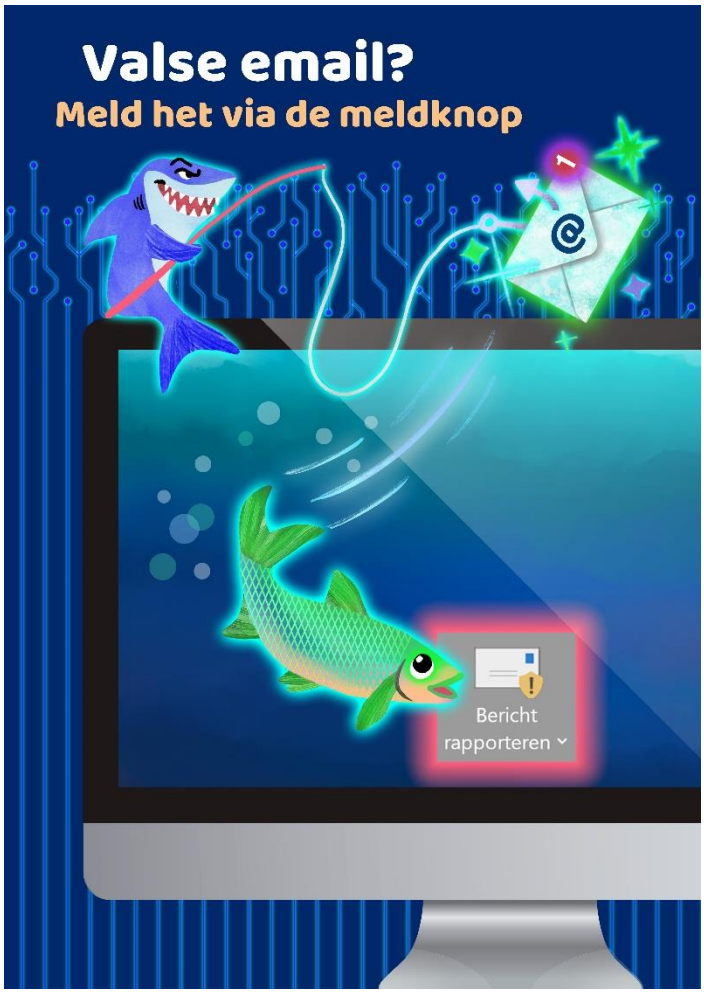
HUMAN FACTORS IN CYBERSECURITY IN MKB-METAAL
Rapportage pilot Cyberveilig Gedrag

Inspire to act
Voor het effectief veranderen van gedrag

DE HAAGSE HOGESCHOOL



november 2021

Voor het effectief veranderen van gedrag
www.inspiretoact.nl
info@inspiretoact.nl
06 29 86 07 89
KVK 62233890

Uitgevoerd in opdracht van:
MKB Nederland

Gesubsidieerd door:
Ministerie van Justitie en Veiligheid

Uitgevoerd door:

Inspire to Act	Karin Bongers
Haagse Hogeschool	Rutger Leukfeldt
	Rick van der Kleij
	Michelle Ancher
	Luuk Bekkers
	Justin Zandvliet

Begeleidingscommissie:

MKB Nederland	Nicole Mallens
Digital Trust Center	Jacco van der Kolk
Ministerie van Justitie en Veiligheid	Michiel Hillenaar
	Stefan Scheeringa

Met medewerking van:

Koninklijke Metaalunie	Rard Metz
	Frans van der Brugh

Inhoud

Samenvatting

Aanleiding

Deze rapportage is onderdeel van het project Human Factors in Cybersecurity in mkb-metaal. Dit project wordt uitgevoerd door Inspire to Act in samenwerking met de Haagse Hogeschool, in opdracht van MKB-Nederland. Het project wordt gefinancierd door het ministerie van Justitie en Veiligheid. In deze rapportage beschrijven we de pilot die is uitgevoerd om medewerkers in het mkb te motiveren preventieve beschermingsmaatregelen te treffen om het risico op slachtofferschap van cybercriminaliteit te verkleinen. Hierbij richten we ons op het gedrag van de medewerkers in mkb-metaal. Wij hebben preventieve beschermingsmaatregelen geconcretiseerd als: 1) Medewerkers melden verdachte e-mails bij een intern meldpunt; en 2) Medewerkers klikken niet op een link in verdachte e-mails.

Gedragsinterventie *VALSE E-MAIL? MELD HET VIA DE MELDKNOP*

Op basis van de bevindingen in de analysefase hebben we de gedragsinterventie *VALSE E-MAIL? MELD HET VIA DE MELDKNOP* ontwikkeld. Deze gedragsinterventie bestaat uit de volgende onderdelen:

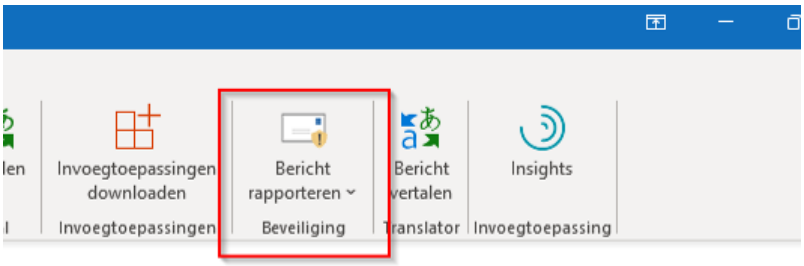
1. intern cybermeldpunt
2. meldknop in e-mailprogramma
3. grote poster
4. kleine poster/ digitale flyer
5. 3D sticker
6. handreiking voor leidinggevenden

Intern cybermeldpunt

Als onderdeel van de gedragsinterventie hebben de bedrijven een intern cybermeldpunt ingesteld. Dit is een e-mailadres (bv. cybermeldpunt@inspiretoact.nl) waar medewerkers intern melding kunnen doen van verdachte zaken met betrekking tot cyberveiligheid.

Meldknop in e-mailprogramma

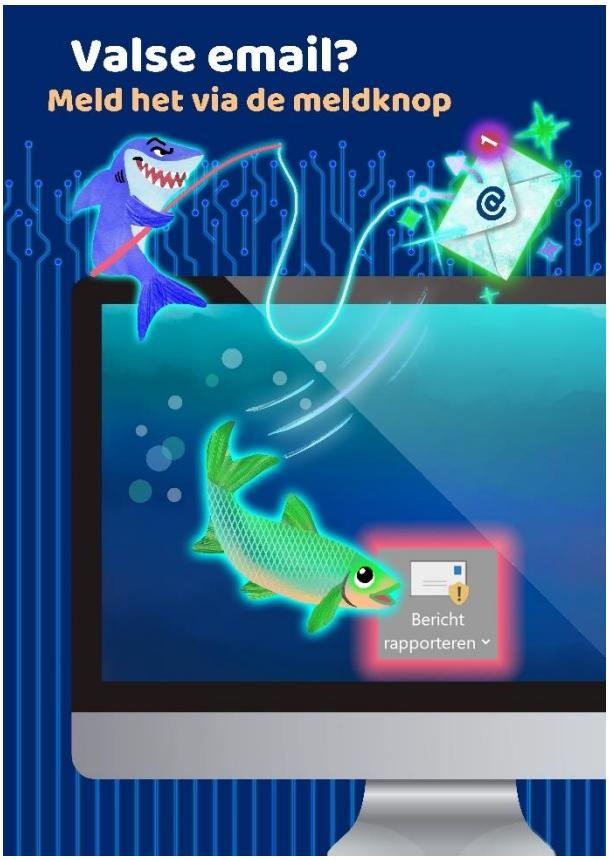
Bedrijven hebben een meldknop geïnstalleerd in hun e-mailprogramma. Met de meldknop kunnen medewerkers heel eenvoudig een verdachte e-mail intern melden.



Meldknop

Grote poster

De grote poster (a2 formaat) dient als reminder voor het gewenste gedrag en zorgt voor bewustwording. De grote posters zijn opgehangen op plekken in het bedrijf waar ze goed zichtbaar zijn. Denk hierbij aan: productieruimte, kantoorruimte, omkleedruimte, kantine, gang/hal, entree, parkeerruimte, etc.



Grote poster

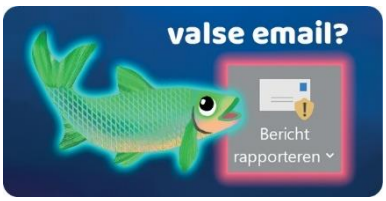
Kleine poster/digitale flyer

Kleine poster/ digitale flyer

De kleine poster (a3-formaat) geeft medewerkers extra informatie en handelingsperspectief over wat ze kunnen doen als ze een valse e-mail ontvangen. De kleine posters zijn opgehangen op plekken waar mensen tijd hebben om te lezen. Denk hierbij aan: koffieautomaat, kopieerruimte, lift, kantine, toiletten, omkleedruimte, kantoorruimte, etc. Daarnaast is de kleine poster ook als digitale flyer naar alle medewerkers toegestuurd.

3D sticker

De 3D sticker is een prompt (of reminder) voor gewenst gedrag. De stickers zijn op de beeldschermen van de computers geplakt en herinneren medewerkers op het juiste moment aan het gewenste gedrag: melden van valse e-mail via de meldknop.



3D sticker

Handreiking voor leidinggevenden

Om cyberveilig gedrag te stimuleren in een bedrijf, is het belangrijk dat zowel leidinggevenden als collega's onderling met elkaar in gesprek gaan hierover. En dat ze aangeven dat ze cyberveilig gedrag belangrijk vinden. Om het gesprek over cyberveiligheid te stimuleren in bedrijven, hebben we een handreiking opgesteld voor leidinggevenden.

Gedragstechnieken

	Intern cyber-meldpunt	Meldknop	Grote poster	Kleine poster/ digitale flyer	3D sticker	Handreiking voor leiding-gevenden
Vereenvoudigen	✓	✓				✓
Prompting		✓	✓	✓	✓	
Handelingsperspectief	✓	✓	✓	✓	✓	
Geanticipeerde spijt				✓		
Kennis en bewustwording				✓		✓
Sociale normen				✓		✓
Urgentie creëren				✓		✓
Inspelen op emoties				✓		
Altercasting				✓		

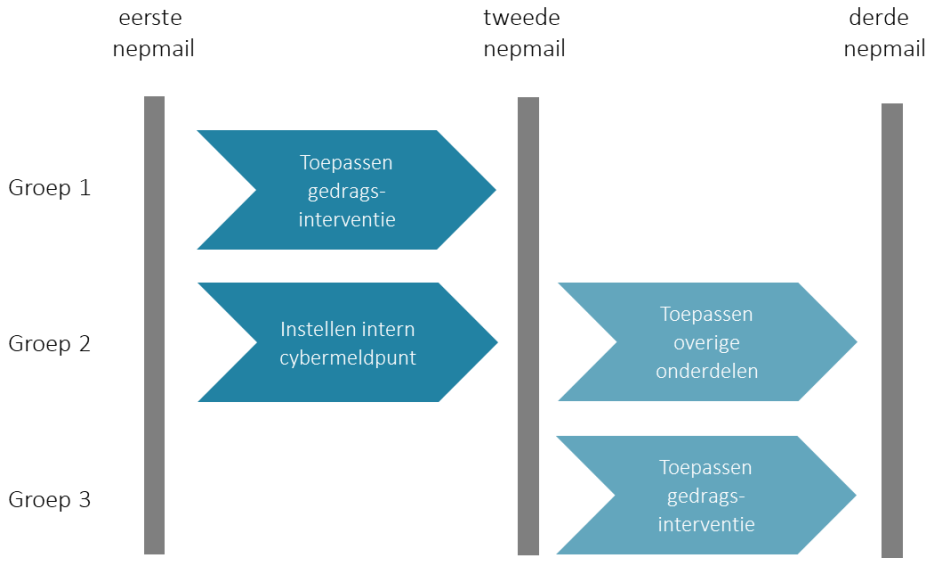
Pilotopzet

Deelnemende bedrijven

Aan de pilot hebben 13 mkb-metaalbedrijven deelgenomen. Deze bedrijven zijn gevestigd door het gehele land. Het aantal medewerkers met een e-mailadres varieert van 10 tot 85, met een totaal aan 410 emailadressen.

Onderzoeksdesign

De pilot bestaat uit drie condities: gehele interventie; intern cybermeldpunt; en geen interventie (controle). Om het meld- en klikgedrag te kunnen meten, hebben we drie nepmails verstuurd. Hieronder staat het onderzoeksdesign schematisch weergegeven.



Onderzoeksdesign

Procedure

In overleg met de bedrijven is de eerste nepmail in week 34 of week 35 verstuurd. Bedrijven in groep 1 pasten daarna de gehele gedragsinterventie toe; bedrijven in groep 2 stelden alleen het interne cybermeldpunt in; en bedrijven in groep 3 pasten geen interventie toe.
Nadat de gehele gedragsinterventie was toegepast (groep 1) of het intern cybermeldpunt geïnstalleerd was (groep 2), werd de tweede nepmail naar alle bedrijven gestuurd (week 38 t/m week 42).
Bij de bedrijven in groep 2 zijn na de tweede nepmail de overige onderdelen van de gedragsinterventie toegepast. Bij de bedrijven in groep 3 zijn alle interventieonderdelen in een keer toegepast, nadat de tweede nepmail is verstuurd. Bij de bedrijven in groep 1 hebben we in deze stap niets gedaan.
Daarna werd de derde nepmail naar alle bedrijven gestuurd (week 44 t/m week 47). Na afloop van de pilot hebben we belevingsonderzoek gedaan bij medewerkers van de deelnemende bedrijven. Hiervoor hebben we de bedrijven een link gestuurd naar een online vragenlijst. De bedrijven hebben deze link intern doorgezet naar alle medewerkers.

Afhankelijke variabele

We hebben twee afhankelijke variabelen: 1). Het aantal keren dat de nepmails intern gemeld worden; en 2) het aantal keren dat er wordt geklikt op de link in de nepmails.

Hypothesen

Aantal interne meldingen

Aantal interne meldingen: gehele gedragsinterventie (groep 1) > intern cybermeldpunt (groep 2) > geen interventie (groep 3).

Aantal keren geklikt

Aantal kliks: gehele gedragsinterventie (groep 1) < intern cybermeldpunt (groep 2) < geen interventie (groep 3).

Langere termijn effect

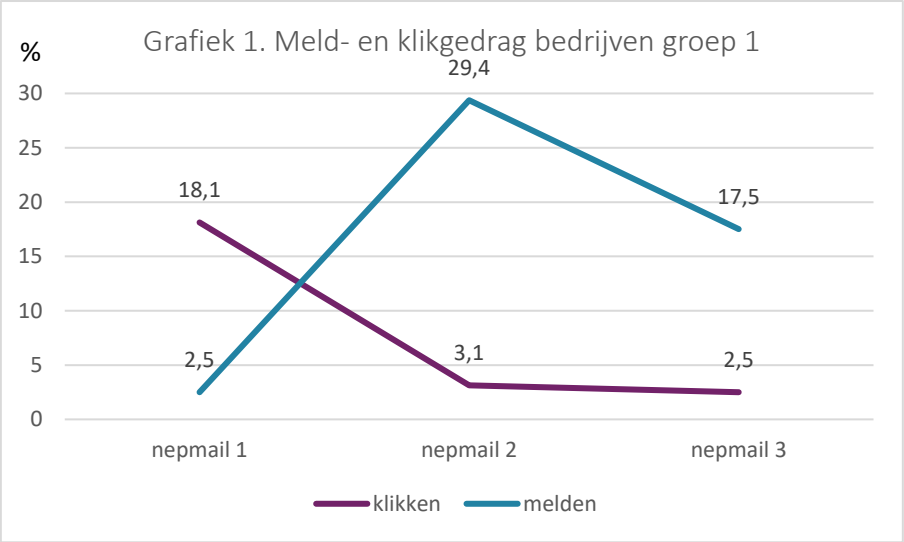
We verwachten dat de gedragsinterventie ook over een langere periode effectief blijft.

Resultaten

Door technische oorzaken ontbreken veel data in groep 2 (intern cybermeldpunt) en is het niet mogelijk om iets te zeggen over de effectiviteit van alleen het instellen van een intern cybermeldpunt. Helaas ontbreken er vanwege technische oorzaken ook veel data in groep 3 (contolegroep). Hierdoor is het niet mogelijk om deze bedrijven als controlegroep te gebruiken.
In groep 1 (gehele interventie) zijn wel voldoende data beschikbaar. De volgende analyses gaan alleen over de bedrijven in groep 1.

Meld- en klikgedrag

Er worden meer interne meldingen gemaakt van nepmail 2 (1-2 weken na interventie) dan van nepmail 1 (voorafgaand aan interventie). Het aantal meldingen van nepmail 3 (6-7 weken na interventie) zit tussen het aantal meldingen van nepmail 1 en 2 in, zie onderstaande grafiek. Het verschil in percentage kliks tussen de drie nepmails is niet significant.



Belevingsonderzoek

Positief over interventie-onderdelen

In totaal hebben 82 medewerkers van 8 bedrijven de belevingsvragenlijst ingevuld. Respondenten zijn overwegend positief over de interventie-onderdelen. Ze vinden zowel de grote als de kleine poster duidelijk en overzichtelijk. Ook vinden respondenten de informatie op de kleine poster handig en goed uitgelegd. Over de 3D sticker zijn de meningen wat meer verdeeld. Respondenten vinden het positief, omdat de sticker hen herinnert aan het gewenste gedrag en het zorgt voor bewustwording. Ook de kwinkslag met phishing wordt positief beoordeeld. Een aantal respondenten is minder positief en geeft aan dat de sticker niet zoveel zegt en niet zo goed opvalt. Over de meldknop zijn respondenten heel positief. Ze vinden de meldknop duidelijk en het maakt het makkelijker om intern meldingen te doen.

Vaker besproken in teamoverleg

Driekwart van de respondenten geeft aan dat er sinds de interventie vaker over cyberveiligheid wordt gesproken in het teamoverleg dan daarvoor.

Meer Alert

Bijna 80% van de respondenten aan dat ze door de gedragsinterventie beter zijn gaan opletten op valse e-mails.

Veel meldingen via de meldknop

Driekwart van de respondenten geeft aan dat ze in de afgelopen twee maanden daadwerkelijk een valse e-mail (of nepmail) intern hebben gemeld. De helft hiervan zelfs meerdere keren. Meer dan de helft van de medewerkers die valse e-mails heeft gemeld, geeft aan dit via de meldknop te hebben gedaan (bijna 60%). Hiermee is de meldknop veruit de meest gebruikte manier om een valse e-mail intern te melden.

Positief over gedragsinterventie als geheel

Bijna tweederde van de respondenten is positief over de gedragsinterventie als geheel. Bijna alle respondenten (84%) vinden het goed dat hun bedrijf heeft meegedaan aan de pilot. Ze vinden het belangrijk dat het bedrijf aandacht besteedt aan cyberveiligheid om gevolgen en risico's zo klein mogelijk te houden.

Conclusies

- Er zijn meer interne meldingen kort na toepassing van de gehele gedragsinterventie dan ervoor. Effect neemt iets af na verloop van tijd.
- Geen effect op klikgedrag in de nepmails.
- Volgens medewerkers wordt er sinds de toepassing van de gedragsinterventie vaker gesproken over cyberveiligheid in het teamoverleg.
- Medewerkers geven aan dat ze meer alert zijn op valse e-mails sinds de toepassing van de gedragsinterventie.
- Medewerkers zijn positief over de gedragsinterventie-onderdelen en de gedragsinterventie als geheel.

Aanbevelingen

Vanwege technische oorzaken zijn veel data verloren gegaan. Hierdoor hebben we geen goede controlegroep gehad. Ook hebben we niet kunnen onderzoeken of alleen het instellen van een intern cybermeldpunt effectief is om meldgedrag te stimuleren. Aangezien dit een kleine stap is voor veel bedrijven, is dit wel waardevolle informatie. Het is dus raadzaam om de pilot nogmaals uit te voeren, met alle drie de condities.
Hierbij is het raadzaam om al bij de aanmelding van bedrijven te controleren op de compatibiliteit van de software van de bedrijven met de technische vereisten voor de installatie van de meldknop. Ook is het raadzaam om bij herhaling van de pilot eerst te testen of de nepmails goed aankomen bij de bedrijven.

Inleiding

Aanleiding

Deze rapportage is onderdeel van het project Human Factors in Cybersecurity in mkb-metaal. Dit project wordt uitgevoerd door Inspire to Act in samenwerking met het Center of Expertise Cybersecurity van de Haagse Hogeschool, in opdracht van MKB-Nederland. Het project wordt gefinancierd door het ministerie van Justitie en Veiligheid.

Doel van het project is om het risico op slachtofferschap van cybercriminaliteit bij mkb-ers te verkleinen. Om het risico op slachtofferschap van cybercriminaliteit te verkleinen, stellen we de human factors centraal in onze aanpak. Dit betekent dat we een gedragsmatige aanpak hanteren, waarbij we ons richten op het gedrag van mkb-ers. Een van de grootste kwetsbaarheden in cyberveiligheid is namelijk de mens.

Om slachtofferschap van cybercriminaliteit bij mkb-ers te reduceren, is het belangrijk om stil te staan bij de volgende twee vragen:

1. Hoe maken we mkb-ers ontvankelijk voor informatie over cyberveiligheid?
2. Hoe motiveren we mkb-ers om preventieve beschermingsmaatregelen te treffen om het risico op slachtofferschap van cybercriminaliteit te verkleinen?

In deze rapportage beschrijven we de pilot die is uitgevoerd om medewerkers in het mkb te motiveren preventieve beschermingsmaatregelen te treffen om het risico op slachtofferschap van cybercriminaliteit te verkleinen. Hierbij richten we ons op het gedrag van de medewerkers in mkb-metaal. Wij hebben preventieve beschermingsmaatregelen geconcretiseerd als: 1) Medewerkers melden verdachte e-mails bij een intern meldpunt; en 2) Medewerkers klikken niet op een link in verdachte e-mails.

Aanpak pilot

Deze pilot is ontwikkeld op basis van de bevindingen uit de analysefase[1]. De werving van bedrijven is verlopen via de Koninklijke MetaalUnie. Zij heeft een oproep voor deelname aan de pilot verstuurd onder haar leden. In totaal hebben 14 bedrijven zich aangemeld. Hiervan hebben 4 bedrijven zich voor de start van de pilot afgemeld. Een bedrijf heeft meegedaan met 4 ondernemingen.
Alle bedrijven zijn willekeurig toegewezen aan een van de 3 condities. Alle bedrijven hebben een intern cybermeldpunt aangemaakt, een meldknop in het e-mailprogramma geïnstalleerd en campagnemiddelen in het bedrijf opgehangen. De volgorde waarin verschilde per conditie.
Gedurende de pilot zijn 3 nepmails verstuurd naar de medewerkers. Per bedrijf is gemeten hoe vaak er op de link in de nepmail is geklikt en hoeveel medewerkers een interne melding heeft gedaan van de nepmail.

Doorlooptijd

De pilot cyberveilig gedrag heeft gelopen van 1 maart 2021 tot en met 30 november 2021.

[1] Human Factors in Cybersecurity in mkb-metaal; tussenrapportage Analysefase.

Hoofstuk 1. Gedragsinterventie

1.1 Gedragsinterventie *VALSE E-MAIL? MELD HET VIA DE MELDKNOP*

Op basis van de bevindingen in de analysefase[2] hebben we de gedragsinterventie *VALSE E-MAIL? MELD HET VIA DE MELDKNOP* ontwikkeld. Deze gedragsinterventie bestaat uit de volgende onderdelen:

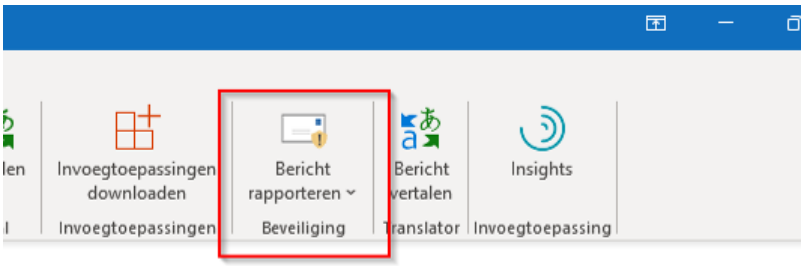
1. intern cybermeldpunt
2. meldknop in e-mailprogramma
3. grote poster
4. kleine poster/ digitale flyer
5. 3D sticker
6. handreiking voor leidinggevenden

Intern cybermeldpunt

Uit de analysefase bleek dat er meestal geen duidelijk meldpunt was bij bedrijven in mkb-metaal. Dit was bij alle deelnemende bedrijven ook het geval. Als onderdeel van de gedragsinterventie hebben de bedrijven een intern cybermeldpunt ingesteld (bv. cybermeldpunt@inspiretoact.nl), waar medewerkers intern melding kunnen doen van verdachte zaken met betrekking tot cyberveiligheid. Alle bedrijven dragen zorg voor een terugkoppeling op alle meldingen die binnenkomen op het cybermeldpunt. Daarnaast zetten zij risicovolle meldingen door naar de (meestal externe) ICT-verantwoordelijke voor verder onderzoek. Door het instellen van een intern cybermeldpunt, wordt het voor medewerkers duidelijker en makkelijker om verdachte zaken te melden.

Meldknop in e-mailprogramma

Bedrijven hebben een meldknop geïnstalleerd in hun e-mailprogramma, zie Figuur 1. Met de meldknop kunnen medewerkers heel eenvoudig een verdachte e-mail intern melden. 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 en de e-mail wordt verwijderd. Met deze meldknop wordt het medewerkers dus makkelijker gemaakt om verdachte zaken te melden bij het interne cybermeldpunt.



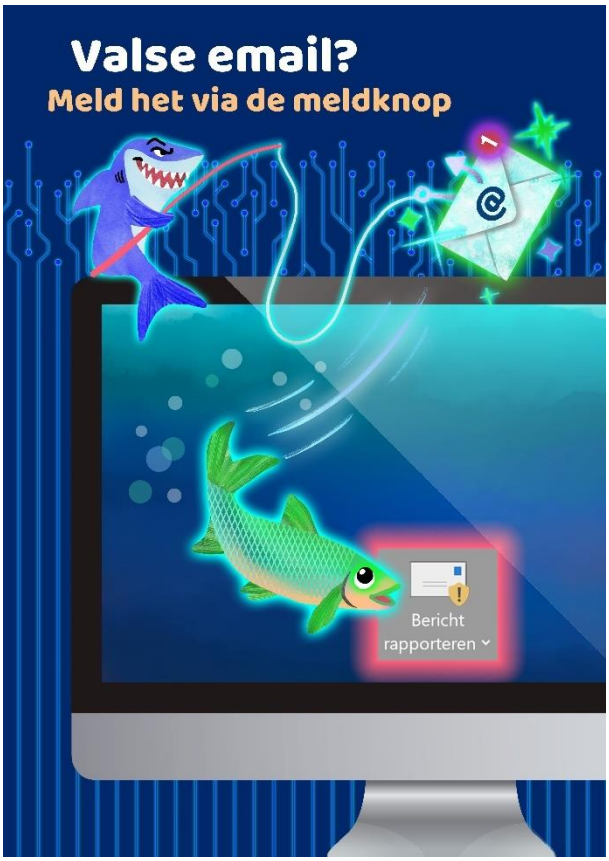
Figuur 1. Meldknop

Grote poster

De grote poster (a2 formaat) dient als reminder voor het gewenste gedrag en zorgt voor bewustwording, zie Figuur 2. 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 ook 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, wat gewenst gedrag stimuleert.

[2] Human Factors in Cybersecurity in mkb-metaal; tussenrapportage Analysefase.

De grote posters zijn opgehangen op plekken in het bedrijf waar ze goed zichtbaar zijn. Denk hierbij aan: productieruimte, kantoorruimte, omkleedruimte, kantine, gang/hal, entree, parkeerruimte, etc.



Figuur 2. Grote poster

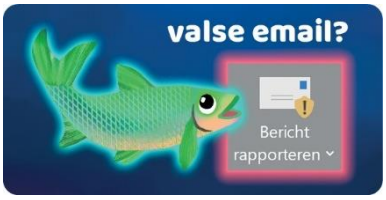
Figuur 3. Kleine poster/ digitale flyer

Kleine poster/ digitale flyer

De kleine poster (a3-formaat) geeft medewerkers extra informatie en handelingsperspectief over wat ze kunnen doen als ze een valse e-mail ontvangen, zie Figuur 3. De kleine poster bevat meer tekst dan de grote poster. Daarom zijn de kleine posters 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.
Daarnaast is de kleine poster ook als digitale flyer naar alle medewerkers toegestuurd. Zo kunnen medewerkers de informatie (terug)lezen op een moment dat hen goed uitkomt.

3D sticker

De 3D sticker is een prompt (of reminder) voor gewenst gedrag, zie Figuur 4. Deze stickers zijn luxe stickers met een 3D-effect. Hierdoor spreken ze meer aan en springen ze meer in het oog dan gewone stickers. De stickers zijn op de beeldschermen van de computers geplakt en herinneren medewerkers op het juiste moment aan het gewenste gedrag: melden van valse e-mail via de meldknop.



Figuur 4. 3D sticker

Handreiking voor leidinggevenden

Uit de analysefase kwam naar voren dat er binnen mkb-metaalbedrijven weinig werd gesproken over cyberveiligheid. Om cyberveilig gedrag te stimuleren, is het belangrijk dat zowel leidinggevenden als collega's onderling met elkaar in gesprek gaan hierover. En dat ze aangeven dat ze cyberveilig gedrag belangrijk vinden. Om het gesprek hierover te stimuleren in bedrijven, hebben we een handreiking opgesteld voor leidinggevenden, zie Bijlage 1. De handreiking bestond uit een aantal tips voor leidinggevenden om het onderwerp bespreekbaar te maken en gedragsverandering te stimuleren bij de medewerkers.

1.2 Gebruikte gedragstechnieken

In de gedragsinterventie *VALSE EMAIL? MELD HET VIA DE MELDKNOP* zijn verschillende gedragstechnieken toegepast. Onderstaand de belangrijkste technieken.

Vereenvoudigen

Door het instellen van een intern cybermeldknop en het installeren van een meldknop in het e-mailprogramma wordt het gewenste gedrag (melden van verdachte e-mails) makkelijker gemaakt. Dit stimuleert gewenst gedrag.

Prompting

Door middel van (grote en kleine) posters worden medewerkers op verschillende plekken in het bedrijf herinnerd aan het gewenste gedrag. De 3D sticker en de meldknop in het e-mailprogramma herinneren medewerkers op de plek waar je gedrag wilt zien aan het gewenste gedrag.

Geanticipeerde spijt en handelingsperspectief

Met geanticipeerde spijt worden gevoelens van spijt of schuld bedoeld die mensen verwachten te ervaren als ze nalaten bepaald gedrag uit te voeren. Als mensen verwachten dat ze zich achteraf schuldig voelen en/of spijt hebben wanneer zij gewenst gedrag nalaten, zal de kans groter zijn dat mensen het gewenste gedrag uitvoeren, zo blijkt uit onderzoek. Zeker als dit in combinatie wordt gebruikt met handelingsperspectief.[3] Door in communicatie gebruik te maken van geanticipeerde spijt, verhoog je dus de kans dat mensen in actie komen.
Op de kleine poster hebben we het risico dat het bedrijf stil komt te liggen door een verkeerde muisklik gebruikt om geanticipeerde spijt op te wekken. Uit een eerdere pilot is gebleken dat dit effectief is om ondernemers ontvankelijk te maken voor informatie over cyberveiligheid.[4] Het handelingsperspectief dat we bieden om geanticipeerde spijt te voorkomen is het melden van valse e-mail via de meldknop.

Bewustwording en handelingsperspectief

Medewerkers worden ervan bewust gemaakt dat valse berichten ook via sms of Whatsapp worden verstuurd. Hierbij wordt ook handelingsperspectief gegeven hoe
ze valse berichten kunnen melden bij het intern cybermeldpunt.

Urgentie creëren en voorkomen inactie door schaamte

Melden van valse e-mail is heel belangrijk, zeker als je op een verdachte link geklikt hebt. Als medewerkers op een verdachte link geklikt hebben, kunnen ze door schaamte hun kop in het zand steken en niets doen. Maar juist dan is actie nog belangrijker. Door aan te geven dat dit kan gebeuren, veroordeel je dit niet en creëer je een veiligere meldomgeving. In combinatie met het creëren van urgentie, verhoogt dit de kans op gewenst gedrag.

[3] bv. Abraham & Sheeran (2004); O'Carroll, Foster, McGeechan, Sandford & Ferguson (2011).
[4] Bongers, et. al. (2021)

Sociale norm en altercasting

Door aan te geven dat het betreffende bedrijf cyberveiligheid heel belangrijk vindt, benadruk je een positieve sociale norm. Bij een positieve sociale norm zijn mensen sneller geneigd zich te gedragen volgens deze norm. Zeker als mensen zich verbonden voelen met deze groep. Met altercasting spreek je medewerkers aan op hun verbondenheid met het bedrijf en hun rol als medewerker van dit bedrijf. Ook wordt de verbondenheid benadrukt door aan te geven dat we samen het bedrijf beschermen. Daarnaast wordt de sociale omgeving gebruikt om gewenst gedrag uit te lokken: Bescherm jezelf en je collega's.

In Tabel 1 staat per interventieonderdeel aangegeven welke gedragstechnieken gebruikt zijn.

	Intern cyber-meldpunt	Meldknop	Grote poster	Kleine poster/ digitale flyer	3D sticker	Handreiking voor leiding-gevenden
Vereenvoudigen	✓	✓				✓
Prompting		✓	✓	✓	✓	
Handelingsperspectief	✓	✓	✓	✓	✓	
Geanticipeerde spijt				✓		
Kennis en bewustwording				✓		✓
Sociale normen				✓		✓
Urgentie creëren				✓		✓
Inspelen op emoties				✓		
Altercasting				✓		

Tabel 1. Gedragstechnieken per interventieonderdeel.

Hoofdstuk 2. Pilot cyberveilig gedrag

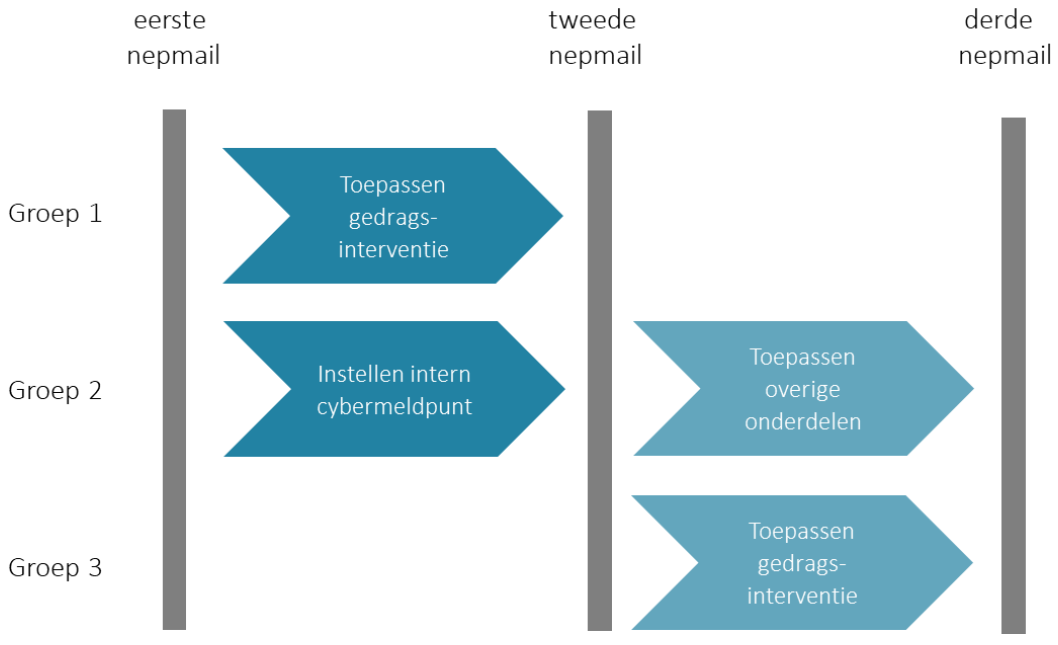
2.1 Deelnemende bedrijven

Via de Koninklijke MetaalUnie hebben 14 mkb-metaalbedrijven zich aangemeld voor deze pilot. Hiervan hebben 4 bedrijven zich voor de start van de pilot afgemeld (zonder opgave van reden). Een bedrijf heeft meegedaan met 4 ondernemingen (mkb-metaalbedrijven). Voorafgaand aan de pilot hebben we een vrijwaring- en verwerkersovereenkomst toegestuurd naar alle bedrijven. Dit was noodzakelijk voor het versturen van 3 nepmails naar de medewerkers. Een bedrijf heeft deze overeenkomst niet geretourneerd en is daarom uitgesloten van de pilot. Uiteindelijke zijn we de pilot gestart met 13 mkb-metaalbedrijven. Deze bedrijven zijn gevestigd door het gehele land. Het aantal medewerkers met een e-mailadres varieert van 10 tot 85, met een totaal aan 410 emailadressen.

2.2 Methode

Onderzoeksdesign

We willen onderzoeken of de gedragsinterventie in zijn geheel (alle onderdelen) effectief is in het stimuleren van meldgedrag en het tegengaan van klikgedrag op verdachte links. Daarnaast willen we onderzoeken wat de effectiviteit is van enkel het instellen van een intern cybermeldpunt. Het instellen van een intern cybermeldpunt is voor bedrijven heel eenvoudig zelf te doen. Voor een eventuele opschaling is het daarom zinvol om dit onderdeel apart te toetsen op effectiviteit. De pilot bestaat dus uit drie condities: gehele interventie; intern cybermeldpunt; en geen interventie (controle). Om het meld- en klikgedrag te kunnen meten, hebben we drie nepmails verstuurd. De eerste nepmail is verstuurd naar alle bedrijven voorafgaand aan de toepassing van de gedragsinterventie (0-meting). De tweede nepmail is verstuurd naar alle bedrijven na het toepassen van de gedragsinterventie of intern cybermeldpunt (en niets in de controleconditie).
Omdat we alle bedrijven uiteindelijk de gedragsinterventie willen aanbieden, hebben we gebruik gemaakt van de mogelijkheid een derde nepmail te versturen. Deze derde nepmail is verstuurd nadat in alle bedrijven de gedragsinterventie is toegepast. Hiermee kunnen we voor de eerste groep de langere termijneffecten in kaart brengen en voor de andere twee groepen opnieuw de effectiviteit van de gedragsinterventie. In Figuur 5 staat het onderzoeksdesign schematisch weergegeven.



Figuur 5. Onderzoeksdesign

Procedure

Eerste nepmail

In overleg met de bedrijven is de eerste nepmail in week 34 of week 35 verstuurd. De eerste nepmail betrof een mail zogenaamd van Coolblue, zie Bijlage 2. In de nepmail zaten verschillende kenmerken van valse e-mails verwerkt, bijvoorbeeld: een algemene aanhef (geachte meneer/mevrouw); een verkeerd tijdstip; ontbreken van adres; typefouten en gekke leestekens; verkeerde spelling van Coolblue (Coolbleu); etc. We hebben ervoor gekozen de nepmail niet te moeilijk te maken. Dit omdat we niet willen meten of medewerkers valse e-mails herkennen, maar omdat we willen weten wat ze doen als ze een valse e-mail ontvangen.

Toepassen gedragsinterventie

Vijf bedrijven pasten de gehele gedragsinterventie toe (groep 1; gehele interventie). Drie bedrijven stelden alleen het interne cybermeldpunt in (groep 2; intern cybermeldpunt).[5] Vijf bedrijven pasten geen interventie toe (groep 3; controle).

Tweede nepmail

Nadat de gehele gedragsinterventie was toegepast (groep 1) of het intern cybermeldpunt geïnstalleerd was (groep 2), werd de tweede nepmail naar alle bedrijven gestuurd (week 38 t/m week 42). De tweede nepmail betrof een mail zogenaamd van PostNL, zie Bijlage 3. Ook in deze mail zaten verschillende kenmerken van valse e-mails verwerkt, bijvoorbeeld: een algemene aanhef (geachte heer/mevrouw); ontbreken van bezorgadres; taalfouten; gekke leestekens; etc. Ook deze mail was niet te moeilijk gemaakt om als valse e-mail te kunnen herkennen.

Toepassen overige onderdelen gedragsinterventie

We wilden alle bedrijven uiteindelijk de gedragsinterventie aanbieden. Daarom zijn bij de bedrijven in groep 2 (intern cybermeldpunt) de overige onderdelen van de gedragsinterventie toegepast. Bij de bedrijven in groep 3 (controle groep) zijn alle interventieonderdelen in een keer toegepast. Bij de bedrijven in groep 1 (gehele interventie) hebben we in deze stap niets gedaan.

Derde nepmail

Doordat alle bedrijven de gedragsinterventie uiteindelijk hebben toegepast, hadden wij de mogelijkheid om met een derde nepmail nogmaals de effectiviteit van de gedragsinterventie in kaart brengen in groep 2 en 3. Ook konden we met de derde nepmail de effecten voor een langere periode monitoren in groep 1. De derde nepmail was een mail zogenaamd van datumprikker.nl en werd naar alle bedrijven gestuurd (week 44 t/m week 47), zie Bijlage 4. Ook in de derde nepmail zaten verschillende kenmerken van valse e-mails verwerkt, bijvoorbeeld: een algemene aanhef (beste Heer/Mevrouw); een datumprikker voor een (niet-bestaande) cursus waarvoor ze zich niet ingeschreven kunnen hebben; een onduidelijke afzender (niet bestaand persoon van een onduidelijk bedrijf); etc. Ook deze mail was niet te moeilijk gemaakt om als valse e-mail te kunnen herkennen.

Belevingsonderzoek

Na afloop van de pilot hebben we belevingsonderzoek gedaan bij medewerkers van de deelnemende bedrijven. Hiervoor hebben we de bedrijven een link gestuurd naar een online vragenlijst. De bedrijven hebben deze link intern doorgezet naar alle medewerkers. Met het belevingsonderzoek brengen we ervaringen van medewerkers met de gedragsinterventie in kaart. De vragen van het belevingsonderzoek zijn als Bijlage 5. toegevoegd.

[5] In eerste instantie waren 4 bedrijven toegewezen aan deze conditie. Het bedrijf dat de vrijwaring- en verwerkersovereenkomst niet heeft geretourneerd, is uit deze conditie weggevallen.

Afhankelijke variabele

We hebben twee afhankelijke variabelen: 1). Het aantal keren dat de nepmails intern gemeld worden; en 2) het aantal keren dat er wordt geklikt op de link in de nepmails.

Hypothesen

Aantal interne meldingen

We verwachten dat de nepmails vaker intern worden gemeld bij bedrijven waar de gehele gedragsinterventie is toegepast (groep 1) dan bij bedrijven waar geen gedragsinterventie is toegepast (groep 3). We verwachten dat het instellen van een intern cybermeldpunt (groep 2) tot meer interne meldingen van de nepmails leidt dan zonder intern cybermeldpunt (groep 3), maar minder dan waar de gehele gedragsinterventie is toegepast (groep 1). Oftewel, aantal meldingen: gehele gedragsinterventie (groep 1) > intern cybermeldpunt (groep 2) > geen interventie (groep 3).

Aantal keren geklikt

We verwachten dat het aantal keren dat er geklikt wordt op de link in de nepmails lager is bij bedrijven waar de gehele gedragsinterventie is toegepast (groep 1) dan bij bedrijven waar geen gedragsinterventie is toegepast (groep 3). We verwachten dat het instellen van een intern cybermeldpunt (groep 2) tot minder kliks leidt dan zonder intern meldpunt (groep 3), maar meer dan waar de gehele gedragsinterventie is toegepast (groep 1). Oftewel, aantal kliks: gehele gedragsinterventie (groep 1) < intern cybermeldpunt (groep 2) < geen interventie (groep 3).

Langere termijn effect

We verwachten dat de gedragsinterventie ook over een langere periode effectief blijft. We verwachten dus dat het aantal interne meldingen en het aantal kliks in de tweede en derde nepmail gelijk blijft bij groep 1. Voor groep 2 en 3 kunnen we de langere termijn effecten niet in kaart brengen.

Procesbegeleiding bedrijven

Intake

We hebben met alle bedrijven apart een online intake gehouden. Tijdens de intake hebben we kennisgemaakt, doel en opzet van de pilot toegelicht, de werkzaamheden van de bedrijven en de onderzoekers afgestemd, afspraken gemaakt over de planning en eventuele vragen beantwoord.

Vrijwarings- en verwerkersovereenkomst

Alle bedrijven hebben een vrijwarings- en verwerkersovereenkomst toegestuurd gekregen. Op een bedrijf na, hebben alle bedrijven deze overeenkomst getekend en geretourneerd. Het bedrijf dat de overeenkomst niet heeft geretourneerd,[6] is uitgesloten van de pilot. Zonder deze overeenkomst is het niet toegestaan om nepmails te versturen.

Draaiboek

Voor alle bedrijven hebben we een draaiboek gemaakt. In het draaiboek stond een gedetailleerde planning. Hierin stond vermeld wanneer de nepmails verstuurd zouden worden, wanneer welke interventieonderdelen toegepast zouden worden en wanneer er intern gecommuniceerd kon worden over de nepmail. Voor de interne communicatie stonden er voorbeeldberichten in het draaiboek die de bedrijven naar hun medewerkers konden versturen als terugkoppeling op de nepmails.

[6] Het bedrijf heeft hiervoor geen redenen gegeven.

Verder stond er een toelichting in het draaiboek over de registratie en opvolging van de interne meldingen. Ook stond er een voorbeeld van een ontvangstbevestiging in, die bedrijven konden sturen naar medewerkers die een interne melding hadden gemaakt.

Invulformat interne meldingen

Om uniformiteit te bewaken en het voor bedrijven zo makkelijk mogelijk te maken om een interne melding te registreren, hebben we een invulformat in Excel gemaakt. Hierin konden bedrijven eenvoudig noteren hoeveel meldingen er van de nepmails zijn binnengekomen, welke meldingen nog meer zijn binnengekomen en welke acties hierop zijn ondernomen.

Intern cybermeldpunt

Alle bedrijven hebben een intern cybermeldpunt ingericht. Hiervoor hebben alle bedrijven een apart e-mailadres aangemaakt. Dit e-mailadres stond ook vermeld op de kleine poster/digitale flyer.

Posters en 3D sticker

De grote en kleine posters en de 3D stickers zijn per post naar de bedrijven gestuurd. Bedrijven hebben deze interventie-onderdelen zelf in het bedrijf opgehangen, zie Bijlage 6. voor een impressie. Hiervoor hebben de bedrijven een ophanginstructie ontvangen.

Digitale flyer en handreiking voor leidinggevenden

De digitale flyer en handreiking voor leidinggevenden is per e-mail naar de bedrijven gestuurd. De bedrijven hebben de digitale flyer naar alle medewerkers gemaild. De handreiking hebben de bedrijven naar alle leidinggevenden gemaild.

Installatie meldknop

Voor de installatie van de meldknop is een stappenplan geschreven. Hiermee konden bedrijven zelf de meldknop in hun e-mailprogramma installeren. Ook was technische ondersteuning beschikbaar. De meeste bedrijven hadden deze ondersteuning ook nodig bij de installatie van de meldknop. Ondersteuning werd online gegeven via een videocall. Samen met het bedrijf werden de stappen doorlopen, waarna de meldknop actief was.
Bij vier bedrijven is het helaas niet gelukt om de meldknop te installeren. Dit kwam doordat deze bedrijven met een (oudere) versie van Microsoft Office werken die niet compatible is met de meldknop. Een van deze bedrijven was ingedeeld in groep 2, drie bedrijven waren ingedeeld in groep 3.
Bij twee bedrijven is de meldknop per ongeluk te vroeg geïnstalleerd. Dit betroffen twee ondernemingen van het bedrijf dat met vier ondernemingen meedeed. Een van deze bedrijven was ingedeeld in groep 2 en is direct overgeheveld naar groep 1, zodat dit bedrijf toch mee kon doen aan de pilot. Het andere bedrijf was ingedeeld in groep 3. Aangezien dit bedrijf in hetzelfde pand gevestigd is als de andere onderneming van dit bedrijf in groep 3, kon deze niet worden overgeheveld naar groep 1.

Versturen nepmails

Voorafgaand aan het versturen van elke nepmail hebben we het e-mailadres van de nepmail doorgegeven aan de bedrijven, met het verzoek dit e-mailadres te whitelisten. Hiermee voorkomen we dat de nepmails worden afgevangen door het spamfilter en daardoor niet in de mailbox van de medewerkers komen. Ondanks het whitelisten zijn sommige nepmails bij een aantal bedrijven toch afgevangen door het spamfilter. Bij deze bedrijven hebben we de nepmail nogmaals verstuurd, nadat zij de instellingen van de spamfilter voor dit e-mailadres hadden aangepast. Meestal kwam de nepmail daarna wel aan. Eén bedrijf is na de tweede nepmail afgehaakt, omdat beide mails in eerste instantie door de spamfilter werden afgevangen. Dit bedrijf was ingedeeld in groep 1.

Vooraankondiging

Een bedrijf heeft een vooraankondiging gedaan naar alle medewerkers.[7] Hierin is aangegeven dat het bedrijf meedoet aan een pilot over cyberveiligheid en is medegedeeld dat er nepmails verstuurd zullen gaan worden. Deze vooraankondiging is een week voorafgaand aan de eerste nepmail intern naar alle medewerkers verstuurd. Deze medewerkers waren dus al alert op nepmails en daardoor niet vergelijkbaar met andere bedrijven. De data van dit bedrijf zijn daarom niet meegenomen in de analyses.

In Tabel 2. staat een overzicht van de bedrijven. Data die niet beschikbaar of bruikbaar zijn, staan aangegeven met een kruis. In de kolom met opmerkingen staat de reden hiervoor toegelicht.

	aantal e-mail-adressen	nepmail 1	nepmail 2	nepmail 3	opmerkingen
GROEP 1					
Bedrijf 1	18	✓	✓	✓	
Bedrijf 2	58	✓	✓	✓	
Bedrijf 3	59	✓	✓	✓	
Bedrijf 4	31	✓	✗	✓	tweede nepmail door spamfilter afgevangen
Bedrijf 5	18	✓	✓	✗	afgehaakt na tweede nepmail doordat mails werden afgevangen door spamfilter[8]
Bedrijf 9	25	✓	✓	✓	overgeplaatst uit groep 2 door te vroeg installeren meldknop
GROEP 2					
Bedrijf 6	12	✓	✓	✓	
Bedrijf 7	26	✓	✓	✗	meldknop werkt niet wegens oud officepakket; derde nepmail niet verstuurd
Bedrijf 8		✗	✗	✗	vrijwarings- en verwerkersovereenkomst niet geretourneerd; uitgesloten van pilot
Bedrijf 9	-	-	-	-	overgeplaatst naar groep 1 door te vroeg installeren meldknop
GROEP 3					
Bedrijf 10	85	✓	✗	✗	meldknop werkt niet wegens oud officepakket; tweede en derde nepmail niet verstuurd
Bedrijf 11	28	✓	✓	✗	meldknop werkt niet wegens oud officepakket; derde nepmail niet verstuurd
Bedrijf 12	15	✗	✗	✗	vooraankondiging gedaan; meldknop werk niet wegens oud officepakket
Bedrijf 13	25	✓	✗	✓	tweede nepmail is afgevangen door spamfilter
Bedrijf 14	10	✓	✗	✗	meldknop na de eerste nepmail al geïnstalleerd; overplaatsing naar groep 1 was niet mogelijk

Tabel 2. Overzicht van bedrijven

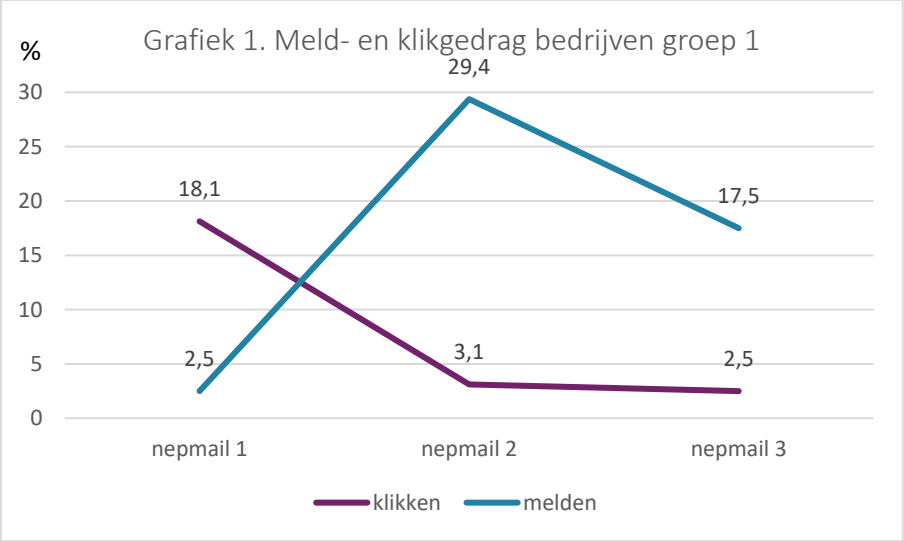
[7] Dit bedrijf was een van de 4 bedrijven waar de meldknop niet geïnstalleerd kon worden.
[8] De eerste twee nepmails zijn opnieuw (succesvol) verstuurd nadat ze door de spamfilter waren afgevangen.

2.3 Resultaten

Doordat er veel data ontbreken in groep 2 (intern cybermeldpunt) is het niet mogelijk om iets te zeggen over de effectiviteit van alleen het instellen van een intern cybermeldpunt. Slechts van één bedrijf zijn de data van alle drie de nepmails beschikbaar. Het betreft een bedrijf met in totaal 12 e-mailadressen. Dit is te weinig om betrouwbare analyses uit te kunnen voeren.
Helaas ontbreken er ook veel data in groep 3 (contolegroep). Van geen enkel bedrijf zijn de data van alle drie de nepmails beschikbaar. Hierdoor is het niet mogelijk om deze bedrijven als controlegroep te gebruiken.
In groep 1 (gehele interventie) zijn meer data beschikbaar. Van vier bedrijven zijn de data van alle drie de nepmails beschikbaar en bruikbaar. In totaal gaat het om 160 e-mailadressen. We kunnen dus wel onderzoeken of er meer meldingen gemaakt worden van nepmail 2 (korte termijn effect) en 3 (langere termijn effect) dan van nepmail 1. Ook kunnen we onderzoeken of er minder geklikt wordt op de link in nepmail 2 (korte termijn effect) en 3 (lagere termijn effect) dan in nepmail 1. De volgende analyses gaan dus alleen over de bedrijven in groep 1.

Meldgedrag

Als we kijken naar het meldgedrag bij bedrijven in groep 1, dan zien we dat er van nepmail 2 (1-2 weken na interventie) meer interne meldingen zijn gemaakt dan van nepmail 1 (voorafgaand aan interventie). Het aantal meldingen van nepmail 3 (6-7 weken na interventie) zit tussen het aantal meldingen op nepmail 1 en 2 in, zie Grafiek 1 voor het percentage meldingen per nepmail (blauwe lijn). Het aantal meldingen per nepmail verschilt significant.[9] Het aantal meldingen van nepmail 2 is marginaal significant hoger dan het aantal meldingen van nepmail 1.[10] Het aantal meldingen van nepmail 3 is niet significant hoger dan van nepmail 1 en niet significant lager dan van nepmail 2.[11]



Klikgedrag

Als we kijken naar het klikgedrag bij bedrijven in groep 1, dan zien we dat er het meest geklikt wordt op de link in de eerste nepmail (voorafgaand aan interventie). In nepmail 2 en 3 wordt nauwelijks meer geklikt op de link (na de interventie), zie Grafiek 1 (paarse lijn). Het verschil in percentage kliks tussen de drie nepmails is niet significant.[12]

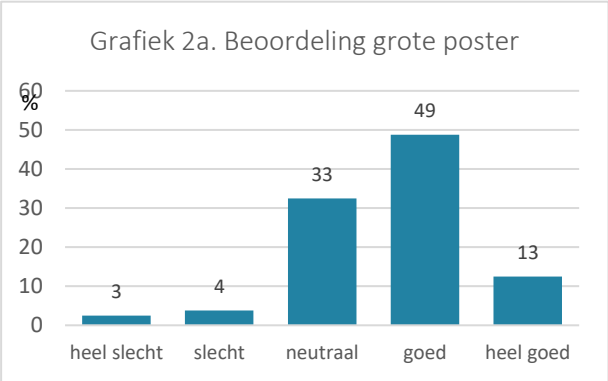
[9] ANOVA Tests of Within-Subject Effects: F(2,6)=6,068; *p*=.036.
[10] ANOVA Tests of Within-Subject Effects: F(1,3)=6,689; *p*=.081.
[11] ANOVA Tests of Within-Subject Effects nepmail 1 en 3: F(1,3)=5,466; n.s.; ANOVA Tests of Within-Subject Effects nepmail 2 en 3: F(1,3)=4,759; n.s.
[12] ANOVA Tests of Within-Subject Contrasts: F(1,3)=2,097; n.s. (lineair); F(1,3)=1,041; n.s. (quadratic); shows no (lineair or quadratic) change over time.

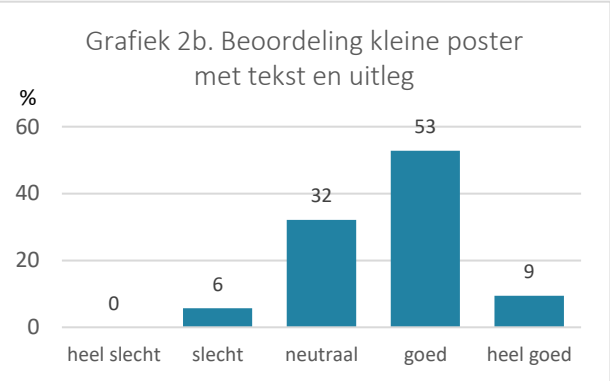
Belevingsonderzoek

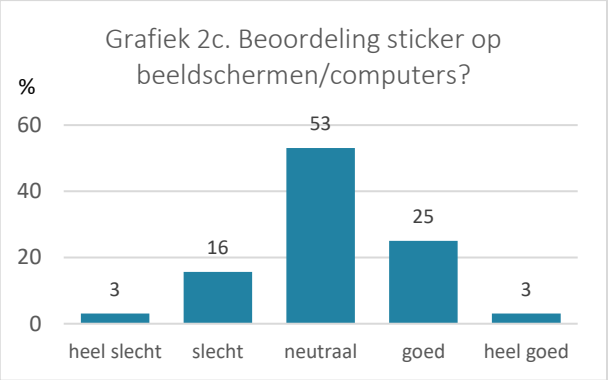
In totaal hebben 82 medewerkers van 8 bedrijven de belevingsvragenlijst ingevuld.

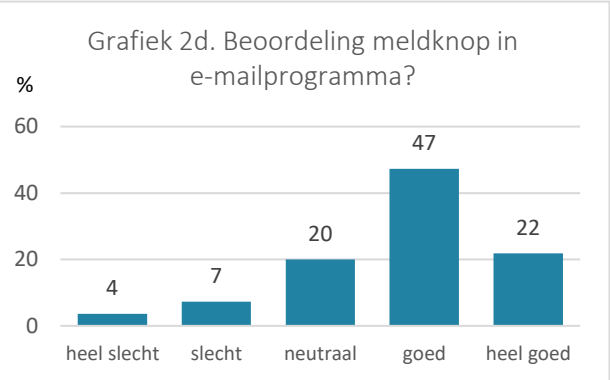
Interventie-onderdelen

Medewerkers zijn overwegend positief over de interventie-onderdelen, zie Grafiek 2 a t/m d. Over de 3D sticker zijn de meningen wat meer verdeeld.









Grote poster

Medewerkers die positief zijn over de poster geven heel vaak als reden dat ze de poster duidelijk en overzichtelijk vinden. Ook wordt genoemd dat de poster er aantrekkelijk en vrolijk uitziet. Daarnaast vinden medewerkers de poster opvallend en denken ze dat het goed is voor bewustwording.
Medewerkers die de poster minder positief beoordelen, geven als reden dat een poster niet voldoende is voor bewustwording of ander gedrag.

Kleine poster

Medewerkers die positief zijn over de poster geven vaak als reden dat de poster duidelijk en overzichtelijk is. Ze vinden de informatie handig en goed uitgelegd. Een medewerker noemt verder dat hij/zij een melding heeft gemaakt bij het interne cybermeldpunt dat op de kleine poster vermeld staat.
Een paar medewerkers die minder positief zijn, geven aan dat ze de kleine poster niet gezien hebben. Een medewerker die minder positief is, noemt dat er veel tekst op de poster staat. Wel geeft hij/zij aan de tekst gelezen te hebben, omdat het op de wc hing.

3D sticker

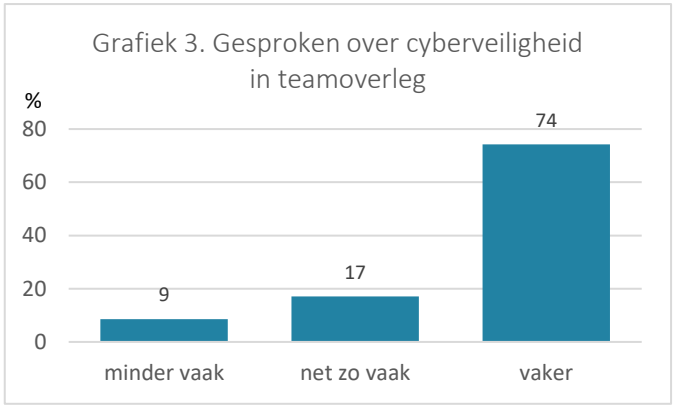
Medewerkers zijn positief over de 3D sticker, omdat het hen herinnert aan gewenst gedrag en zorgt voor bewustwording. Ook de kwinkslag met phishing wordt positief beoordeeld. Minder positief vinden medewerkers dat de sticker niet zoveel zegt en dat de sticker niet zo goed opvalt.

Meldknop

Medewerkers die positief zijn over de meldknop geven veelal als reden dat de meldknop duidelijk is en het makkelijk maakt om intern meldingen te doen. Medewerkers die minder positief zijn, hebben de meldknop niet gevonden of missen feedback nadat ze een melding hebben gemaakt met de meldknop.[13]

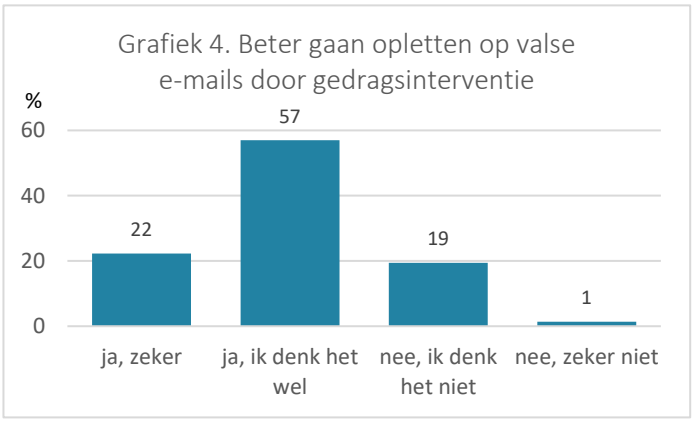
Teamoverleg

Bijna de helft van de respondenten (47%) geeft aan dat er in de afgelopen 2 maanden in het teamoverleg gesproken is over cyberveiligheid. Driekwart van de respondenten geeft aan dat er in de afgelopen 2 maanden vaker over cyberveiligheid is gesproken in het teamoverleg dan daarvoor, zie Grafiek 3.



Alertheid

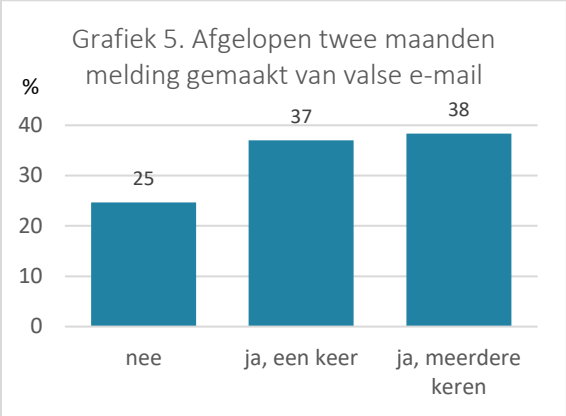
Vier op de vijf respondenten geeft aan dat ze door de gedragsinterventie beter zijn gaan opletten op valse e-mails, zie Grafiek 4. Alle respondenten die aangeven dat ze niet beter zijn gaan opletten, geven als reden dat ze altijd al goed opletten op valse e-mails.

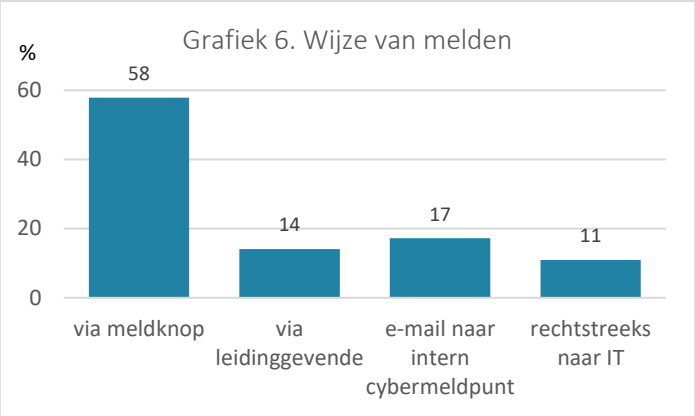


Meldgedrag

Vrijwel alle respondenten (97%) geven aan dat ze weten hoe ze intern een melding kunnen maken van een valse e-mail. Driekwart van de respondenten geeft aan dat ze in de afgelopen twee maanden daadwerkelijk een valse e-mail (of nepmail) intern hebben gemeld, zie Grafiek 5. De helft hiervan zelfs meerdere keren. De meldknop is veruit de meest gebruikte manier om een valse e-mail intern te melden, zie Grafiek 6.

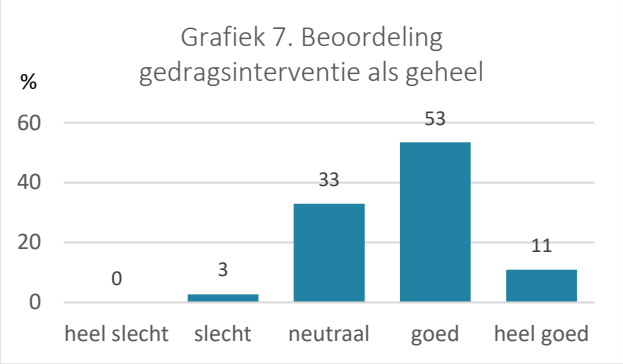
[13] We hadden met bedrijven afgesproken dat zij op elke melding een terugkoppeling zouden geven. Hiervoor hebben we in het draaiboek voorbeeldmails aangeleverd.

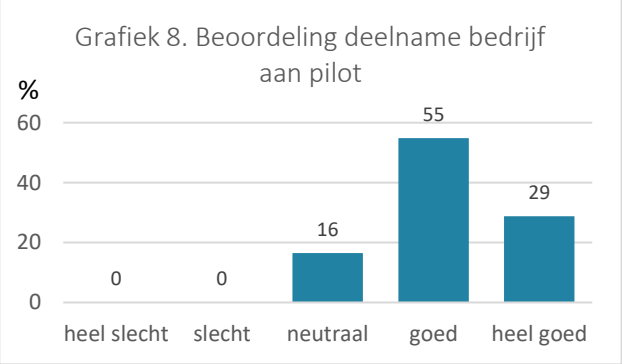




Algemene beoordeling

Bijna tweederde van de respondenten is positief over de gedragsinterventie als geheel, zie Grafiek 7. Respondenten die positief waren, geven veelal aan dat ze cyberbewustzijn belangrijk vinden. Ook zijn respondenten positief over hoe duidelijk de gedragsinterventie was.
Respondenten die niet zo positief waren, gaven aan dat de e-mails te makkelijk waren om als valse e-mail te herkennen. Liever hadden zij moeilijkere nepmails ontvangen.





Bijna alle respondenten (84%) vinden het goed dat hun bedrijf heeft meegedaan aan de pilot, zie Grafiek 8. De reden die veelal wordt gegeven, is dat het belangrijk is om aandacht aan te besteden aan cyberveiligheid om gevolgen en risico's zo klein mogelijk te houden.

2.4 Conclusies

Meer interne meldingen

De gedragsinterventie in zijn geheel zorgt ervoor dat mensen verdachte e-mails vaker intern melden. Dit effect lijkt over tijd iets af te zwakken. Deze conclusie moeten we wel met enige voorzichtigheid interpreteren, omdat we geen controlegroep hebben. Het zou kunnen zijn dat nepmail 2 makkelijker als nepmail te identificeren is dan nepmail 1 en dat er daardoor meer meldingen zijn gemaakt.
Wel geeft 80% van de medewerkers in het belevingsonderzoek aan dat zij door de gedragsinterventie beter zijn gaan opletten op valse e-mails. Ook zien we dat meer dan de helft van het aantal interne meldingen de laatste twee maanden via de meldknop worden gedaan, wat onderdeel is van de gedragsinterventie.

Geen effect op klikgedrag

De gedragsinterventie heeft geen effect op het klikgedrag: er is geen significant verschil in het aantal keren dat er op een link geklikt wordt tussen de verschillende nepmails. Op de eerste nepmail wordt

door 18% van de medewerkers geklikt. Dit komt overeen met eerder onderzoek.[14] Na de gedragsinterventie (op nepmail 2 en 3) klikt nog maar 2,5-3% van de medewerkers op de link in de nepmails. Er kan sprake zijn van een flooreffect. Dat wil zeggen dat dit percentage niet meer verder kan afnemen, doordat er altijd medewerkers zijn die per ongeluk op een link in een nepmail klikken.

Vaker over cyberveiligheid gesproken

Er wordt sinds de gedragsinterventie vaker gesproken over cyberveiligheid in het teamoverleg. Dit is belangrijk, omdat hiermee een signaal wordt afgegeven dat het bedrijf cyberveilig gedrag belangrijk vindt. Dit stimuleert cyberveilig gedrag.

Meer alertheid

Medewerkers zeggen dat ze sinds de gedragsinterventie meer op valse e-mails letten dan daarvoor.

Medewerkers positief over gedragsinterventie

Medewerkers zijn positief over de gedragsinterventie als geheel. Vooral de meldknop wordt positief beoordeeld. De meldknop maakt het voor medewerkers eenvoudiger om een valse e-mail intern te melden. Over het nut van de sticker op de computers/beeldschermen zijn de meningen wat meer verdeeld.

[14] Sommestad & Karlzén (2019)

Hoofstuk 3. Aanbevelingen

Bij aanmelding controleren op compatibiliteit

Door technische oorzaken zijn veel data verloren gegaan. Grootste technisch obstakel was de installatie van de meldknop. Een aantal bedrijven in onze pilot werkt met een (oudere) versie van Microsoft Office die niet compatible is met de meldknop. Hierdoor is het niet gelukt om bij deze bedrijven de meldknop te installeren. Het is raadzaam om bij herhaling van de pilot al bij de aanmelding te controleren op de compatibiliteit van de software van de bedrijven met de technische vereisten voor de installatie van de meldknop ofwel deze compatibiliteit als voorwaarde te stellen voor deelname.

Vooraf testen op afvangen spamfilter

Ander technisch obstakel was dat sommige nepmails door de spamfilter werden afgevangen. Om dit te voorkomen, hebben we alle bedrijven gevraagd de e-mailadressen van de nepmails te whitelisten. Helaas werden ondanks whitelisting nog een aantal nepmails afgevangen door spamfilters. Het is raadzaam om bij herhaling van de pilot eerst te testen of de nepmails goed aankomen bij de bedrijven.

Pilot herhalen

Vanwege technische oorzaken zijn veel data verloren gegaan. Hierdoor hebben we geen goede controlegroep gehad en kunnen we niet met zekerheid zeggen dat de gedragsinterventie effectief is geweest. Ook hebben we niet kunnen onderzoeken of alleen het instellen van een intern cybermeldpunt effectief is om meldgedrag te stimuleren. Aangezien dit een kleine stap is voor veel bedrijven, is dit wel waardevolle informatie. Het is dus raadzaam om de pilot nogmaals uit te voeren, met alle drie de condities.

Geraadpleegde bronnen

Abraham, C., & Sheeran, P. (2004). Deciding to exercise: The role of anticipated regret. British journal of health psychology, 9(2), 269-278.

Bongers, K.C.A., Leukfeldt, E.R., Kleij van der, R., Bekkers, L. & Ancher, M. (2020). Human Factors in Cybersecurity in mkb-metaal; tussenrapportage Analysefase. Inspire to Act i.s.m. Haagse Hogeschool.

Bongers, K.C.A., Leukfeldt, E.R., Kleij van der, R., Bekkers, L. & Ancher, M. (2020). Human Factors in Cybersecurity in mkb, Rapportage pilots Ontvankelijkheid bij Ondernemers, Inspire to Act i.s.m. Haagse Hogeschool.

O'Carroll, R. E., Foster, C., McGeechan, G., Sandford, K., & Ferguson, E. (2011). The “ick” factor, anticipated regret, and willingness to become an organ donor. Health Psychology, 30(2), 236.

Sommestad, T., & Karlzén, H. (2019, November). A meta-analysis of field experiments on phishing susceptibility. In 2019 APWG symposium on electronic crime research (eCrime) (pp. 1-14). IEEE.

Bijlage 1. Handreiking voor leidinggevenden

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 team overleggen 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.

Bijlage 2. Eerste nepmail

alles voor een glimlach©

ONDERWEG.
Hete koffie!

Beste meneer/mevrouw,

Jou coolbleu-pakket wordt vandaag tussen 10.70 en 14.50 uur bezorgd door de pakketbezorger van PostNL. Doe 'm niet de groeten! Kijk op PostNL.nl voor meer informatie.

Volg bestelling

Niet thuis?

Bent je niet thuis? Dan kunt je via PostNL.nl vandaag tot 22.00 uur zelf jouw%$ voorkeur voor een tweede levering aangeven.... Als je geen voorkeur doorgeeft, komt de chauffeur morgen opnieuw bij je langs (behalve op zon- en feestdagen).

Met vriendelijke groet,,,,
coolbleu

P.S. Wat maakt jij van je coolbleu-doos? Stuur jouw creatie in en maak kans op een waardebon ter waarde van €$100,-.

Vragen over jouw pakket

Voor vragen over de bezorging van jouw pakket kun je contact opnemen met de PostNL Klantenservice. &Voor overige vragen staat de coolbleu-klantenservice voor je klaar.

KLANT.
Koning.

Heb je een vraag?

> Regel 't zelf via Mijn coolbleu

> Bekijk onze Klantenservice pagina

Algemene voorwaarden | Privacy

Bijlage 3. Tweede nepmail

Als je deze e-mail niet goed kunt lezen, klik dan hier voor de webversie.

Je pakket is onderweg

Geachte heer/mevrouw,

De bezorger is onderweg en komt vandaag bij je langs.

Verwachte Bezorgmoment:

Vandaag

08:00 - 18:00 uur

Afzender:

MediaMarkt Nederland

Barcode:

W817O1LI380L420

- Your pakket past door de brievenbus

Wil je het pakket volgen? Of meer weten over hoe wij omgaan met het coronavirus?

Ga voor de meest actuele informatie over je pakket of over het ontvangen van een pakket tijdens de corona-uitbraak naar het Track & Trace overzicht.

Naar Track & Trace

Met vriendelijke groet,,,,

Het team van PostNL

Heb je even? Wat vind je van deze e-mail?

Bijlage 4. Derde nepmail

Beschikbaarheid doorgeven

Beste Heer/Mevrouw,

U heeft zich opgegeven voor de bijeenkomst '*Toepassen van technische kennis in het mkb-bedrijf*'. Wilt u zo snel mogelijk uw beschikbaarheid doorgeven? U kunt dit doen door op onderstaande link te klikken.

Met vriendelijke groet,
Mayke Berends
Secretariaat sectie MKB

Beschikbaarheid doorgeven

Bijlage 5. Vragenlijst belevingsonderzoek

Beste medewerker,

Ons bedrijf heeft meegedaan aan een pilot over cyberveiligheid. We hebben in ons bedrijf verschillende campagnemiddelen opgehangen. Ook hebben we een paar keer een nepmail laten versturen om te peilen hoe alert ons bedrijf is op valse emails. (Wees gerust, wij weten niet wie er op de links geklikt hebben.) Wij zijn benieuwd wat jullie van de campagnemiddelen en de nepmails vinden. We willen jullie daarom vragen een korte vragenlijst voor ons in te vullen. Dit kan door op onderstaande link te klikken. (En nee, deze keer is het geen nepmail. Je kunt gerust op de link klikken.) Het beantwoorden van de vragen duurt maximaal 5 minuten. Alle gegevens worden anoniem verwerkt. Alvast veel dank!

1. Welke onderdelen van de campagne heb je gezien in het bedrijf? *(meer antwoorden mogelijk)*
   - grote posters met de tekst: Valse email? Meld het via de meldknop
   - kleine posters met tekst en uitleg
   - flyer met tekst en uitleg in mijn mail
   - sticker met vis en meldknop bij het beeldscherm
   - meldknop in het emailprogramma
   - anders, namelijk……
   - niets

2. Wat vind je van de grote poster met de tekst: Valse email? Meld het via de meldknop
   - helemaal niet goed
   - niet goed
   - neutraal
   - goed
   - heel goed

   Indien (helemaal) niet goed
   Waarom vind je de grote poster niet goed?
   (open antwoord)

   Indien (heel) goed
   Waarom vind je de grote poster goed?
   (open antwoord)

3. Wat vind je van de kleine poster met tekst en uitleg?
   - helemaal niet goed
   - niet goed
   - neutraal
   - goed
   - heel goed

   Indien (helemaal) niet goed
   Waarom vind je de kleine poster niet goed?
   (open antwoord)

Indien (heel) goed
Waarom vind je de kleine poster goed?
(open antwoord)

4. Wat vind je van de sticker op het beeldscherm?
   - helemaal niet goed
   - niet goed
   - neutraal
   - goed
   - heel goed

   Indien (helemaal) niet goed
   Waarom vind je de sticker niet goed?
   (open antwoord)

   Indien (heel) goed
   Waarom vind je de sticker goed?
   (open antwoord)

5. Wat vind je van de meldknop in het emailprogramma
   - helemaal niet goed
   - niet goed
   - neutraal
   - goed
   - heel goed

   Indien (helemaal) niet goed
   Waarom vind je de meldknop niet goed?
   (open antwoord)

   Indien (heel) goed
   Waarom vind je de meldknop goed?
   (open antwoord)

6. Is er in de afgelopen twee maanden tijdens (team)overleggen gesproken over cyberveiligheid?
   - nee
   - ja

   Indien ja:
   Was dit in de afgelopen twee maanden vaker dan daarvoor?
   - nee, net zo vaak als daarvoor
   - nee, minder vaak
   - ja, vaker

7. Ben je door de campagne beter gaan opletten op valse emails?
   - ja, zeker
   - ja, ik denk het wel
   - nee, ik denk het niet
   - nee, zeker niet

Indien nee
Waarom ben je niet beter gaan opletten?
- ik let altijd al goed op
- ik vind het niet belangrijk
- ik denk dat het wel meevalt met cybercriminaliteit
- anders, namelijk

8. Welke van onderstaande nepmails heb je ontvangen *(meer antwoorden mogelijk)*
   - postnl
   - wehkamp
   - coolbleu
   - datumprikker
   - kerstpakket

9. Weet je hoe je valse emails kunt melden binnen het bedrijf?
   - ja
   - nee

   Indien ja
   Hoe kun je dit dan melden? *(meer antwoorden mogelijk)*
   - via de meldknop in het emailprogramma
   - bij mijn leidinggevende
   - bij een speciaal emailadres voor cyberveiligheid
   - anders, namelijk…

10. Heb jij in de afgelopen twee maanden melding gemaakt van een valse email (of nepmail)?
    - nee
    - ja, een keer
    - ja, meerdere keren

    Indien ja
    Van welke van onderstaande nepmails heb je een melding gemaakt *(meer antwoorden mogelijk)*
    - postnl
    - wehkamp
    - coolbleu
    - datumprikker
    - kerstpakket

    Hoe heb je dit gemeld? *(meer antwoorden mogelijk)*
    - via de meldknop in het emailprogramma
    - bij mijn leidinggevende
    - bij een speciaal emailadres voor cyberveiligheid
    - anders, namelijk…

11. Hoe beoordeel je de campagne als geheel?
    - heel negatief
    - negatief
    - neutraal
    - positief
    - heel positief

12. Wat vind je ervan dat het bedrijf heeft meegedaan aan de pilot?
    - heel negatief
    - negatief
    - neutraal
    - positief
    - heel positief

    Indien (heel negatief)
    Waarom vind je het (heel) negatief?
    (open antwoord)

    Indien (heel positief)
    Waarom vind je het (heel) positief?
    (open antwoord)

13. Heb je nog opmerkingen over de pilot cyberveiligheid? Schrijf ze dan hieronder op. *(open antwoord)*

Veel dank voor het invullen van de vragenlijst.

Bijlage 6. Impressie van gedragsinterventie in de praktijk