



# **D**IGITALE **H**ULP **V**ERLENER

EERSTE HULP BIJ HET VOORKOMEN  
VAN DIGITALE ONGELUKKEN

# Wat is een Digitale Hulpverlener?

**DHV'er (Digitale Hulpverlener) [zelfst. naamw.]**

Een DHV'er is iemand binnen de organisatie die collega's helpt bij digitale veiligheid en IT-vragen. Geen IT-specialist, maar wél getraind om risico's te signaleren, helder uitleg te geven en snel te schakelen bij incidenten.

Vergelijk het met een BHV'er, maar dan voor digitale noodgevallen.

Doordat een DHV'er dichtbij de werkvloer staat, wordt de drempel lager om vragen te stellen, twijfels te bespreken of een melding te doen.

Zo groeit bewustzijn van binnenuit dankzij mensen die cyber-veiligheid begrijpelijk maken én het goede voorbeeld geven.

Bekijk de [animatie](#) voor een korte samenvatting.



# Waarom een Digitale Hulpverlener?

Zowel het mkb als particulieren zijn steeds vaker doelwit van cybercrime. Uit het Cybercrimebeeld Nederland 2024 blijkt dat maar liefst 16% van alle Nederlanders slachtoffer werd. Dat zijn 2,3 miljoen slachtoffers.

Specifiek voor het mkb zijn zowel de risico's als de impact van een aanval groot. Onderzoek door Kaspersky toont aan dat maar liefst 77% van het mkb in de afgelopen twee jaar minstens één keer te maken kreeg met cybercrime.

Cybercrime kost het mkb gemiddeld € 270.000 per incident

Bedrijven lopen vooral risico op verstoringen of zelfs bedrijfsuitval, door ransomware.





# Wat doet een Digitale Hulpverlener?

## 1. Stelt gerust

Een DHV'er schrikt niet van digitale meldingen of onzekerheid. Juist op het moment dat iemand stress of twijfel ervaart, zorgt de DHV'er voor rust en overzicht. Geen paniek, wel vertrouwen dat er iets mee gedaan wordt.

## 2. Is empathisch

Een DHV'er luistert zonder meteen in de oplossing te schieten. Hij of zij begrijpt dat digitale problemen verwarrend of zelfs beschamend kunnen zijn, en sluit aan bij wat de ander nodig heeft.

## 3. Oordeelt niet

Of iemand nu per ongeluk op een verkeerde link klikte of een wachtwoord deelde: de DHV'er is er niet om te wijzen, maar om te helpen. Een veilige houding zorgt ervoor dat mensen hun verhaal durven doen.

## 4. Kent de eerste stappen

Een DHV'er weet wat te doen als er iets niet pluis is. Van een vermoeden van phishing tot een laptop die verdacht traag wordt: hij of zij weet welke acties passen bij de situatie, en wanneer het tijd is om op te schalen.

# Wat doet een Digitale Hulpverlener?

## 5. Kent de organisatie

De DHV'er weet hoe de lijnen lopen binnen de organisatie. Wie moet je hebben, hoe meld je iets, welke regels zijn er? Zo wordt hulp geen zoektocht, maar iets dat vlot geregeld wordt.

## 6. Staat in contact met experts

Een DHV'er hoeft niet alles te weten, maar weet wel bij wie je terecht kunt voor specialistische hulp. Zo is er altijd een betrouwbare schakel tussen de werkvloer en de cybersecurity-experts.



# Hulpmiddelen

Bescherm jezelf vandaag al tegen  
cyberaanvallen met de handige Toolkit  
voor de DHV'er





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 alle 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.

# Templates





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](#)



# Templates



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](#)



# Templates





## 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.

- 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.

### 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.

### 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'](#)



# Checklist





## 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"?

- **Bekijk de afzender.**
- **Check links en bijlages.**
- **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 bedreigd 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





## 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.

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

### 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 verzonden.
- Er staan onbekende apparaten of locaties in je inloggeschiedenis.

### 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.

### 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.

[klik hier voor meer informatie](#)



# Checklist





## 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.

### 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.

### 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..

### 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.

### 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

[klik hier voor meer informatie](#)



# Checklist



## Check de (ver)koper

Voordat u met iemand zaken doet via een handelssite of webshop, kunt u hier meldingen over deze (ver)koper zijn gedaan.

Controleer op

bv: oplichter@mail.com; www.website.nl; 0612345

### Welke gegevens kunt u controleren?

- rekeningnummer (gebruik alleen letters en cijfers, bijvoorbeeld NL12BANK)
- E-mailadres (niet van toepassing voor Marktplaats-adressen - lees meer)
- Telefoonnummer (gebruik alleen cijfers, bijvoorbeeld 0201234567)
- De url van een webwinkel (bijvoorbeeld www.eenwinkel.nl)

### Let op!

Aan deze checkfunctie kunt u geen rechten ontleen. Mogelijk heeft u gelezen meldingen zijn tegen de (ver)koper. Of dat de politie (op dit moment) nog geen melding heeft gemaakt van een strafbaar feit. Toch kunt u nog steeds risico lopen bij een verdere transactie. Wees alert en gebruik uw gezonde verstand. Wanneer iets te mooi is om waar te zijn, is het vaak ook zo.

*[Bekijk ook deze tips om veilig te handelen op internet.](#)*

# Tools

<https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html>



## Check je hack

De politie is actief in het bestrijden van cybercriminaliteit. In datasets die in beslag komen soms privégegevens van burgers die door criminelen zijn gebruikt. Om schade te beperken is het belangrijk te checken of uw e-mailadres in datasets voorkomt. Dat kan met onze datasets zijn op dit moment doorzoekbaar:

- 5 april 2023 - [Genesis market](#)
- 29 augustus 2023 - [Qakbot](#)
- januari 2024 - [Bankhelpdeskfraude](#)
- 30 mei 2024 - [Endgame](#)
- 28 januari 2025 - [Heart Blocker](#)

### Hoe werkt het?

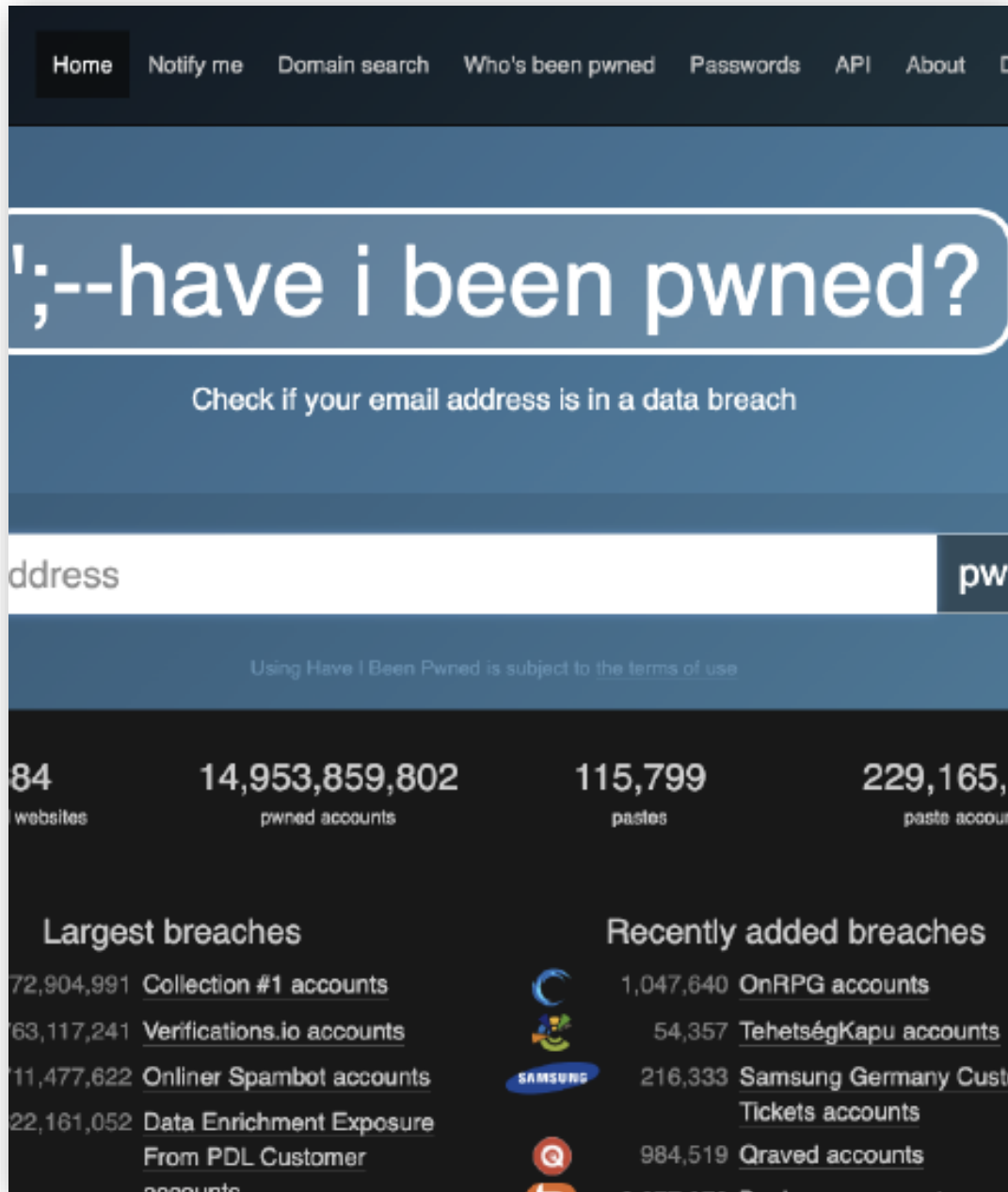
Voer uw e-mailadres in. Als uw e-mailadres voorkomt in een dataset, ontvangt u een e-mail van de politie op dit ingevoerde e-mailadres. Kijk voor de zekerheid ook in de dataset die u heeft ontvangen. Als het e-mailadres niet voorkomt, ontvangt u geen e-mail. Voor meer informatie zie de [FAQ](#).

Geef e-mailadres op

# Tools

<https://www.politie.nl/informatie/checkje-hack.html>

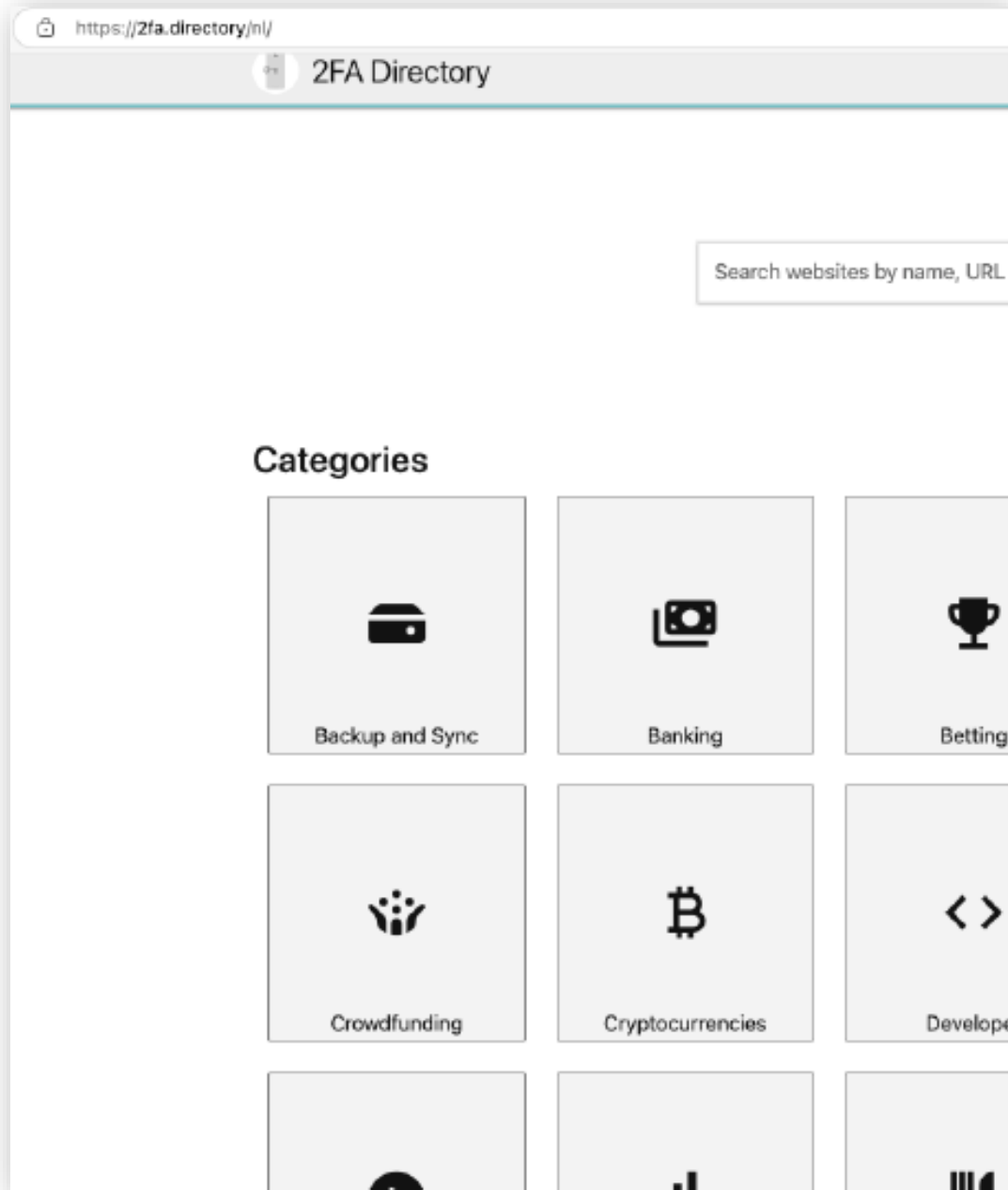




# Tools

<https://haveibeenpwned.com/>





# Tools

<https://2fa.directory/nl/>



# Laat Je Niet Hack Maken



*Bang dat je ex in je Facebook zit? Dat je computer wordt gegijzeld door ransomware? Of dat criminele hackers jouw bankrekening plunderen?*

**inhoud:** wat zijn hackers . de basis . computer . telefoon en tablet . sociale media . chatten en bellen . geavanceerd . tot slot

**verander:** lettertype . groter . kleiner . English 🇺🇸

Deze handleiding legt op een begrijpelijke manier uit hoe je jezelf **beschermt tegen hackers**. Aan de handleiding hebben zes professionele hackers 🧑🏻 meegewerkt.

Laat Je Niet Hack Maken garandeert geen honderd procent veiligheid. Dat bestaat niet op het internet. Wel kun je het hackers en hun virussen zo lastig mogelijk maken door deze tips te volgen.

## Tools

<https://laatjeniethackmaken.nl/>



urlscan.io Home Search Live API Blog Docs Prio

# www.brandaris.it

2a03:9700:8000::7:79 Public Scan

Submitted URL: <http://www.brandaris.it/>  
 Effective URL: <https://www.brandaris.it/nl/>  
 Submission: On May 08 via manual (May 8th 2025, 2:54:11 pm UTC) from – Scanned from

Summary HTTP 32 Redirects Links 1 Behaviour Indicators Similar DOM

## Summary

This website contacted 4 IPs in 3 countries across 3 domains to perform 32 HTTP transactions. The main IP is 2a03:9700:8000::7:79, located in Netherlands and belongs to PREVIDER-AS Previder B.V., NL. The main domain is www.brandaris.it. TLS certificate: Issued by R11 on March 17th 2025. Valid for: 3 months.

[www.brandaris.it](#) scanned 5 times on urlscan.io [Show Scans](#)

urlscan.io Verdict: No classification

### Live information

Google Safe Browsing: No classification for www.brandaris.it  
 Current DNS A record: 31.7.7.79 (AS20847 - PREVIDER-AS Previder B.V., NL)

### Domain & IP information

IP/ASNs	IP Detail	Domains	Domain Tree	Links	Certs	Frames
29	2a03:9700:8000::7:79					
1	2a00:1450:4001:829::2008					
1	54.183.0.47					
2	2001:4860:4802:32::36					
32				4		

# Tools

<https://urlscan.io/>



# Aan de slag

met 3 scenarios



# Aan de slag

## Iedereen kiest een template

Ben je met collega's van dezelfde organisatie?  
→ Werk samen óf kies ieder een andere template.

### Je kunt kiezen uit:

3 Templates: applicaties, crisiscommunicatie, DHV'er

4 Checklists: Phishing, Ransomware, Accountdiefstal, DHV'er

## Werktijd: ~30 minuten

Gebruik de tijd om écht iets in te vullen. Het hoeft niet perfect, wél bruikbaar.

## Daarna bespreken we:

- Wat lukte goed?
- Wat was lastig?
- Wat neem je mee naar je organisatie?

# Scenario 1

Een collega kan ineens niet meer inloggen.

Ze krijgt meldingen dat haar wachtwoord is gewijzigd, terwijl ze niets heeft gedaan.

Er blijken ook e-mails te zijn verzonden vanuit haar account naar externe contacten.



## Scenario 2

Een medewerker ontvangt een e-mail van “Microsoft Support” met het bericht dat haar wachtwoord verloopt.

Ze wordt gevraagd om snel in te loggen via een link. De stijl lijkt net echt.

Een collega twijfelt: moet ze klikken of niet?



# Scenario 3

Op dinsdagochtend merkt iemand dat zijn bestanden ineens niet meer openen.

Overal staan bestanden met de extensie \*.encrypted en er verschijnt een scherm met “Uw bestanden zijn versleuteld – betaal binnen 48 uur.”

Netwerkschijven zijn niet meer bereikbaar.



# Samenvattend

## Check regelmatig je checklisten

Zorg dat je de signalen van phishing, ransomware en accountdiefstal herkent. Eén keer “ja” is al reden om actie te ondernemen.

## Werk je crisiskaart en applicatielijst bij

Zorg dat je weet wie je moet bellen bij incidenten. En houd bij welke applicaties gebruikt worden, met eigenaars en contactpersonen.

## Twijfel je? Handel meteen

Bij twijfel: wacht niet. Schakel hulp in. Beter één keer te vaak dan te laat.

## Plan een vaste controle-moment

Minstens twee keer per jaar: check de lijsten, bespreek opvallende signalen, en update waar nodig.

## Maak veilig melden makkelijk

Hang de checklisten zichtbaar op en zorg dat collega's weten waar ze terecht kunnen.

**BEDANKT**



**DIGITALE  
HULP  
VERLENER**

EERSTE HULP BIJ HET  
VOORKOMEN VAN  
DIGITALE ONGELUKKEN