Cybersecurity do's en don'ts

Cybercriminelen mikken niet alleen op IT-systemen, maar vooral op mensen. Zonder het te beseffen, kan één verkeerde klik je hele organisatie in gevaar brengen. Met deze tips wapen je jezelf én je organisatie tegen gewiekste technieken als phishing en social engineering, en bouw je zo een echte menselijke firewall.

Do's

Hou je toestellen up-to-date.
Dankzij regelmatige updates blijft je toestel beter beschermd tegen nieuwe aanvalstechnieken. Vergeet ook niet je telefoon of andere privétoestellen te updaten, zeker als je die ook gebruikt voor het werk.

Ga slim om met wachtwoorden.
Gebruik sterke, unieke wachtwoorden voor elke account, ook privé. Een sterk wachtwoord heeft minstens 12 tekens, met hoofletters, cijfers en symbolen. Met een paswoordmanager kan je al je wachtwoorden makkelijk beheren.

Schakel tweestapsverificatie (multifactor-authenticatie of MFA) in.
Tweestapsverificatie voegt een extra beveiligingslaag toe, zelfs als je wachtwoord in verkeerde handen valt. Dankzij MFA hebben hackers niet genoeg met je wachtwoord, maar moeten ze ook toegang hebben tot je telefoon, je e-mail of een fysieke sleutel, wat de kans op succesvolle inbraak aanzienlijk verkleint.

Denk na vooraleer je op een link klikt.
Een link in een e-mail, je browser of WhatsApp? Klink nooit impulsief verder! Controleer het e-mailadres van de afzender, hover even over een link om te controleren welke url erachter zit, stel jezelf de vraag of de boodschap niet te mooi is om waar te zijn, let op wanneer iets als heel dringend wordt gevraagd.

Dubbelcheck bij twijfel.
Twijfel je of een e-mail van een persoon die je kent (een collega, manager) echt is? Zijn/haar e-mailaccount kan inderdaad gehackt zijn en misbruikt worden. Neem de telefoon en bel je contactpersoon even op om te dubbelchecken.

Wees voorzichtig op social media.
Social engineers gebruiken openbare informatie (zoals je functie, collega's, vakantieplannen) om gerichte phishing-aanvallen te doen. Deel geen gevoelige bedrijfsinformatie en check je privacy-instellingen. Zelfs onschuldig lijkende details kunnen misbruikt worden. Wees ook kritisch over wat je ziet.

Een incident? Meld het meteen aan je IT-beheerder.
Merk je verdachte activiteit, twijfel je of een e-mail vals is of heb je op een verdachte link geklikt? Laat het meteen weten aan je IT-afdeling. Zij kunnen verder controleren of een e-mail al dan niet echt is, en bij een incident meteen ingrijpen om te voorkomen dat een aanval het hele bedrijf lamlegt.

Je eigen security awareness verbeteren?
Probeer eens de zelftests op Safeonweb.be.

Don'ts

Gebruik niet meerdere keren hetzelfde wachtwoord voor zowel privé- als zakelijke accounts.
Als je hetzelfde wachtwoord hergebruikt en één account wordt gehackt (bijvoorbeeld je privé-e-mail), dan kunnen aanvallers dit wachtwoord proberen op andere accounts, zoals je bedrijfsmail of interne systemen. Eén datalek kan zo leiden tot meervoudige inbraken, met mogelijk grote schade voor je organisatie. Unieke wachtwoorden per account beperken dit risico.

Deel niet zomaar wachtwoorden of inloggegevens met anderen.
Gebruik geen eenvoudig standaardwachtwoord (zoals Paswoord1) voor accounts die je met anderen deelt. Gebruik in de plaats daarvan een complex wachtwoord dat je op een veilige manier deelt via je paswoordmanager of via onetimesecret.com.

Gebruik geen onbeveiligd open wifinetwerk.
Openbare wifi-netwerken zijn vaak onbeveiligd, wat betekent dat data die je verstuurt (zoals inloggegevens, e-mails of bedrijfsdocumenten) door anderen kan worden onderschept. Gebruik altijd een VPN als je op een openbaar netwerk moet werken, of schakel over op je mobiele data. Zo blijft je communicatie versleuteld en veilig.

Laat je toestel niet onbeheerd achter in openbare ruimtes.
Een onbeheerd toestel is een gemakkelijk doelwit voor 'shoulder surfing' (meekijken). Binnen enkele seconden kan iemand je e-mails of documenten bekijken of zelfs je sessie overnemen als je niet bent uitgelogd. Zelfs als je gewoon even van je bureau wegstapt op kantoor, vergrendel je maar beter altijd je scherm.

Installeer niet zomaar onbekende software of apps op je pc of telefoon.
Onbekende software of apps kunnen malware bevatten die je gegevens steelt, je systeem gijzelt of het hele bedrijfsnetwerk infecteert. Zelfs ogenschijnlijk onschuldige programma's kunnen spyware of ransomware verbergen, met grote gevolgen voor je organisatie. Vraag altijd eerst advies aan IT voordat je iets installeert.

Negeer securitywaarschuwingen van bijvoorbeeld je browser of firewall niet.
Meld verdachte activiteiten, zoals rare pop-ups, of een vertraagd systeem, meteen aan IT.

Klik niet impulsief op links en wees op je hoede met bijlages.
Creëer een zesde zintuig voor phishing met enkele goede gewoontes: hover altijd over links en knoppen, let de kleine op details in url's of bestandsnamen, en vraag bij twijfel advies aan IT.

Handel niet zomaar, vooral als iets heel dringend lijkt.
Voel je druk om iets snel te doen (een betaling, iets downloaden of installeren)? Dubbelcheck dan eerst en vraag in geval van twijfel advies aan je IT-afdeling.

Gebruik geen USB-sticks die je gevonden of gekregen hebt.
Een onbekende USB-stick kan malware bevatten die zichzelf automatisch installeert wanneer je de stick aansluit op je pc, zonder dat je er iets van merkt. Vertrouw gevonden of gegeven sticks dus niet, geef ze af aan IT en gebruik alleen vertrouwde, door het bedrijf goedgekeurde opslagmedia.

Het cyberbewustzijn in je organisatie verder versterken?
Bekijk onze oplossingen via www.savaco.com/nl/user-awareness