9 tips voor een veilige IT-thuisomgeving

Keesomstraat 26 • 6716 AB Ede • +31 318 648 888 • info@cts-it.nl • www.cts-it.nl

“De belangrijke rol van IT-security”

In dit internettijdperk is security (oftewel veiligheid) belangrijker dan ooit. In het nieuws zie je regelmatig berichten over gehackte bedrijven, phishingmails, gestolen persoonsgegevens en meer digitale criminaliteit. Hackers richten zich tegenwoordig ook steeds meer op het innen van losgeld in ruil voor gestolen data, ook wel ransomware genoemd.

Iedere organisatie kan slachtoffer worden van hackers. Het is naïef om te denken dat zoiets alleen je buurman overkomt. Met de versnelde opmars van thuiswerken door COVID19 gebruiken we bovendien steeds meer slecht beveiligde wifi en apparaten in huis.
Het risico op een cyberaanval neemt daardoor explosief toe.

Hoe kun je veilig thuiswerken, beschermd tegen cybercriminaliteit?

Is je thuiswerkplek net zo goed beveiligd als je zakelijke werkplek? Gebruik je privé apparatuur om verbinding te maken met je zakelijke netwerk en systemen? Benader je e-mails, documenten of een werkplek op afstand met een onveilige computer? Of, misschien wel het meest risicovol: bewaar je bedrijfsgegevens op onveilige apparaten?

Niet alleen door je bedrijfsgegevens kun je slachtoffer worden van cybercriminelen. Ook je privédata is interessant voor hackers. Er is een grote toename van cybercriminaliteit gericht op particulieren. Phishing, identiteitsfraude en hacks maken steeds meer slachtoffers. Het is daarom belangrijk om jezelf ook de vraag te stellen: Zijn mijn persoonlijke accounts, apparaten en data veilig tegen cybercriminelen?

CTS It helpt je veilig werken vanuit huis

In deze whitepaper leggen we uit hoe je veilig kunt thuiswerken. Met negen simpele tips helpen wij je thuiswerkplek te beschermen tegen hackers. Maar om de risico's in te schatten, moet je eerst weten waar je nu staat. Dat bepaal je eenvoudig met onze checklist.

Doorloop onderstaande checklist en beantwoord elke vraag voor jezelf met 'ja' of 'nee'. Elke vraag die je met 'ja' beantwoordt, betekent een potentieel risico voor je IT-security:

Bekijk je privégegevens (e-mail, apps, documenten en meer) vanaf een apparaat van de zaak (laptop, smartphone of anders)?

Ja/Nee

Staat er bedrijfsdata (e-mail, documenten en meer) op één van je persoonlijke apparaten?

Ja/Nee

Gebruik je op meerdere plekken dezelfde wachtwoorden (waar geen meervoudige authenticatie actief is)?

Ja/Nee

Gebruik je jouw telefoon voor zowel privé als zakelijke doeleinden?

Ja/Nee

Gebruik je jouw smartphone zowel zakelijk als privé?

Ja/Nee

Deel je weleens bedrijfsdata via tools die niet door de organisatie zijn aangeboden (WhatsApp, persoonlijke OneDrive, Dropbox, WeTransfer, Google Docs, etc)?

Ja/Nee

Gebruik je thuis slimme apparaten die verbinding maken met internet (denk aan webcams, een slimme deurbel of thermostaat, of een alarminstallatie)?

Ja/Nee

Maken meerdere personen thuis gebruik van dezelfde IT-apparatuur?

Ja/Nee

De 9 tips van CTS IT voor een veilige IT-thuisomgeving

Keesomstraat 26 • 6716 AB Ede • +31 318 648 888 • info@cts-it.nl • www.cts-it.nl

1. Houd je computer up-to-date

Updates van je computer wegklikken? Dat is geen goed idee. Zowel zakelijk als privé is het ontzettend belangrijk dat je apparaten up-to-date zijn, oftewel voorzien van de meest recente (beveiligings)software. Controleer daarom regelmatig of Windows nog updates heeft, en zorg dat je met een ondersteunde versie van Windows werkt.
Hier kun je zien welke Windows 10-versies je hebt (microsoft.com.) Meer weten over de nieuwste updates? Windows 10 bijwerken doe je hier.

2. Zorg voor goede beveiliging met een virusscan en firewall

Een virusscanner en firewall houden ongewenste indringers tegen. Tegenwoordig biedt Microsoft zelf oplossingen voor account- en apparaatbeveiliging. Een goed voorbeeld daarvan is het programma Defender. Zorg altijd dat in ieder geval de standaard beveiliging van je computer is geactiveerd. Hoe je dat doet in Windows ontdek je hier. Daarnaast kun je aanvullende software aanschaffen om de beveiliging van je apparaat uit te breiden.
Zo zorg je voor de hoogst haalbare bescherming.

3. Scherm je netwerk af

Hoe veilig is jouw thuisnetwerk? Dat is meestal een lastige vraag om te beantwoorden als particuliere internetgebruiker. Vaak kies je een provider uit en trek je daar pas aan de bel als je geen verbinding meer hebt. De details van je netwerk weet je vaak niet, al zijn de meeste wifi-netwerken voldoende beveiligd voor thuisgebruik.

Het grote gevaar treedt op als je wijzigingen aanbrengt op de standaard instellingen. Maar ook als je wifi-apparaten aansluit op je netwerk loop je risico. Denk hierbij aan slimme apparaten zoals een slimme thermostaat, lampen of camera's. Het gemiddelde Nederlandse huishouden heeft vijf van dit soort apparaten.

Zorg ervoor dat deze apparaten allemaal de nieuwste software bevatten en gebruik sterke, unieke wachtwoorden. Bekijk ook eens de huidige instellingen van je wifi-netwerk: dat is een goede

4. Beveilig je accounts met MFA

Vroeger beveiligde je een account simpelweg met een wachtwoord, maar dat is tegenwoordig niet meer veilig. Wachtwoorden van grote netwerken kunnen namelijk worden gehackt, zoals bijvoorbeeld gebeurd is bij Linkedin. Duizenden namen en wachtwoorden van gebruikers lagen op straat. Als hackers eenmaal je wachtwoord achterhalen, kunnen ze ook andere gebruikersaccounts hacken. Zo komen ze bij je e-mails, foto's en documenten. De vraag is dan of je überhaupt nog iets van je verloren data terug kunt halen.

Met Multi-Factor Authenticatie (MFA) kun je gelukkig je accounts beschermen met een tweede vorm van authenticatie naast het wachtwoord. Dat betekent dat je meerdere stappen doorloopt om in te loggen, zoals het invoeren van een wachtwoord én goedkeuring via een smartphone app. Gebruik MFA tenminste voor je belangrijke en meest gebruikte accounts zoals je e-mail, social media en zakelijke systemen.

Ontdek alles over meervoudige verificatie (microsoft.com) of bekijk direct hoe je nooit meer een nieuw wachtwoord hoeft te bedenken met MFA (cts-it.nl)

Gebruik daarnaast voor elk account een uniek wachtwoord, hoe ingewikkeld het ook is. Sla je wachtwoorden op in een beveiligde wachtwoordenkluis. Dat kan offline zijn maar ook online via een speciaal programma of een app.

5. Beveilig je smartphone en apps

Smartphones spelen een belangrijke rol in ons dagelijks leven. Via je telefoon communiceer je, handel je bankzaken af, lees je e-mails, beheer je jouw agenda en nog veel meer. Een smartphone is daarmee onmisbaar en het verlies ervan heeft grote impact op je dagelijkse routine. Maar is je smartphone ook veilig?

De Consumentenbond heeft een handige stappenlijst waarmee je een goede start maakt in het beveiligen van je telefoon. Daarnaast kun je de belangrijkste apps beveiligen met meervoudige verificatie. Op een smartphone kan dit vaak met een pincode, vingerafdruk of zelfs met gezichtsherkenning.

6. Maak een privé back-up

Heb je een reservekopie van je data? Kun je op elk moment je foto's, e-mails en meer terughalen? Een back-up van gegevens wordt helaas vaak pas een prioriteit nadat een apparaat is gestolen of gehackt. En dan is het te laat!

"Veel thuisgebruikers hebben geen back-up van hun privé-data"

Daar kun je vrij gemakkelijk verandering in brengen. Je kunt bijvoorbeeld via je smartphone instellen dat er automatisch een back-up in de Cloud wordt gezet. Ook voor je computer kun je kiezen een Cloud back-up te maken met bijvoorbeeld OneDrive, iCloud
of Dropbox. Een andere optie is een lokale back-up met een netwerkschijf of lokale schijf.

Stel jezelf een aantal vragen om te bepalen welk type back-up voor jou passend is:

1. Welke data wil ik opslaan in de back-up?
2. Op welk apparaat/welke apparaten wil ik deze data bewaren?
3. Wil ik een realtime back-up (data wordt direct gekopieerd naar een separate opslag) of een back-up op frequentie (bijvoorbeeld dagelijks, wekelijks of maandelijks)?
4. Wil ik de back-up opslaan binnen mijn eigen huis of wil ik mijn gegevens ook ergens buitenshuis opslaan, zodat de data veilig is in het geval van brand of inbraak?

Op basis van de antwoorden op bovenstaande vragen kun je een type back-up kiezen dat past bij jouw behoeften.

Gebruik daarnaast voor elk account een uniek wachtwoord, hoe ingewikkeld het ook is. Sla je wachtwoorden op in een beveiligde wachtwoordenkluis. Dat kan offline zijn maar ook online via een speciaal programma of een app.

7. Sluit een verzekering tegen cybercriminaliteit af

Als particulier loop je steeds meer risico om slachtoffer te worden van cybercriminaliteit. Naast technische maatregelen kun je daarom ook een verzekering afsluiten om jezelf te beschermen. Je bent dan vaak verzekerd tegen identiteitsfraude, cyberafpersing, inbreuk op privacy, verlies van geld op je bankrekening door phishing, malware en hacks. Je kunt een cyberverzekering al afsluiten vanaf €16 per maand. Er zijn bovendien steeds meer aanbieders om uit te kiezen. CTS IT raadt de cybersecurity verzekering iedereen aan, ook als particulier. De financiële schade die een hacker kan aanbrengen is vele malen hoger dan die maandelijkse premie.

8. Houd werk en privé gescheiden

Het is een gevoelig onderwerp, de scheiding tussen werk en privé. Want wie van ons opent nooit zijn persoonlijke e-mail op de werklaptop, of andersom? Toch kan de impact van die vertroebelde grens tussen werk en privé grote impact hebben op je IT-veiligheid. Want wat gebeurt er als je vanuit je persoonlijke mailadres per ongeluk een phishing e-mail opent op je werklaptop? Dan kun je onbedoeld je bedrijf infecteren en een deur openzetten voor hackers.

Houd zakelijke gegevens en persoonlijke gegevens zoveel mogelijk te scheiden. Het grootste deel van hacks bij bedrijven wordt veroorzaakt door gebruikers die onbewust hun bedrijf infecteren en dat gebeurt vaak vanuit de privédata.

9. Ben altijd bewust van de actuele risico's

Misschien wel de belangrijkste tip die CTS IT kan geven? Ken de risico's. Bewust zijn van gevaren is de kern van goede beveiliging. Wat doe je als er iemand van Microsoft belt en toegang tot je computer vraagt? Hoe herken je een phishing mail en wat is Whatsapp fraude? Door bewust te zijn van actuele vormen van cybercriminaliteit en security kun je jezelf zo goed mogelijk beschermen. De wereld van cybercriminaliteit beweegt in hoog tempo, en het is noodzaak mee te bewegen om veilig te zijn.

Veilig digitaal leven en ondernemen

Het is altijd belangrijk om bewust om te gaan met IT en security, met name in dit tijdperk van thuiswerken. Dat betekent dat je gebruik van internet, telefoons en computers ook met andere gezinsleden bespreekt. Zorg dat je samen alert bent op verschillende vormen van cybercriminaliteit. Vertrouw je een situatie niet? Stop dan waar je mee bezig bent en controleer via websites als de Fraudehelpdesk of je met een potentieel risico te maken hebt. Beter een dubbele check dan een hack!

Veilig thuiswerken?

Dat is dankzij deze 9 tips voor jou nu een eitje. Maar hoe zit het eigenlijk met je zakelijke werkplek? Ook binnen de muren van het kantoor kan er veel misgaan op het gebied van IT-security. Benieuwd hoe veilig jouw organisatie is?

CTS IT staat klaar om met je te sparren over security en alles dat erbij komt kijken.

Keesomstraat 26 · 6716 AB Ede · +31 318 648 888 · info@cts-it.nl · www.cts-it.nl