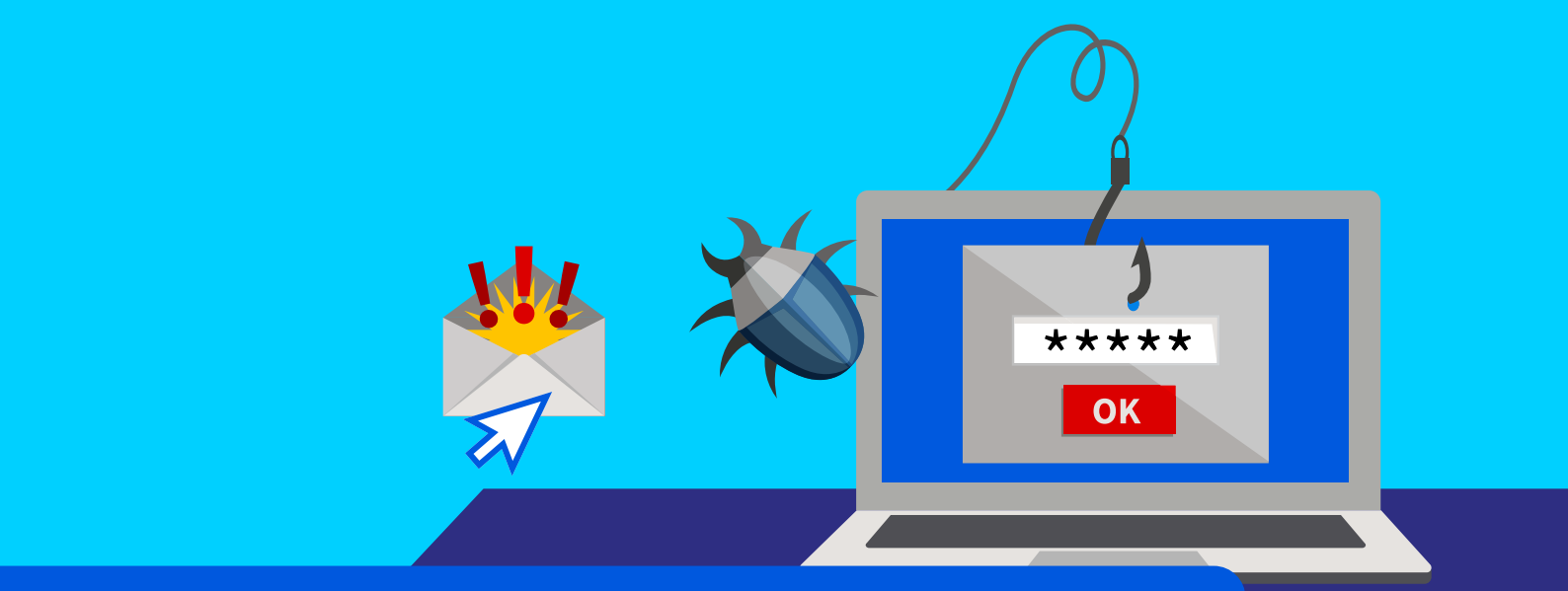
whitepaper

In 7 stappen veiliger werken in het mkb

Zet een hek om onveilige websites



Ook gehoord over die cyberaanval die de universiteit van Maastricht zeker een week lamlegde? Dat overkomt jou toch niet? Toch is de kans hierop groot want uit onderzoek blijkt dat juist mkb'ers steeds vaker slachtoffer worden van cybercrime. Eén verkeerde klik op een link kan jouw digitale bedrijfsvoering voor langere tijd volledig uitschakelen. Hier lees je hoe je door deze 7 stappen te volgen nooit meer op onveilige websites belandt.

Zeker de helft van de mkb'ers heeft te maken met cybercrime en één op de vijf werd in 2019 zelfs slachtoffer. Desondanks loopt het mkb achter in digitale veiligheid. Cybercriminelen weten dat en sturen massaal moeilijk van echt te onderscheiden e-mails. Je hebt ze vast al wel eens langs zien komen. Zo'n nepmail van een bank, waar je niet eens klant bent, met de vraag even in te loggen om je betaalrekening te ontgrendelen. Of een e-mail van de 'post' dat je een pakket hebt gemist. Klik je op de track & trace-link dan vind je geen pakketje, maar installeer je kwaadaardige software op je computer.

Ransomware gijzelt je hele bedrijfsvoering

Zo zijn er talloze voorbeelden te vinden van crimi-mails die je om de tuin proberen te leiden. Klik je erop, dan kan het maar zo zijn dat je computer of het hele netwerk wordt gegijzeld. Je kunt niet meer bij je bestanden, behalve als je een geldbedrag overmaakt aan de cybercriminelen.
Waar eerst grote bedrijven voornamelijk het doelwit waren, nemen criminelen nu vaker het midden- en kleinbedrijf onder vuur.

Criminelen stelen inloggegevens

Er zijn verschillende soorten cybercriminaliteit; de meest voorkomende manier zijn de e-mails die je naar websites sturen. De ene keer installeert het een virus op je computer, de andere keer stuurt het je naar een authentiek lijkende website zoals bijvoorbeeld Facebook. Of je even wil inloggen om je account te ontgrendelen. Tegenwoordig sturen criminelen vaker persoonlijke e-mails 'vanuit' bekende organisaties.

Hierdoor lijken e-mails nog authentieker waardoor je nietsvermoedend naar een website gaat, inlogt en… de crimineel heeft nu je inloggegevens.

Bewustzijnsniveau mkb'ers cybergevaar te laag

De meeste risico's komen uit menselijk handelen. Collega's klikken onbewust door op links in foute e-mails, of surfen naar websites op zoek naar gratis software. Hoewel de gevaren door dit digitaal gedrag enorm zijn, is het bewustzijn erg laag. Dat weten ondernemers, maar desondanks doet volgens onderzoek van Centraal Beheer slechts een derde van hen iets om het bewustzijn van medewerkers te vergroten. Bijna 70 procent van de ondernemers schuift de verantwoordelijkheid af naar de ICT-dienstverlener. Er draait toch antivirussoftware op onze computers? De e-mailfilters en pop-up-blockers houden het cybergevaar toch buiten de deur? Helaas zijn al deze maatregelen onvoldoende. Wat kun je wel doen om veilig te werken? We zetten de 7 belangrijkste stappen op een rij.

1 Maak je collega's bewust van de risico's

Een eerste stap om veiliger te werken is alle collega's informeren over de risico's en het cyberbewustzijn in de organisatie vergroten. Dit doe je bijvoorbeeld door aan je collega's te vragen wat zij doen om veilig te werken. Staat een virusscanner en spamfilter aan? Kijken ze kritisch naar verdachte e-mails? Doe samen de gratis online test van de overheid. En hoe zit het met je eigen cyberbewustzijn? Wellicht kan het geen kwaad om met je ICT-leverancier samen te kijken hoe de cybersecurity op dit moment is geregeld en of dat afdoende is.

2 Kijk kritisch naar e-mailadressen

Cybercriminelen zijn steeds gewiekster en e-mailen minder vaak met rare e-mailadressen. Een nieuwe trend is spearfishing waarmee niet het hele bedrijf, maar een bepaalde groep of individuen persoonlijk worden aangesproken. Omdat het e-mailadres vaak is gekaapt van een legitieme afzender is deze fraude op maat moeilijk te identificeren.

3 Controleer de inhoud van e-mails

De afgelopen jaren is de inhoud van e-mails soms niet van echt te onderscheiden. De tijd van Afrikaanse prinsen die in gebrekkig Engels gouden bergen beloven ligt al even achter ons. Toch zijn de meeste fraudemails taaltechnisch nog niet volmaakt. Wees alert op e-mails met slecht lopende zinnen, spel- en grammaticafouten en Engelse woorden. Authentieke afzenders vragen je nooit om in te loggen en vragen je nooit jouw beveiligingscodes of persoonlijke gegevens in te vullen. Tegenwoordig zijn ook dreigmails populair. Afzenders waarschuwen je computer te hacken, snel tot actie over te gaan want anders... En dan heb je ook nog de meldingen dat rekeningen zijn geblokkeerd; of je die even wilt ontgrendelen. Trap er niet in!

4 Check de links in de e-mails

Check het adres van een link in e-mails. Dat doe je door er met je muis op te gaan staan, zonder te klikken natuurlijk. Kijk goed of je vreemde dingen in de URL ziet staan, al is dat soms erg moeilijk omdat criminelen alles uit de kast halen om je om te tuin te leiden. Twijfel je? Dan kun je via allerlei online tools het adres verifiëren.

5 Neem meldingen van het spamfilter serieus

Ondernemers zijn ook nieuwsgierige mensen, daarom klikken sommigen toch nog op e-mails die in quarantaine zijn gezet. Doe dat echt niet, behalve als je zeker weet dat een e-mail ten onrechte is gefilterd.

6 Ga niet op zoek naar gratis software

Software is niet altijd goedkoop en sommige ondernemers durven het aan om illegale software te downloaden. Dit is om verschillende redenen zeer onverstandig. Het is strafbaar, de software kan het netwerk ontregelen en zelfs het bezoek aan zo'n illegale download-site is al voldoende om schade te veroorzaken.

7 Laat je ontzorgen

Ondernemers willen natuurlijk ondernemen en niet de hele tijd bezig zijn met het checken van e-mails en websites. Daarom ziet 64 procent van de ondernemers het wel zitten als een externe ICT-partij cybersecurity volledig op zich neemt. Dat werkt ook een stuk zorgelozer, niet?!
Anders moet je elk e-mailtje en iedere website nauwgezet controleren, tijd die je liever in je klanten steekt. Hoe zou het zijn als je altijd veilig kunt internetten?

Zet een hek om onveilige sites...

Extra Veilig Internet (EVI) zet een hek om alle gevaarlijke websites. Op die manier komen collega's vanuit jouw internetaansluiting of wifi niet meer op de frauduleuze plekken van het internet. Ze kunnen nog wel overal komen, maar als een site malware of andere gevaarlijke content bevat, wordt deze geblokkeerd en zie je een waarschuwingspagina.

...en voorkom contact met cybercriminelen

Het mooie is dat het twee kanten op werkt. Zo wordt ook verdacht netwerkverkeer naar onveilige webadressen geblokkeerd. Komt een collega met zijn gekaapte laptop binnen, dan kan dat niet door criminelen worden misbruikt. Ook wanneer je vergeten bent je virusscanner te updaten en ben je geïnfecteerd, kan een kwaadaardige site geen gegevens bij je ophalen. Tegelijk voorkomt EVI ook dat hackers toegang krijgen tot slimme, op internet aangesloten apparaten van beveiligingscamera's tot thermostaten.

Extra bescherming

Deze dienst blokkeert onveilige websites op basis van een continu bijgehouden database met malafide websites. Bovendien zet het een webfilter in dat speurt naar schadelijke inhoud op webpagina's. Zo voorkom je dat jij of collega's per ongeluk op onveilige sites belanden.
Dat onderneemt een stuk veiliger én zorgelozer.

Wil je ook vooral ondernemen en je geen zorgen hoeven te maken om cybersecurity?
Vraag dan je ICT-leverancier naar Extra Veilig Internet.