Alert Online zijn: 10 tips voor ondernemers

1. Oud besturingssystemen, browser en hulpprogramma's up-to-date
Zo loop je het minste kans op virussen. Ook draaien de programma's beter omdat updates ook bedoeld zijn om de functionaliteit doorlopend te verbeteren.

2. Beveilig je draadloze bedrijfsnetwerk met een wachtwoord
Je loopt het risico dat je bedrijfsinformatie en klant- en personeelsgegevens in handen van anderen komen. Denk hierbij aan bestanden als contracten en productinformatie, maar ook aan creditcardgegevens of wachtwoorden van klanten en zakenrelaties

3. Zorg ervoor dat iedereen in je bedrijf phishingmails herkent
Het versturen van nepmails – phishing - is een populaire manier onder criminelen om zakelijke gegevens en geld van ondernemers te ontfutselen. Om de ontvangers onder druk te zetten, worden de nepmails vaak verstuurd uit naam van officiële instanties zoals de Belastingdienst, het Centraal Justitieel Incassobureau (CJIB), een bank of andere crediteurs.

4. Maak regelmatig een back-up van je bedrijfsdata
Je gebruikt een back-up om belangrijke bestanden te herstellen als deze beschadigd zijn, of als het apparaat waarop deze staan kapot, verloren of gestolen is. Bewaar je back-up op een veilige plek en versleutel de bestanden eventueel voor extra bescherming.

5. Gebruik verschillende én sterke wachtwoorden
Met een wachtwoord bescherm belangrijke gegevens. Als je verschillende wachtwoorden gebruikt loop je echter niet het risico dat als ergens je wachtwoord bekend wordt (bijvoorbeeld omdat een van de diensten waar je gebruik van maakt gehackt is), al je accounts en al je gegevens toegankelijk zijn.

6. Ga zorgvuldig om met de privacy van klanten
Een datalek van persoonsgegevens is voor alle betrokkenen erg vervelend. De privacy van je klanten en/of websitebezoekers wordt geschonden waardoor je bedrijf reputatieschade kan oplopen. Daarnaast loop je het risico op een (forse) boete van het College bescherming persoonsgegevens (CBP) als je geen melding maakt van een datalek. Want volgens de wet ben je verplicht een datalek te melden bij het CBP en bij de betrokken klanten en/of websitebezoekers.

7. Maak afspraken met je werknemers die hun eigen apparaat gebruiken
Als ondernemer wil je dat je werknemers overal hun werk kunnen doen. Maar als jouw werknemers niet veilig draadloos werken met bijvoorbeeld hun eigen computer, tablet of smartpone, dan loop je de kans dat anderen toegang krijgen tot bedrijfsinformatie. Maak daarom duidelijke afspraken met je werknemers die hun eigen apparaat gebruiken.

8. Weeg de voor- en nadelen van werken in de cloud tegen elkaar af
De cloud staat voor een plek op internet waar je bestanden, zoals facturen, bestellingen en klantgegevens opslaat. Al deze bestanden kun je via al je apparaten met internetverbinding beheren. Dat is handig, want daardoor kunnen jij en je werknemers altijd en overal bij deze bestanden. Maar het vraagt wel om extra bescherming om te voorkomen dat onbevoegden bij je bedrijfsinformatie

9. Stel een sociale media-beleid op voor maximaal effect en minimaal afbreukrisico
Je bedrijf heeft een reputatie en die wil je beschermen. Op sociale media wordt de kleinste misstap al een stuk groter als tien mensen hierover twitteren. Laat staan als dit er honderd of duizend worden. Stel een sociale media-beleid op om vast te leggen op welke manier je bedrijf omgaat met sociale media en deel dit met je werknemers. Is je Twitter-account gehackt of heeft iemand onder je bedrijfsnaam een Facebook-pagina aangemaakt, onderneem dan stappen.

10. Koop goederen en diensten bij betrouwbare webwinkels
Tijdens het online bestellen sta je veel zakelijke informatie af. Zoals je adresgegevens, KvK-nummer en bank- en creditcardgegevens. Je wilt niet dat iemand misbruik maakt van je bedrijfsinformatie. Bijvoorbeeld door identiteitsfraude te plegen en goederen en diensten op naam van jouw bedrijf te bestellen. Winkel daarom alleen online bij betrouwbare webwinkels die bij voorkeur ook een keurmerk hebben.

Meer weten? Neem dan een kijkje op veiliginternetten.nl