

MKB Cyber Campus - Training

Dit document bevat alle onderwerpen die we behandelen tijdens onze training en meer. Hierin hebben we elk thema toegelicht, met ook per onderwerp de maatregelen die u kunt toepassen om de digitale weerbaarheid te verhogen.



Onderwerpen

- Wachtwoorden
- Wachtwoordmanagers
- Phishing
- Malware
- DDoS-aanval
- Man-in-the-middle-aanval
- Social engineering
- Veilige werkplek
- Openbare Wi-Fi
- Datalekken
- Havelbeenpwned
- Spoofing
- Help, Ik ben gehackt?!
- Digitale voetafdruk
- Video's
- Handige links
- Contact

/ Bedreigingen voor het MKB

Wat zijn de grootste cyberbedreigingen voor ondernemers?



Slecht geïnformeerde medewerkers



Weinig kennis van gebruikte systemen



Geen back-up van systeem beschikbaar



Wachtwoorden

Je wachtwoord is heel belangrijk, en daarom moet die ook goed bewaard blijven en zo moeilijk mogelijk zijn. Vroeger zeiden ze dat het uit allemaal speciale tekens moest bestaan, maar die tijd zijn we inmiddels alweer voorbij. Tegenwoordig gaat het om de lengte van je wachtwoord. Elk wachtwoord is te kraken maar hoe langer het wachtwoord is, hoe langer de hacker ermee bezig is om het te kraken. Om een voorbeeld te noemen:

“**Tennis8**” als wachtwoord kost de hacker 1 minuut om te hacken.

Mochten je wachtwoorden net zo makkelijk zijn of voldoen aan wat in het kaartje rood of oranje is gekleurd, dan raden we sterk aan om het aan te passen.

Om het wat makkelijker te maken een lang wachtwoord te bedenken en te onthouden kun je ook een wachtwoord zin maken.
Bijvoorbeeld: “**1KwiLsT@mp0T**” het wachtwoord is 12 tekens en bevat alles, wat het heel moeilijk maakt om te kraken, een hacker zou hier 34.000 jaar over doen. Tenzij je het wachtwoord laat slingeren en ze er op een andere manier achter komen.

Ook raden we aan om elk jaar je wachtwoord aan te passen en overal verschillende wachtwoorden te gebruiken.

Voor het onthouden van al deze wachtwoorden zijn er tegenwoordig apps, ook wel wachtwoordmanagers genoemd. Dit wordt hieronder uitgelegd.

Aantal tekens	Alleen cijfers	Alleen letters	Alleen kleine en hoofdletters	Nummers, hoofd en kleine letters	Nummers, hoofd en kleine letters, symbolen
4	Gelijk	Gelijk	Gelijk	Gelijk	Gelijk
5	Gelijk	Gelijk	Gelijk	Gelijk	Gelijk
6	Gelijk	Gelijk	Gelijk	1 seconde	5 seconden
7	Gelijk	Gelijk	25 seconden	1 minuut	6 minuten
8	Gelijk	5 seconden	22 minuten	1 uur	8 uur
9	Gelijk	2 minuten	19 uur	3 dagen	3 weken
10	Gelijk	58 minuten	1 maand	7 maanden	5 jaar
11	2 seconden	1 dag	5 jaar	41 jaar	400 jaar
12	25 seconden	3 weken	300 jaar	2.000 jaar	34.000 jaar
13	4 minuten	1 jaar	16.000 jaar	100.000 jaar	2 miljoen jaar
14	41 minuten	51 jaar	800.000 jaar	9 miljoen jaar	200 miljoen jaar
15	6 uur	1.000 jaar	43 miljoen jaar	600 miljoen jaar	15 biljoen jaar
16	2 dagen	34.000 jaar	2 biljoen jaar	37 biljoen jaar	1 triljoen jaar
17	4 weken	800.000 jaar	100 biljoen jaar	2 triljoen jaar	93 triljoen jaar
18	9 maanden	23 miljoen jaar	6 triljoen jaar	100 triljoen	4 quadriljoen jaar

Wachtwoordmanagers

Vind jij het lastig om al je wachtwoorden te onthouden? Dan is daar een goede oplossing voor.

Wachtwoordmanagers zijn handige tools die al jouw accounts in een digitale kluis opslaan. Om die kluis te openen hoef je maar 1 sterk wachtwoord te onthouden. De app van de wachtwoordmanager vult dan automatisch jouw gegevens in nadat jij het wachtwoord van de kluis hebt ingevuld.

Goede wachtwoordmanagers zijn bijvoorbeeld:

- Nordpass
- 1Password
- Dashlane



Phishing

Bij phishing proberen criminelen u een e-mail te sturen die als doel heeft u naar een valse website te lokken. Op deze manier proberen ze je uw persoonlijke gegevens, inloggegevens of pincodes te achterhalen. Om deze informatie vervolgens tegen u te gebruiken.

Als afzender van de e-mail staat de naam van je bank, creditcardmaatschappij of een andere betrouwbare instantie vermeld. In het bericht staat bijvoorbeeld dat de bank je gegevens wil controleren vanwege een update of dat je rekening is geblokkeerd. Of je zou bijvoorbeeld een prijs hebben gewonnen of een erfenis krijgen.

Door de betrouwbaar ogende afzender kun je geneigd zijn te antwoorden op de vraag om je inloggegevens of pincode in de nepmail. **Doe dit nooit.** Een bank of andere betrouwbare instantie vraagt niet per e-mail om je persoonlijke gegevens aan ze door te geven. Je bank verstuurt alleen berichten naar je die je kunt vinden nadat je bent ingelogd in de app of op de website.

Klik ook nooit op een link in de e-mail. Als je dit wel zou doen, wordt er ongemerkt op je computer een kwaadaardig programma geïnstalleerd.

Mocht iemand wel een link openen en het bedrijf blootstellen aan criminelen kan het bedrijf onder andere te maken krijgen met de volgende problemen:

- Ransomware
- Malware
- Datalekken
- Spoofing



Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

Wat kun je doen tegen phishing?

Waar moet je opletten?

- Wordt gevraagd om geld over te maken?
- Wordt gevraagd om ergens in te loggen of persoonsgegevens op te sturen?
- Zit er haast bij?

Wat moet je checken?

- Controleer de afzender
- Kijk naar taalfouten
- Bestanden die worden mee gestuurd **(niet openen)**
- Linkje checken via <https://checkjelinkje.nl/> (Eigen Risico)

(Niet door er op te klikken maar de link te kopiëren)

Rechter muisklik erop en dan kopiëren selecteren of CTRL + C

- Krijg je een betaalverzoek van een bedrijf of een bekende? Bel dan het bedrijf of de persoon op om te horen of het klopt. Bel het nummer wat bij jou bekend is en niet wat in de verdachte mail staat genoemd.

Bij twijfel, niets doen.

Staat er in de mail dat er dingen geblokkeerd worden binnen zoveel uur? Als het echt zo belangrijk is, sturen ze nog wel een mail of nemen ze telefonisch contact met je op.



Actuele phishing mails

Ziggo

Verlenging lidmaatschap

Cyberdreiging

ZIGGO- Opzegging Lidmaatschap
Uw lidmaatschap is gesloten op
17/11/2023.
[Definitieve Kennisgeving]

Accountgegevens	
Rekening ID:	
Gebruiker:	
Korting:	90 %
Beperkte Tijd:	17/11/2023

We hebben verschillende pogingen gedaan om contact met u op te nemen over belangrijke meldingen en waarschuwingen voor uw account, maar helaas hebben we nog geen reactie van u ontvangen.

Uw online beveiliging is onze topprioriteit en we raden u ten zeerste aan uw abonnement te verlengen om uw digitale aanwezigheid te blijven beschermen tegen potentiële cyberbedreigingen en hackers.

Als je je lidmaatschap niet binnen de volgende 48 uur hebt verlengd, houd er dan rekening mee dat je account kan worden opgeschort.

Beveilig Uw Apparaat

ZIGGO Ondersteuningsteam

McAfee

Dekking voorbij

McAfee

Je dekking is voorbij

E-mail:
Uitdrukking: 2023-09-26 00:00:00

Uw account is tijdelijk opgeschort vanwege het verlopen van de licentie. We hebben je meerdere keren geprobeerd te bereiken, maar je nam niet op. Probeer de licentie te verlengen om deze te ontgrendelen. Doe je niets, dan wordt je account binnen 48 uur verwijderd.

**AUTOMATISCHE VERLENGING
INSCHAKELEN**

Deze bevestigingscode en link verlopen na 24 uur

Proost
Klantenservice

MediaMarkt

Kans op cadeaukaart

Media Markt

Cadeaukaart

Maak kans op een Media Markt Cadeaukaart!

Doe mee aan ons online winkelonderzoek en deel jouw stem! We zijn benieuwd naar jouw mening en ervaringen als online shopper. We waarderen jouw tijd en als dank maak je kans op een **Media Markt Cadeaukaart!** Doe vandaag nog mee en draag bij aan het begrijpen en verbeteren van de online winkelervaring voor iedereen.

IK DOE MEE

Het genoemde marktbedrijf is niet de organisator of sponsor van deze campagne en is op geen enkele wijze gereleueerd aan de organisatie indien expliciet vermeld. Deze commerciële e-mail ('hostmailing') is verzonden door de 'verspreider' en/of 'bestands-eigenaar' zoals beschreven in Code verspreiding reclame via e-mail. De Adverteerder is niet de eigenaar van de e-mailadressen. De bestands-eigenaar waaruit deze mail is verzonden is verantwoordelijk voor beveiliging van uw data en afreidmogelijkheden.

[uitschrijven](#)

De adverteerder beheert uw abonnement niet. Als u liever geen verdere communicatie ontvangt, kunt u zich afmelden [hier](#).

Check voor meer actuele phishing mails op:

<https://www.fraudehelpdesk.nl/actueel/valse-emails/>

Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

Test je phishing kennis

<https://www.digitaltrustcenter.nl/test-je-kennis-phishing>

Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

Malware

Malware, of "kwaadaardige software", is een overkoepelende term dat een kwaadaardig programma of code beschrijft die schadelijk is voor computersystemen.

Vijandelijke, opdringerige en opzettelijk boosaardige malware probeert computers, computersystemen, netwerken, tablets en mobiele apparaten binnen te dringen, te beschadigen of uit te schakelen, vaak door gedeeltelijk de controle over te nemen over de werking van een apparaat. Het apparaat kan hierdoor niet meer normaal functioneren.

Malware probeert om u op illegale wijze geld afhandig te maken. Malware kan uw gegevens stelen, versleutelen of verwijderen en daarnaast kan het basisfuncties van uw computer wijzigen of kapen en uw computeractiviteit bespieden, zonder uw medeweten of toestemming.

De tijd waarin de meeste malware werd ontwikkeld door minderjarige grappenmakers ligt inmiddels al ver achter ons. Tegenwoordig zitten hier grote criminele organisaties achter. Mocht je niet weten hoe je ze moet betalen om je gegevens terug te krijgen? Daar hebben ze gewoon een klantenservice voor om hierbij te helpen. Zover ontwikkeld is de ontwikkeling van malware inmiddels al.



Tips voor een betere bescherming:

- Apparaten Up-to-date houden en automatisch laten updaten
- Antivirus & Firewall
- Back-up (offline)
- Download alleen van erkende websites
- Installeer een pop-up/adblocker

Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

Back-ups

Regelmatig een back-up maken is belangrijk. Zo voorkom je dat foto's, video's en andere bestanden verloren gaan. Je kunt een back-up maken op een externe harde schijf of in de cloud. Bewaar een back-up bij voorkeur altijd op 2 plaatsen: in huis en buitenshuis.

Om extra veilig te zijn wordt er geadviseerd om fysieke back-ups te maken op externe harde schijven. Deze kan niet digitaal worden benaderd door aanvallers.

Test het terugzetten van een back-up zodat u zeker weet dat de back-ups bruikbaar zijn.

Voor hulp bij het maken van een back-up kunt u gebruik maken van de volgende links.

[Back-ups maken in Mac OS X](#)

[Back-ups maken in Windows 10](#)

[Back-ups maken in Windows 11](#)



Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

DDoS-aanval

Met een (**D**istributed) **D**enial-**o**f-**S**ervice-aanval (DDoS-aanval) wordt de capaciteit van onlinediensten of de ondersteunende servers en netwerkkaparaatuur aangevallen.

Het resultaat van deze aanval is dat diensten slecht of helemaal niet meer bereikbaar zijn voor medewerkers of klanten. Dit kan leiden tot grote (imago)schade. Het vormt een reële dreiging voor alle organisaties met onlinedienstverlening, zoals websites, waarvan de continuïteit van belang is.

Vaak wordt bij een DDoS-aanval een zogenoemd 'botnet' gebruikt. Een botnet is een groep op afstand bestuurbare computers, die via (stiekem geïnstalleerde) malware een lawine aan serververzoeken kan doen. Overigens kan ook een teveel aan legitiem netwerkverkeer piekmomenten veroorzaken met hetzelfde gevolg als een DDoS-aanval. Zo kunnen nieuwssites geblokkeerd raken tijdens een grote ramp, omdat mensen allemaal tegelijk de informatie opvragen.

Wat kan je doen als je slachtoffer bent van een DDoS-aanval?

Niet één DDoS-aanval is hetzelfde én een DDoS-aanval is niet te voorkomen. Bedrijven kunnen wel zorgen voor een DDoS-reponsplan om zo de impact van de DDoS-aanval te beperken. Op de website van het Digital Trust Center vind je maatregelen die je kunt treffen om de kans op een DDOS-aanval te verkleinen.

<https://www.digitaltrustcenter.nl/informatie-advies/ddos-aanval>

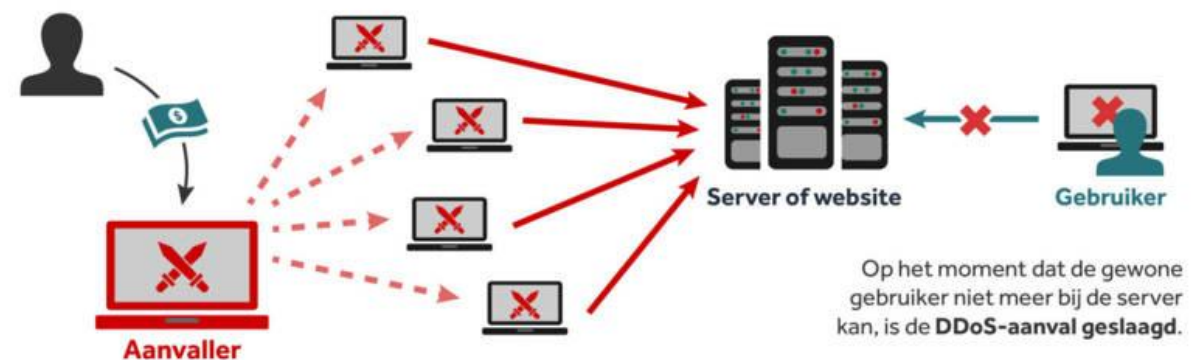
Zo werkt een DDoS-aanval

Op speciale websites worden **DDoS-aanvallen besteld**. Zelf een aanval opzetten kan ook.

De aanvaller **infecteert** een hoop computers. Zo **rekruteert** hij een leger voor de aanval.

Door alle computers in het netwerk de **opdracht te geven** om data van en naar een server te sturen...

... Wordt die server zo zwaar belast, dat hij het **verkeer niet aan** kan.



Man-in-the-middle-aanval

Een man-in-the-middle-aanval is een cyberaanval waarbij een hacker de communicatie tussen twee partijen onderschept. Deze aanvallen kunnen gericht zijn op elk type online communicatie. Denk aan e-mailverkeer, berichtenverkeer via social media of zelfs websitebezoeken. Hackers kunnen zo jouw persoonlijke data bekijken en inzicht krijgen in jouw gesprekken, inloggegevens of financiële informatie. Ze kunnen ook gegevens verzenden en ontvangen zonder dat je dat weet.

Veelvoorkomende doelwitten van man-in-the-middle-aanvallen zijn:

- Websites van banken.
- Websites waarvoor je moet inloggen.
- Versleutelde verbindingen, waaronder chatgesprekken.

Een man-in-the-middle-aanval is moeilijk te detecteren, maar gelukkig zijn er wel maatregelen die je kan toepassen om jezelf en je bedrijf zo beter te beschermen. Denk hierbij aan de volgende punten:

- Gebruik een goed antivirusprogramma.
- Gebruik geen openbare Wi-Fi punten. Maak je wel gebruik van de Wi-Fi, dan raden we aan om een VPN te gebruiken.
- Gebruik altijd het HTTPS-protocol als je websites bezoekt.
- Gebruik een wachtwoordmanager, om sterke wachtwoorden te maken en onthouden.
- Verwijder cookies uit je browser.

VERSCHILLENDE SOORTEN MAN-IN-THE-MIDDLE-AANVALLEN



TIPS OM MAN-IN-THE-MIDDLE-AANVALLEN TE VOORKOMEN



Social engineering



Social engineering is een techniek waarbij een computerkraker een aanval op computersystemen tracht te ondernemen door de zwakste schakel in de computerbeveiliging, namelijk de mens, te kraken.

Dit gebeurt op veel verschillende manieren, phishing en spoofing zijn hier ook voorbeelden van. Hierdoor is het lastig om eenduidige richtlijnen te geven. Wees in ieder geval alert als het volgende zich voordoet:

- U wordt gevraagd persoonlijke informatie af te geven aan willekeurige (onbekende) personen, zoals een kopie van een paspoort.
- Aanbiedingen die te mooi klinken om waar te zijn.
- Er lijkt iets mis te gaan tijdens het surfen en er verschijnt direct een pop-up om u uit de brand te helpen.
- U krijgt de mededeling dat er iets mis is gegaan bij het bezoek aan een site en vervolgens krijgt u het advies op een link te klikken om dit probleem op te lossen.
- Een e-mail van een bekende lijkt vreemd.
- U krijgt een e-mail van een afzender die u niet kent.
- Via internet worden persoonlijke gegevens aan u gevraagd.
- Tijdens een chatsessie wordt u gevraagd met iDEAL of met internetbankieren te betalen voor bijvoorbeeld een filmpje of foto's.

Social Engineering Tactics to Watch For

Knowing the red flags can help you avoid becoming a victim.



Your 'friend' sends you a strange message.



Your emotions are heightened.



The request is urgent.



The offer feels too good to be true.



You're receiving help you didn't ask for.



The sender can't prove their identity.

Veilige werkplek

Ook wel "Clean Desk Policy" genoemd

Je gaat even naar het toilet en dat resulteert in een gesprek op de gang wat zomaar een kwartier kan duren. Herkenbaar? Ondertussen, terwijl je op de gang bent, kan er vertrouwelijke informatie op je bureau liggen of op je computerscherm zichtbaar zijn die eenvoudig gelezen kan worden door toevallige voorbijgangers waarvoor deze informatie niet bedoeld is. Of erger nog, de toevallige voorbijganger gaat aan de haal met de informatie.

Een doemscenario, want als bedrijf wil je niet dat je vertrouwelijke informatie op straat komt te liggen. Om dit soort situaties te voorkomen kun je denken aan een Clean Desk Policy en een Clear Screen Policy. Daarmee wordt de kans dat een ongeautoriseerd persoon aan de haal gaat met vertrouwelijke informatie, zowel in fysieke als digitale vorm, aanzienlijk kleiner.



Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

Veilige werkplek

Ook wel "Clean Desk Policy" genoemd

Het invoeren van een Clean Desk Policy en Clear Screen Policy heeft diverse voordelen. Hieronder benoemen we een aantal:

- Ongeautoriseerde gebruikers kunnen vanaf de werkplek niet in computers en andere apparaten en dus geen digitale informatie ontvreemden.
- Er slingeren geen vertrouwelijke documenten rond in kantoor, zodat deze ook niet meegenomen kunnen worden door toevallige voorbijgangers.
- Opgeruimde bureaus zorgen voor een professionele uitstraling richting klanten.
- Je kunt als organisatie eenvoudiger flexibele werkplekken inrichten, aangezien er niet overal documenten van iemand anders op bureaus liggen.
- Uit onderzoek is gebleken dat werknemers beter functioneren in een goed georganiseerde omgeving.
- Het is voor de facilitaire dienst makkelijker om de bureaus te poetsen.
- Wanneer je van plan bent om een ISO 27001 certificering te gaan behalen, is dit relevant, omdat dit beleid verplicht onderdeel is van de certificering.



Afgesloten machine, opgeruimd bureau.

Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

Windows vergrendelen

Op het moment dat u wegloopt van uw bureau raden wij aan de machines te vergrendelen. Hierdoor hebben onbevoegde minder snel toegang tot gegevens.

Doormiddel van vlaggetje  + L vergrendelt u de computer na gebruik. De volgende keer moet (indien er een wachtwoord op het gebruikers account staat) ingelogd worden met een wachtwoord.



Mac vergrendelen

Op het moment dat u wegloopt van uw bureau raden wij aan de machines te vergrendelen. Hierdoor hebben onbevoegde minder snel toegang tot gegevens.

Doormiddel van **Control + Command + Q** vergrendelt u de computer na gebruik. De volgende keer moet er ingelogd worden met een wachtwoord.



Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

Openbare Wi-Fi

Openbare wifi is heel aantrekkelijk om te gebruiken. Het wordt op veel plekken aangeboden. Denk bijvoorbeeld aan het openbare netwerk in de trein of bij de McDonalds. Je maakt hier heel gemakkelijk verbinding mee op je laptop, smartphone of tablet. Maar zorg ervoor dat je weet hoe je via een openbaar Wi-Fi-netwerk veilig kunt internetten.



Als je openbare wifi wilt gebruiken, zorg dan voor een Virtual Private Network (VPN) om veilig te internetten. Of kies ervoor toch je databundel (3G of 4G) te gebruiken.

VPN staat voor 'virtual private network' of virtueel privénetwerk – een dienst die je internetverbinding en online privacy beschermt. Een VPN creëert een versleutelde tunnel voor je gegevens, beschermt je online identiteit door je IP-adres te verbergen en stelt je in staat openbare wifi-hotspots veilig te gebruiken.



Als MKB-ondernemer loop je het risico slachtoffer te worden van cybercriminaliteit. Maar wat kun je eraan doen? Hoe kun je als ondernemer je digitale weerbaarheid vergroten? De MKB Cyber Campus is dé plek waar bedrijfsleven, onderwijs en overheid samen bouwen aan digitale weerbaarheid voor het MKB.

Datalekken

Voorbeelden van een datalek

Een datalek is bijvoorbeeld:

- persoonsgegevens die aan een verkeerde geadresseerde zijn verstuurd;
- inzage in een medisch dossier door een onbevoegde medewerker;
- het verlies van een USB-stick met niet-versleutelde persoonsgegevens;
- Een cyberaanval waarbij persoonsgegevens zijn buitgemaakt;
- Een besmetting met ransomware (gijzelsoftware) waarbij persoonsgegevens ontoegankelijk zijn gemaakt.

Een datalek kan in iedere organisatie gebeuren. Door snel te handelen, beperkt u als organisatie de gevolgen van het datalek voor de privacy van bijvoorbeeld uw klanten, patiënten of werknemers. Ook kunt u imagoschade voorkomen of beperken door snel in actie te komen bij een datalek. Verder moet u het datalek mogelijk melden aan de Autoriteit Persoonsgegevens (AP) en soms ook aan de slachtoffers.



Hoe weet je of je slachtoffer bent van een datalek?

www.HaveIBeenPwned.com

Voor het checken van e-mails, 06-nummers en wachtwoorden.
Dit is een database voor gehackte websites.

';--have i been pwned?

Check if your email or phone is in a data breach

info@mkbcybercampus.nl

pwned?

Good news — no pwnage found!
No breached accounts and no pastes (subscribe to search sensitive breaches)

';--have i been pwned?

Check if your email or phone is in a data breach

*****@hotmail.com

pwned?

Oh no — pwned!
Pwned in 4 data breaches and found no pastes (subscribe to search sensitive breaches)

Spoofing

Bij spoofing nemen internetcriminelen een andere identiteit aan. De cybercrimineel doet zich voor als een bank, een verzekeringsmaatschappij, een overheidsinstantie of kennis of goede bekende, zelfs wel eens als je vader of moeder. Als zogenaamde bekende of erkende afzender probeert de cybercrimineel achter je persoonsgegevens of je pincode te komen, malware op je computer te plaatsen of je direct geld afhandig te maken.

Een helpdesk belt jou niet!

- Als je gebeld wordt door een helpdesk is het eigenlijk altijd een nephelpdesk.
- Word je gebeld door een helpdesk en word je gevraagd om geld te betalen of software te downloaden? Niet doen! Verbreek direct de verbinding en meld dit bij Fraudehelpdesk.
- Ben je op zoek naar een helpdesk? Zorg ervoor dat bij een echte helpdesk terecht komt.

Overheidsinstanties

- Overheidsinstanties vragen nooit naar persoonlijke gegevens, wachtwoorden of betaalgegevens. Ook vragen ze niet of je software op je computer wil installeren. Wordt dit aan je gevraagd, dan heb je te maken met een oplichter.

Banken

- De bank belt niet voor persoonsgegevens of om te zeggen dat geld moet worden overgemaakt. Of dat ze je pasje komen ophalen omdat er iets mee gebeurd is.

Betrouwbare Helpdesk

- <https://www.fraudehelpdesk.nl/>



Er lijkt iets mis met je ING-rekening  Inbox x



Klantenservice ING <klanten@ing-service.net>

aan mij ▾



Geachte klant,

We hebben zojuist een melding ontvangen waaruit blijkt dat er meerdere malen is geprobeerd om in te loggen op uw account, vanuit Turkije.

We vragen je met spoed om via [deze link](#) jouw rekening weer veilig te stellen.

Met vriendelijke groet,

Annet van der Hoek
Directeur Klantenservice

Deze e-mail is afkomstig van ING Bank N.V te Amsterdam



Voorbeelden van Spoofing

Texting with +34 5901017622324 (SMS/MMS)



UPS: Uw pakket NL4923214Z is onderworpen aan douanekosten (2,99€) die u moet betalen onder: <http://ups.com-tracking.nl/>

Monday, 28 Aug • 15:37



UPS: Uw pakket NL4923214Z is onderworpen aan douanekosten (2,99€) die u moet betalen onder: <http://ups.com-track.nl/>

15:37



Text message



Help, ik ben gehackt?!

- **Stap 1: Kalm blijven.** Gehackt ben je al dus je hoeft je niet te haasten waardoor je verkeerde beslissingen kan nemen.
- **Stap 2: Verbreek je verbinding met het Wi-Fi-netwerk.** Sluit je laptop/telefoon **niet** af, zo kan je bestanden kwijtraken mocht je documenten niet opgeslagen hebben.
- **Stap 3: Verander al je wachtwoorden.** Lukt het je nog om op accounts te komen, verander dan meteen het wachtwoord. Indien het mogelijk is, op een ander apparaat.
- **Stap 4: Zoek uit wat er precies aan de hand is.** Voer scans uit en probeer erachter te komen hoe en waarvan je slachtoffer bent geworden. Kom je er niet uit, dan kun je ook via de politie een specialist om hulp vragen. Doe daarnaast aangifte.
- **Stap 5:** Voorkomen is beter dan genezen.

Digitale voetafdruk

Wat is een digitale voetafdruk?

Telkens wanneer je het internet gebruikt, laat je een spoor van informatie achter. Dat spoor noemen we je digitale voetafdruk. Je digitale voetafdruk wordt op allerlei manieren steeds groter, bijvoorbeeld als je een bericht plaatst op social media, als je je aanmeldt voor een nieuwsbrief en als je online winkelt of een review achterlaat.

Het is niet altijd duidelijk dat je je digitale voetafdruk achterlaat. Websites kunnen bijvoorbeeld je activiteiten bijhouden door cookies op je apparaat te installeren en bepaalde apps verzamelen gegevens zonder dat je het weet. Als je een organisatie eenmaal toegang hebt gegeven tot je informatie, kunnen ze je gegevens verkopen of delen met andere partijen. Erger nog, je persoonlijke informatie kan in verkeerde handen vallen door een gegevenslek.



Voorbeelden van de digitale voetafdruk

Online winkelen

- Aankopen doen op e-commerce-websites
- Je aanmelden voor kortingen of een account maken
- Winkel-apps downloaden en gebruiken
- Je aanmelden voor nieuwsbrieven van merken

Sociale media

- Sociale media gebruiken op je computer of apparaat
- Inloggen op andere websites met de inloggegevens van je sociale media
- Vrienden en contacten volgen op internet
- Informatie, gegevens en foto's delen met je contacten
- Je aanmelden bij een datingsite of -app

Het nieuws lezen

- Je abonneren op een online nieuwsbron
- Artikelen bekijken in een nieuws-app
- Je aanmelden voor een nieuwsbrief
- Artikelen en informatie doorsturen

Online bankieren

- Een app gebruiken voor online bankieren
- Aandelen kopen of verkopen
- Je aanmelden voor financiële publicaties en blogs
- Een creditcardrekening openen

Digitale voetafdruk

Tips om de digitale voetafdruk verkleinen

- Verwijder oude sociale media accounts.
- Gebruik een privé- en een bedrijfsaccount
- Denk er aan wat wel en niet online moet.
- Is het nodig dat elke app je locatie weet?
- Let op welke cookies je toestaat
- Vermijd onveilige websites
- Deel geen privacygegevens via een openbaar Wi-Fi-netwerk

Gebruikte YouTube video's:

De Telegraaf – Wachtwoorden

<https://www.youtube.com/watch?v=ziseUzMgyvw&t=22s>

Arjen Lubach – Ransomware

https://www.youtube.com/watch?v=fuO_yUE3RM8&t=255s

NOS op 3 – Hoe criminelen cashen met digitale gijzelingen

<https://www.youtube.com/watch?v=7hZflge5aEs&t=13s>

Don't share your kids personal information

https://www.youtube.com/watch?v=-r_2a064dWY&t=12s

Handige links

www.HaveIBeenPwned.com

Om te kijken of je in een datalek voorkomt. Dit kan een oorzaak zijn voor phishingmails

www.testjewachtwoord.nl en <https://veiliginternetten.nl/wachtwoordkraak-test/>

Websites om je wachtwoordsterkte te controleren

www.checkjelinkje.nl

Kun je gebruiken om hyperlinks te controleren, als je mails niet vertrouwt (eigen risico)

Nooit op de link klikken! Kopieer en plak de link.

<https://leakpeek.com/>

(zelfde idee als HaveIBeenPwned, maar dan met meer wachtwoordinformatie)

<https://tweakers.net>

Website met het laatste tech-nieuws

<https://www.security.nl/>

Website met de laatste cybernieuws en een forum

<https://www.digitaltrustcenter.nl/>

Website van de overheid met informatie en advies omtrent veilig ondernemen

Voor vragen mag u altijd contact met ons opnemen



+316 38 64 03 75



info@mkbcybercampus.nl



www.mkbcybercampus.nl