Ministerie van Economische Zaken
en Klimaat

Social media tips

Handreiking voor cyberweerbaarheidsnetwerken

digital trust
center.

Inhoud

Inleiding

Voor het bieden van kennis en informatie aan je samenwerkingsverband is het inrichten van een website een goede basis. Een website is echter passief. Mensen bezoeken je website pas als ze gericht zoeken naar de content die op je website staat. Social media kan helpen om meer mensen naar je website te krijgen en om je (online) bereik te vergroten. Welke keuze je hierin maakt hangt af van het doel dat je nastreeft en de tijd die je hierin kunt/wilt steken. We geven je hier een aantal tips welke kanalen je zou kunnen inzetten. Dit is zeker geen allesomvattende lijst, maar het kan je helpen om een begin te maken.

Bronnen

Wil je verder verdiepen in het gebruik van social media? Kijk dan ook eens op de volgende websites:

- www.frankwatching.com/
- www.marketingfacts.nl
- www.dutchcowboys.nl/

Social media tips

Zelf doen of uitbesteden?
Allereerst moet je je afvragen hoeveel tijd je erin kunt en wilt steken. Iets waar men zich vaak op verkijkt is het onderhouden van een social media kanaal. Dit kost tijd en energie. Onderhoud van je social media kanalen kan een fulltime job zijn, maar vereist op zijn minst wel een paar uur per week. Als je zelf geen tijd hebt dan kan het een optie zijn om een bureau in te schakelen om je social media kanelen te onderhouden. Hier hangt uiteraard wel een prijskaartje aan.

Kies je kanalen zorgvuldig
Je hoeft niet op alle social media kanalen aanwezig te zijn. LinkedIn en Twitter zijn waarschijnlijk de meest relevante kanalen voor je zakelijke doelgroep. Afhankelijk van je branche kan het zijn dat er ook nog veel van Facebook gebruik wordt gemaakt. Pinterest en Instagram kan nuttig zijn als je veel visuele content hebt en misschien een wat jongere doelgroep.

Denk vanuit de behoeftes van je doelgroep
Denk van tevoren na over het soort content waar je doelgroep behoefte aan heeft. Dit kunnen ontwikkelingen in het cyberweerbaarheidsnetwerk zijn, maar ook actuele dreigingsinformatie, artikelen uit landelijke of regionale pers, tools of producten die je netwerk weerbaarder maken tegen digitale dreigingen of bijvoorbeeld tips en tricks om digitaal weerbaarder te worden.

Beeld werkt
Het cliché luidt: een beeld zegt meer dan duizend woorden. Zeker in social media is dit sterk van toepassing. Houd je teksten beknopt en to the point, en maak waar mogelijk gebruik van beeld om je boodschap te ondersteunen. Zo val je op tussen de enorme hoeveelheid berichten die je doelgroep dagelijks te zien krijgt. Denk aan het delen verschillende soorten content, zoals illustraties, foto's, infographics, vlogs, animatie of video. Vanuit het DTC stellen wij een aantal van onze beelden ter beschikking.

Maak een content kalender
Het inplannen van je content in een kalender helpt om structuur aan te brengen in je berichten naar buiten. Je kan de content van je kalender afstemmen op belangrijke actuele communicatiemomenten die in Nederlands plaatsvinden. Zo kan je er bijvoorbeeld voor kiezen om tijdens de Cybersecurity Week een extra campagne te gaan voeren omdat dan heel Nederland bezig is met cybersecurity. Of alvast nadenken over een inhaak-bericht op World Password day (eerste donderdag van mei). Het kan ook interessant zijn om aan te haken bij campagnes die plaatsvinden binnen jouw cyberweerbaarheidsnetwerk. Zo kun je elkaar op een mooie manier versterken.

Wat wil je bereiken?
Denk na over wat je met je social media kanalen wilt bereiken. Als je meer bezoekers op je website wilt krijgen is het verstandig om berichten te plaatsen waarin je met linkjes verwijst naar de website. Houd je berichten op social media kort en bondig en zorg dat ze de interesse wekken om naar je website te gaan. Geef dus niet alle informatie maar gebruik een 'cliffhanger'.

Wanneer moet je iets posten?
Hier zijn genoeg theorieën over te vinden, die verschillen per kanaal, regio, doelgroep, sector etc. Over het algemeen zijn maandag, dinsdag en donderdag de 'drukste' dagen op social media. Het DTC plaatst meestal berichten rond 09:00u op deze dagen.

Wees voorbereid op interactie

Social media is per definitie een interactief medium. Berichten die je plaatst kunnen vragen en reacties oproepen. Dit kan zowel positief als negatief zijn. Je hoeft hier niet (altijd) op te reageren maar weet dat dit vaker gebeurt zodra je netwerk groter wordt. Interactie is goed. Zo bouw je een band op met je doelgroep en zo word je zichtbaar in het netwerk van je directe volgers. Als interactie het doel is van een bericht, dan helpt het om een gerichte vraag te stellen. Ook bieden platforms als Twitter en Facebook tools om een korte poll uit te zetten.

Gebruik ambassadeurs

Ambassadeurs zijn mensen die jouw boodschap door kunnen geven aan hun netwerk. Dit begint bij je eigen medewerkers. Zij kunnen berichten vanuit jouw kanaal delen in hun eigen netwerk. Dit is een goed startpunt. Ook kun je nadenken over het samenwerken met ambassadeurs in het netwerk van je organisatie. Bijvoorbeeld branchegenoten of bedrijven binnen je cyberweerbaarheidsnetwerk. Niet alleen kunnen ze jouw berichten delen, je kunt ook gezamenlijk content maken. Bijvoorbeeld in de vorm van een interview, video, artikel of whitepaper.

Kanalen

Hieronder volgt een beknopt overzicht van de mogelijke social media kanalen en hoe je ze kunt gebruiken. We beperken ons hier tot LinkedIn, Twitter en Facebook omdat dit in onze ogen de meest relevante kanalen zijn om een zakelijke doelgroep te bereiken.

Kanaal: LinkedIn

Voor wie:	Zakelijke gebruikers
Waarom gebruiken:	Op LinkedIn kun je vrij eenvoudig een bedrijfspagina aanmaken, waarmee je je zakelijke doelgroep kunt bereiken. Op deze pagina kun je verschillende soorten content plaatsen (tekst, papers, visuals, infographics, videos) en kun je verwijzen naar content op je eigen website. Ook kun je hier interessante content van partners of andere partijen, zoals brancheverenigingen of -genoten delen.
Wanneer gebruiken?	Twee keer per week is een mooi streven.
Do's:	Gebruik beeld bij je berichten en verwijs naar content die op je eigen website staat.
Don'ts:	Misschien een open deur, maar gebruik je LinkedIn pagina niet om hobby's of persoonlijke uitjes onder de aandacht te brengen. Denk vanuit je achterban en waar zij behoefte aan hebben.
Voorbeelden	Zie bijlage 1

Kanaal: Twitter

Voor wie:	Veel soorten gebruikers, ook zakelijke
Waarom gebruiken:	Twitter is platform waar je korte, laagdrempelige berichten kunt delen van max 140 tekens. Ook kan je eenvoudig andere berichten liken en retweeten en kun je met hashtags (#) specifieke onderwerpen volgen.
Wanneer gebruiken:	Op twitter kun je prima elke dag iets van je laten horen. Hou het wel bij max 1 á 2 berichten per dag.
Do's	Hou het – noodgedwongen - kort en bondig. Twitter is een laagdrempelig medium. Gebruik het ook vooral om interessante tweets van anderen te liken of retweeten.
Don'ts:	Ga niet lukraak iedereen volgen. Maak van tevoren een selectie van interessante personen, media of organisaties die jouw/je doelgroep interessante informatie kunnen bieden en volg hen. Zorg ook dat je niet alleen maar berichten retweet maar combineer dit met eigen content.
Voorbeelden	Zie bijlage 2

Kanaal: Facebook

Voor wie:	Persoonlijke gebruikers en bedrijven. Jongeren laten het steeds meer links liggen.
Waarom gebruiken:	Ondanks het teruglopende gebruik – en de privacy schandalen – blijven veel mensen van Facebook gebruik maken. In potentie heb je hier dus nog een groot bereik voor je berichten. Facebook kan een mooie aanvulling zijn op je LinkedIn pagina.
Do's:	Maak het visueel. Meer dan LinkedIn worden gebruikers 'verwend' met mooi vormgegeven content. Een droog stuk tekst zal dus niet snel opvallen en gelezen worden.
Don'ts:	Let op dat Facebook gericht is op advertentie-inkomsten. Met je Facebook bedrijfspagina heb je nauwelijks nog organisch bereik, omdat Facebook wilt dat je advertenties op het platform plaatst. Het kan dus zijn dat je merkt dat je weinig reacties krijgt op berichten op de facebook pagina.
Voorbeelden	Het DTC is (nog) niet actief op Facebook. Dit is een bewuste keuze omdat wij al een groot gedeelte van onze doelgroep bereiken via LinkedIn en Twitter. Daarnaast, zoals hierboven beschreven, is het organische bereik van je Facebook pagina relatief laag, omdat Facebook wilt dat je met name gesponsorde berichten plaatst (oftewel adverteert op hun platform).

Bijlage 1: voorbeelden LinkedIn berichten

Wifi-netwerken
Werk je wel eens buiten de deur, zoals in een koffietent? Grote kans dat je dan wel eens gebruik maakt van een open of gesloten wifi-netwerk. Het is goed te weten dat dit risico's met zich meebrengt. Wil je weten hoe je veilig buiten de kantoormuren werkt? Lees hier onze tips: https://www.digitaltrustcenter.nl/informatie-en-advies/voorkomen/wifi

Email
Als je aan de slag wilt gaan met je digitale veiligheid, moet je met veel dingen rekening houden. Gaan jij en/of je collega's verantwoord om met e-mail? Worden facturen gecheckt op echtheid voordat ze betaald worden? Word je wel eens gebeld door iemand met een dubieuze vraag? Lees hier hoe je verdachte zaken kunt herkennen, zoals valse e-mails, onveilige websites, spookfacturen, neptelefoontjes, verdachte social media connecties en social engineering: https://www.digitaltrustcenter.nl/informatie-en-advies/herkennen

Diefstal mobiele apparatuur
O nee... je werk-laptop is gestolen. Wat nu? Als er gevoelige informatie op je laptop staat kan dit grote (al dan niet financiële) gevolgen hebben voor je organisatie. Wat moet je doen bij diefstal van een laptop of mobiel apparaat? Lees het hier: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/verlies-van-laptop

Wachtwoorden (video)
Een sterk wachtwoord is belangrijk om je bedrijfsdata en systemen te beveiligen. Maar wat zijn sterke wachtwoorden en hoe bedenk je ze? Gebruik in ieder geval geen voor de hand liggende woorden of reeksen, zoals de naam van je partner of kinderen, "12345", "qwerty", "welkom01" of een bestaand woord uit een woordenboek. Wat dan wel? Lees hier onze tips en adviezen: https://www.digitaltrustcenter.nl/informatie-en-advies/voorkomen/wachtwoorden

Phishing

Wel eens een vreemd telefoontje gehad over een (niet-bestaand) probleem met je computer? Waarschijnlijk was dit Tech Support Scam. Dit is een vorm van oplichting waar criminelen met bangmakerij en psychologische trucs proberen geld te ontfutselen voor hulp met niet-bestaande computerproblemen. Weten hoe je dit kunt herkennen hoe je er mee om moet gaan? Lees het hier: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/tech-support-scam

Gehackt

(1) Gehackt, wat nu? Als je bedrijf wordt getroffen door een hack, kan dit ernstige gevolgen hebben. Vermoed je dat er sprake is van een hack? Kom dan snel in actie. Lees hier onze tips en adviezen: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/gehackt-wat-nu

(2) Als ondernemer weet je als geen ander dat 100% zekerheid niet bestaat. Risico's zijn nooit helemaal uit te sluiten. Dat geldt ook voor cyberrisico's. Tijdens de dagelijkse werkzaamheden kun je zomaar te maken krijgen met een cyberindcident of datalek. Jij of een medewerker klikt per ongeluk op een link in een phishingmail of je krijgt te maken met diefstal of verlies van (mobiele) apparatuur. Hoe te handelen in zo'n situatie? Bekijk hier onze praktische tips en informatie: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren

Botnet

Botnets zijn belangrijke hulpmiddelen van cybercriminelen over de hele wereld. Een botnet is een netwerk van besmette computers die door criminelen zijn overgenomen. Deze computers, ook wel zombie-computers genoemd, kunnen op afstand worden aangestuurd om criminele activiteiten te verrichten. Ze worden gebruikt om spam te versturen, DDoS-aanvallen uit te voeren en gegevens te stelen. Weten hoe je een botnetbesmetting kunt herkennen? Lees het hier: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/botnet

Basisprincipes [beelden en video's beschikbaar]

Algemeen

(1) Wil je zelf aan de slag met het digitaal beveiligen van je bedrijf? Dit kan lastig zijn. Hoe moet je beginnen en waar moet je op letten? Onze vijf basisprincipes van veilig digitaal ondernemen helpen je op weg! Kijk voor meer info op https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

(2) Aan de slag met de digitale veiligheid van je bedrijf? Moeilijk is het niet! Het begint met deze 5 basisprincipes:

1. Inventariseer welke data en informatie van je bedrijf kritisch en gevoelig zijn.
2. Kies de meest veilige verbindingen voor apparatuur, software en internetverbinding.
3. Houd apparaten en software up-to-date.
4. Geef mensen alleen toegang tot de data en systemen die ze nodig hebben.
5. Bescherm jezelf tegen virussen en andere malware.

Ga vandaag nog aan de slag! Kijk op https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

Basisprincipe 1

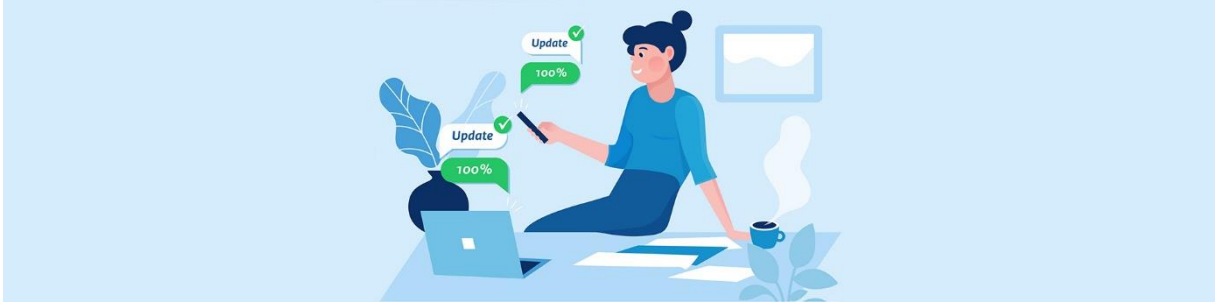
Basisprincipe 1: Een inventarisatie van de kwetsbare onderdelen voor cyberdreigingen binnen jouw bedrijf bestaat uit verschillende onderdelen. Je inventariseert niet alleen welke apparatuur, software, netwerkverbindingen en gegevens je in huis hebt en wat de kwetsbaarheden zijn, maar je brengt ook de technische afhankelijkheid van leveranciers in kaart. Wil je meer weten over hoe je dit doet? https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/1-inventariseer-kwetsbaarheden

Basisprincipe 2

Basisprincipe 2: kies veilige instellingen. Leveranciers van apparatuur en software kiezen vaak standaardinstellingen. Ook staan vaak standaard alle instellingen op 'aan'. Dit is handig als je snel en eenvoudig nieuwe spullen wilt installeren of voor het krijgen van internettoegang. Maar als ondernemer ben je erg kwetsbaar voor cyberdreigingen als je deze instellingen vanaf het eerste gebruik niet wijzigt. Je zet dan de deur open voor onbevoegden. Wat zijn veilige instellingen en hoe kies je ze? We leggen het hier voor je uit. https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/2-kies-veilige-instellingen

Basisprincipe 3

Basisprincipe 3: Voer updates uit. Als je apparaten en software up-to-date zijn, loopt je bedrijf het minste kans op virussen en blijf je beschermd tegen de meest actuele cyberdreigingen en -risico's. Een virus maakt namelijk gebruik van kwetsbaarheden in oudere versies van apparaten en software. Meer weten? Kijk op https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/3-voer-updates-uit



Basisprincipe 4

Basisprincipe 4: Beperk Toegang Wees bewust wie je toegang geeft tot welke data en services! Om de kans op ongelukken en misbruik zo klein mogelijk te maken, is het belangrijk dat iedereen binnen en buiten de onderneming alleen toegang heeft tot de systemen die passen bij de werkzaamheden en de periode waarvoor toegang nodig is. Uitgebreide toegangsrechten moeten alleen worden gegeven voor wie dit nodig is. Meer weten? Kijk op https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/4-beperk-toegang

Basisprincipe 5

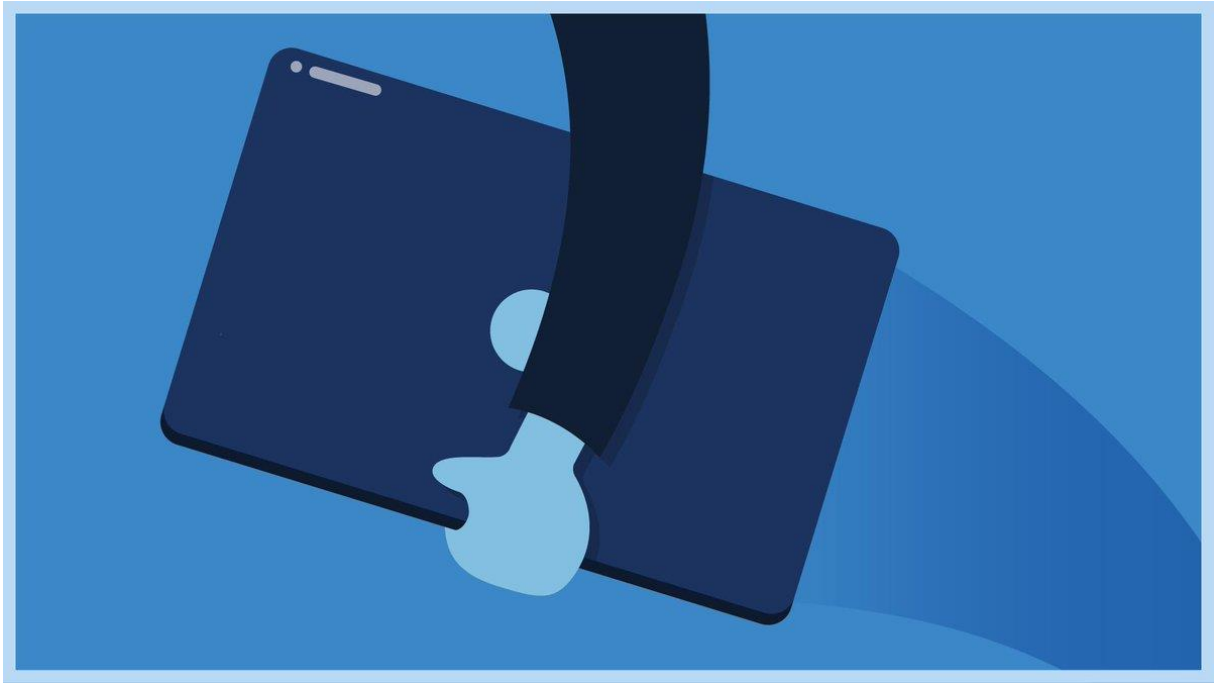
Basisprincipe 5: Voorkom virussen en andere malware. Waarom? Zo voorkom je dat personen en/of organisaties van buitenaf via 'foute software' schade kunnen veroorzaken aan je apparaten, software of data. Ook voorkom je dat ze de controle over jouw systemen kunnen overnemen en wat ze alleen ongedaan willen maken na betaling van 'losgeld'. Wil je weten hoe je jezelf hiertegen moet beschermen? Kijk op https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/5-voorkom-virussen-en-andere-malware

Bijlage 2: voorbeelden Twitter berichten

Wifi-netwerken
Werk je wel eens buiten de deur, zoals in een koffietent? Zorg dan dat je dit veilig doet. Een open (of gesloten) wifi-netwerk is namelijk eenvoudig te hacken. Lees hier onze tips: https://www.digitaltrustcenter.nl/informatie-en-advies/voorkomen/wifi

Email
Hoe herken je valse e-mails, onveilige websites, spookfacturen, neptelefoontjes, verdachte social media connecties of social engineering? Lees het hier: https://www.digitaltrustcenter.nl/informatie-en-advies/herkennen

Diefstal mobiele apparatuur
O nee... je werk-laptop is gestolen. Wat nu? Als er gevoelige informatie op je laptop staat kan dit grote (al dan niet financiële) gevolgen hebben voor je organisatie. Wat moet je doen bij diefstal van een laptop of mobiel apparaat? Lees het hier: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/verlies-van-laptop



Wachtwoorden
Wat zijn sterke wachtwoorden en hoe bedenk je ze? Gebruik in ieder geval geen voor de hand liggende woorden of reeksen, zoals "12345", "qwerty" of "welkom01". Wat dan wel? Lees hier onze tips en adviezen: https://www.digitaltrustcenter.nl/informatie-en-advies/voorkomen/wachtwoorden

Phishing

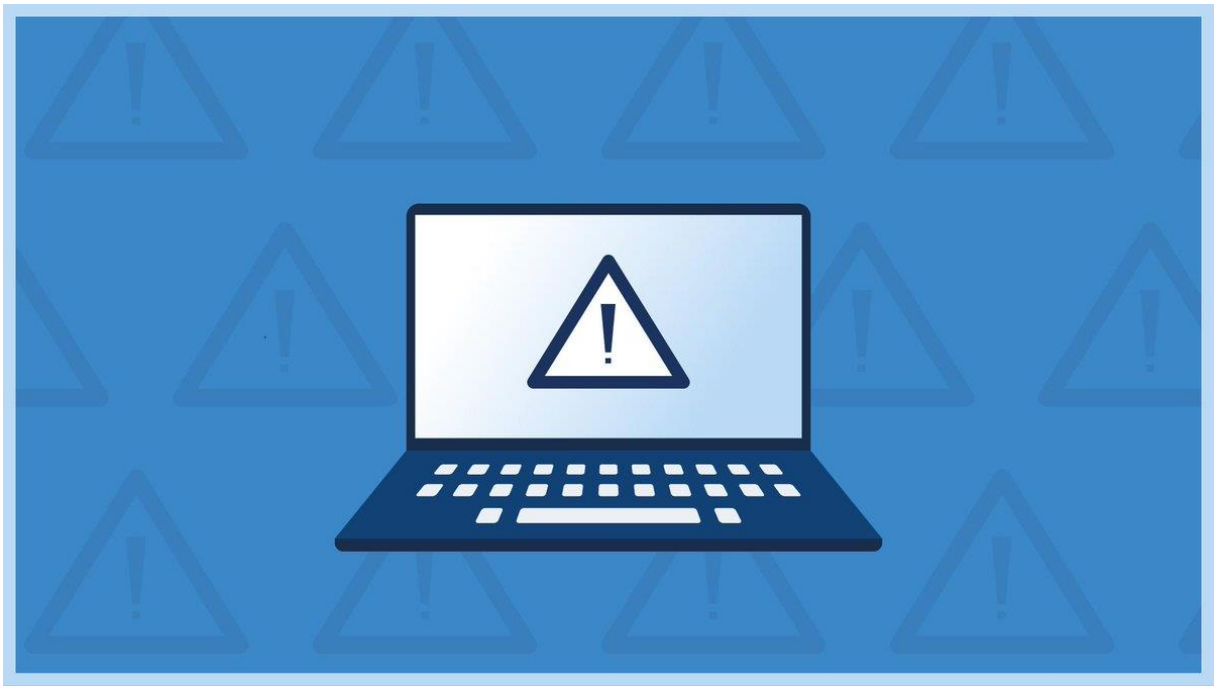
Iedereen kan slachtoffer worden van phishing. Het is vaak moeilijk om phishing te herkennen, vooral als het gaat om gerichte phishing aanvallen. Wat doe je als je het slachtoffer bent geworden van phishing? Lees het hier: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/phishing

Gehackt

Gehackt, wat nu? Als je bedrijf wordt getroffen door een hack, kan dit ernstige gevolgen hebben. Vermoed je dat er sprake is van een hack? Kom dan snel in actie. Lees hier onze tips en adviezen: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/gehackt-wat-nu

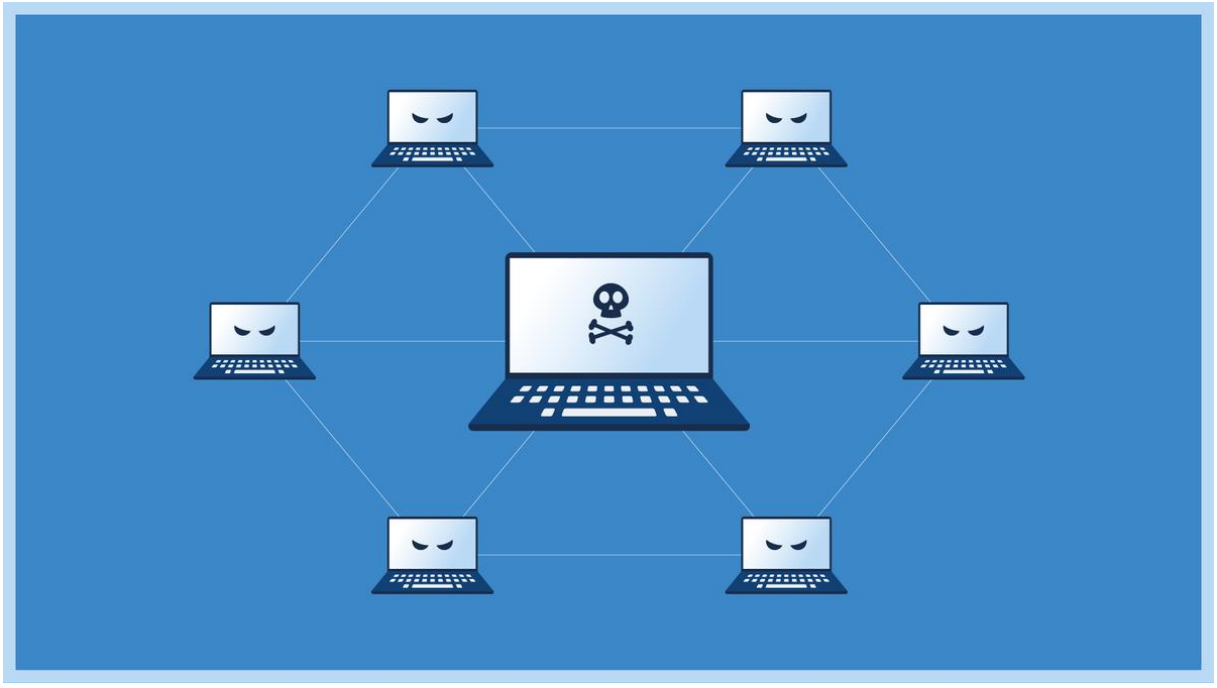
Elke vorm van cybercrime is strafbaar. Denk aan virussen en andere malware, phishing, identiteitsfraude, factuurfraude, CEO-fraude en ransomware. Doe altijd aangifte van cybercrime! Lees hier onze tips en adviezen: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/aangifte-of-melding-doen

Als ondernemer weet je als geen ander dat 100% zekerheid niet bestaat. Tijdens de dagelijkse werkzaamheden kun je zomaar te maken krijgen met een #cyberincident of #datalek. Hoe te handelen in zo'n situatie? Bekijk hier onze praktische tips en informatie: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren



Botnet

Een botnet is een netwerk van besmette computers die door criminelen zijn overgenomen. Ze worden gebruikt om spam te versturen, DDoS-aanvallen uit te voeren en gegevens te stelen. Meer weten over botnets? Lees het hier: https://www.digitaltrustcenter.nl/informatie-en-advies/reageren/botnet



Basisprincipes [beelden en video's beschikbaar]

Algemeen

(1) Wil je zelf aan de slag met het digitaal beveiligen van je bedrijf? Dit kan lastig zijn. Hoe moet je beginnen en waar moet je op letten? Onze vijf basisprincipes van veilig digitaal ondernemen helpen je op weg! https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

(2) Aan de slag met de digitale veiligheid van je bedrijf? Moeilijk is het niet! Het begint met de 5 basisprincipes voor veilig digitaal ondernemen. https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen

Basisprincipe 1

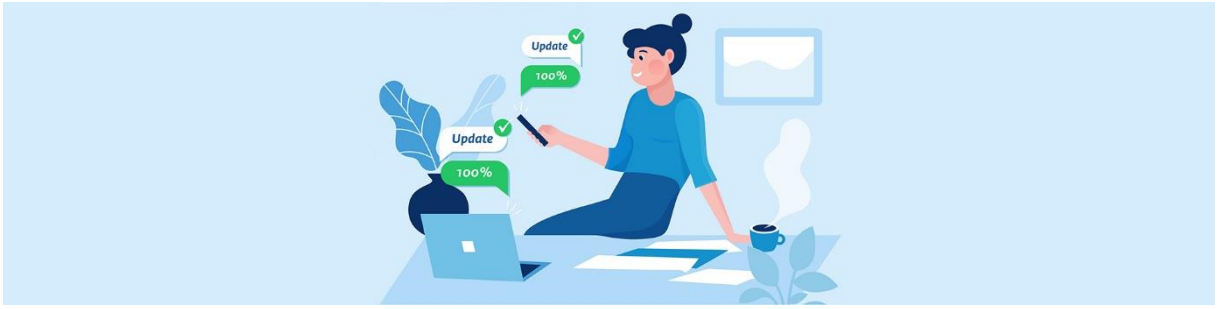
Basisprincipe 1: Een inventarisatie van de kwetsbare onderdelen voor cyberdreigingen binnen jouw bedrijf bestaat uit verschillende onderdelen. Wil je meer weten over hoe je dit aan kan pakken? Kijk dan op: https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/1-inventariseer-kwetsbaarheden

Basisprincipe 2

Basisprincipe 2: Kies veilige instellingen. Als ondernemer ben je erg kwetsbaar voor #cyberdreigingen als je de fabrieksinstellingen van software of hardware vanaf het eerste gebruik niet wijzigt. Hoe kies je veilige instellingen? Lees het hier: https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/2-kies-veilige-instellingen

Basisprincipe 3

Basisprincipe 3: Voer updates uit. Als je apparaten en software up-to-date zijn, loopt je bedrijf het minste kans op virussen en blijf je beschermd tegen de meest actuele cyberdreigingen en -risico's. Meer weten? Kijk op https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/3-voer-updates-uit



Basisprincipe 4

Basisprincipe 4: Beperk Toegang en wees bewust wie je toegang geeft tot welke data en services! Uitgebreide toegangsrechten moeten alleen worden gegeven voor wie dit nodig is. Meer weten? Kijk op https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/4-beperk-toegang

Basisprincipe 5

Basisprincipe 5: Voorkom virussen en andere malware. Virussen en andere malware kunnen flinke schade aan je apparaten, software of data veroorzaken. Hoe werkt dit en wat kan je er tegen doen? Lees het hier https://www.digitaltrustcenter.nl/de-5-basisprincipes-van-veilig-digitaal-ondernemen/5-voorkom-virussen-en-andere-malware

Digital Trust Center
Ministerie van Economische
Zaken en Klimaat
Bezoekadres
Bezuidenhoutseweg 73
2594 AC Den Haag
Telefoonnummer: 070-379 8911

Postadres
Postbus 20401
2500 EK Den Haag

www.rijksoverheid.nl/ezk