5 TIPS OM VEILIG THUIS TE WERKEN

Mickey Habte

4Consult/Startportaal

Vanwege het corona virus werkt een groot gedeelte van Nederland vanuit huis en wordt er veel informatie gedeeld en is het zaak om veilig te werken vanuit huis. Niet voor iedereen is het vanzelfsprekend dat zij thuiswerken en kan het een uitdaging zijn om hun eigen pc of laptop beveiligd te hebben.

Reden genoeg dus om een aantal handige tips te delen waar mee je veilig vanuit huis kunt werken.

1. Maak gebruik van een vaste kabel.

De internetverbinding tussen een laptop of pc is stabieler bij het gebruik van een ethernetkabel dan met wifi. Bij het gebruik van wifi kunnen er onderbrekingen ontstaan. Door bijvoorbeeld de wifi van de buren of andere elektrische apparaten, denk hierbij aan Bluetooth apparaten of draadloze beveiligingsapparatuur. Hierbij is wifi voor criminelen eenvoudiger te onderscheppen dan een vaste kabel. Is het niet mogelijk om een vaste kabel te gebruiken zorg er dan voor dat jouw wifinetwerk gesloten is en beveiligd met een wachtwoord.

2. Zorg dat je alle updates hebt uitgevoerd die nodig zijn.

Het uitvoeren van updates kan voor sommige een irritante melding zijn die ze krijgen, maar houd hier rekening mee dat een update niet alleen wordt doorgevoerd om software of besturingssystemen te verbeteren qua gebruiksgema. Vaak genoeg zijn het ook beveiligingsupdates. Deze beveiligingsupdates zorgen ervoor dat eventuele kwetsbaarheden in de software of besturingssystemen voorkomen kunnen worden en u als gebruiker veilig door kunt werken.

Het uitvoeren van updates is dus een cruciale zaak. Om te voorkomen dat je vergeet een update uit te voeren is het handig om de updates in te stellen als automatisch uitvoeren. Dit kan je instellen in de instellingen van de software of besturingssysteem die je gebruikt.

3. Maak gebruik van antivirus software.

In het afgelopen jaar hebben we kunnen zien aan de hand van de cijfers van het CBS dat tot bijna 30% van de grote concerns te maken heeft gehad met cyberaanvallen en tot 20% voor het MKB. Heb je dus geen goed antivirussoftware geïnstalleerd en kom je in een cyberaanval terecht dan sta je er vaak genoeg kansloos voor.

De meeste werkgevers zullen hun werknemers hebben voorzien van een werklaptop met daarop een goede antivirussoftware waardoor zij veilig thuis kunnen doorwerken zoals voorheen op kantoor. Dit geldt echter niet voor iedereen.

Wat vaak in de praktijk gebeurd is dat werknemers genoodzaakt of niet hun eigen laptop of pc in gebruik nemen om te kunnen werken. Het kan zijn dat jouw werkgever antivirus software beschikbaar stelt voor jou om te kunnen installeren op je persoonlijke laptop of pc. Het is hierbij goed om bij je werkgever na te vragen of dit het geval is en of er bepaalde richtlijnen zijn die vooraf al bepaald zijn vanuit de organisatie.

4. Zorg voor een goede firewall.

Naast het hebben van een goede antivirussoftware is het ook noodzakelijk om een goede firewall te hebben op je pc of laptop. Een firewall zorgt ervoor dat er een soort beveiliging laag ontstaat om jouw pc of laptop heen, waardoor het voor indringers van buitenaf lastig wordt gemaakt om toegang te kunnen krijgen tot jouw pc of laptop. Dit geld ook voor besmette software die probeert te verbinden met een netwerk van buitenaf. Het is dus noodzakelijk om een goede firewall te hebben om veilig thuis te kunnen werken.

De meeste laptops en pc’s hebben al een firewall geïnstalleerd zo is dat het geval bij bijvoorbeeld Windows en Apple. Ondanks dat dit goede firewalls zijn kan het geen kwaad om een extra firewall te installeren om extra beveiligd te zijn.

Het kan zijn dat jouw werkgever firewallsoftware beschikbaar stelt voor jou om te kunnen installeren op je persoonlijke laptop of pc. Het is hierbij goed om bij je werkgever na te vragen of dit het geval is en of er bepaalde richtlijnen zijn die vooraf al bepaald zijn vanuit de organisatie.

5. Zorgvuldig delen van informatie.

Doordat er nu veelal thuis wordt gewerkt is niet meer mogelijk om even langs een collega te lopen om het een en ander te vragen. Het gevaar hierbij is dat er informatie gedeeld wordt op verschillende soorten manieren. Hierbij kan gedacht worden aan informatieverspreiding via mobiele chat zoals WhatsApp of via mailverkeer.

Om te voorkomen dat er onnodig gevoelige informatie wordt gedeeld online is het mogelijk om te video bellen met collega's en het daarin te bespreken. Een goede applicatie om daarvoor te gebruiken is bijvoorbeeld Microsoft Teams. Hierin kan je namelijk collega's in een video call laten meekijken met jouw scherm en de zaken meteen bespreekbaar maken. Dit scheelt een aantal mailtjes of appjes die je anders zou versturen.

Is het noodzakelijk dat er toch een document gedeeld moet worden dan is het mogelijk om bestanden beveiligd te versturen. Dit kan met bijvoorbeeld Microsoft Word. Maak je gebruik van een Windows computer of laptop dan doe je dit als volgt:

Nadat je het document hebt gemaakt wat je wilt versturen, ga je naar de balk boven in en druk je op **Bestand** vervolgens op **Informatie** dan zie je de optie **Document beveiligen** en kies je voor **versleutelen met wachtwoord.**

Voor de Macgebruikers is het iets anders daarvoor ga je naar de balk bovenin en kies je voor **Controleren** vervolgens verschijnt in de balk aan de rechterkant een optie met **Document beveiligen**. Als je daarop klikt verschijnt er een scherm met daarin de verschillende soorten opties om het document te beveiligen.

Na je document te hebben versleuteld met een wachtwoord, kan je dit wachtwoord delen met diegene naar wie je dit document wilt versturen. Let hierbij op dat je het wachtwoord niet deelt met het document, maar op een aparte manier bijvoorbeeld via een beveiligde chat.

Als laatst is het natuurlijk de zaak om de richtlijnen te volgen die zijn opgedragen vanuit jouw werkgever omtrent het delen van informatie en hoe daar mee omgegaan wordt.