TOOLKIT

CYBERVEILIG GEDRAG IN MKB

Aanpak om medewerkers te stimuleren verdachte e-mails intern te melden

Aan de slag!

Cyberveilig gedrag in MKB

WEGWIJZER

Een van de grootste kwetsbaarheden voor cyberveiligheid in het mkb is het gedrag van medewerkers: met één verkeerde muisklik kan het bedrijf al geraakt worden door cybercriminelen.
In 2020 heeft MKB Nederland een effectieve aanpak laten ontwikkelen door Inspire to Act en de Haagse Hogeschool om medewerkers te stimuleren verdachte e-mails intern te melden. De gedragsaanpak is getest binnen het mkb-metaal. Daar zorgde de gedragsinterventie VALSE E-MAIL? MELD HET VIA DE MELDKNOP ervoor dat medewerkers verdachte e-mails 10x vaker intern melden. Ook werd er nauwelijks meer geklikt op een link in verdachte e-mails. Op basis van de proeftuin is deze Toolkit ontwikkeld. Met behulp van de Toolkit kunnen mkb-ers eenvoudig zelf aan de slag om medewerkers in hun bedrijf te stimuleren verdachte e-mails intern te melden. De gedragsaanpak en de Toolkit zijn gefinancierd door het ministerie van Justitie en Veiligheid.

Proeftuin VALSE E-MAIL? MELD HET VIA DE MELDKNOP

Benieuwd naar het volledige rapport van de proeftuin? Kijk dan hier. Iets minder tijd? De essentie leest u in deze samenvatting.

Aan de slag!

Direct aan de slag? Het stappenplan geeft houvast om op de juiste wijze de gedragsaanpak toe te passen in uw bedrijf. In het interventiepakket staat een duidelijk overzicht van alle onderdelen van de gedragsinterventie **VALSE E-MAIL? MELD HET VIA DE MELDKNOP.** In het investeringsoverzicht staat een indicatie van de kosten.

Onderdelen gedragsinterventie

Deze gedragsinterventie bestaat uit de volgende onderdelen:

1. **Intern cybermeldpunt**
2. **Meldknop in e-mailprogramma**
3. **Tips voor leidinggevenden**
4. **Campagneposter**
5. **Flyer**
6. **3D sticker**

Op de volgende pagina's worden alle onderdelen toegelicht.

Hoofdbeeld gedragsinterventie

Als campagnebeeld is gekozen voor een vis en een valse haai. Met de vis spelen we in op de associatie met de naam phishing. Een metafoor dat vaker gebruikt wordt in deze context en daardoor zorgt voor herkenning. De valse haai staat symbool voor gehaaide cybercriminelen.

Campagnematerialen

Het interventiepakket bevat verschillende campagnematerialen. Alle materialen die in deze Toolkit beschikbaar worden gesteld, zijn vrij te gebruiken. Hier vindt u de downloads van:

Campagneposter
Poster A2 > Ophangen in het bedrijf
Flyer
Digitaal gepersonaliseerd > Ophangen in het bedrijf en versturen per e-mail
3D sticker
Bubbel sticker > voor op beeldschermen

Stappenplan

Gedragsaanpak
VALSE E-MAIL? MELD HET VIA DE MELDKNOP

Stap 1.
Voorbereiding treffen

- Instellen intern cybermeldpunt
- Installeren meldknop in e-mailprogramma

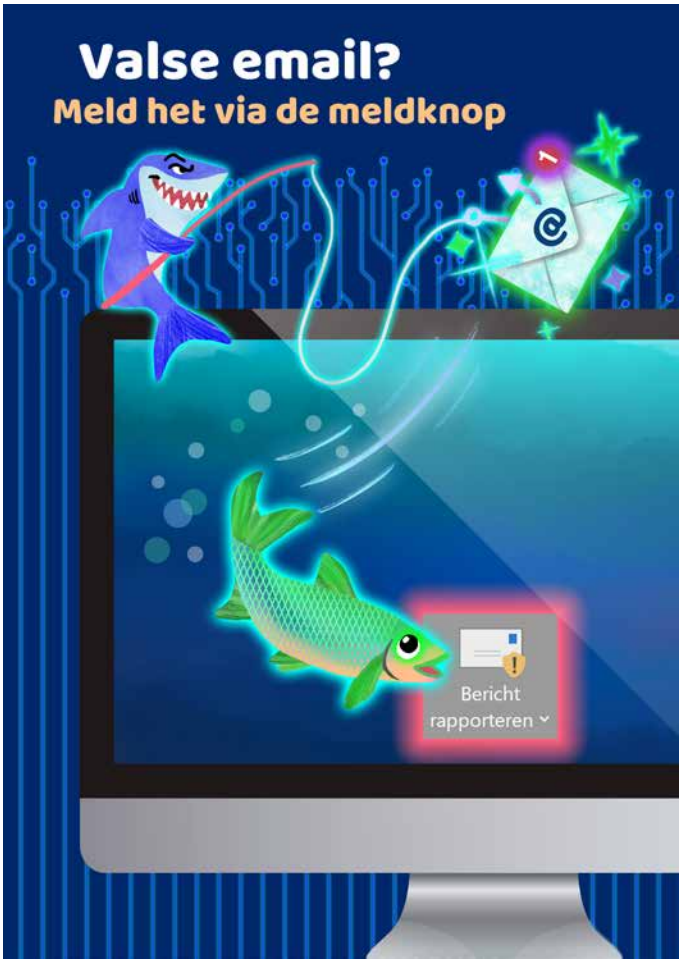
Stap 2.
Tips aan leidinggeven sturen

- Tips voor leidinggevenden bespreken of mailen naar leidinggevenden

Stap 3.
Campagnematerialen toepassen in bedrijf

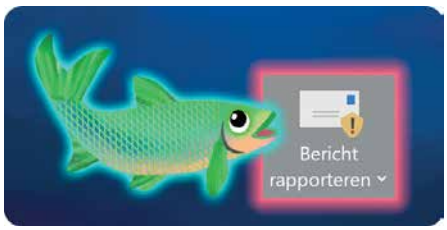
- Campagneposters ophangen in bedrijf
- 3D sticker aanbrengen op alle beeldschermen
- Flyers ophangen in bedrijf en mailen naar alle medewerkers

Interventiepakket
VALSE E-MAIL? MELD HET VIA DE MELDKNOP



A2 Campagneposter

A3 Flyer koffieautomaat



3D-Sticker voor op beeldscherm

Digitale Flyer per email versturen

1. Intern cybermeldpunt

Wat is het?
Een e-mailadres waar medewerkers verdachte zaken rondom cyberveiligheid kunnen melden; bij voorkeur een makkelijk te onthouden e-mailadres, bijvoorbeeld: cybermeldpunt@bedrijfsnaam.nl.

Waar toepassen?
Gehele bedrijf.

Wat doet het?
Met een intern cybermeldpunt geeft een bedrijf aan het belangrijk te vinden dat er meldingen gedaan worden. Tevens maakt een intern cybermeldpunt het voor medewerkers duidelijker en makkelijker om verdachte zaken intern te melden. Dit stimuleert het doorgeven van verdachte zaken rondom cyberveiligheid.

Let op!
- Het is belangrijk dat medewerkers weten dat er een intern cybermeldpunt is en wat het e-mailadres hiervan is. Plaats een bericht hierover op het intranet met een oproep om verdachte zaken te melden bij het intern cybermeldpunt. Zet ook het emailadres van het meldpunt erbij. Stuur tevens een e-mail naar alle medewerkers met de oproep tot melden en het e-mailadres van het meldpunt. Idealiter wordt de oproep en het e-mailadres ook besproken in het teamoverleg.
- Het is belangrijk dat alle meldingen die binnenkomen bij het interne meldpunt worden opgevolgd. Dit kan als volgt:

  - **Stuur bij elke melding een ontvangst-bevestiging naar de melder (zie voorbeeld-ontvangstbevestiging hiernaast).**
  - **Beoordeel of er extra actie noodzakelijk is.**

Als de verdachte e-mail een potentieel risico is, stuur dan de e-mail door voor nader onderzoek; bijvoorbeeld naar een (externe) ICT-deskundige, ICT-leverancier of Fraudehelpdesk.
Ook kan het verstandig zijn om een intranetbericht te plaatsen om andere medewerkers te waarschuwen voor de mail. Overleg of dit nodig is met de ICT-deskundige, ICT-leverancier of Fraudehelpdesk.

VOORBEELD
AANKONDIGING CYBERMELDPUNT

Intern cybermeldpunt

Omdat wij bij [bedrijfsnaam] cyberveiligheid heel belangrijk vinden, hebben wij een intern cybermeldpunt ingesteld: cybermeldpunt@bedrijfsnaam.nl.
Stuur verdachte e-mails altijd door naar het cybermeldpunt. Daar wordt onderzocht of verdere actie noodzakelijk is.

VOORBEELD
ONTVANGSTBEVESTIGING MELDING BIJ MELDPUNT

Veel dank voor je melding. Wij gaan de melding beoordelen en ondernemen actie indien nodig. Dankzij jouw melding kunnen we ons bedrijf beter tegen cybercriminaliteit beschermen. Graag verdachte berichten blijven melden!

Met vriendelijke groet,

2. Meldknop in e-mailprogramma

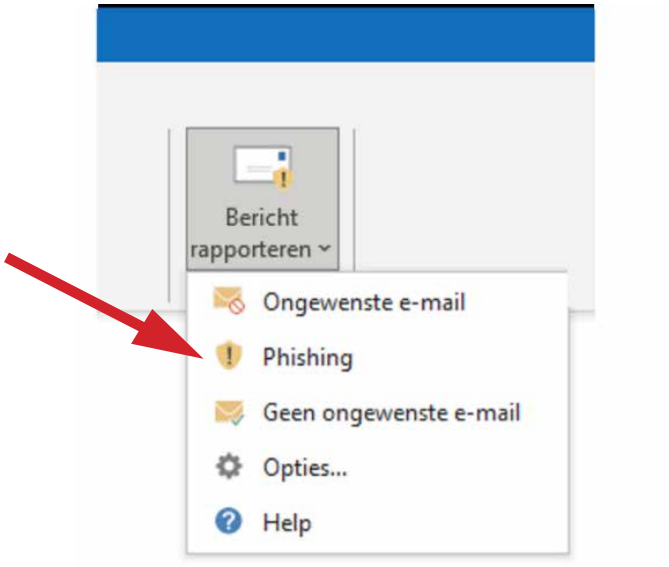
Download hier het installatieplan

Hiermee kunnen bedrijven zelf de meldknop installeren.

Wat is het?
Een button/knop in het e-mailprogramma.

Waar toepassen?
In het e-mailprogramma van alle medewerkers (op afstand in te stellen).

Wat doet het?
De meldknop maakt het voor medewerkers heel eenvoudig en laagdrempelig om verdachte e-mails te melden bij het intern cybermeldpunt. Als een medewerker op de meldknop klikt, verschijnt er een pop-up. De medewerker selecteert phishing en de e-mail wordt op een veilige manier doorgestuurd naar het interne meldpunt. De e-mail wordt daarna in het e-mailprogramma verwijderd.



Let op!
Het installatieplan is geschreven voor installatie van de meldknop in:
- Outlook on the web
- Outlook 2013 SP1 or later
- Outlook 2016 for Mac
- Outlook included with Microsoft 365 apps for Enterprise
- Outlook app for iOS and Android

Komt u er niet uit of heeft u een ander e-mailprogramma, informeer dan bij uw (externe) ICT-deskundige of ICT-leverancier.

3. Tips voor leidinggeven

Wat is het?
Handreiking met tips voor leidinggevenden

Waar toepassen?
Bespreken met leidinggevenden of versturen via e-mail.

Wat doet het?
Deze tips helpen leidinggevenden om het onderwerp cyberveiligheid bespreekbaar te maken in het team en stimuleren gedragsverandering bij de medewerkers. Door het gesprek over cyberveiligheid aan te gaan met het team en aan te geven dat cyberveilig gedrag belangrijk is, wordt de sociale norm versterkt.

Tips voor leidinggevenden

Om ons bedrijf tegen cybercriminaliteit te beschermen is het belangrijk om over cyberveiligheid te praten met onze medewerkers. Hieronder staan een paar tips die stimuleren dat medewerkers alert zijn en actie ondernemen als zij verdachte berichten ontvangen.

- Benadruk regelmatig in teamoverleggen dat je het belangrijk vindt om het bedrijf te beschermen tegen cybercriminaliteit. Geef aan dat medewerkers hierbij kunnen helpen door verdachte berichten te melden bij het interne cybermeldpunt.

- Vertel het aan medewerkers als er veel gemeld wordt bij het cybermeldpunt. Dit stimuleert andere medewerkers om ook verdachte berichten te gaan melden.

- Geef aan dat als medewerkers op een link hebben geklikt in een verdachte mail, het heel belangrijk is om het zo snel mogelijk te melden bij het interne cybermeldpunt. Gelukkig is het niet altijd heel ernstig.

- Sta open voor vragen van medewerkers over cyberveiligheid. Het geeft niet als je het antwoord niet weet. Verwijs medewerkers met vragen door naar het interne cybermeldpunt.

4. Campagneposter

Download hier de bestanden

Deze zijn vrij te gebruiken.

Wat is het?

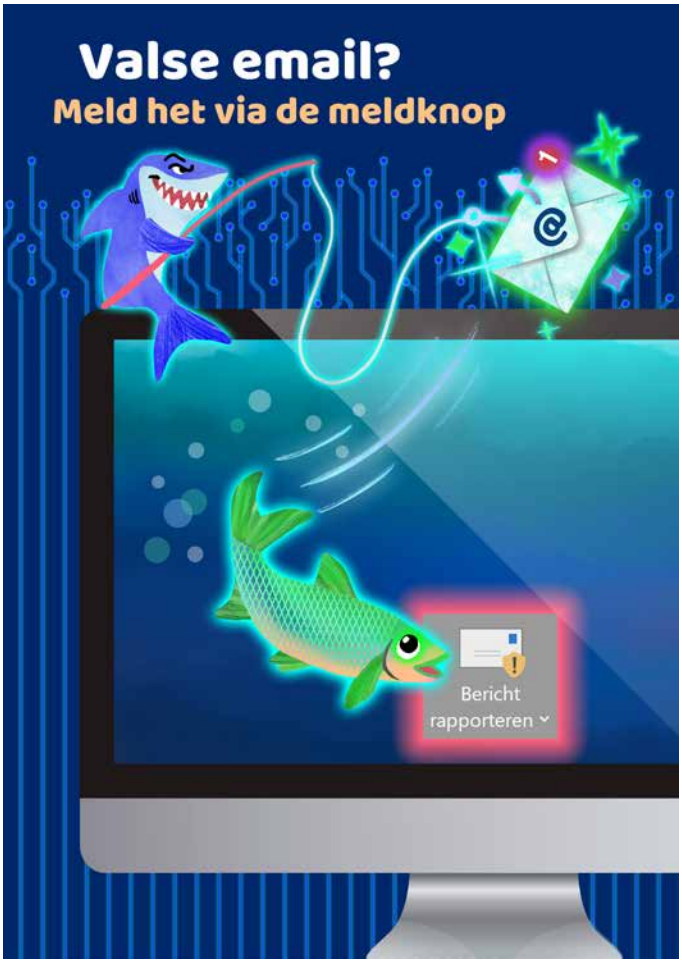
Poster, formaat kan afgestemd worden op beschikbare ruimte.

Waar toepassen?

De campagneposters kunt u het beste ophangen op plekken waar ze goed zichtbaar zijn. Denk hierbij aan: productieruimte, kantoorruimte, omkleedruimte, kantine, gang/hal, entree, parkeerruimte, etc.

Wat doet het?

Het versterkt de zichtbaarheid van de campagne, zorgt voor bewustwording en herinnert aan en motiveert tot het gewenste gedrag, namelijk verdachte e-mails melden bij het interne cybermeldpunt.
Op de poster staat duidelijk handelingsperspectief (melden van valse email via de meldknop). Daarnaast staat de meldknop afgebeeld op precies dezelfde manier zoals de meldknop in het e-mailprogramma eruit ziet. Dit zorgt voor herkenning en stimuleert gewenst gedrag. Visueel laat de poster het gewenste gedrag zien. De valse haai probeert met een valse e-mail naar gegevens te vissen; de vis stuurt de ongelezen mail via de meldknop direct door naar het interne cybermeldpunt. Doordat tekst en beeld overeenkomen, wordt het doelgedrag versterkt.



Campagneposter

5. Flyer

Download hier de bestanden

Deze zijn vrij te gebruiken.

Wat is het?
(digitale) Flyer, formaat kan afgestemd worden op beschikbare ruimte.

Waar toepassen?
Flyers kunt u het beste ophangen op plekken waar mensen tijd hebben om te lezen. Vaak is dit op plekken waar mensen moeten wachten. Denk hierbij aan: koffieautomaat, kopieerruimte, lift, kantine, toiletten, omkleedruimte, kantoorruimte, etc.
Digitale flyers kunnen via mail verstuurd worden naar alle medewerkers.

Wat doet het?
De flyer geeft medewerkers extra informatie (kennis en bewustwording) en handelingsperspectief over wat ze kunnen doen als ze een valse e-mail ontvangen. De flyer herinnert aan en motiveert tot het gewenste gedrag door o.a. in te spelen op geanticipeerde spijt en het benadrukken van de sociale norm.

Flyer algemeen

6. 3D-Sticker

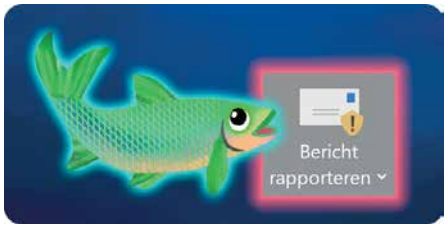
Download hier de bestanden

Deze zijn vrij te gebruiken.

Wat is het?
3d-sticker

Waar toepassen?
3d-Stickers kunt u aanbrengen op alle beeldschermen in het bedrijf.

Wat doet het?
Het herinnert aan het gewenst gedrag (verdachte e-mail melden bij het interne cybermeldpunt) op de plek waar je het gewenste gedrag wilt zien (bij de computer).



3D-sticker

Investeringsoverzicht

In onderstaand overzicht staat een indicatie van de benodigde materialen per bedrijf en een kosten-indicatie (exclusief BTW). Deze inschatting is gemaakt op basis van onze ervaring in mkb-metaal. Het is mogelijk dat er in uw bedrijf juist meer of minder materialen nodig zijn. Dit is afhankelijk van de inrichting en de aanwezige faciliteiten in het bedrijfspand, zoals kantoorruimte, omkleedruimte, koffieautomaten, kopieerruimte, lift en toiletten.

Tip! Bestel het materiaal voor meerdere vestigingen tegelijk; zo wordt de stukprijs goedkoper.

Materialen	Aantal stuks	Kosten (excl. btw)
Campagneposters (a2-formaat)		€50–65,-
• < 10 medewerkers	5	
• 10-50 medewerkers	10	
• > 50 medewerkers	15-20	
Flyers (a3-formaat)		€25–35,-
• < 10 medewerkers	5	
• 10-50 medewerkers	10	
• > 50 medewerkers	15-20	
3d-Stickers (50x25mm)		€50–75,-
• Voor elk beeldscherm	10-100	

Het instellen van het cybermeldpunt, het installeren van de meldknop en het bespreken/versturen van de tips voor leidinggevenden kunnen intern uitgevoerd worden. De kosten hiervan bestaan uit bestede uren. Indien ondersteuning van een externe partij nodig is, adviseren wij gebruik te maken van bestaande contracten met ICT-partijen.