVM. Er zijn al tientallen voorbeelden van phishingmails met corona. Bijna alle wordt al geblokkeerd maar er komt zo nu en dan toch wat doorheen.
- De bank lijkt een mailtje te sturen dat bankpassen ingeleverd moeten worden in verband met corona quarantaine.
- Valse mails van pakketbezorgers (nu veel winkels dichtgegaan zijn en alleen online bezorgen).
- Valse whatsapp-berichten en sms-berichten. De afzender lijkt en bekende (maar het is vrij simpel om een foto van een bekende te gebruiken). Als er om geld gevraagd wordt bel eerst even naar het nummer om zeker te weten dat het diegene is die je verwacht.
- Zorg dat je thuis een goed wachtwoord op je router hebt, heb je geen wachtwoord of een simpel wachtwoord kunnen kwaadwillenden zien wat je doet en je inloggegevens van o.a. Fokus en je bank onderscheppen. Je internet leverancier kan je hier eventueel mee helpen, de helpdesk van Fokus kan dat niet
- Voer ook altijd de updates van slimme apparaten uit, zoals slimme tv's en beveiligingscamera's.
- Pas op met het installeren van apps over corona. Er zijn kwaadwillende apps die je mobiel vergrendelen.
- Pas op voor websites met informatie over corona. Soms klopt de informatie wel, maar de website probeert alle computers van bezoekers met kwaadaardige software (malware) te besmetten.
- Stuur nooit zakelijke informatie door naar privé mails en gmails enz.
- Verander zo nu en den het wachtwoord van je prive email en kies voor minstens 14 karakters (bijvoorbeeld een zin).
- Pas op voor phishingmails met OneDrive koppelingen. Weet je zeker dat het van je bedrijf komt? Klik op de afzender en zweef even met je muis boven de link in de e-mail om de betrouwbaarheid te checken.
- Let vooral op e-mails waarin je gevraagd wordt om in te loggen op tools die de organisatie gebruikt. Vaak krijg je een nep inlogscherm die heel professioneel nagemaakt is.
- Let op emails die afkomstig lijken van een collega met het verzoek om met spoed geld over te maken of gegevens door te sturen. Het is vrij simpel om mail te versturen namens een bekend mail adres Bedrijven raken op deze manier enorme bedragen kwijt.
- Vergrendel je mobiel met minstens 6 cijfers of vingerafdruk/gezichtsherkenning en gebruik geen simpele wachtwoorden.
- Er zijn phishingmails die medicijnen voor corona beloven. De cybercriminelen hopen dat je op de link klikt of de bijlage opent, doe dit niet
- Pas op voor oproepen om te helpen bij het vinden van een geneesmiddel voor Covid-19, dit zijn bijna altijd hackers

- Er is ook veel spam over corona. Blokkeren, verwijderen en eventueel melden, maar nooit doorsturen. Als meerdere collega's dit krijgen dan zal de IT deze zo snel mogelijk uit alle mailboxen verwijderen
- Meld het altijd aan de ICT-afdeling als je iets niet vertrouwt. Ook als je per ongeluk ergens op geklikt hebt: altijd zo snel mogelijk melden. Zo kun je het bedrijf redden. Veel computervirussen worden helaas te laat ontdekt.

Je kunt de ICT helpdesk bellen op 050 5217125 of mailen naar helpdesk@fokuswonen.nl