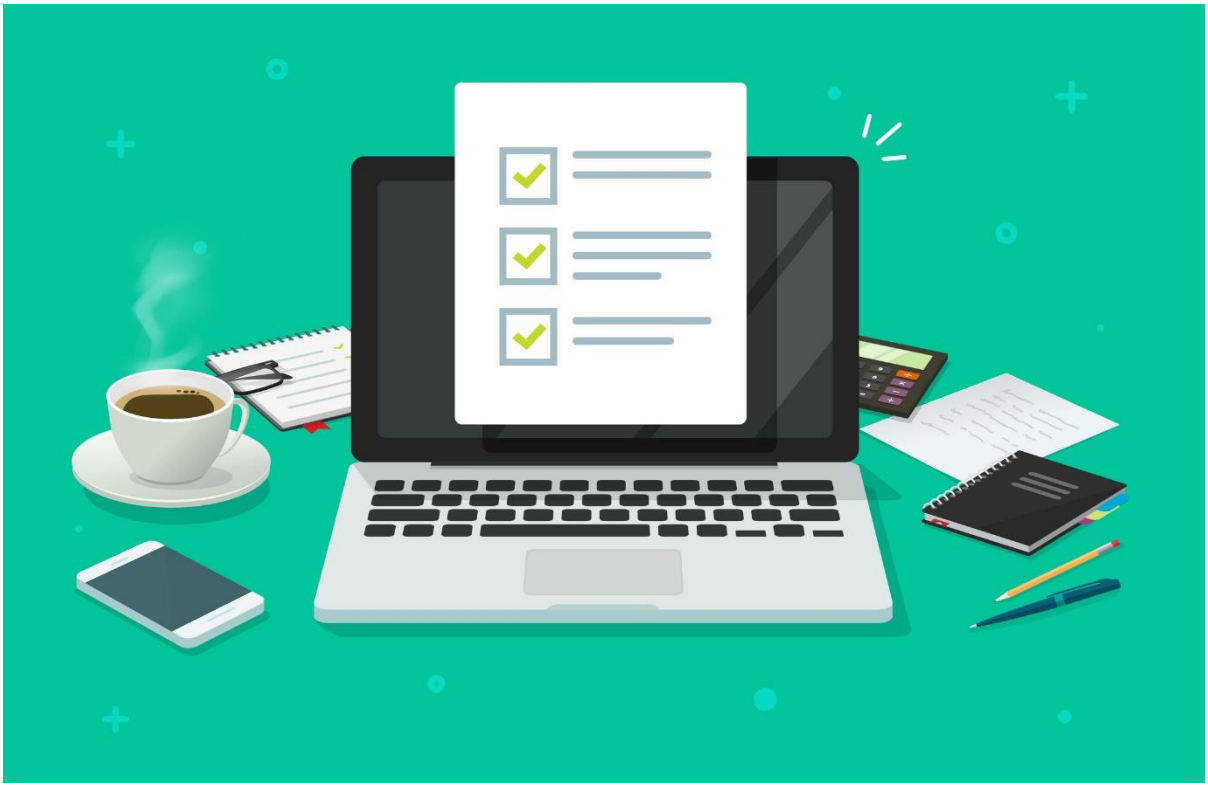
Leidraad en tips voor thuiswerkers om digitaal veilig te werken



De cybercriminelen maken misbruik van de zorgen van het grote publiek over het coronavirus. Zij maken gebruik van de situatie door het sturen van e-mails om deze te verleiden tot het klikken op dubieuze links. Wie klikt op zo'n link, komt op een malafide site die malware probeert te installeren of wachtwoorden probeert te ontfutselen. We geven hiervoor enkele tips om deze te herkennen.
Ook is het belangrijk om uw apparaten up-to-date te houden en antivirus te hebben geïnstalleerd. We zetten de belangrijkste maatregelen voor u op een rijtje. Ook geven we tips hoe u phishing mails kunt herkennen:

Laat computers niet onbeheerd achter

De kans is aanwezig dat u nu veel thuis werkt waardoor computers of

andere apparaten onbeheerd achter worden gelaten. Kinderen of anderen kunnen hier gebruik van maken door bijvoorbeeld filmpjes te kijken of muziek af te spelen. Het is daarom extra belangrijk om uw apparaat te vergrendelen wanneer u deze zelf niet gebruikt. Daarnaast is het belangrijk dat u alle gegevens op de verschillende apparaten standaard versleuteld. In het geval van verlies of diefstal kunnen kwaadwillenden dan nooit met bedrijfsgegevens aan de haal gaan. De meeste apparaten beschikken tegenwoordig over ingebouwde encryptie, maar het is mogelijk dat gebruikers deze apart moeten inschakelen of configureren. Hiervoor kunt u ook contact opnemen met uw systeembeheerder.

Houd uw apparaten up-to-date door tijdig te patchen

Bij veel organisaties gebruiken medewerkers hun eigen apparaten (smartphone, tablet, desktop pc of laptop) bij hun werkzaamheden (Bring Your Own Device, BYOD). Het is belangrijk dat op deze apparaten de laatste versie van het besturingssysteem is geïnstalleerd en zijn voorzien van de meest up-to-date antivirussoftware. Dat is belangrijk omdat ontdekte kwetsbaarheden of een betere beveiliging altijd via (security) patches worden aangeboden. Installeer dus in elk geval altijd direct de meest recente patches zodat uw apparaten zo goed als mogelijk zijn beveiligd. Door dit tijdig te doen bent u grotendeels beschermd tegen de meest actuele cyberrisico’s. Vaak maken cybercriminelen namelijk gebruik van kwetsbaarheden in oudere versies van software en besturingssystemen.

Is uw apparaat up-to-date? Check:

Microsoft Windows 10 computer updaten

Digital Trust Centre

Apple iOS telefoon/iPad updaten

Google Android telefoon/tablet updaten

Gebruik veilige wifi

Nu de meeste openbare gelegenheden zijn gesloten vanwege het coronavirus zal het niet veel voorkomen dat u gebruikmaakt van openbare wifi. Er wordt sowiesoafgeraden om openbare wifi te gebruiken, ondanks dat het erg handig kan zijn. Het is voor hackers relatief eenvoudig om een kwaadaardige wifi-hotspot te maken. Deze hotspots hebben meestal dezelfde naam als de reguliere variant. Na het verbinden met het kwaadaardige wifi-punt lijkt er niets aan de hand en werkt het internet zoals u gewend bent. Deze hotspot is echter volledig onder controle van de aanvaller en het internetverkeer wordt bekeken op bruikbare informatie als gebruikersnamen, wachtwoorden, bankgegevens, interessante mailtjes en klantinformatie. Met deze informatie kan de aanvaller zich vervolgens toegang verschaffen tot

allerlei vertrouwelijke informatie en (bedrijfs)systemen. Ook kunnen aanvallers kwaadaardige wifi-hotspots en slechte of onbeveiligde wifi-netwerken gebruiken
om kwaadaardige software (malware) te verspreiden op apparaten die op het netwerk zijn aangesloten. Zodra uw laptop of mobiele apparaat het delen van bestanden toestaat is het voor een aanvaller zeer eenvoudig om malware via het netwerk op verbonden apparaten te zetten. Let daar dus op wanneer de huidige maatregelen weer worden ingetrokken.
Maar ook uw thuiswifi kan kwetsbaar zijn. Wilt u weten of uw wifi de juiste (veilige) instellingen heeft? Check de site van het Digital Trust Center. De stappen die hierin worden genoemd zijn ook van toepassing op uw thuiswifi.

Gebruik sterke wachtwoorden of een wachtwoordmanager

Wachtwoorden worden gebruikt om toegang te krijgen tot uw gegevens en systemen. Met een wachtwoord beveiligt u bijvoorbeeld bedrijfsgegevens op uw apparaten, maar bijvoorbeeld ook uw e-mailaccount of (bedrijfs)data in de cloud. Een sterk wachtwoord is daarom essentieel. Maar wat is een sterk wachtwoord? Een sterk wachtwoord is niet te raden en moeilijk te kraken door een computer. Een goed wachtwoord bestaat naast gewone letters en cijfers ook uit hoofdletters, leestekens en bijzondere karakters. U kunt ook gebruik maken van een lange wachtwoordzin (passphrase). Hoe langer de zin, hoe veiliger. Een wachtwoordmanager is nog beter. Immers voor heel veel verschillende systemen en programma’s heeft u dan niet elke keer een uniek wachtwoord nodig. Met een wachtwoordmanager worden al uw wachtwoorden beheerd. Er zijn ook wachtwoordmanagers die zelf (moeilijke) wachtwoorden kunnen maken, zodat u hier zelf niet over hoeft na te denken. Hierdoor loopt u geen risico dat als ergens uw

wachtwoord bekend wordt al uw andere accounts en zakelijke gegevens ook toegankelijk zijn.

Digital Trust Centre

Installeer antivirus

Om uw apparaten veilig te houden is antivirussoftware essentieel. Een virus is schadelijke software die door cybercriminelen gebruikt wordt om binnen te komen. Antivirus kan virussen identificeren, tegenhouden en bestaande virussen verwijderen. Daarom is het verstandig om op al uw apparaten de laatste versies van antivirus te hebben.

Herken phishingmails

Momenteel wordt door cybercriminelen veel gebruikgemaakt van de onzekerheden rondom corona om phishingmails te sturen. Phishingmails zijn links of bijlagen binnen e-mails, tekstberichten of betaalverzoeken waarvan lijkt of het van een bekend en vertrouwd (contact)persoon afkomstig is, maar waar cybercriminelen achter zitten. Phishing wordt gebruikt om wachtwoorden of toegangscodes te achterhalen zodat cybercriminelen via uw apparaten bijvoorbeeld bij het netwerk van uw organisatie komen. Het is dus belangrijk om ze tijdig te herkennen. We hebben een aantal veelvoorkomende indicatoren voor het herkennen van een phishingmail op een rij gezet:

1. Check altijd de URL wanneer u een tekstbericht of e-mail krijgt met daarin een verwijzing naar een website. Cybercriminelen kunnen bijvoorbeeld een website maken waarin de URL lijkt op die van het RIVM (bijvoorbeeld www.r1vm.nl).
2. Check de aanhef. Hoe onpersoonlijker de mail is, hoe groter de kans dat de mail mogelijk een phishingmail is.
3. Wordt er gevraagd om persoonsgegevens aan te leveren? Banken, de overheid of verzekeringsmaatschappijen zullen dit nooit via e-mail doen.

4. Ontvangt u een mail met daarin een .exe-bijlage? Check dan goed of u de afzender kent. Wanneer dit niet het geval is dan kunt u het beste de mail niet openen en bij uw systeembeheerder hiervan melding maken. Hij/zij kan dan onderzoeken of het daadwerkelijk een phishingmail is.

> *Kortom: klik niet op links in e-mailberichten, open geen onbekende bijlagen en vul geen gegevens in bij e-mailberichten die u niet verwacht of van een onbekende afzender zijn.*

Wat moet u doen als u al hebt geklikt?

Het belangrijkste is dat u niet in paniek raakt. Ook nu zijn er een aantal stappen die u kunt nemen:

- Open de antivirussoftware en voer een volledige systeemscan uit. Volg de eventuele instructies van de antivirussoftware op. Zie hiervoor ook de Windows helpdesk voor Windows en Apple support voor Mac-computers.
- Heeft u per ongeluk een wachtwoord gegeven of ingetypt? Zorg dan dat u onmiddellijk uw wachtwoord wijzigt.

Gebruikt u een apparaat van uw werkgever, neem dan onmiddellijk contact op met de systeembeheerder.

Meer informatie

Wilt u meer informatie over veilig digitaal werken? We hebben een aantal handige websites voor u op een rijtje gezet:

Digital Trust Center van het Ministerie van Economische Zaken en Klimaat:

Digital Trust Center

Vijf basisprincipes

Informatie en Advies

Nationaal Cybersecurity Centrum van het Ministerie van Justitie en Veiligheid:

Nationaal Cybersecurity Centrum

Actueel nieuws

Veilig Internetten:

Veilig Internetten

Algemene informatie over corona:

Rijksoverheid

Rijksinstituut voor Volksgezondheid en Milieu (RIVM)