



DIGITALE HULP

VERLENER

EERSTE HULP BIJ HET VOORKOMEN
VAN DIGITALE ONGELUKKEN



INLEIDING



De Digitale Hulpverlener



Eén op de vijf ondernemers wordt slachtoffer van cybercriminaliteit. Bij mkb-bedrijven en zzp'ers ligt dit aantal zelfs nog hoger. Criminelen sturen **nepfacturen, stelen gegevens, lekken bedrijfsinformatie of leggen complete systemen plat**. De gevolgen zijn groot: van financiële schade tot persoonlijke stress en schaamte.



Bij een fysieke brand is er meestal veel begrip, maar bij een **“digitale brand”** heerst vaak **onbegrip**. Ondernemers bereiden zich vaak goed voor op een fysieke brand met **brandblussers, nooduitgangen en plannen**, maar veel ondernemers bereiden zich niet voor op een “digitale brand”.



In de praktijk wordt het onderwerp echter nog vaak gezien als ingewikkeld of uitsluitend een taak van de IT-afdeling. Dit starterspakket laat zien dat het anders kan. Met de Digitale Hulpverlener (DHV'er) wordt digitale veiligheid **begrijpelijk en praktisch** aan te pakken. Een Digitale Hulpverlener is een collega die weet hoe digitale **incidenten te voorkomen**, erop te reageren en het gesprek over het onderwerp binnen de organisatie op de agenda zet. Net zoals een BHV'er onmisbaar is bij een brand, is een DHV'er dat bij een “digitale brand”.



Dit starterspakket beschrijft wat een DHV'er precies is, doet en hoe je zorgt voor een DHV'er in je eigen organisatie. Daarnaast behandelt het de **'5 basisprincipes'** voor de DHV'er en de rest van de organisatie, aangevuld met praktische tips.



Het document sluit af met een **Toolkit** die direct door de DHV'er gebruikt kan worden. Zo maken we **digitale veiligheid samen overzichtelijker, begrijpelijker en haalbaar** voor elke onderneming.



Wil je na het lezen van dit document de belangrijkste punten nog even terugzien? Bekijk de **animatie** voor een korte samenvatting.





INHOUDSOPGAVE



Wat is een Digitale Hulpverlener (DHV'er)? **5**

- Kenmerken van een DHV'er **6**
- Het stappenplan DHV **7**



De 5 basisprincipes van veilig digitaal ondernemen **8**

- Waarom de 5 basisprincipes? **9**
- Basisprincipe 1: Breng de risico's in kaart **10**
- Basisprincipe 2: Werk digitaal veilig **11**
- Basisprincipe 3: Bescherm systemen, applicaties en apparaten **12**
- Basisprincipe 4: Beheer toegang tot data en diensten **13**
- Basisprincipe 5: Bereid je voor op incidenten **14**



Vraag & antwoord **15**

Alles wat jij nog meer wilt weten over de Digitale Hulpverlener.



Checklist en templates **19**

- Digitale Hulpverlener **20**
- Crisis communicatie **21**
- Applicaties **22**
- Checklist DHV'er **23**
- Checklist Phishing **24**
- Checklist Accountdiefstal **25**
- Checklist Ransomware **26**



Wat is een Digitale Hulpverlener?

Een collega voor
digitale veiligheid
binnen jouw
organisatie.

Verdachte situatie?

Meld het bij de DHVer.
Ook bij twijfel!





Wat is een Digitale Hulpverlener?



De Digitale Hulpverlener is te vergelijken met een BHV'er, maar dan voor digitale incidenten. Het is dé ambassadeur voor digitale veiligheid binnen de organisatie. Geen IT'er, maar een collega die weet wat te doen bij een incident en hoe dit te voorkomen.



Denk aan:

- Meekijken met collega's of een link in een e-mail betrouwbaar is.
- Herkennen en melden van een datalek.
- Promoten van sterke wachtwoorden.
- Stimuleren van tijdige software-updates.



Een DHV'er weet wat te doen, helpt collega's én verhoogt de digitale weerbaarheid van jouw organisatie. Daarmee versterk je ook het vertrouwen van klanten en partners.



De Digitale Hulpverlener (DHV'er) is een medewerker binnen jouw bedrijf die:

- Basiskennis heeft van digitale risico's.
- Digitale veiligheid actief op de agenda zet.
- Collega's helpt bij vragen.
- Verdachte situaties herkent en direct actie onderneemt.
- Het contact onderhoudt met externe experts indien nodig.



Dit startpakket biedt de nieuwe DHV'er gouden basistips, praktische tools en checklists die direct toegepast kunnen worden in jouw organisatie. Je hoeft geen IT-specialist te zijn om een verschil te maken. Een oplettende collega met de juiste handvatten kan al veel ellende voorkomen.



Maak vandaag nog **iemand in jouw organisatie verantwoordelijk als Digitale Hulpverlener** en vergroot zo de digitale weerbaarheid!



Kenmerken voor een DHV'er:

Oplettend

Heeft oog voor signalen en risico's

Weerbaar

Staat stevig in onverwachte situaties

Benaderbaar

Collega's stappen makkelijk op hem/haar af

Daadkrachtig

Durft beslissingen te nemen en actie te ondernemen

Het stappenplan DHV'er

STAP
1

Kies je Digitale Hulpverlener

Bepaal wie in jouw organisatie geschikt is en **interesse** heeft in digitale veiligheid, **oog voor detail** heeft en **makkelijk aanspreekbaar** is voor collega's.

DHV'er volgt de basistraining en gebruik het starterspakket

Hiermee krijgt hij of zij **praktische tips, checklists en handvatten** om direct aan de slag te gaan.

STAP
2

STAP
3

DHV'er stemt af met IT-specialist of CISO

Laat de DHV'er kennismaken met de externe IT-partij of interne CISO. Zo weet iedereen **wie welke taken heeft** en hoe er **samengewerkt wordt bij een incident**.

[Klik hier voor de 'praatplaat'](#)

Maak de rol van DHV'er zichtbaar binnen het bedrijf

Zorg dat collega's de DHV'er **makkelijk vinden** en weten wat je aan de DHV'er hebt.

STAP
4

STAP
5

DHV'er zet digitale veiligheid op de agenda

De DHV'er deelt regelmatig **tips, updates en bespreekt verdachte situaties** in teamoverleggen.

Samen evalueren en verbeteren

Wat gaat goed, wat kan beter, en heeft de DHV'er nog **extra kennis of middelen nodig?**

STAP
6

De 5 basis principes van veilig digitaal ondernemen

Tips voor de DHV'er om het bedrijf weerbaarder te maken tegen cyberrisico's.





De 5 basisprincipes



Waarom de 5 basisprincipes?

De 5 basisprincipes van veilig digitaal ondernemen zijn opgesteld om ondernemers te helpen de basisbeveiliging op orde te brengen en te houden. Ondernemers die de 5 basisprincipes opvolgen, vergroten hun weerbaarheid tegen cyberrisico's die de bedrijfsvoering kunnen verstoren. Deze basisprincipes zijn gebaseerd op het basisprincipes van Digital Trust Center (DTC).



[Klik hier voor de 'basisprincipes'](#)



Voor wie?

De 5 basisprincipes zijn zo opgesteld dat iedere ondernemer, of die nu zzp'er of mkb'er is, ermee uit de voeten kan. De maatregelen zijn toegankelijk en praktisch opgeschreven. Wacht dus niet langer en ga direct aan de slag zodat jouw bedrijf weerbaarder is tegen cyberrisico's.



De 5 basisprincipes op een rij:

1. Breng je risico's in kaart
2. Werk digitaal veilig
3. Bescherm systemen, applicaties en apparaten
4. Beheer toegang tot data en diensten
5. Bereid je voor op incidenten



Bescherm je bedrijf tegen cybercriminelen met deze maatregelen



CONTROLEER DE BEVEILIGINGSSTANDAARDEN VAN JE E-MAIL



GEbruik ANTI-VIRUS SOFTWARE



MAAK EEN OFFLINE BELLIJST



LEER PHISHING HERKENNEN

NEEM INFORMATIEBEVEILIGING ALTIJD SERIEUS. ONZE KLANTEN EN COLLEGA'S VERTROUWEN EROP!



ZET AUTOMATISCHE UPDATES AAN



MAAK EEN BACK-UP VAN JE BESTANDEN



STEL INLOGGEN IN MEERDERE STAPPEN IN





Basisprincipe 1

Breng de risico's in kaart

Bepaal welke systemen en gegevens voor jouw organisatie belangrijk zijn en welke risico's deze lopen. Door risico's en zwakke plekken in kaart te brengen, kun je bewust kiezen welke maatregelen en investeringen nodig zijn om je bedrijf weerbaarder te maken.

[Klik hier voor 'meer informatie'](#)

Denk hierbij niet alleen aan technologie, maar ook aan menselijk handelen en processen: vaak ontstaan incidenten door onoplettendheid of miscommunicatie.

Wat kun je doen?

- Maak een inventarisatie van je ICT-systemen en voer regelmatig een risicoanalyse uit. [Klik hier voor 'stappenplan risicoanalyse'](#)
- Betrek collega's, leveranciers en afnemers, leg afspraken vast en bespreek verantwoordelijkheden.
- Bespreek cyberveiligheid met andere organisaties in jouw bedrijfsketen: je cyberveiligheid is zo sterk als de zwakste schakel.

Moet ik mijn systeem vergrendelen als ik koffie haal?

Mag een collega met mij mee naar binnenlopen?

Heb ik toegang tot voldoende maar niet teveel gegevens?

Mag ik mijn wachtwoord delen als ik op vakantie ga?





Basisprincipe 2



Werk digitaal veilig



Menselijk gedrag is vaak de oorzaak van digitale incidenten. Creëer een cultuur waarin medewerkers bewust en veilig omgaan met digitale middelen en incidenten melden. Door veilig gedrag te stimuleren en fouten bespreekbaar te maken, voorkom je incidenten. [Klik hier voor 'bevorder veilig gedrag'](#)



Wat kun je doen?

- Maak het laagdrempelig om incidenten te melden, bijvoorbeeld bij de DHV'er.
- Help medewerkers met hun cyberbewustzijn
Leer hen bijvoorbeeld wat phishing is.



Phishing, waar moet je op letten?

Controleer altijd het e-mailadres, de afzender en de inhoud van een bericht. Let daarbij op onder andere deze punten:



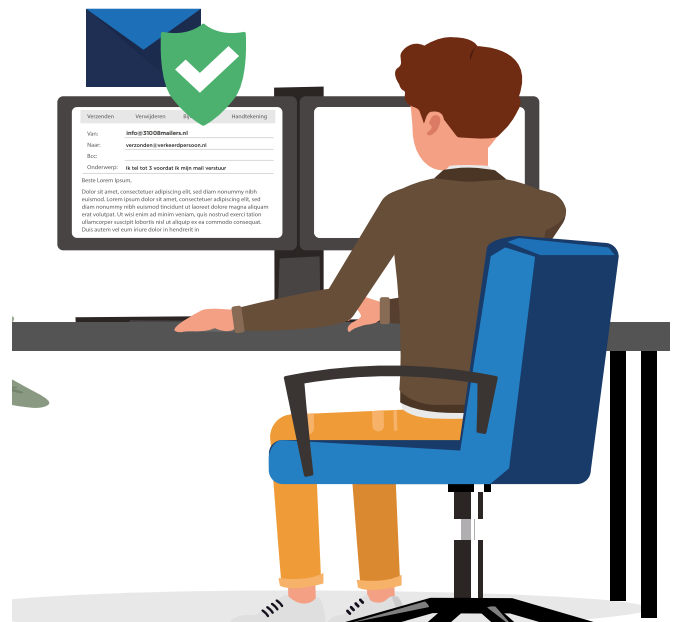
- Controleer of de domeinnaam en het e-mailadres van de afzender hetzelfde zijn.
- Controleer of de domeinnaam overeenkomt met het website-adres.
- Let op de details: zie jij het verschil tussen `info@31008mailers.nl` en `info@31008mailers.nl?`
- Klik niet op een link als je het niet vertrouwt, maar beweeg (hover) met de aanwijzer van je muis over de link. Zo ontdek je waar de link écht naar toe gaat.
- Maak veilig gedrag makkelijker (bijv. met wachtwoordmanagers of een phishing-meldpunt).



Daag één van je collega's uit!

Hoeveel bingovakjes kun je afstrepen met de **phishingmail** die je ontvangen hebt? Speel **Phishing bingo** en **trap er niet meer in**.

[Klik hier voor 'Phishing bingo'](#)





Basisprincipe 3

Bescherm systemen, applicaties en apparaten

Veilige instellingen, actuele software en goede monitoring beschermen je bedrijf tegen misbruik van kwetsbaarheden. Veel cyberaanvallen maken misbruik van fabrieksinstellingen of verouderde systemen. Door proactief te beveiligen, verklein je de kans op schade.

[Klik hier voor meer informatie](#)

Wat kun je doen?

- **Gebruik sterke wachtwoorden en multifactorauthenticatie.**

Met multifactorauthenticatie (MFA) voeg je aan het inloggen met een wachtwoord een extra inlogvereiste toe. Dit heet ook wel inloggen in twee stappen of tweefactorauthenticatie (2FA). Hiermee voorkom je misbruik van je account. Je vergrendelt je account bijvoorbeeld met een code van een authenticatieapp of via je vingerafdruk.

- **Activeer een firewall en gebruik antivirussoftware.**

- **Beveilig mobiele apparaten van je bedrijf met wachtwoorden en sla jouw data op de veilige plaats op.**

- **Voer updates tijdig uit.**

Software-updates bevatten vaak verbeteringen en beveiligingsupdates. Voer je een update niet of later uit, dan kan je beveiliging kwetsbaar worden. Zo kan er bijvoorbeeld een beveiligingslek ontstaan. Kwaadwillenden zoeken actief naar manieren om binnen te dringen via zo'n lek.

Wacht daarom niet met het updaten van apparaten die met het internet verbonden zijn. Zet bij voorkeur 'automatisch updaten' aan. Denk hierbij niet alleen aan je computer of smartphone, maar ook aan je printer, slimme deurbel, website, server en router.





Basisprincipe 4



Beheer toegang tot data en diensten



Geef medewerkers alleen toegang tot wat ze écht nodig hebben en pas rechten direct aan bij functiewijzigingen. Onnodige of gedeelde toegang verhoogt het risico op misbruik van informatie en datalekken.

[Klik hier voor meer informatie](#)



Wat kun je doen?

- **Bepaal per medewerker tot welke systemen en data zij toegang moeten hebben. Denk hierbij ook aan medewerkers die uit dienst gaan of die van functie veranderen.**



- **Vergrendel je scherm en toegang tot belangrijke applicaties.**



- **Gebruik unieke accounts en MFA.**

- **Gebruik veilige, sterke en verschillende wachtwoorden.**

Met een wachtwoord bescherm je de vaste en mobiele apparaten van je bedrijf. Maar ook je bedrijfsgegevens in de cloud, draadloze netwerken, e-mailaccounts en sociale media-accounts. De meeste wachtwoorden bestaan uit een combinatie van letters en cijfers, maar er zijn ook andere opties zoals het gebruik van een pincode, Touch ID of beveiligingspatroon. Je kunt ook overwegen om gebruik te maken van passkeys.



- **Wachtzin.**

Gebruik daarom zo'n lang mogelijke wachtzin en gebruik voor elk account een ander wachtwoord. Anders heeft iemand die jouw wachtwoord achterhaalt namelijk toegang tot ál je accounts.

[Klik hier voor 'tips voor een sterk wachtwoord'](#)



... ik heb wel heel veel toegangsrechten?





Basisprincipe 5



Bereid je voor op incidenten

[Klik hier voor meer informatie](#)



De vraag is niet óf je een digitaal incident meemaakt, maar wanneer. En dan telt elke seconde. Op zo'n moment wil je direct weten wat je moet doen.



Volledig voorkomen kan niet, maar je kunt wél voorbereid zijn. Met een noodplan en beveiligde back-ups beperk je de schade en draait je bedrijf sneller weer door.



Door vooraf scenario's te oefenen, rollen en verantwoordelijkheden vast te leggen en te zorgen voor duidelijke communicatie, vergroot je de kans dat je organisatie snel en effectief reageert. Zo houd je grip, ook in crisissituaties.



Wat kun je doen?

- Maak een incidentresponsplan, dat helpt je in je reactie op een incident.

[Klik hier voor het 'Incidentresponsplan'](#)



- Maak en test regelmatig back-ups (online én offline).



- Zorg voor een papieren belijst met contactgegevens om snel te kunnen handelen bij incidenten.

[Klik hier voor de 'Belijst bij cyberincident'](#)



Vraag & antwoord

Alles wat jij nog meer wilt weten over de Digitale Hulpverlener.

!?

CC

BCC

E-mail versturen met
persoonsgegevens...





Vraag & Antwoord



Digitale veiligheid roept vaak praktische vragen op. Wat doet een Digitale Hulpverlener precies? Hoeveel tijd kost het? En wat heb je ervoor nodig? In dit overzicht vind je de meestgestelde vragen, met duidelijke antwoorden die je direct verder helpen.



Waarom een Digitale Hulpverlener onder eigen medewerkers?

- **Herkenbaar en toegankelijk**

Collega's stappen sneller op een bekende af dan op een externe partij. Dat verlaagt de drempel om vragen te stellen of fouten te melden en juist die snelheid is cruciaal bij incidenten.



- **Inzicht in de organisatie**

Een medewerker kent de processen, systemen en gevoeligheden beter dan een buitenstaander en kan sneller de juiste acties ondernemen.



- **Verantwoordelijkheid dichtbij**

Je laat als werkgever zien dat digitale veiligheid onderdeel van het werk is. Dat vergroot het bewustzijn in het hele team.



- **Kostenbesparend**

Veel situaties kunnen intern opgelost worden. Alleen bij complexe problemen is externe hulp nodig.



Hoe is een DHV'er anders dan de IT-specialist die ik heb ingehuurd voor mijn bedrijf?

De IT-specialist richt zich vaak op de technische inrichting, updates en het oplossen van storingen. De DHV'er richt zich op het gedrag en bewustzijn binnen de organisatie: voorkomen dat collega's in phishing trappen, direct reageren bij een incident, en digitale veiligheid bespreekbaar maken. Ze werken aanvullend op elkaar.



Heb ik speciale apparatuur of software nodig voor een DHV'er?

Nee, een DHV'er kan aan de slag met de middelen die je bedrijf al heeft. Vaak is het voldoende om bestaande apparaten veilig in te stellen (zoals sterke wachtwoorden en automatische updates aanzetten) en gebruik te maken van gratis of goedkope beveiligingstools. Denk bijvoorbeeld aan een wachtwoordmanager, tweestapsverificatie en een virusscanner. Het gaat vooral om kennis en alertheid, niet om dure systemen.





Is een DHV'er alleen interessant voor een groot bedrijf?

Nee, juist kleine bedrijven en zzp'ers lopen een groot risico omdat ze vaak minder middelen hebben om digitale veiligheid te organiseren. Eén oplettende collega (of zelfs de ondernemer zelf) kan al veel schade voorkomen.



Hoeveel tijd kost het om DHV'er te zijn?

Gemiddeld kost het een paar uur per maand. Het gaat vooral om het op de hoogte blijven van ontwikkelingen, signaleren, reageren op vragen, en af en toe een korte update of tip aan collega's. Bij het opstarten of bij een incident kan het tijdelijk wat meer tijd vragen.



Moet een DHV'er altijd bereikbaar zijn?

Nee, het is niet nodig dat een DHV'er 24/7 bereikbaar is. Het is wel handig om binnen het team af te spreken wie het aanspreekpunt is bij een digitaal incident en om een vaste vervanger te hebben voor momenten van afwezigheid. Op die manier is er altijd iemand die weet wat er moet gebeuren als er bijvoorbeeld een verdachte e-mail binnenkomt of een datalek wordt ontdekt.



Hoe leert een DHV'er wat hij of zij moet doen?

De DHV'er volgt een korte training en gebruikt het startpakket als handleiding. Hierin staan duidelijke instructies, praktische tips en checklists voor het herkennen en voorkomen van digitale risico's. Daarnaast kan een DHV'er op de hoogte blijven via de website van bijvoorbeeld het DTC. Door regelmatig korte opfrismomenten in te plannen, blijft de kennis actueel.



[Klik hier voor de 'DTC website'](#)



Wat kost het om een DHV'er aan te wijzen?

Behalve wat tijd voor de DHV-training en het bijhouden van kennis kost het vaak niets extra. De investering zit vooral in het vrijmaken van een paar uur per maand. Deze tijd betaalt zich snel terug, omdat veelvoorkomende problemen intern kunnen worden opgelost en de kans op kostbare incidenten flink wordt verkleind.



Wat als mijn medewerkers weinig digitale kennis hebben?

Juist dan is een DHV'er van grote waarde. De training en het startpakket zijn geschreven in begrijpelijke taal en bevatten concrete voorbeelden. De DHV'er kan collega's stap voor stap meenemen, zodat digitale veiligheid vanzelf een vast onderdeel wordt van de dagelijkse routine. Zelfs kleine verbeteringen, zoals betere wachtwoorden of het herkennen van phishing, maken al een groot verschil.



Bescherm jezelf vandaag al tegen cyber- aanvallen

Met de handige Toolkit
voor de DHV'er





Toolkit



Basisbeveiliging



Bij het aan de slag gaan als DHV'er kun je onderstaande checklists en templates gebruiken:



Digitale Hulpverlener

Template voor het invullen van de gegevens van de Digitale Hulpverlener(s). Twijfel je ergens over? Denk aan vreemde mailtjes en vreemde meldingen op je apparaat. Trek aan de bel. Liever een keer te vaak dan te laat.



Checklist DHV'er

Gebruik deze checklist als je twijfelt of je moet ingrijpen of doorzetten.



Crisiscommunicatie

Handige template met informatie over wie er intern of extern verantwoordelijk is bij incidenten zoals datalekken, systeemuitval, ransomware of verdachte mails.



Applicaties

Template om per applicatie overzicht te houden van eigenaarschap, verantwoordelijken en externe contacten.



Checklist Phishing

Herken signalen van Phishing! Gebruik deze lijst om snel te bepalen of een e-mail verdacht is. Eén keer 'ja' kan al genoeg reden zijn om alert te zijn.



Checklist Accountdiefstal

Gebruik deze checklist om te herkennen of je account is overgenomen en hoe je kunt handelen.



Checklist Ransomware

Een handige lijst om snel te bepalen of je te maken hebt met een ransomware-aanval.



Poster De 5 basis principes van veilig digitaal ondernemen

Poster Even weg van je werkplek PC

Poster Even weg van je werkplek MAC

Poster Weet wie de DHV'ers zijn



Hang de posters op waar iedereen ze ziet en versterk de digitale weerbaarheid.





TEMPLATE

Digitale Hulpverleners

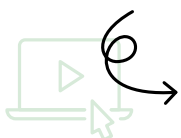


Naam	E-mail	Telefoonnr.	Locatie



Snelle tips: Wat kan jij vandaag al doen?

- Vergrendel je systeem als je even wegloopt.
- Installeer updates zodra je een melding krijgt.
- Negeer geen systeemmeldingen, meld ze bij je digitale hulpverlener.
- Gebruik sterke, unieke wachtwoorden voor álle accounts.
- Zet waar mogelijk Multi-Factor Authenticatie (MFA) aan.
- Behandel je e-mail met aandacht, fouten ontstaan vaak uit routine.
- Klik nooit zomaar op links in e-mails die je niet verwacht.
- Wees alert als je ineens iets "snel" moet regelen.
- Deel je wachtwoord nooit met collega's, ook niet "voor even".



[klik hier voor meer informatie](#)

- Gebruik geen privé-opslagdiensten voor werkbestanden.
- Sluit USB-sticks of onbekende apparaten niet zomaar aan.

Twijfel je? Stel jezelf deze vraag:

"Klinkt dit logisch -of voel ik ergens dat het rammelt?" Toch niet zeker? Check het even met een van de digitale hulpverleners.

In noodgevallen:

Bij echte spoedsituaties (Alles ligt eruit, vreemde schermen, datalek):

- Neem contact op met de Digitale Hulpverlener.
- Bel samen met de Digitale Hulpverlener direct met de IT specialist.
- Geef zo duidelijk mogelijk aan wat is er gebeurd, wanneer en bij wie.





TEMPLATE

Crisiscommunicatie

Wie bel je wanneer het misgaat?
Vul hieronder in wie intern of extern verantwoordelijk is bij incidenten zoals datalekken, systeemuitval, ransomware of verdachte e-mails.

- Print en hang bij werkplekken of afdeling.
- Houd het overzicht actueel, min. 2x per jaar.
- Plaats de lijst ook digitaal op een veilige, toegankelijke plek (intranet of noodmap).

Roi/Verantwoordelijk	Naam	Telefoonnr.	E-mail
Eerste aanspreekpunt IT			
Digitale Hulpverlener (DHV'er)			
Security / Privacy Officer			
Externe IT-partner / Leverancier			
Verantwoordelijke directie / MT-lid			
Communicatie / Persvoorlichting (indien nodig)			
Overig (bijvoorbeeld functioneel beheerder)			

[klik hier voor meer informatie](#)



TEMPLATE

Applicaties

Gebruik deze lijst om per applicatie overzicht te houden van eigenaarschap, verantwoordelijken en externe contacten. Dit helpt bij incidenten, vragen en beveiliging.

- Print uit en sla veilig digitaal op.
- Gebruik bij nieuwe applicaties of updates.
- Actualiseer deze lijst jaarlijks.
- Koppel aan crisis-checklist voor snelle actie incidenten.

Naam applicatie	
Omschrijving	
Type applicatie	
Kritiek voor de organisatie?	
Verwerkt persoonsgegevens?	
Applicatie-eigenaar intern	
Externe leverancier / partij	
Contactpersoon extern	
Toegang op basis van rollen?	
Beheerder (technisch/functioneel)	
Back-up geregeld?	
Laatste controle/beoordeling	
Opmerkingen	



[klik hier voor meer informatie](#)





CHECKLIST

DHV'er



Een vreemd gevoel, een traag systeem of rare meldingen? Volg je instinct en handel alert. Deze checklist helpt je stap voor stap bepalen wat er aan de hand is en wat je direct kunt doen om schade te voorkomen.

Wat is er aan de hand?

- Is er afwijkend gedrag van een apparaat? (bijv. traag of pop-ups)
- Ziet de medewerker bestanden die ineens weg of versleuteld zijn?
- Is er een mail ontvangen met dringende toon, afwijkende link of bijlage?
- Is er sprake van onverwachte inlogverzoeken, SMS-codes of meldingen?
- Is er gevoelige info verzonden aan de verkeerde persoon?

Wat zegt je onderbuikgevoel?

- Voelt dit anders dan normaal?
- Zou je dit door laten gaan als het om klantdata of geld ging?
- Durf je 100% zeker te zeggen dat dit geen risico vormt?

Wat doe je nu?

- Weet je zeker dat er niets is? Koppel terug naar de gebruiker met uitleg.
- Twijfel? Als je het niet 100% vertrouwt, zet het door. Liever een onnodige melding dan een gemiste aanval.
- Is er druk of onrust? Blijf kalm, maak aantekeningen en communiceer helder.

- **Let op afwijkend gedrag van systemen of bestanden**
- **Iets wat vreemd voelt, is dat vaak ook.**
- **Meld direct bij je Digitale Hulpverlener of ICT'er.**

Als er sprake is van een risico, onderneem dan de volgende stappen:

Wel doen:

- Verzamel screenshots of foto's (liefst met eigen telefoon).
- Zet het apparaat in overleg met een beheerder apart of offline (netwerkkabel eruit en wifi verbinding verbreken).
- Noteer alles wat je ziet of hoort.
- Informeer je IT'er zo snel mogelijk.
- Vraag de IT'er om uit voorzorg de betrokken gebruikers uit te loggen.

Niet doen:

- Zelf zomaar bestanden openen, verplaatsen of verwijderen.
- Systeem opnieuw opstarten zonder overleg.
- Onrust zaaien of aannames delen.

[klik hier voor de 'checklist DHV'er'](#)



**DIGITALE
HULP
VERLENER**
EERSTE HULP BIJ HET
VOORKOMEN VAN
DIGITALE ONGELUKKEN





CHECKLIST

Phishing



Phishing is een veelgebruikte manier om bedrijven binnen te dringen. Eén verkeerde klik kan leiden tot datadiefstal, of stilstand. Gebruik deze checklist om Phishing te herken. Twijfel je? Meld het bij de Digitale Hulpverlener. Liever één keer te vaak dan te laat.

Bekijk de afzender

- Komt de e-mail van een publiek domein (zoals @gmail.com) terwijl het lijkt alsof het van een organisatie komt?
- Zit er een spelfout in het domein? (Bijv. "paypl" in plaats van "paypal")
- Wijkt het e-mailadres af van het gebruikelijke adresformaat van de organisatie?



Controleer inhoud en schrijfstijl

- Bevat het bericht grammaticale fouten of rare zinsconstructies?
- Zet de e-mail je onder druk om snel te handelen? (Bijv. "Direct actie nodig" of "Je account wordt geblokkeerd")
- Is de toon of stijl anders dan je van deze afzender gewend bent?



Check links en bijlagen

- Komt de link waar je overheen beweegt niet overeen met de zichtbare linktekst?
- Word je gevraagd om onverwachte bijlagen te downloaden?
- Bevat het bericht vage knoppen zoals "Klik hier" of "Log nu in"?



**DIGITALE
HULP
VERLENER**
EERSTE HULP BIJ HET
VOORKOMEN VAN
DIGITALE ONGELUKKEN



- **Bekijk de afzender.**
- **Check links en bijlagen.**
- **Controleer inhoud en schrijfstijl.**
- **Let op rode vlaggen rond veiligheid.**
- **Wat te doen bij twijfel?**

Let op rode vlaggen rond veiligheid

- Vraagt de e-mail om gevoelige informatie zoals wachtwoorden of bankgegevens?
- Word je gevraagd om normale beveiligingsregels te negeren?
- Wordt er gedreigd met gevolgen als je niet direct handelt?

Wat te doen bij twijfel?

- Klik nergens op en open geen bijlagen.
- Neem contact op met de afzender via een bekend en betrouwbaar kanaal.
- Meld de e-mail bij de digitale hulpverlener.

[klik hier voor meer informatie](#)





CHECKLIST

Accountdiefstal



Accountdiefstal kan iedereen overkomen. Deze checklist helpt je snel te herkennen of jouw account mogelijk is overgenomen. Eén opvallend signaal is vaak al genoeg om actie te ondernemen of melding te doen bij de Digitale Hulpverlener.



Vreemd gedrag in je account?

- Je kunt niet meer inloggen, terwijl je wachtwoord klopt.
- Er zijn e-mails verzonden vanuit jouw naam die jij niet hebt verstuurd.
- Er staan onbekende apparaten of locaties in je inloggeschiedenis.



Onverwachte meldingen?

- Je ontvangt plotseling verificatiecodes of beveiligingsmeldingen.
- Wachtwoordherstelmails die je zelf niet hebt aangevraagd.
- Collega's melden vreemd gedrag of verdachte e-mails uit jouw naam.



Controleer toegang en verbonden accounts

- Kijk welke apparaten of gebruikers toegang hebben tot jouw account.
- Verwijder onbekende of oude inlogsessies.
- Controleer of er koppelingen zijn met onbekende apps of diensten.



- Gebruik voor elk account een uniek, sterk wachtwoord.
- Activeer Multi-Factor Authenticatie.
- Deel nooit wachtwoorden via e-mail of chat.

Versterk je beveiliging

- Gebruik voor elk account een uniek en sterk wachtwoord.
- Activeer Multi-Factor Authenticatie (MFA).
- Werk regelmatig je herstelgegevens bij.

Wat te doen bij twijfel?

- Verander direct je wachtwoord (als je nog kunt inloggen).
- Schakel Multi-Factor Authenticatie (MFA) in.
- Meld het bij je Digitale Hulpverlener; het kan breder spelen dan alleen jouw account.

[klik hier voor meer informatie](#)





CHECKLIST

Ransomware



Ransomware vergrendelt je bestanden en eist losgeld om ze vrij te geven. Met deze checklist herken je snel de signalen van een ransomware aanval. Eén duidelijk teken is vaak al genoeg om direct actie te ondernemen en hulp in te schakelen.

- Gebruik voor elk account een uniek, sterk wachtwoord
- Activeer Multi-Factor Authenticatie
- Deel nooit wachtwoorden via e-mail of chat



Vreemd gedrag van je systeem

- Bestanden openen niet of zijn plotseling versleuteld.
- Je ziet vreemde bestandsextensies (bijv. .locked, .crypt, .encrypted).
- Er verschijnt een pop-up of schermmelding met een losgeldeis.

Beperk de schade

- Isoleer het apparaat: verbreek netwerkverbinding en koppel externe schijven los.
- Meld het incident direct bij je Digitale Hulpverlener of ICT-beheerder.
- Betaal nooit losgeld - er is geen garantie dat je toegang terugkrijgt.



Systeem reageert anders dan normaal?

- Je apparaat is trager of reageert niet meer.
- Je hebt geen toegang meer tot gedeelde mappen of netwerkschijven.
- Er zijn bestanden of snelkoppelingen verdwenen of vervangen.

Wat te doen bij twijfel?

- Sluit je apparaat af of verbreek de verbinding met het netwerk
- Meld het direct bij je Digitale Hulpverlener
- Probeer het niet zelf op te lossen; snel handelen is belangrijk



Voorkom besmetting

- Installeer updates van besturings-systemen en software direct.
- Maak regelmatig back-ups en bewaar die offline of in de cloud.
- Wees alert op phishing-mails en onbekende bijlagen of links.
- Installeer antivirus-software..

[klik hier voor meer informatie](#)



De 5 basis principes van veilig digitaal ondernemen

Tips om het bedrijf weerbaarder te maken tegen cyberrisico's

TIP 1



Breng risico's in kaart

TIP 2



Bevorder veilig gedrag

TIP 3



Bescherm systemen, apparaten en applicaties

TIP 4

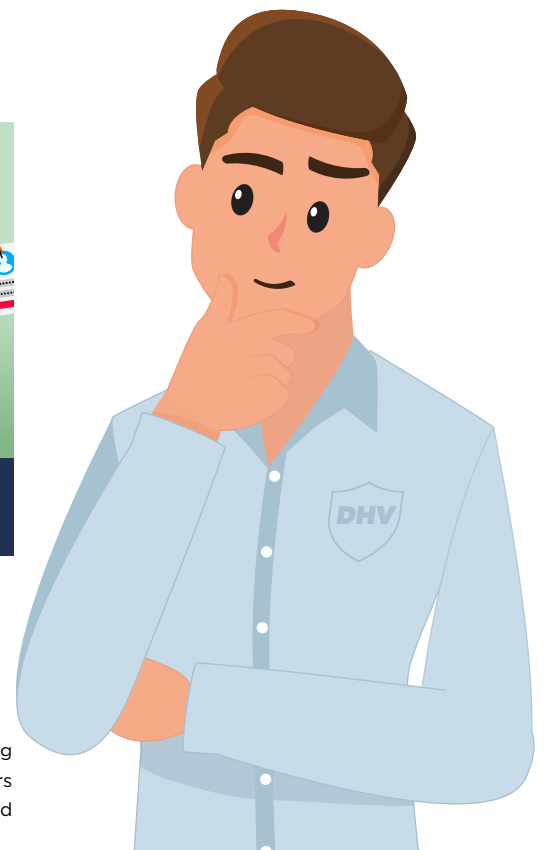


Beheer de toegang

TIP 5



Bereid je voor op incidenten



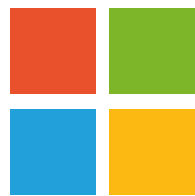
Waarom de 5 basisprincipes?

Om ondernemers te helpen de basisbeveiliging op orde te brengen en te houden. Ondernemers die ze opvolgen, vergroten hun weerbaarheid tegen cyberrisico's.



Even weg van je werkplek?

Neem je (werk)telefoon mee,
leg je dossiers weg en zet je
scherm op slot met:



+L -toets



**DIGITALE
HULP
VERLENER**
EERSTE HULP BIJ HET
VOORKOMEN VAN
DIGITALE ONGELUKKEN

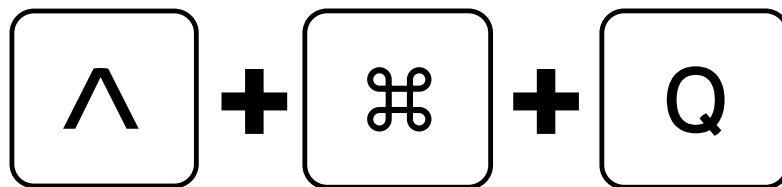
Werk volgens de 5 basisprincipes

om ondernemers te helpen de basisbeveiliging op orde te brengen en te houden. Ondernemers die ze opvolgen, vergroten hun weerbaarheid tegen cyberrisico's.



Even weg van je werkplek?

Neem je (werk)telefoon mee,
leg je dossiers weg en zet je
scherm van je MAC op slot met:



**DIGITALE
HULP
VERLENER**
EERSTE HULP BIJ HET
VOORKOMEN VAN
DIGITALE ONGELUKKEN

Werk volgens de 5 basisprincipes

om ondernemers te helpen de basisbeveiliging op orde te brengen en te houden. Ondernemers die ze opvolgen, vergroten hun weerbaarheid tegen cyberrisico's.



Weet wie de DHV'er is?

Wie van jouw collega's zorgt er voor digitale veiligheid binnen jullie organisatie?



**DIGITALE
HULP
VERLENER**
EERSTE HULP BIJ HET
VOORKOMEN VAN
DIGITALE ONGELUKKEN

Werk volgens de 5 basisprincipes

om ondernemers te helpen de basisbeveiliging op orde te brengen en te houden. Ondernemers die ze opvolgen, vergroten hun weerbaarheid tegen cyberrisico's.

