Verwacht jij dat?

Waar je niet gauw cybercrime zou verwachten zijn openbare wifi, inscannen van QR codes, Openbare opladers, informatie op sociale media en downloads van bestanden/programma's bij op het oog lijkende bekende en vertrouwde sites.

Openbare Wifi
Wees voorzichtig met openbare wifi – Vermijd het gebruik van onbeveiligde netwerken of gebruik een VPN om je verbinding te versleutelen. Je bent aan het werk in een koffietentje of hebt ingecheckt in je hotel en ziet daar een bordje met netwerknaam en wachtwoord staan voor het wifi netwerk. Mooi! Dat bespaart weer mobiele data. Maar wees je bewust van de gevaren, want is zo'n openbaar wifi-netwerk wel veilig? Het antwoord op deze vraag is meestal 'nee'. Zodra je inlogt op een openbaar wifi-netwerk is je laptop of smartphone mogelijk toegankelijk voor cybercrimelen. Zij kunnen daardoor toegang krijgen tot je persoonlijke gegevens. Dit kan mogelijke identiteitsfraude als gevolg hebben. Betekent dit dat je er nooit gebruik van kan maken? Nee, dat kan wel, maar doe dat altijd via een VPN verbinding (een virtueel privénetwerk).

QR codes
Wees waakzaam voor QR codes. Het gevaar bij QR-codes is dat ze vaak officieel en vertrouwd lijken, maar net als bij phishing kan het linkje in een QR-code ook nep zijn. Gebruik hier je gezonde verstand. Krijg je een menukaart van een restaurant met een QR code, dan is deze waarschijnlijk wel veilig. Maar scan niet zo maar in het wilde weg alle QR-codes die je tegenkomt. Het is niet altijd duidelijk of de QR code die je scant officieel is. De FBI waarschuwt bijvoorbeeld voor criminelen die QR codes op parkeerautomaten vervalsen en zo jouw betaling innen. Gebruik dus altijd je gezonde verstand. Enkele tips om QR-code-fraude te voorkomen: Als het om een app gaat download deze dan via de app/play store. Controleer altijd het webadres net als bij (phishing)berichtjes met linkjes. Check het webadres het liefst bij het scannen, voordat je doorklikt. Laat je niet misleiden door officieel uitziende documenten. Bijvoorbeeld een brief van je bank, met daarin een QR-code. Een verkorte link (zoals bit.ly) in een QR-code is extra verdacht. Er is immers ruimte genoeg voor een volledig webadres.

Openbare Opladers
Openbare opladers? Liever niet Lege telefoon op het vliegveld of in de bus? Pas op met het gebruiken van openbare usb-poorten en oplaadkluisjes. Deze kunnen gebruikt worden om jouw gegevens uit te lezen en malware te installeren. In het Engels heet het 'juice jacking'. En ook al is het (nog) geen grootschalig probleem, het is zeker mogelijk. Gebruik dus liever een stopcontact of zet je telefoon uit tijdens het laden.

Informatie die voor iedereen op sociale media staat.
Beheer je instellingen voor sociale media. Zorg dat je persoonlijke en privégegevens achter slot en grendel zitten. Zet je reisplannen bijvoorbeeld niet op sociale media.
Cybercriminelen die sociale engineering gebruiken, kunnen je persoonlijke informatie vaak aan de hand van een paar gegevens achterhalen. Hoe minder je dus openbaar deelt, hoe beter. Als je bijvoorbeeld de naam van je huisdier of de meisjesnaam van je moeder noemt, kun je de antwoorden op twee algemene beveiligingsvragen onthullen.

Downloads van bestanden en programma's bij op het oog lijkende bekende en vertrouwde sites.
In bestanden en apps die we downloaden kunnen ook virussen en malware bevatten.
Gebruik daarom bij downloaden zoveel mogelijk of alleen officiële bronnen zoals officiële website van het programma of via vertrouwde platforms zoals Microsoft Store, Apple App Store of Google Play Store.
Let op neplinks en url's die misleidend of net echt lijken.
Lees reviews: Als een app veel negatieve recensies krijgt of amper gedownload is, wees voorzichtig.
Laat je antivirus de nieuwe bestanden automatisch scannen alvorens te installatie.
Als je twijfelt, kun je de programma's eerst in een virtuele omgeving testen voordat je ze op je hoofdapparaat installeert.

Alex Hol