VEILIG WERKEN

vanuit huis

Maykel Schoonus
functionaris gegevensbescherming

VEILIG THUISWERKEN

Nu de scholen dicht zijn, werken we zo veel mogelijk thuis. Er zijn nieuwe werkplekken gecreëerd, bouwmarkten en elektronicazaken draaien topomzetten en overal worden webcams geplaatst, zodat we de collega's ook nog af en toe kunnen zien. Maar hoe zit het met de privacy in deze nieuwe werkomgeving?

Wanneer je thuis werkt, is het belangrijk om goed te letten op het beheer en de overdracht van informatie. Dat moet uiteraard veilig gebeuren, ondanks de andere omstandigheden. Juist in tijden als deze is er een piek te zien in cybercriminaliteit. Er wordt meer phishing verzonden dan normaal en gebruik gemaakt van de coronacrisis om jou om de tuin te leiden. Denk aan de mails die zogenaamd namens het RIVM verzonden worden, maar eigenlijk bedoeld zijn om een computervirus te verspreiden. Als je informatie wilt over het coronavirus, ga je dus zelf rechtstreeks naar de website van het RIVM of een andere vertrouwde organisatie.

Gelukkig zijn er voldoende zaken die je zelf kunt regelen om de kans te verkleinen dat er iets mis gaat.

VEILIG THUISWERKEN

Tip 1

Sommigen van ons werken al langer zo nu en dan vanuit huis en voor hen is het gesneden koek. Laptop open, veilige verbinding met het schoolnetwerk en werken maar. Voor anderen is het helemaal nieuw. Werk je nu ineens op je eigen laptop thuis en weet je niet eens hoe de beveiliging geregeld is. Check daarom de volgende zaken:

- Is mijn computer goed beveiligd? Heb ik een goede firewall en virusscanner of andere manier van beveiliging?
- Is alle software waar ik mee werk, goedgekeurd door school?
- Zijn alle updates uitgevoerd? Heb je alle Windows-updates uitgevoerd bijvoorbeeld?
- Is de internetverbinding veilig genoeg of moet je naar een VPN (Virtual Private Network) overschakelen? Een VPN zorgt voor een versleutelde internetverbinding, zodat buitenstaanders niet zo maar mee kunnen kijken met wat je aan het doen bent.

Tip 2

Werk je thuis op WiFi of via een bedrade connectie? Die laatste optie is vele malen stabieler dan draadloos en veel veiliger, omdat inbreken van buitenaf moeilijker is. Gebruik je een computer of laptop van school, dan kan je die beter niet aan je thuisnetwerk toevoegen. Zo voorkom je dat eventuele virussen of malware van je privélaptop, iPad of andere apparaten overspringen naar je bedrijfscomputer.

Tip 3

Volg meldingen over Windows updates direct op. Ze bevatten vaak cruciale beveiligingsoplossingen. De nieuwste versie van de software is er niet alleen om het gebruiksgemak te verbeteren, maar ook om een lek in de beveiliging te dichten. Let wel goed op: zo'n Windows-update komt nooit per mail. Klik dus nooit op mails waarin een update aangekondigd wordt.

VEILIG THUISWERKEN

Tip 4

Heb je een goede virusscanner op je privécomputer of -laptop staan? Als je die niet hebt, is het raadzaam om er wel een aan te schaffen. Een goede oplossing wordt geboden door Norton, Kaspersky en Trend Micro bijvoorbeeld. Ook is het standaard antivirusprogramma van Windows meer dan voldoende, mits je niet op verdachte links klikt.

Tip 5

Even naar je collega lopen om iets te vragen, is nu een stuk lastiger. We delen dus veel meer informatie online en dat betekent veel meer risico op beveiligingsincidenten en datalekken. Heb dus geduld in je werk. Je hebt zo op beantwoord allen gedrukt, terwijl dat niet de bedoeling was. Het automatisch aanvullen van mailadressen kan op je thuiscomputer heel makkelijk andere resultaten geven dan je gewend was op school, met alle vervelende gevolgen van dien. Sowieso is je dagelijkse werkritme waarschijnlijk heel anders en werk je met afleidingen waar je op school niet aan gewend bent. Wees daarom geduldig, en neem de tijd voor je handelingen. Haast en onoplettendheid zijn grote veroorzakers van beveiligingsincidenten.

Houd rekening met een lagere productiviteit door capaciteits- en verbindingsproblemen. Programma's draaien vaak lang zo goed en snel niet als op school. Sla voor de zekerheid je werk regelmatig tussentijds op (gebruik bijvoorbeeld de automatisch opslaan-functie in OneDrive) en sluit zo veel mogelijk programma's, bestanden en tabbladen die je even niet nodig hebt. Wellicht kun je zelfs (tijdelijk) een abonnement met meer internetcapaciteit afsluiten. Zeker handig als er meerdere mensen tegelijk thuis online zijn.

VEILIG THUISWERKEN

Tip 6

Let op richtlijnen van school voor de beveiliging en overdracht van informatie. Denk bijvoorbeeld aan de privacywetgeving omtrent gegevens van leerlingen: die mag je niet zomaar thuis op een privélaptop opslaan. Ga ook voorzichtig om met de informatie die je, anders dan je gewend bent, nu opeens bespreekt in groepsapps en videochats.

Gebruik bij voorkeur Microsoft Teams voor je videovergaderingen. Daar hebben we contracten mee afgesloten die de veiligheid van de gegevens garanderen. Vermijd dus programma's waar we zo'n contract niet mee hebben.

Check bij het delen van bestanden wel of je de juiste methode hebt gekozen om een bijlage te verzenden, volgens de voorschriften die ook op school gelden. Zet een extra wachtwoord op een bestand als je dat wilt mailen. In MS Word ga je daarvoor naar bestand > informatie > document beveiligen > versleutelen met wachtwoord. In Office voor Mac kun je in het betreffende bestand bovenin via 'tools' kiezen voor 'protect document' en een wachtwoord toevoegen. Deel het wachtwoord vervolgens met de ontvanger. Doe dit niet in de e-mail met die bijlage, maar bijvoorbeeld per sms.

Tip 7

We gebruiken onze smartphones voor vrijwel alles, zowel zakelijk als privé. Wie toegang krijgt tot je mobieltje kan daarmee ook bij al je gegevens. Al het bovenstaande geldt daarom óók voor je smartphone en andere mobiele apparatuur (tablet). Ga dus ook op die mobiele devices heel bewust om met de software, en update apps zodra daar om wordt gevraagd. Beveilig je Whatsapp met een extra beveiligingscode. Door je mobiele apparaten te vergrendelen en altijd veilig op te bergen, maak je het indringers al een stuk moeilijker om bij je gegevens te komen. Doe daar waar het kan er met een sterk wachtwoord nog een schepje bovenop. Gebruik bijvoorbeeld niet het password voor je Netflix-account ook voor zakelijke apps, e-mail of bestanden, hoe verleidelijk dat ook is. De grootste datalekken van wachtwoorden zijn namelijk vaak privésystemen. Gebruik andersom je zakelijke mail niet voor privézaken.