



Spot
MAAKT ICT

De 3 belangrijkste ICT lessen voor jouw bedrijf

Gratis advies zonder dat je
die vervelende verkoper
aan de deur hebt!



A background image showing a person in a dark shirt working on a laptop in an office setting. In the foreground, another person's hands are visible typing on a laptop, wearing a watch and a ring. A white coffee cup is on the desk. Three overlapping circles (two light gray, one white) are positioned in the upper right area of the image.

Inhoud

1. Inleiding
2. Les 1: Veiligheid
3. Les 2: Bereikbaarheid
4. Les 3: Thuiswerken
5. Checklist

Inleiding

Afgelopen jaar zijn we als gevolg van de coronacrisis met z'n allen in het diepe gegooid als het gaat om massaal thuiswerken. Met alle bijbehorende ongemakken! Sommige bedrijven hadden het geluk dat hun ICT daar al op was ingesteld, anderen moesten in no-time een inhaalslag zien te maken om te zorgen dat medewerkers geheel tijd en plaats onafhankelijk konden werken.

Als full service ICT organisatie hebben wij dat allemaal van nabij meegemaakt en willen we graag onze ervaringen met jullie delen. Het is tijd om de balans op te maken. Wat zijn de belangrijkste lessen die jullie (en wij) hebben geleerd?

Wij hebben dit vertaald in een aantal tips die we je graag mee willen geven om het de komende tijd net wat makkelijker te maken. Want eigenlijk wil je niet nadenken over je ICT, die moet het gewoon doen.

Van onze kant gratis advies zonder dat je de vervelende verkoper over de vloer hebt! En als kers op de taart hebben we nog een checklist toegevoegd met praktische handvaten voor meer veiligheid en zekerheid.



Gerard Smith
Business Manager SPOT ICT

Les 1

Veiligheid

Je zit op je gemak te werken achter je laptop. Niet thuis maar bij de plaatselijke koffiezaak. Ideaal dat dit nu kan. Zo kun je toch het werk doen dat je moet doen en ondertussen een écht lekker kopje koffie drinken. Je kijkt op je horloge. Oei, je wist niet dat het al zo laat was. Je moet zo thuis zijn om een pakketje in ontvangst te nemen. Dat wordt haasten. Snel raap je al je paperassen bij elkaar, stopt ze in je rugtas en fietst naar huis. Bij thuiskomst haal je je rugzak leeg. Oh nee, je bent je laptop vergeten!



De afgelopen maanden zijn er weer genoeg berichten in de media geweest over bedrijven die gehackt zijn. Cybercriminaliteit is aan de orde van de dag. Je denkt altijd dat het je niet overkomt, maar het gebeurt. En je kunt de digitale veiligheid binnen je bedrijf nog zo op orde hebben, een ongeluk zit een klein hoekje, zo maakt nevenstaande anekdote duidelijk.

Tip 1

Log in via Azure Active Directory

Veel mensen loggen thuis in vanaf de computer die zij ook privé gebruiken. Als je inlogt via Azure Active Directory, kun je toch op een veilige manier bij al je online opgeslagen bestanden omdat deze realtime worden opgeslagen. Als je laptop onverhoopt stuk gaat kun je inloggen op elk ander bedrijfsapparaat en kun je gewoon verder met het werk waar je gebleven was, net zoals op je oude laptop.

Tip 2

Zorg dat je je data centraal opslaat

Data centraal opslaan kun je door op een centrale server te werken met behulp van Remote Desktop Protocol (RDP). Het voordeel is dat je op deze manier nooit gevoelige data op je laptop hebt staan. Je kunt er ook voor kiezen bestanden online op te slaan via bijvoorbeeld Sharepoint of SPOT CloudDrive. Het mooie van deze optie is dat je gesynchroniseerde data indien nodig op afstand kunt wissen terwijl deze wel gewoon beschikbaar blijven in de cloud. Bekijk het dus van de zonnige kant: tijd voor een nieuwe laptop!

"Awareness is alles: creëer en behoud bewustzijn over cybersecurity in jouw organisatie."

Tip 3

Stel een rechtenmatrix op

Zeker als je veel werknemers in dienst hebt, is het haast onmogelijk om het overzicht te houden over wie toegang heeft tot welke bestanden. Tante Els van de financiële administratie zit opeens thuis met corona en wat blijkt: zij is de enige die gemachtigd is om essentiële bedrijfsgegevens in te zien. En die heb je toevallig net vandaag nodig voor een rapportage... Het opstellen van een rechtenmatrix kan je hierbij helpen. Het geeft vast een geruster gevoel als je op basis van feiten kunt zeggen dat je je AVG beleid op orde hebt. Goed om te weten: dit kan niet alleen op een server zoals de meeste mensen denken maar ook in een online bestandsopslag zoals SPOT CloudDrive.

Tip 4

Vraag voor al je medewerkers een Office 365 licentie aan

In de praktijk delen sommige medewerkers dezelfde Office 365 licentie, vooral bij startende bedrijven. AVG-technisch is dat niet helemaal verantwoord omdat je zo elkaars documenten kunt inzien. Prima oplossing als je net begint maar als je je bedrijf serieus neemt, is het toch slim op een gegeven moment voor iedereen een eigen licentie aan te vragen. Wel jammer dat je nu niet meer ziet wat je collega allemaal voor privé dingen doet onder werktijd...

Les 2

Bereikbaarheid

Het is kwart voor negen. Over een kwartiertje gaat de servicedesk open en jij en je collega hebben de eerste shift. De verwachting is dat het druk gaat worden want er is net een nieuw product gelanceerd en aan de reacties te merken is er veel vraag naar. Je wordt gebeld op je mobiel. Je collega belt dat hij vanwege een coronabesmetting in zijn gezin in quarantaine moet en kan niet naar kantoor komen. Je krijgt het warm en voelt dat je rode wangen krijgt. Hoe ga je dit in hemelsnaam oplossen?

Het is zomaar een voorbeeld van waar je als bedrijf tegenaan loopt als werknemers onverwacht uitvallen of vanuit huis moeten werken. Hoe zorg je er dan toch voor dat je bereikbaar blijft?



Tip 1**Maak gebruik van VoIP**

VoIP staat voor Voice over Internet Protocol. Dit houdt in dat je draadloos via internet belt. Ideaal voor een telefonische servicedesk die (deels) wordt bemand door mensen die vanuit huis werken. En dus ook perfect als iemand onverwacht thuis komt te zitten omdat hij of zij bijvoorbeeld in quarantaine moet vanwege een coronageval in je omgeving, of omdat je medewerkers preventief vanuit huis moeten werken vanwege een mogelijke besmetting op de werkvloer. Je kunt gebruik maken van een speciale VoIP telefoon. Het is ook mogelijk om gewoon via je eigen mobiel te bellen: de mensen die je bellen zien dan je zakelijke nummer en niet je privénummer (je zit er niet echt op te wachten dat je op je vrije dagen wordt lastiggevallen door klanten...). Ander voordeel: het kost je zo zelf ook geen belminuten.

Tip 2**Maak onderling duidelijke afspraken over de bereikbaarheid**

Als je thuiswerkt, houd je er soms andere werktijden op na dan op kantoor. Die flexibiliteit is belangrijk om de combinatie werk en privé net iets makkelijker te maken. Tegelijkertijd is het nu eenmaal zo dat je wel op bepaalde tijden bereikbaar moet zijn voor collega's en klanten. Het is handig om daar een concrete planning voor op te stellen. Niet alleen voor bijvoorbeeld bemanning van een servicedesk maar ook voor informeel collegiaal overleg. Dan is het duidelijk wanneer je echt achter je computer moet zitten en wanneer je wat meer bewegingsvrijheid hebt. Dat geeft rust en scheelt ongetwijfeld ook veel onnodig heen en weer bellen.

Tip 3**Creëer een mobiele thuiswerkplek**

Maak gebruik van een zogenaamde thin client, een extra dunne laptop die je gemakkelijk overal mee naar toe kunt nemen. Op die manier is je IT omgeving flexibel beschikbaar en kun je gewoon op de normale manier inloggen. Je hebt er bovendien geen kabels voor nodig dus dat bespaart je veel gehannes.

Tip 4**Gebruik een camera waarmee je in een conference call een hele groep kunt filmen**

We hebben het dan over Yaelink. De ene ploeg werkt namelijk waarschijnlijk op kantoor en de andere ploeg thuis. Wij gebruiken deze bijvoorbeeld bij onze wekelijkse kick-off op maandag.

"Ja, ik geef toe, af en toe moet ik even een sprintje trekken om de telefoon op te kunnen nemen."

Les 3

Thuiswerken

Je zit net in een belangrijke Teams meeting met een klant en een aantal collega's. Iedereen praat door elkaar dus af en toe is het lastig om je aandacht erbij te houden. Tot je schrik zie je je kinderen aan komen lopen in de tuin met wat vriendjes, richting huis. Oh nee, ze komen thuis van school, je had er eigenlijk op gerekend dat de meeting dan al afgelopen zou zijn. Luid schreeuwend ('Papa, we zijn thuis!!') komen ze binnen. Met gebaren probeer je duidelijk te maken dat je bezig bent maar ze komen al lachend en pratend de huiskamer binnen. Snel demp je de microfoon en zet je het beeld uit. Je stuurt de kinderen naar de speelzolder en gaat weer achter de computer zitten. Je zet de microfoon en het beeld weer aan. Je verstijft bij het horen van je naam: 'Dirk, wat vind jij daar nou van?'

Nee, thuiswerken was en is bepaald geen zegen, zeker niet als je een gezin hebt.





"Af en toe wandel ik rond tijdens een telefoongesprek, zo krijg ik toch nog wat beweging"

Tip 1

Zorg voor een goede werkplek

Een goede bureaustoel is het minimale. Maar misschien behoort een zit/sta bureau ook wel tot de mogelijkheden. Dan kun je eindelijk die stapel bakstenen weghalen die je gebruikte om je tafel te verhogen.

Tip 2

Wees alert op wat er op de achtergrond te zien is

Klinkt wat overbodig, maar het is een beetje lullig als je partner zich niet bewust is van het feit dat jij aan het videobellen bent en snel even in haar onderbroek haar blouse van de bank pakt. Het is heel simpel op te lossen: je kunt de achtergrond vervagen of er een afbeelding zetten met bijvoorbeeld het logo van je bedrijf.

Tip 3

Demp de microfoon als je niet praat

Ben je niet aan het woord tijdens een meeting? Demp dan het geluid. Vergeet hem alleen niet in te schakelen als je weer iets wilt zeggen...

Tip 4

Gebruik een goede koptelefoon

Geloof ons, het is het geld echt waard: een goede headset die je op kunt doen tijdens het videobellen. Bij voorkeur een 'noise-cancelling' koptelefoon die allerlei storende omgevingsgeluiden dempt. Opeens is het niet zo erg meer als de hond keihard begint te blaffen, als de postbode langskomt of als je kinderen op de achtergrond kabaal maken.

Tip 4

Eet niet tijdens het videogesprek

Je zit thuis in je vertrouwde omgeving dus de verleiding is groot om lekker even te snacken achter de laptop. Niet doen! Jouw eetgeluiden zijn luid en duidelijk te horen door de microfoon.

Checklist

ICT zonder kopzorgen

Om je op weg te helpen hierbij nog een samenvattende checklist. Zorg dat je deze punten geregeld hebt ten aanzien van je ICT, dan kom je al een heel eind.

Checklist

cyberrisico's

1. Zorg dat jouw antivirus software up-to-date is

Zo heb je steeds de laatste scanlijsten van je leverancier en kan het programma bij een nieuwe dreiging direct updates doorvoeren.

2. Gebruik 2 Factor Authenticatie (2FA)

Dit is een manier van inloggen waarbij je naast je login en wachtwoord ook gebruik maakt van een code aangemaakt op een ander apparaat. Denk daarbij aan een app op je smartphone, een vingerafdruk of een sms naar een vooraf gekozen telefoonnummer. Zo maak je het hackers een stuk lastiger.

3. Verander regelmatig je wachtwoord

Ja, we weten het, dit is een open deur maar helaas gebeurt het echt nog steeds te weinig. Gewoon doen dus. En nee, wachtwoorden op een post-it schrijven en dit op je beeldscherm plakken, is niet slim...

4. Gebruik zo min mogelijk draagbare media

Zoals een USB-stick of een externe harde schijf. Die kun je namelijk kwijt raken en dan liggen al deze ongetwijfeld gevoelige bedrijfsgegevens op straat.

5. Maak regelmatig back-ups

ICT is jammer genoeg niet onfeilbaar dus het is een must om regelmatig back-ups te maken. Dat hoeft je niet zelf te doen, je kunt gewoon instellen dat de computer dit automatisch voor je doet. Geloof me, dat scheelt de nodige kopzorgen.

6. Log uit aan het einde van de dag en zet je computer uit

Hackers wachten met pogingen wagen tot na werktijd. Als je PC of laptop uit staat, is hij simpelweg niet toegankelijk.

7. Maak geen gebruik van Free Wifi

Free Wifi is vaak onbeveiligd en gemakkelijk te hacken. Een 4G-verbinding is veilig. Kies dus altijd voor 4G als dit mogelijk is. Is 4G niet aanwezig, gebruik dan een VPN verbinding.

8. Stel een rechtenmatrix op

Zo weet je welke afdelingen toegang hebben tot welke bestanden. Op die manier voorkom je fouten en fraude.

9. Stel ransomware detectie in op al je devices

Ransomware is malware die een apparaat kan vergrendelen of de inhoud kan versleutelen om geld te persen. De juiste software is hier alert op, waarmee je voorkomt dat malware binnendringt in je netwerk en computersystemen. Ook pogingen tot inbraak worden opgemerkt door deze systemen.

10. Wees alert op phishing

Bij phishing worden je medewerkers verleid om op 'kwaadaardige' links in e-mails te klikken. Door training kun je je medewerkers leren om phishing e-mails te herkennen en er alert op te zijn.

Tot slot

We hopen je met deze whitepaper een helpende hand te hebben geboden.

Heb je toch nog wat hulp nodig om je ICT op orde te brengen?

SPOT neemt je ICT graag uit handen, dus neem vooral contact met ons op!



Newtonstraat 30
🏠 1446 VR Purmerend
📞 088 - 235 77 68
🌐 spotict.nl