MKB PHISHINGTEST

Onderzoeksrapport

Colofon

Dit rapport is opgesteld door het Behavioural Insights Team van het Ministerie Economische Zaken en Klimaat (BIT EZK) op verzoek van het Digital Trust Center (DTC) en Regionaal Platform Criminaliteitsbeheersing Noord-Holland (RPC NH).

Datum: 24 juni 2022

Samenvatting

Aanleiding
De afgelopen jaren is er een sterke toename van cybercriminaliteit. Phishing is één van de meest voorkomende vormen en is vaak het begin van andere cyberaanvallen (zoals malware en ransomware). Het mkb vormt een kwetsbare groep met betrekking tot cybercriminaliteit. Ruim een kwart van de medewerkers binnen het mkb heeft afgelopen jaar een phishingmail ontvangen. Bovendien zijn mkb-bedrijven vaak onderdeel van grotere toeleveringsketens van kritische processen, waardoor een kwetsbaar mkb-bedrijf gevolgen kan hebben voor een hele keten van bedrijven.

Doel
Het doel van de MKB Phishingtest is om inzicht te krijgen in de kwetsbaarheid van het mkb voor phishing en daarnaast te kijken hoe de cyberweerbaarheid van het mkb te vergoten. Aan de hand van een grootschalig veldexperiment (RCT) is daarbij onderzocht of een phishingtest een effectieve methode is om de cyberweerbaarheid van het mkb te vergroten en zo ja, hoe lang dit effect stand houdt.

Opzet
In totaal namen er 33.016 medewerkers werkzaam bij 667 bedrijven deel aan het experiment. Van mei tot en met oktober 2021 ontvingen zij ieder twee verschillende (imitatie) phishingmails met diverse tijdsintervallen. Zodra de medewerker op de link in de phishingmail klikte, belandde hij/zij op een feedbackpagina met informatie over waar ze de phishingmail aan hadden kunnen herkennen. Aan de hand van verschillende vragenlijsten zijn kenmerken van zowel de deelnemende bedrijven en medewerkers uitgevraagd om te onderzoeken of deze kenmerken samenhangen met het klikken op de phishingmail.

Conclusies
Op basis van de resultaten kunnen de onderstaande punten worden geconcludeerd. De uitgebreide resultaten en analyses zijn te vinden in hoofdstuk 3 van het rapport.

- *Het mkb is kwetsbaar voor phishing*. Ruim 1 op de 5 medewerkers (22%) werkzaam binnen het mkb klikte op een onbetrouwbare link in een generieke phishingmail.
- *Er zijn aanwijzingen voor een effect van een phishingtest op korte termijn, maar niet op de (middel)lange termijn*. Medewerkers die ongeveer een maand eerder een phishingmail hadden ontvangen klikten significant minder vaak op een tweede phishingmail dan de medewerkers die nog niet deze eerste phishingmail hadden ontvangen (9,9% t.o.v. 19,8%). Er was geen significant effect van een phishingtest op de middellange termijn (ca. 2,5 maand) en de lange termijn (ca. 3,5 maand).
- *Risicozoekende mensen hebben het meeste baat bij een phishingtest*.
  Risicovoorkeur bleek ook positief samen te hangen met een van de significante voorspellers voor het klikken op een phishingmail.

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

De afgelopen jaren is er in lijn met de ontwikkelingen op het gebied van digitalisering ook een sterke toename van cybercriminaliteit waarneembaar.[1] Uit het Cybersecurity onderzoek Veilig Online 2021 bleken phishingmails de meest voorkomende vorm binnen het bedrijfsleven in Nederland; ruim een kwart van de bedrijven heeft afgelopen jaar een phishingmail ontvangen.[2] In deze e-mails zitten vaak schadelijke links of zijn bijlagen toegevoegd wat het begin kan zijn van andere cyberaanvallen (zoals het installeren van malware ransomware, of identiteitsfraude). Uit de cybersecuritymonitor van CBS (2020) kwam naar voren dat grotere bedrijven vaker en meer verschillende maatregelen nemen tegen cyberdreigingen dan kleine(re) bedrijven.[3] Het mkb vormt een kwetsbare groep met betrekking tot cybercriminaliteit. Zij hebben niet altijd de juiste kennis, vaardigheden en middelen om zich te beschermen tegen cybercriminaliteit.[4] Ook hebben mkb-bedrijven niet altijd besef van de urgentie om maatregelen te nemen, hoewel ook zij vaak slachtoffer zijn van cybercriminaliteit.[2,5,6] Daarnaast is het mkb vaak onderdeel van grotere toeleveringsketens van kritische processen, waardoor een kwetsbaar mkb-bedrijf gevolgen kan hebben voor een hele keten van bedrijven.[7]

1.2 Gedragsanalyse

Om bedrijven weerbaar(der) te maken tegen cyberaanvallen is het nemen van technische maatregelen op zichzelf niet meer voldoende, menselijk gedrag is vaak de zwakste schakel. Cybercriminelen passen steeds vaker social engineering toe, waarbij ze gebruik maken van menselijke eigenschappen zoals nieuwsgierigheid, angst, hebzucht en onwetendheid om via phishing vertrouwelijke informatie te verkrijgen of malware te installeren en hiermee toegang te krijgen tot computersystemen, met alle gevolgen van dien. De afgelopen jaren worden deze phishingmails steeds realistischer ontworpen en hebben ze steeds vaker een zeer gepersonaliseerde boodschap, waardoor de mail voor de ontvanger lastig te onderscheiden is van de realiteit.

Vanuit de literatuur weten we dat de volgende gedragsfactoren een rol spelen bij het klikken op een link in een phishingmail:

- *Gebrek aan aandacht*: Te midden van de hoeveelheid informatie die op ons af komt, hebben mensen over het algemeen maar weinig aandacht en tijd om mails heel nauwkeurig te bekijken. Mensen klikken daarom vrij gedachteloos en uit gewoonte op links.
- *Kenmerken van het slachtoffer*: Mensen die meer vertrouwen hebben in anderen en minder geduldig zijn klikken over het algemeen vaker op een phishingmail. Mensen die meer risicomijdend zijn en meer computervaardig klikken over het algemeen minder vaak.[8]
- *Gebrek aan kennis/vaardigheden*: Mensen weten niet precies op welke kenmerken ze moeten letten om frauduleuze mails te herkennen. Meer kennis over de kenmerken van een phishingmail kan de weerbaarheid vergroten,[9] echter lijkt het ervaren van een phishingmail nuttiger.[10]

[1] Politie (2022), geregistreerde cybercrime misdrijven Nederland
[2] I&O Research (2021), Cybersecurity onderzoek Veilig Online 2021; Deelrapport bedrijfsleven
[3] CBS (2020), Cybersecurity Monitor
[4] CCV (2019), Nationaal Cybersecurity Bewustzijnsonderzoek
[5] MKB Nederland (2021), Cybercrime: álle alarmbellen moeten rinkelen
[6] De Haagse Hogeschool (2017), Nulmeting cybersecurity in het mkb
[7] CSAN (2021), Cyber Security Assessment Netherlands
[8] Curtis, S. R., Rajivan, P., Jones, D. N., & Gonzalez, C. (2018). Phishing attempts among the dark triad: Patterns of attack and vulnerability. Computers in Human Behavior, 87, 174-182.
[9] Norris, G., Brookes, A., & Dowell, D. (2019). The psychology of internet fraud victimisation: A systematic review. Journal of Police and Criminal Psychology, 34(3), 231-245.
[10] Baillon, A., De Bruin, J., Emirmahmutoglu, A., Van De Veer, E., & Van Dijk, B. (2019). Informing, simulating experience, or both: A field experiment on phishing risks. PloS one, 14(12), e0224216.

1.3 Doel en onderzoeksvragen

Het doel van de MKB Phishingtest is om inzicht te krijgen in de kwetsbaarheid van het mkb voor phishing en daarnaast te kijken hoe de cyberweerbaarheid van het mkb te vergoten.

Aan de hand van een grootschalig veldexperiment zijn daarbij de volgende onderzoekvragen onderzocht:

1) Is een phishingtest een effectieve methode om de cyberweerbaarheid van het mkb te vergroten?
2) En hangt dit effect af van het tijdsinterval waarmee deze phishingtest plaatsvindt?

De MKB Phishingtest is een samenwerking tussen het Regionaal Platform Criminaliteitsbeheersing Noord-Holland (RPC NH), het Digital Trust Center (DTC) en het Behavioural Insights Team van het Ministerie Economische Zaken en Klimaat (BIT EZK). De data-analyse is uitgevoerd door Erasmus Universiteit Rotterdam (EUR). De phishingtests zijn uitgevoerd door een extern IT-bedrijf.

2. Onderzoeksopzet

2.1 Proces

De verschillende stappen in het proces zijn weergegeven in figuur 1 en worden hieronder toegelicht.

Figuur 1. Visuele weergave van het proces van de MKB Phishingtest

Werving deelnemers

De bedrijven zijn op verschillende manieren geworven. Via nieuwsbrieven van verschillende brancheorganisaties, ondernemersverenigingen, en de netwerken van de initiatiefnemers zijn mkb-bedrijven geïnformeerd over de MKB Phishingtest. Omdat de respons hierop onvoldoende was, is besloten om te werven via het rechtstreeks aanschrijven van bedrijven. Er is een brief uitgestuurd met informatie over de MKB Phishingtest en aanmelding. Bedrijven konden via een formulier op de website van RPC aangeven dat ze interesse hadden om deel te nemen aan de MKB Phishingtest (zie bijlage A en B). Daarbij was er ook een aparte pagina op de website van DTC (zie bijlage C), waarop informatie over de phishingtest stond en werd doorverwezen naar de website van RPC om het bedrijf aan te melden voor de MKB Phishingtest. Bedrijven met minimaal 8 en maximaal 250 medewerkers (met een zakelijk e-mailadres) konden gratis deelnemen aan de MKB Phishingtest. Bedrijven met minder dan 8 werknemers konden niet deelnemen omdat de privacy van werknemers niet geborgd kon worden. Het rechtstreeks aanschrijven bleek effectief te zijn. In totaal deden er 33.016 medewerkers werkzaam bij 667 bedrijven mee aan de phishingtest.

Formaliseren deelname en randomisatie

Per bedrijf was er een contactpersoon voor de communicatie en afstemming met het IT-bedrijf over het versturen van de phishingmails. Om de deelname te formaliseren, moesten de contactpersonen van de bedrijven een dienstverleningsovereenkomst inclusief verwerkingsovereenkomst tekenen. Na ondertekening van deze documenten leverde de contactpersoon de zakelijke e-mailadressen van de medewerkers aan. Daarbij werd de contactpersoon ook verzocht een vragenlijst in te vullen over de verschillende kernmerken van het bedrijf (zie bijlage G). De bedrijven zijn vervolgens willekeurig toegewezen aan één van de onderzoeksgroepen (zie figuur 3). De onderzoeksgroepen zijn zo ingedeeld dat ze vergelijkbaar zijn op basis van het aantal bedrijven en kenmerken van die bedrijven (aantal werknemers, sector en IT-beveiliging).

Whitelisten

Voorafgaand aan de phishingtest is er onaangekondigd een testmail gestuurd om te controleren of deze mail in de spamfolder zou belanden. Bij 91% van de bedrijven kwam deze mail aan. Vervolgens werden in afstemming met de contactpersonen van de bedrijven de specifieke domeinnamen gewhitelist van de phishingmails die voor dit onderzoek gebruik zijn. Dit zorgt ervoor dat de phishingmails in het Postvak IN

van de medewerkers terechtkomen en niet worden tegengehouden door de mailserver of in de spamfolder belandt.

Versturen phishingmails

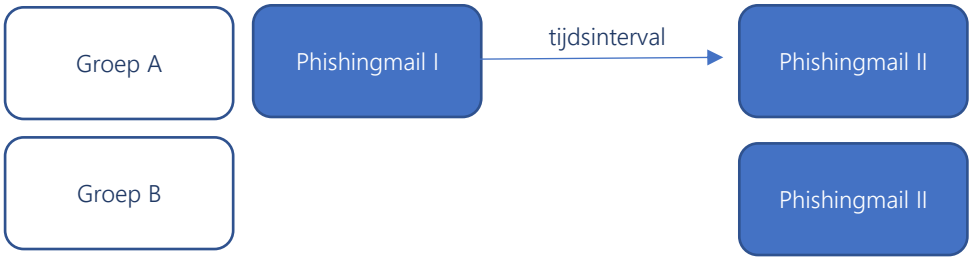
In de periode van mei tot en met oktober 2021 zijn de phishingmails uitgestuurd naar de medewerkers van de desbetreffende bedrijven. In figuur 3 is een overzicht weergegeven van wanneer welke type mail verstuurd is. Een week voor het versturen van de phishingmail werden de contactpersonen van de bedrijven geïnformeerd over het precieze moment van verzending. De contactpersonen werden erop geattendeerd om de medewerkers vooraf niet te informeren over de phishingmail en het moment van versturen. Zodra de medewerker op de link in de phishingmail klikte, belandde hij/zij op een feedbackpagina met informatie over waar ze de phishingmail aan hadden kunnen herkennen. In tegenstelling tot een 'echte' phishingmail had het klikken op de link in dit onderzoek uiteraard geen gevolgen. De inhoud van de verschillende phishingmails en feedbackpagina's zijn weergegeven in bijlage D, E en F. Een week na het versturen van de phishingmail werden de medewerkers verzocht een vragenlijst in te vullen (zie bijlage I).

Rapportage bedrijven

Na het versturen van beiden phishingmails naar het bedrijf, ontvingen de contactpersonen van de bedrijven een rapportage met de (anonieme) resultaten van hun bedrijf. Daarbij werden zij verzocht een vragenlijst in te vullen (zie bijlage H).

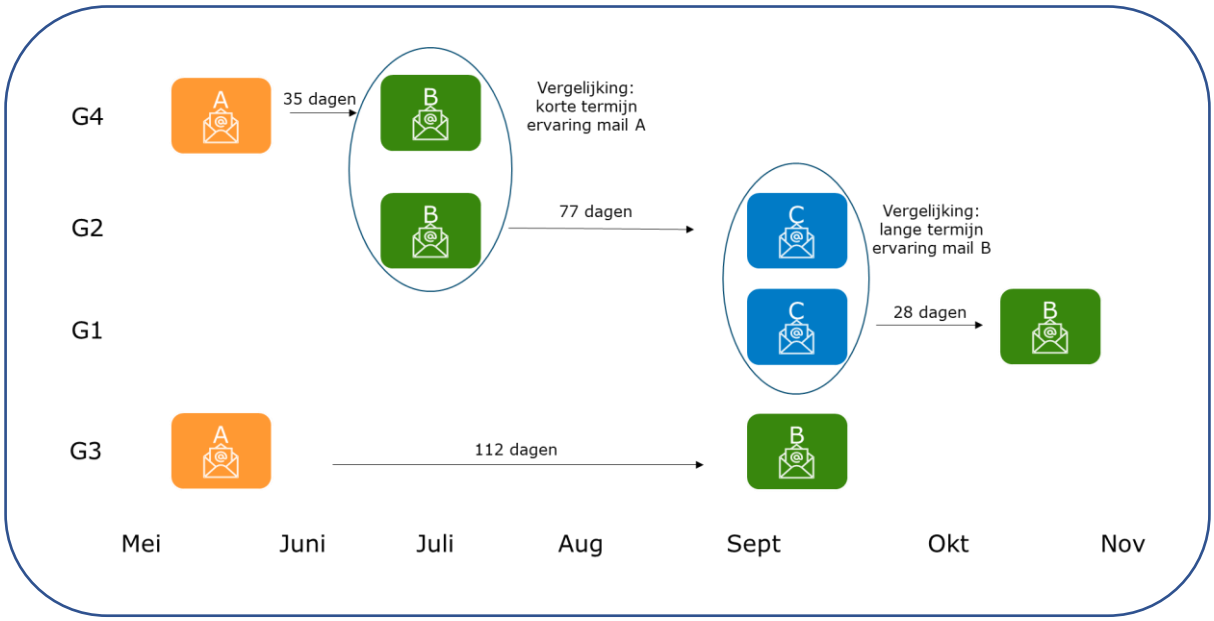
2.2 Onderzoeksdesign: RCT

Het versturen van de phishingmail is zowel een interventie als een manier om te meten welk gedrag wordt vertoond. Het doel van het versturen van de phishingmails op verschillende momenten is om te meten of de ervaring van een phishingtest (i.e. het ontvangen van een phishingmail en bij klikken op de link feedback ontvangen over hoe je een phishingmail herkent) leidt tot in het vervolg minder snel klikken op een link in een phishingmail. De toelichting hierop is gevisualiseerd in figuur 2. Het effect van de ervaring van "Phishingmail I" wordt gemeten door de klikpercentages bij "Phishingmail II" te vergelijken tussen groep A (die al eerder Phishingmail I ontving) en groep B (die niet eerder Phishingmail I ontving).



Figuur 2. Toelichting van het meten van het effect van een phishingmail

In dit onderzoek is gebruik gemaakt van een Randomized Control Trial (RCT). De deelnemende bedrijven werden ingedeeld in vier groepen. De groepen zijn zo ingedeeld dat ze vergelijkbaar zijn op basis van aantal bedrijven en kenmerken van die bedrijven (aantal werknemers, sector en IT-beveiliging). Elke groep ontving twee phishingmails op verschillen de momenten zoals weergegeven in figuur 3.



Figuur 3. Visualisatie onderzoeksdesign

2.3 Interventie: phishingmails en feedbackpagina

Voor de MKB Phishingtest zijn drie verschillende phishingmail scenario's uitgewerkt. Bij het uitwerken van de phishingmails is er rekening gehouden met de actualiteiten die op dat moment speelden en in hoeverre de inhoud van de phishingmail relevant is voor de verschillende mkb-bedrijven. Voorafgaand aan het experiment is er aan de hand van een pilot onderzoek gekeken of de phishingmails vergelijkbaar zijn op het gebied van: aanzetten tot actie, geloofwaardigheid en betrouwbaarheid. In de phishingmail werden medewerkers, net als in een 'echte' phishingmail, gestimuleerd om op de link in de phishingmail te klikken. Zodra zij op deze link klikten, belandden zij op een feedbackpagina. Op deze feedbackpagina

stond aangegeven dat het om een gesimuleerde phishingmail ging en stonden er een aantal tips over hoe zij de phishingmail hadden kunnen herkennen. In figuur 4 is een voorbeeld weergegeven van de feedbackpagina van phishingmail A. De inhoud van de alle phishingmails en de feedbackpagina's staan in bijlage G, H en I.

Figuur 4. Voorbeeld feedbackpagina van phishingmail A

2.4 Vragenlijsten

Naast het versturen van de phishingmails, zijn er ook verschillende vragenlijsten verstuurd naar zowel de contactpersonen van de deelnemende bedrijven als de medewerkers van deze bedrijven.

Vragenlijst contactpersoon bedrijven vooraf

Bij het formaliseren van de aanmelding is er door de contactpersonen ook een vragenlijst ingevuld (zie bijlage G). Deze vragenlijst omvatte vragen over de kenmerken van het bedrijf; aantal medewerkers, sector, mogelijke veranderingen in bedrijfsvoering en werkplek van de werknemers ten gevolge van de coronapandemie. Daarnaast zijn er ook verschillende vragen gesteld als indicator voor hoe gevoelig het bedrijf is voor phishingaanvallen; afhankelijkheid van internet en computers, uitbesteding IT-service, gebruik van cloudservice en back-ups).

Vragenlijst medewerkers

Een week na het versturen van elk van de phishingmails ontvingen alle medewerkers een vragenlijst over hun kenmerken (geslacht, leeftijd, risicoprofiel), hun ervaring met phishingmails en kennis over digitale veiligheid. Ook zijn er enkele (controle)vragen gesteld of ze de phishingmail hebben ontvangen, waar ze op dat moment werkten en of ze van tevoren zijn gewaarschuwd door hun werkgever of een collega. Deze vragenlijst is te vinden in bijlage I.

Vragenlijst contactpersoon bedrijven achteraf

Zodra beide phishingmails naar het bedrijf waren verstuurd, kregen de contactpersonen van de bedrijven een korte vragenlijst over hoe ze de phishingtest hadden ervaren en of ze van plan waren maatregelen te nemen om de weerbaarheid tegen phishing te vergroten (zie bijlage H).

3. Resultaten

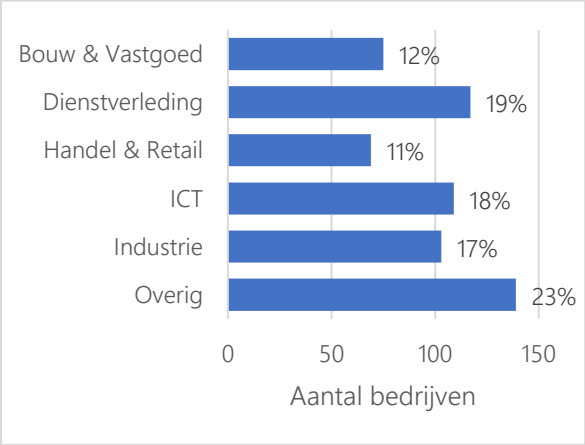
3.1 Analyse en exclusiecriteria

Er is een analyse uitgevoerd met de data van het klikken op de phishingmails en de kenmerken van de bedrijven en medewerkers op basis van de antwoorden op de verschillende vragenlijsten. In totaal zijn er 31.340 medewerkers werkzaam bij 620 bedrijven meegenomen in de analyse van de resultaten. Enkele bedrijven zijn uitgesloten van de analyse wanneer zij voldeden aan (één van) de exclusiecriteria:

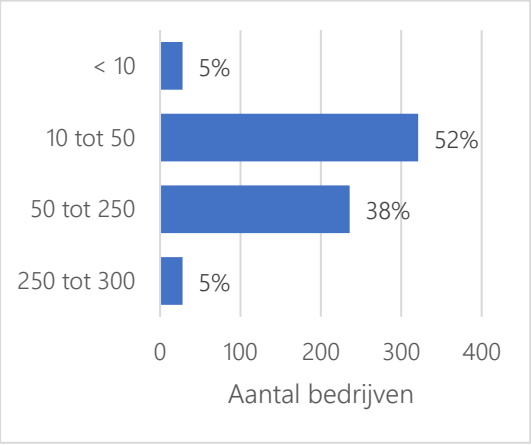
- *Bedrijven met een klikpercentages van 100% én waarbij alle kliks binnen dat bedrijf binnen 10 minuten plaatsvonden*. Bij deze bedrijven is het aannemelijk dat er sprake is van een URL-scanner die de mailinhoud checkt op spam. Hierbij wordt een "klik" geregistreerd, terwijl de mail (nog) niet is geopend door een medewerker. Het is daarbij niet te herleiden of de medewerker wel of niet op de mail heeft geklikt. 16 bedrijven vielen onder dit criterium en zijn niet meegenomen in de analyse.
- *Bedrijven waarbij meer dan 50% van de medewerkers die de vragenlijst hadden beantwoord aangaf vooraf door een werkgever op de hoogte te zijn gesteld over de phishing test*. Bij deze bedrijven zijn de klikpercentages niet meer betrouwbaar omdat medewerkers van tevoren over de mail zijn geïnformeerd. 31 bedrijven vielen onder dit criterium en zijn niet meegenomen in de analyse.

3.2 Kenmerken bedrijven

Hieronder zijn de resultaten weergeven van de antwoorden op de vragenlijst aan de contactpersonen van de bedrijven (n=620). De bedrijven die deelnemen aan de MKB Phishingtest zijn actief in verschillende sectoren (zie figuur 5). Daarnaast is aan de hand van het aantal medewerkers gekeken naar de bedrijfsgrootte van de deelnemende bedrijven (zie figuur 6).



Figuur 5. Aantal bedrijven per sector

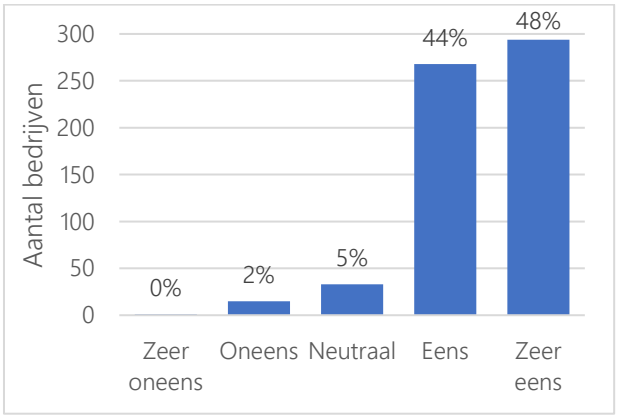


Figuur 6. Aantal medewerkers per bedrijf

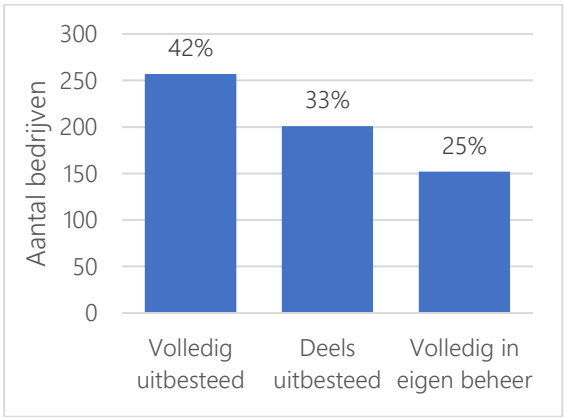
Afhankelijkheid van IT

Daarnaast zijn er verschillende vragen gesteld om een indicatie te krijgen hoe kwetsbaar het bedrijf is voor cyberaanvallen en hoe de IT-beveiliging van het bedrijf geregeld is. De resultaten zijn hieronder weergegeven:

- Het overgrote deel van de bedrijven (92%) geeft aan (zeer) afhankelijk te zijn van internet en computers (zie figuur 7).
- Op het gebied van het internetgebruik zijn er bij 39% van de bedrijven geen beleidsafspraken gemaakt (bijvoorbeeld met een inlogprocedure).
- Bij driekwart van de bedrijven (75%) is de IT-beveiliging deels of volledig uitbesteed aan een extern bedrijf (zie figuur 8).



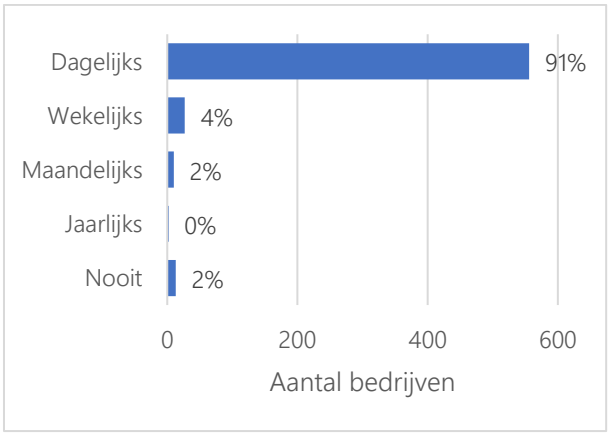
Figuur 7. Afhankelijkheid van internet en computers



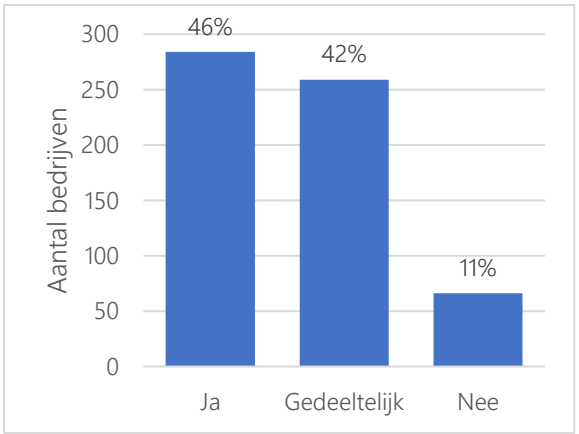
Figuur 8. Uitbesteding van IT-beveiliging

Gebruik cloudservices en back-ups

De frequentie van het maken van een back-up is erg hoog; 91% van de bedrijven maakt dagelijks een back-up (zie figuur 9). Ook is er een klein aantal bedrijven (2%) die helemaal geen back-ups maakt. Daarnaast maakt het overgrote deel van de bedrijven (88%) volledig of gedeeltelijk gebruik van cloudservices (zie figuur 10).



Figuur 9. Frequentie van het maken van back-ups



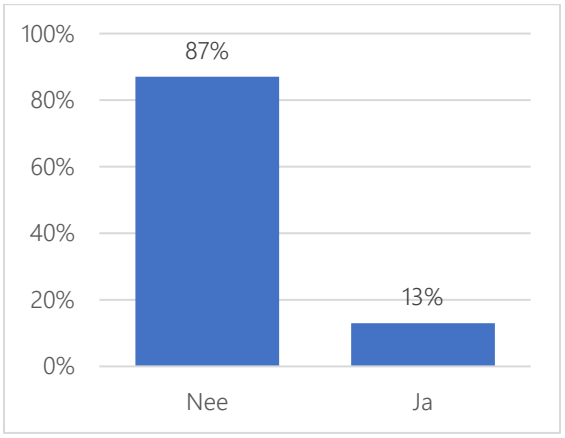
Figuur 10. Gebruik van cloudservices

3.3 Kenmerken medewerkers

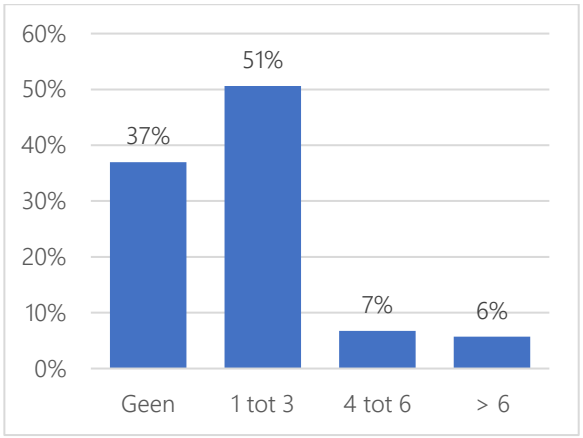
Van de 31.340 medewerkers die zijn meegenomen in de analyse, hebben 8.617 medewerkers de vragenlijst ingevuld na de 1e phishingmail en 7.374 medewerkers na de 2e phishingmail (38% vrouw; gemiddelde leeftijd = 42,8 jaar; SD = 11,9; range 17-67 jaar). Hieronder volgen de resultaten op basis van de antwoorden van de medewerkers op de vragenlijsten die zijn verstuurd na het ontvangen van de phishingmail.

Ervaring met phishing

Het overgrote deel van de medewerkers (87%) geeft aan nog nooit eerder slachtoffer te zijn geweest van phishing (zie figuur 11). In figuur 12 is weergegeven hoeveel phishingmails medewerkers de afgelopen 12 maanden hebben ontvangen (met uitzondering van de phishingmail uit het experiment).



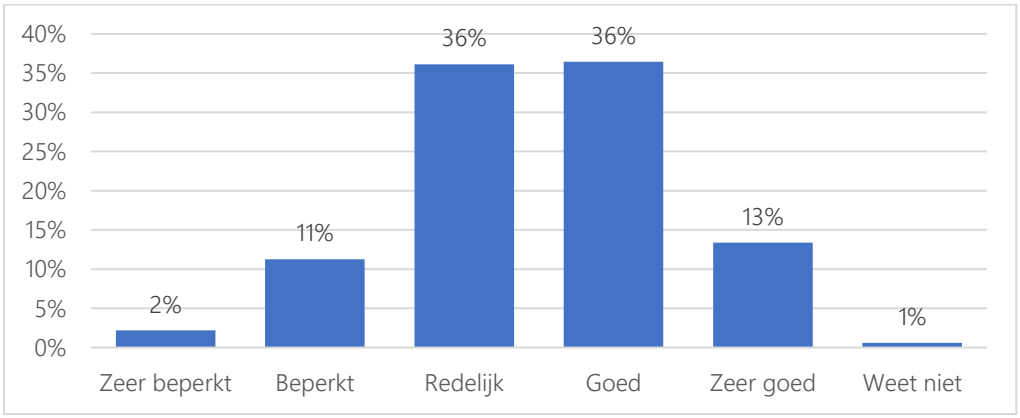
Figuur 11. Eerder slachtoffer phishing



Figuur 12. Aantal ontvangen phishingmails

Kennis over digitale veiligheid

De helft van de medewerkers (49%) gaf aan (zeer) goede kennis van digitale veiligheid te hebben. 13% van de medewerkers gaf aan dat deze kennis (zeer) beperkt is (zie figuur 13).



Figuur 13. Kennis over digitale veiligheid

3.4 Klikpercentages

Om inzicht te krijgen in de kwetsbaarheid van het mkb voor phishing en in de effectiviteit van een phishingtest om kwetsbaarheid te verlagen is er gekeken naar:

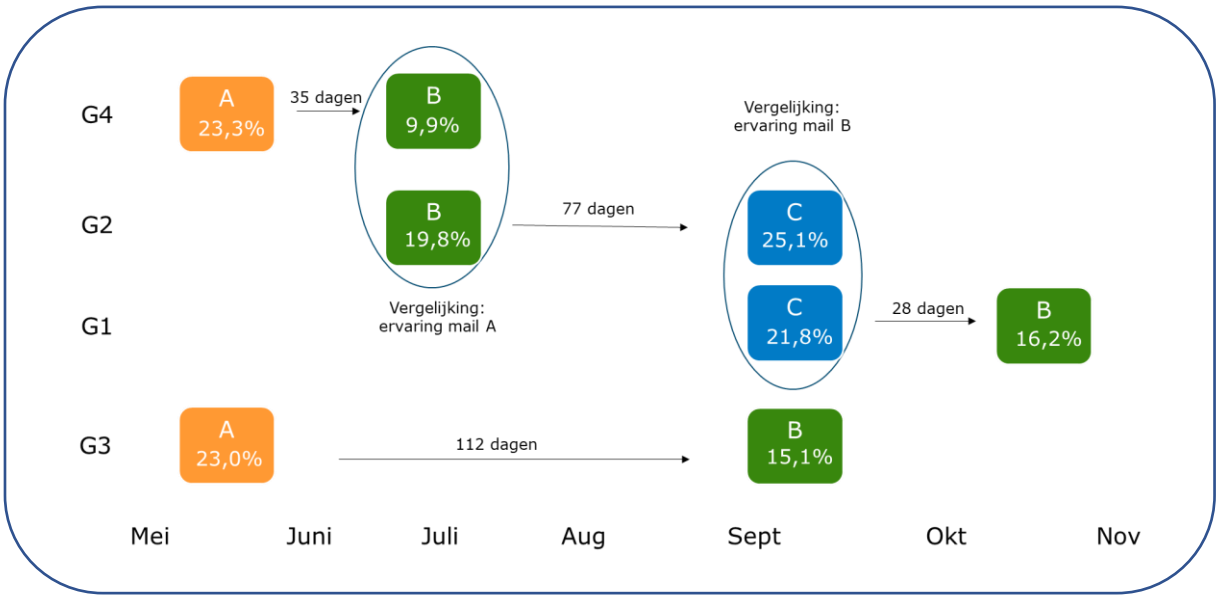
- *Gemiddelde klikpercentages per type mail, medewerkers- en bedrijfskenmerken*. Welk percentage van de medewerkers heeft op de phishingmails geklikt? En hoe verschillen de gemiddelde klikpercentages voor verschillende kenmerken van medewerkers en bedrijven?
- *Het effect van de phishingtest op klikgedrag*. Verlaagt het eerder hebben ontvangen van een (imitatie) phishingmail het klikpercentage op de volgende (imitatie)phishingmail? Op basis van een regressie analyse is gekeken welke voorspellende waarde een phishingtest heeft op klikgedrag. Doordat er bij verschillende onderzoeksgroepen verschillende tijdsintervallen zaten tussen de eerste en de tweede mail kunnen uitspraken gedaan worden over een effect op korte termijn (ca. 1 maand), middellange termijn (ca. 2,5 maand) en lange termijn (ca. 3,5 maand).
- *De samenhang tussen kenmerken van medewerkers en klikgedrag*. Op basis van een regressiemodel is gekeken hoe verschillende kenmerken van medewerkers samenhangen met het klikgedrag en de effecten van de phishingtest.

Er zijn verschillende analyses uitgevoerd met betrekking tot het klikgedrag van de medewerkers in relatie tot verschillende bedrijfskenmerken en kenmerken van medewerkers. Aan de ene kant is gekeken naar de absolute getallen van de gemiddelde klikpercentages. Aan de andere kant is er in een regressieanalyse onderzocht in hoeverre verschillende factoren een voorspellende waarde hebben voor het wel of niet klikken op een phishingmail.

Gemiddelde klikpercentages per type mail

Als je kijkt naar alle eerste momenten waarop de onderzoeksgroepen een phishingmail ontvingen, klikte gemiddeld 22% van de medewerkers. Onder 'klikken' wordt verstaan dat een medewerker de phishingmail heeft geopend en op de link in de phishingmail heeft geklikt. Dit eerste moment is belangrijk omdat de deelnemers hier nog niet beïnvloed waren door de phishingtest. Er waren geen grote verschillen in gemiddelde klikpercentages tussen de type mails, wat suggereert dat de phishingmails vergelijkbaar waren in hoe moeilijk ze te detecteren waren.

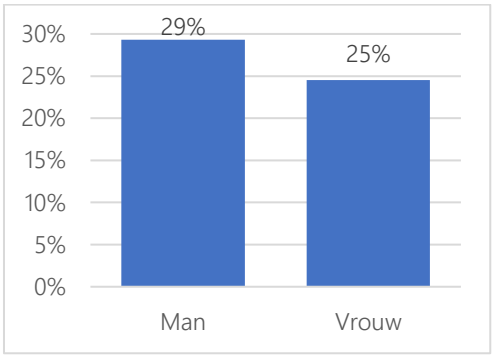
In figuur 14 is een overzicht weergegeven van de gemiddelde klikpercentages van de verschillende mails op de verschillende momenten.



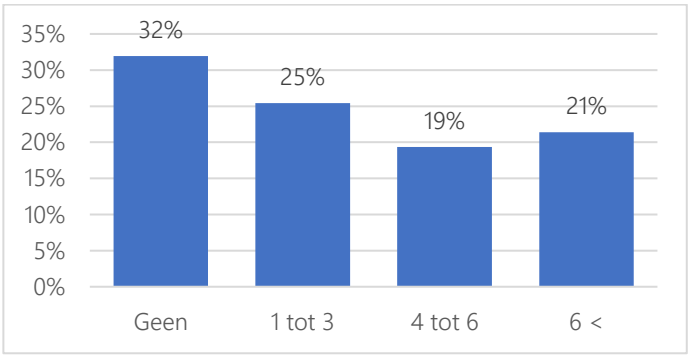
Figuur 14. Overzicht gemiddelde klikpercentages per phishingtest

Gemiddelde klikpercentages en kenmerken medewerkers

Ook is gekeken naar de gemiddelde klikpercentages en de verschillende kenmerken van de medewerkers op basis van de antwoorden uit de eerste vragenlijst (n=8.617).[11] Er is specifiek gekeken naar de gemiddelde klikpercentages van de eerste momenten waarop de onderzoeksgroepen een phishingmail ontvingen, aangezien deze percentages nog niet beïnvloed zijn door de phishingtest. Hieruit resulteerde dat mannen vaker op de link in de phishingmail klikten dan vrouwen (zie figuur 15). Ook is gekeken naar de ervaring van medewerkers met phishingmails. In figuur 16 zijn de gemiddelde klikpercentages weergeven op basis van het aantal phishingmails dat medewerkers de afgelopen 12 maanden hebben ontvangen (met uitzondering van de phishingmail uit het experiment). Hieruit bleek dat medewerkers die de afgelopen 12 maanden geen phishingmails hadden ontvangen gemiddeld vaker klikten dan medewerkers die wel eerder phishingmails hadden ontvangen.



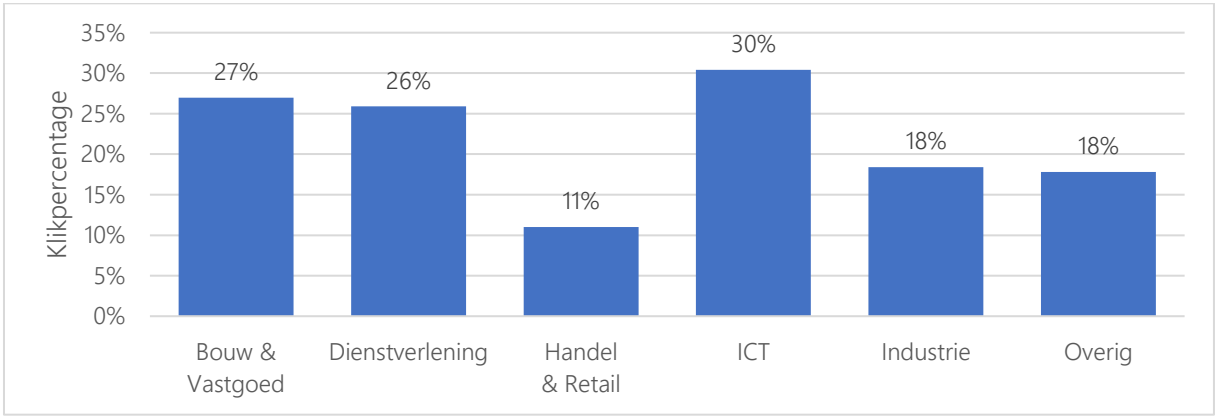
Figuur 15. Klikpercentages en geslacht



Figuur 16. Klikpercentages en aantal ontvangen phishingmails

Gemiddelde klikpercentage en bedrijfskenmerken

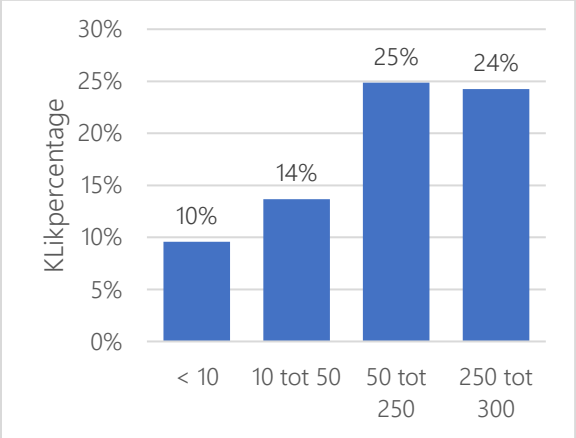
Ook is gekeken naar de gemiddelde klikpercentages en de verschillende bedrijfskenmerken op basis van de vragenlijst die de bedrijven vooraf hebben ingevuld (n=620). Hierbij is gekeken naar de gemiddelde klikpercentages van de eerste momenten waarop de onderzoeksgroepen een phishingmail ontvingen, aangezien deze percentages nog niet beïnvloed zijn door de phishingtest. In figuur 18 zijn de gemiddelde klikpercentages per sector weergegeven. Binnen de sectoren kunnen er allerlei onderliggende verschillen zijn tussen de kenmerken van medewerkers uit deze sector die deze verschillen in gemiddelde klikpercentages kunnen verklaren.



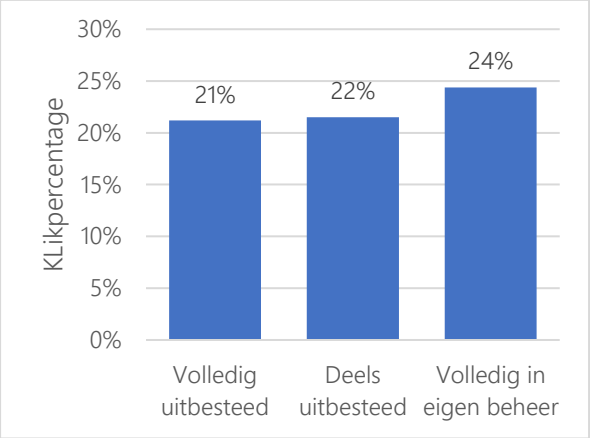
Figuur 18. Gemiddelde klikpercentages per sector

[11] Bij het interpreteren van deze klikpercentages moet rekeningen worden gehouden dat dit gaat over een gedeelte van het totaal aantal medewerkers. Mogelijk is er bij het invullen van de vragenlijst sprake van een zelfselectie bias. Van de medewerkers die de vragenlijst hebben ingevuld was het klikpercentage van alle eerste phishingmails gemiddeld 27,5%.

In figuur 19 zijn de klikpercentages weergegeven in verhouding tot het aantal medewerkers per bedrijf. Medewerkers die werkzaam zijn bij relatief grotere bedrijven (50 tot 300 medewerkers) klikken vaker op de phishingmails dan medewerkers die werkzaam zijn bij relatief kleinere bedrijven (tot 50 medewerkers). Bij de klikpercentages in verhouding tot uitbesteding van de IT-beveiliging zijn er geen grote verschillen tussen de klikpercentages op de eerste phishingmail (zie figuur 20).



Figuur 19. Klikpercentages en aantal medewerkers



Figuur 20. Klikpercentage en IT-beveiliging

Effect van phishingtest op klikgedrag

Daarnaast is gekeken naar het effect van het ervaren van een eerdere phishingtest op het vervolgens klikken op een volgende phishingmail. Zijn medewerkers beter in staat een phishingmail te herkennen als zij eerder een phishingtest hebben ervaren? En hoe lang houdt een eventueel effect aan?

In het eerste regressiemodel (bijlage J, model 1) is gekeken naar het effect van de ervaring van een phishingmail met verschillende tijdsintervallen op het wel of niet klikken op de volgende phishingmail. Uit de resultaten van de regressie analyse kunnen we opmaken dat:

- Er zijn aanwijzingen voor een effect van de ervaring van phishingmail A op de korte termijn. Oftewel, de ervaring van mail A resulteert in significant minder klikken op mail B, die 33 dagen later werd verstuurd (B=-0,10; p<0,1). Medewerkers die voorafgaand aan mail B in juli al eerder mail A in mei hadden ontvangen klikten significant minder (groep 4; 9,9%) dan medewerkers die geen eerdere phishingmail hadden ontvangen (groep 2; 19,8%). Er is geen significant effect van de ervaring van mail C op het klikken op mail B op de korte termijn.[12]
- Er is geen bewijs voor een effect van de ervaring van phishingmail B op de middellange termijn. Er is geen significant verschil tussen de klikpercentages op mail C in september van de medewerkers die zo'n 2,5 maand (77 dagen) eerder al mail B hadden ontvangen (groep 2; 25,1%) en de medewerkers die nog niet eerder een phishingmail hadden ontvangen (groep 1; 21,8%).
- Er is geen bewijs voor een effect van de ervaring van phishingmail A op de lange termijn.[12] Er is geen significant verschil tussen het klikpercentage op mail B in september van de medewerkers die zo'n 3,5 maand (112 dagen) eerder mail A hadden ontvangen (groep 3; 15,1%) en het klikpercentage op mail B in juli van de medewerkers die nog niet eerder phishingmail hadden ontvangen (groep 2; 19,8%).

[12] Dit is geen zuivere vergelijking maar een benadering van het effect van de phishingmail, omdat de klikpercentages van de medewerkers worden vergeleken die niet op hetzelfde moment dezelfde phishingmail ontvingen.

Samenhang kenmerken medewerkers met klikgedrag

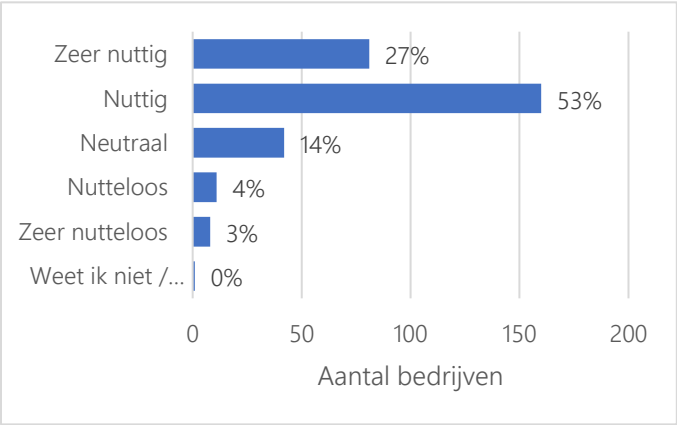
Vervolgens is er ook een regressie gedaan waarbij de antwoorden van de medewerkersvragenlijsten zijn toegevoegd in het regressiemodel (bijlage J, model 2). Hierbij kon alleen de data van het klikgedrag van de medewerkers worden meegenomen die ook de vragenlijst hadden ingevuld.
In dit model is onderzocht welke individuele kenmerken van de medewerkers samenhingen met het wel of niet klikken op de link in de phishingmail. Belangrijk om hierbij te noemen dat het bij de medewerkerskenmerken gaat om de samenhang met het klikgedrag, en niet om een causaal verband. Dit in tegenstelling tot de effecten van de ervaring van de phishingmails, waarbij je door de onderzoeksopzet wel conclusies kan trekken over causaliteit.
Uit dit regressiemodel kwam naar voren dat vrouwen marginaal significant minder vaak klikken dan mannen (B=-0,04; p<0,1; zie figuur 15) en dat medewerkers die aangaven dat zij de afgelopen 12 maanden geen phishingmail hadden ontvangen vaker klikten dan medewerkers die aangaven één of meerdere phishingmail(s) te hebben ontvangen (B=0,04; p<0,01, zie figuur 16). Ook bleek het persoonskenmerk risicovoorkeur een significante voorspeller; medewerkers die aangaven in het algemeen in hun leven meer risicozoekend te zijn klikten vaker dan medewerkers die aangaven meer risicomijdend te zijn (B=0,05; p<0,05).

Om te onderzoeken of de phishingtest ook een ander effect heeft op mensen die meer of minder risicozoekend zijn, is er nog een regressiemodel uitgevoerd (bijlage K, model 3). De resultaten van dit regressiemodel laten zien dat er een significant interactie-effect is (B=-0.12; p<0,01). Het effect van de ervaring van phishingmail A op later klikgedrag lijkt gedreven te worden door risicovoorkeur. Oftewel, medewerkers die aangeven meer risicozoekende te zijn, hebben meer baat bij de ervaring van phishingmail A op korte termijn dan medewerkers die aangeven risicomijdend te zijn.

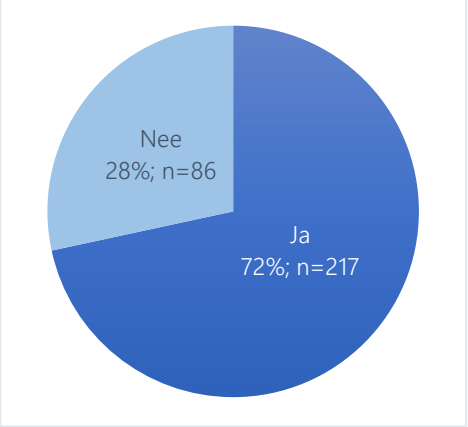
3.5 Vervolgstappen bedrijven

Zodra beide phishingmails naar het bedrijf waren verstuurd, ontvingen de contactpersonen van de bedrijven een rapportage met de (anonieme) resultaten van hun bedrijf en een vragenlijst over hoe nuttig zij de test hebben ervaren en welke vervolgstappen het bedrijf eventueel van plan is op te nemen. De resultaten van deze vragenlijst zijn hieronder weergegeven (n=303).

80% van de bedrijven gaf aan dat ze het (zeer) nuttig vonden om deel te nemen aan de MKB Phishingtest (zie figuur 21). Daarbij zijn ook enkele vragen gesteld over de eventuele maatregelen die het bedrijf van plan is de komende periode te nemen om de cyberweerbaarheid van hun bedrijf te vergroten. Bijna driekwart van de bedrijven (72%) gaf aan dit van plan te zijn (zie figuur 22).

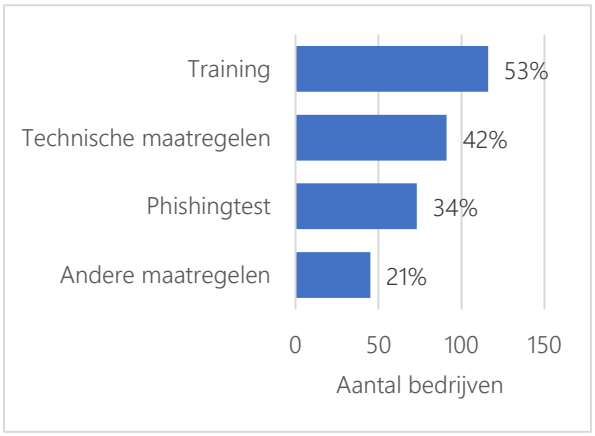


Figuur 21. Ervaring deelname aan MKB Phishingtest

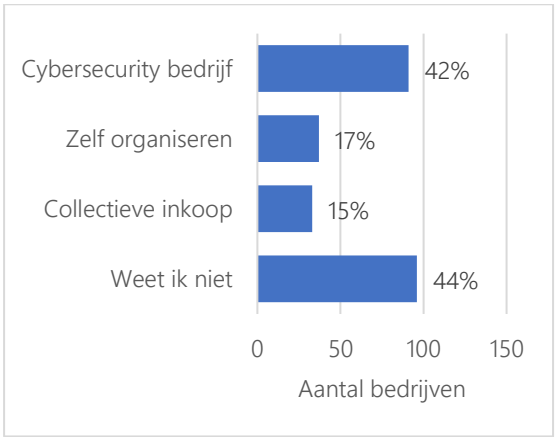


Figuur 22. Van plan om maatregelen te nemen

Aan de contactpersonen van de bedrijven die aangaven maatregelen te willen nemen (n=217) werd ook gevraagd welke maatregelen ze van plan waren te nemen, waarbij meerdere antwoorden mogelijk waren (zie figuur 23). De meest gekozen maatregel was het geven van een training aan werknemers over cybersecurity (53%), gevolgd door het nemen van technische maatregelen (42%) en het (vaker) uitvoeren van een phishingtest (34%). Andere maatregelen die in de open antwoorden genoemd werden: medewerkers informeren over de gevaren van cybersecurity, bewustwording creëren (door een campagne) en het opstellen van een protocol of ICT gedragscode. Daarnaast kwam in veel antwoorden terug dat dit niet gaat om een eenmalige, maar herhaaldelijke acties gaat. Ook is gevraagd op welke manier het bedrijf een phishingtest zou willen uitvoeren, waarbij meerdere antwoorden mogelijk waren (zie figuur 24). Een groot deel van de contactpersonen (44%) gaf aan dit nog niet te weten. Van de andere opties bleek het uitvoeren door een cybersecurity bedrijf (42%) de meest populaire optie, gevolgd door het zelf organiseren van een phishingtest (17%) en het collectief inkopen van een phishingtest (15%).



Figuur 23. Type maatregel



Figuur 24. Uitvoering van phishingtest

4. Conclusies en aanbevelingen

Het doel van de MKB Phishingtest is om inzicht te krijgen in de kwetsbaarheid van het mkb voor phishing en daarnaast te kijken hoe de cyberweerbaarheid van het mkb te vergoten. Aan de hand van een grootschalig veldexperiment (RCT) is verder onderzocht of een phishingtest een effectieve methode is om de cyberweerbaarheid van het mkb te vergroten en of dit effect afhangt van het tijdsinterval waarbij deze phishingtest plaatsvindt. Op basis van de resultaten kunnen een aantal zaken worden geconcludeerd.

Het mkb is kwetsbaar voor phishing

Ruim 1 op de 5 medewerkers (22%) werkzaam binnen het mkb klikte op een onbetrouwbare link in een generieke phishingmail. Naar alle waarschijnlijkheid is dit percentage een onderschatting van de kwetsbaarheid van het MKB voor phishingaanvallen. Hogere klikpercentages vallen te verwachten, wanneer door cybercriminelen specifieke phishingmails worden ingezet. Denk hierbij bijvoorbeeld aan het versturen van een phishingmail waarin het net lijkt of je te maken hebt met een collega of een bestaande relatie of waarin de medewerker persoonlijk bij naam wordt aangeschreven in plaats van een algemene aanhef. Daarnaast klikten medewerkers die aangaven afgelopen 12 maanden géén phishingmail te hebben ontvangen gemiddeld vaker op de link in de phishingmail dan medewerkers die aangaven één of meerdere phishingmails te hebben ontvangen (geen mails, 32%; 1 tot 3 mails, 25%; 4 tot 6 mails, 19%; >6 mails, 21%). Dit suggereert dat medewerkers die beter een phishingmail kunnen herkennen minder vaak klikken.

Er zijn aanwijzingen voor een effect van een phishingtest op de korte termijn, maar niet op de (middel)lange termijn

Aan de hand van een regressieanalyse is gekeken in hoeverre de ervaring van het ontvangen van phishingmails met verschillende tijdsintervallen een voorspellende waarde heeft voor het wel of niet klikken op een phishingmail. Hieruit bleek dat er aanwijzingen zijn voor een effect van het ervaren van een generieke phishingmail op de korte termijn; medewerkers die ongeveer een maand eerder een phishingmail hadden ontvangen klikten significant minder vaak op een tweede phishingmail dan de medewerkers die nog niet deze eerste phishingmail hadden ontvangen. Er was geen significant effect van een phishingtest op de middellange termijn (ca. 2,5 maand) en de lange termijn (ca. 3,5 maand).

Risicozoekende mensen hebben het meeste baat bij een phishingtest

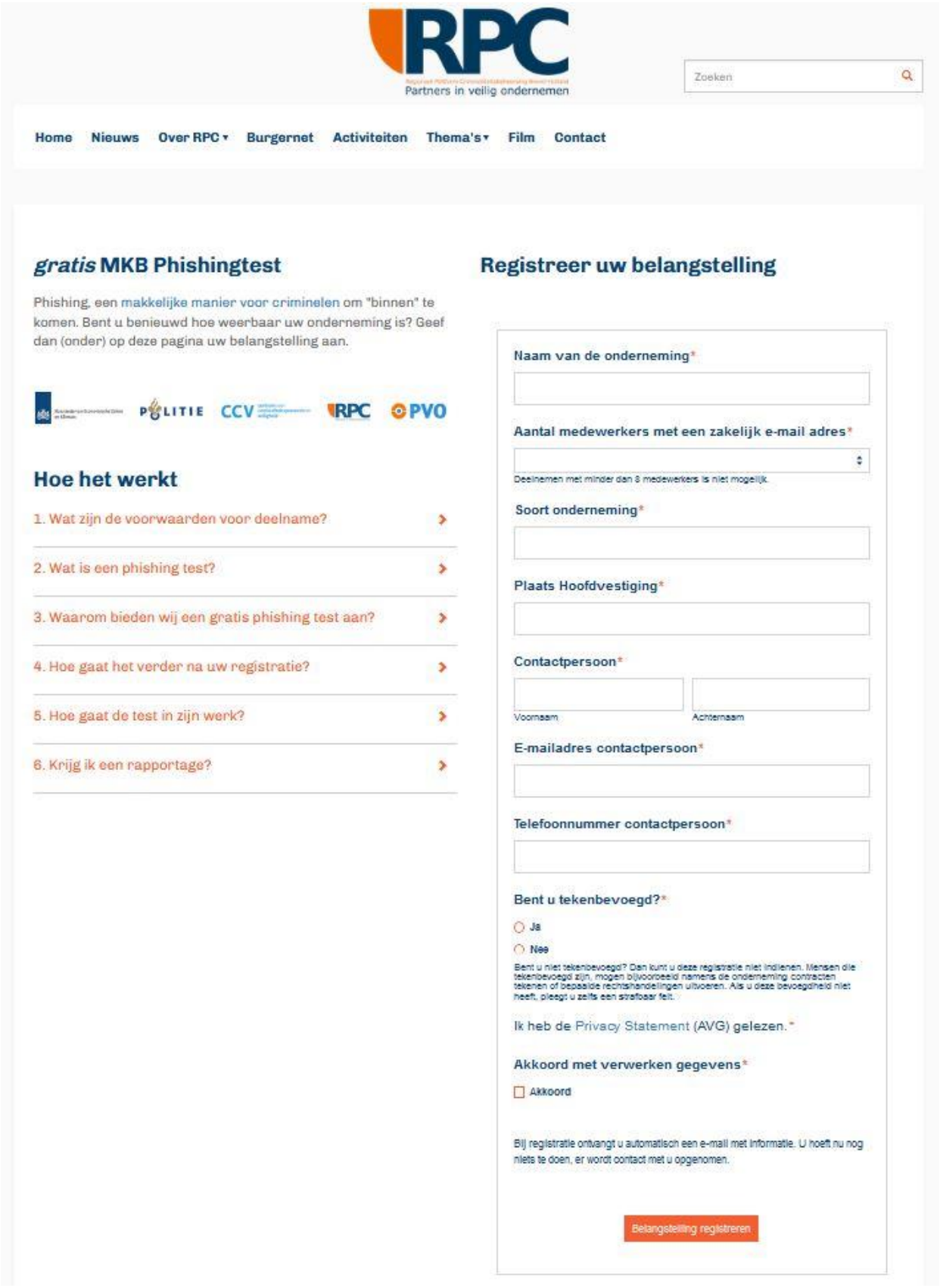
Risicovoorkeur bleek een van de significante voorspellers voor het klikken op een phishingmail. Uit verdere regressieanalyses bleek dat er een interactie-effect is tussen risicovoorkeur en het korte termijn effect van een phishingtest. Oftewel, medewerkers die aangeven meer risicozoekende te zijn hebben meer baat bij de ervaring van een phishingtest op korte termijn dan medewerkers die aangeven meer risicomijdend te zijn.

Een eerste stap om de cyberweerbaarheid van het mkb te vergroten is het vergroten van het urgentiebesef voor het nemen van maatregelen tegen cybercriminaliteit. De MKB Phishingtest heeft hieraan bijgedragen door de (anonieme) resultaten in een bedrijfsrapportage terug te koppelen aan het bedrijf met daarbij tips om het bedrijf weerbaarder te maken tegen phishingaanvallen. Daarnaast hebben medewerkers met hun deelname kennis en ervaringen opgedaan door het ontvangen van de (imitatie) phishingmails en de feedback die is meegegeven over het herkennen van een phishingmail.

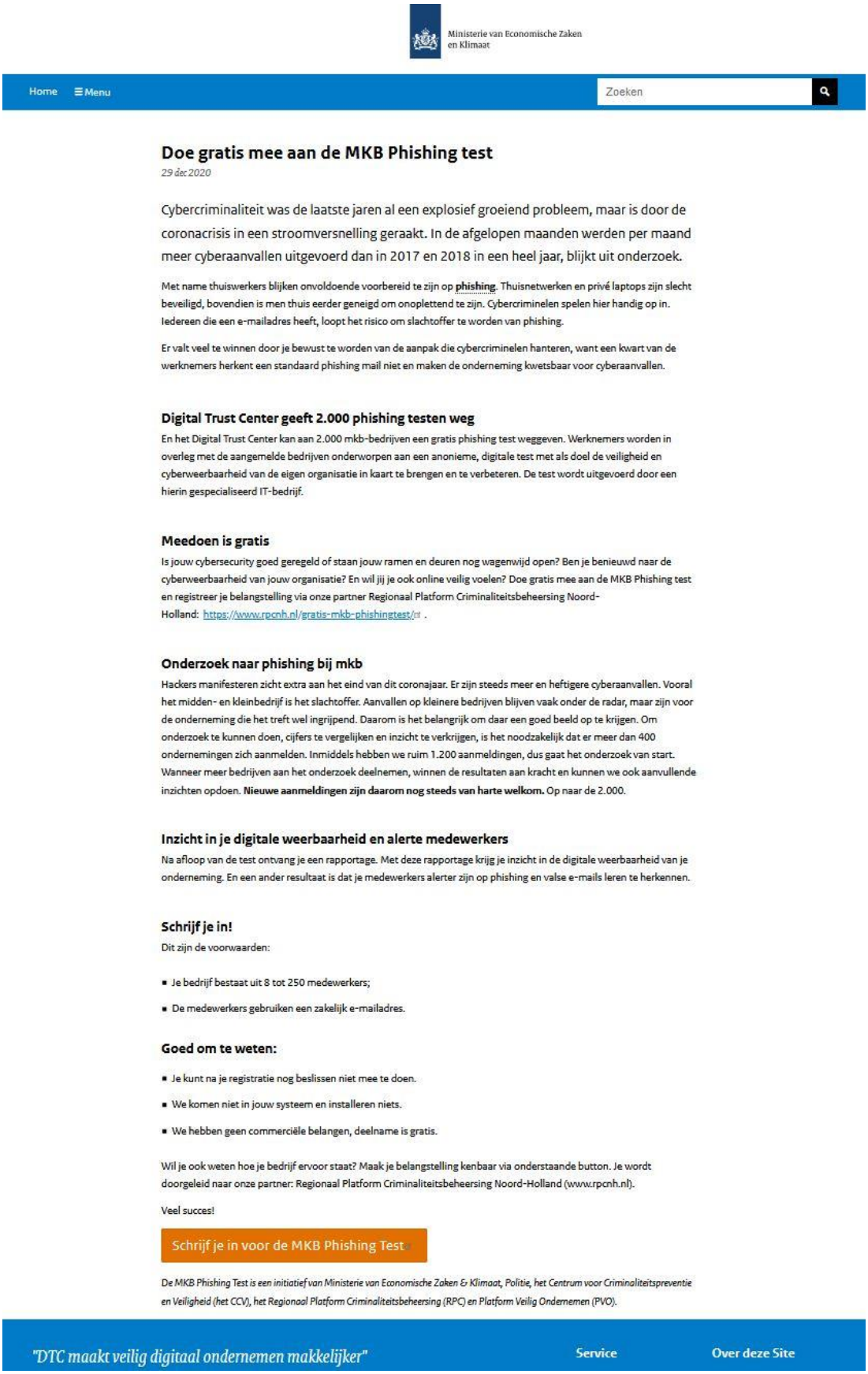
5. Bijlagen

A. Landingspagina website RPC

B. Aanmeldformulier website RPC



C. Landingspagina website DTC



Ministerie van Economische Zaken en Klimaat

Home ☰ Menu Zoeken

Doe gratis mee aan de MKB Phishing test

29 dec 2020

Cybercriminaliteit was de laatste jaren al een explosief groeiend probleem, maar is door de coronacrisis in een stroomversnelling geraakt. In de afgelopen maanden werden per maand meer cyberaanvallen uitgevoerd dan in 2017 en 2018 in een heel jaar, blijkt uit onderzoek.

Met name thuiswerkers blijken onvoldoende voorbereid te zijn op **phishing**. Thuisnetwerken en privé laptops zijn slecht beveiligd, bovendien is men thuis eerder geneigd om onoplettend te zijn. Cybercriminelen spelen hier handig op in. Iedereen die een e-mailadres heeft, loopt het risico om slachtoffer te worden van phishing.

Er valt veel te winnen door je bewust te worden van de aanpak die cybercriminelen hanteren, want een kwart van de werknemers herkent een standaard phishing mail niet en maken de onderneming kwetsbaar voor cyberaanvallen.

Digital Trust Center geeft 2.000 phishing testen weg

En het Digital Trust Center kan aan 2.000 mkb-bedrijven een gratis phishing test weggeven. Werknemers worden in overleg met de aangemelde bedrijven onderworpen aan een anonieme, digitale test met als doel de veiligheid en cyberweerbaarheid van de eigen organisatie in kaart te brengen en te verbeteren. De test wordt uitgevoerd door een hierin gespecialiseerd IT-bedrijf.

Meedoen is gratis

Is jouw cybersecurity goed geregeld of staan jouw ramen en deuren nog wagenwijd open? Ben je benieuwd naar de cyberweerbaarheid van jouw organisatie? En wil jij je ook online veilig voelen? Doe gratis mee aan de MKB Phishing test en registreer je belangstelling via onze partner Regionaal Platform Criminaliteitsbeheersing Noord-Holland: https://www.rpcnh.nl/gratis-mkb-phishingtest/ .

Onderzoek naar phishing bij mkb

Hackers manifesteren zicht extra aan het eind van dit coronajaar. Er zijn steeds meer en heftigere cyberaanvallen. Vooral het midden- en kleinbedrijf is het slachtoffer. Aanvallen op kleinere bedrijven blijven vaak onder de radar, maar zijn voor de onderneming die het treft wel ingrijpend. Daarom is het belangrijk om daar een goed beeld op te krijgen. Om onderzoek te kunnen doen, cijfers te vergelijken en inzicht te verkrijgen, is het noodzakelijk dat er meer dan 400 ondernemingen zich aanmelden. Inmiddels hebben we ruim 1.200 aanmeldingen, dus gaat het onderzoek van start. Wanneer meer bedrijven aan het onderzoek deelnemen, winnen de resultaten aan kracht en kunnen we ook aanvullende inzichten opdoen. **Nieuwe aanmeldingen zijn daarom nog steeds van harte welkom.** Op naar de 2.000.

Inzicht in je digitale weerbaarheid en alerte medewerkers

Na afloop van de test ontvang je een rapportage. Met deze rapportage krijg je inzicht in de digitale weerbaarheid van je onderneming. En een ander resultaat is dat je medewerkers alerter zijn op phishing en valse e-mails leren te herkennen.

Schrijf je in!

Dit zijn de voorwaarden:

- Je bedrijf bestaat uit 8 tot 250 medewerkers;
- De medewerkers gebruiken een zakelijk e-mailadres.

Goed om te weten:

- Je kunt na je registratie nog beslissen niet mee te doen.
- We komen niet in jouw systeem en installeren niets.
- We hebben geen commerciële belangen, deelname is gratis.

Wil je ook weten hoe je bedrijf ervoor staat? Maak je belangstelling kenbaar via onderstaande button. Je wordt doorgeleid naar onze partner: Regionaal Platform Criminaliteitsbeheersing Noord-Holland (www.rpcnh.nl).

Veel succes!

Schrijf je in voor de MKB Phishing Test

De MKB Phishing Test is een initiatief van Ministerie van Economische Zaken & Klimaat, Politie, het Centrum voor Criminaliteitspreventie en Veiligheid (het CCV), het Regionaal Platform Criminaliteitsbeheersing (RPC) en Platform Veilig Ondernemen (PVO).

"DTC maakt veilig digitaal ondernemen makkelijker" Service Over deze Site

D. Phishingmail A en feedbackpagina

Phishingmail A

Titel: Bedankje in Coronatijd namens je werkgever
Afzender: anna@bedrijfsgeschenken.nl

Beste werknemer,

Al ruim een jaar hebben we te maken met de gevolgen van COVID-19. Het heeft op ons allemaal invloed, privé en zakelijk. Je werkgever wil je graag een hart onder de riem steken en je bedanken voor je inzet in de afgelopen periode. Daarom mogen wij jou blij maken met een cadeau.

Kies vandaag nog jouw cadeau uit in onze webshop, dan heb je het morgen in huis.

Met vriendelijke groeten,

Anna de Wit
Bedrijfsgeschenken.com

Bedrijfsgeschenken
Omdat medewerkers waardevol zijn

Feedbackpagina

E. Phishingmail B en feedbackpagina

Phishingmail B

Titel: Controleer of uw persoonsgegevens gehackt zijn
Afzender: r.meijer@ncdv.nl

Geachte meneer/mevrouw,

De afgelopen maanden zijn bij een aantal toonaangevende organisaties persoonsgegevens gehackt, waardoor de kans groot is dat ook uw persoonsgegevens op straat liggen. Vanuit het Nationaal Centrum Digitale Veiligheid (NCDV) is aan de hand van een grootschalig onderzoek een database samengesteld waarin u kunt achterhalen of uw gegevens zijn gestolen.

Voorkom dat u slachtoffer wordt van cybercriminaliteit. Controleer hier direct of uw gegevens openbaar zijn.

Met vriendelijke groeten,

Roos Meijer
Nationaal Centrum Digitale Veiligheid

Nationaal Centrum Digitale Veiligheid
Overheid en het MKB veilig online

Feedbackpagina

F. Phishingmail C en feedbackpagina

Phishingmail C

Titel: Je werkgever biedt je artikelen aan voor een comfortabele (thuis)werkplek
Afzender: m.peters@werkplekcomfort.nl

Beste werknemer,

De afgelopen periode heeft laten zien dat een comfortabele werkplek belangrijk is, zowel op kantoor als thuis. Je werkgever heeft daarom een vergoeding beschikbaar gesteld om je eigen comfortabele (thuis)werkplek te kunnen inrichten. Hierbij heb je de keuze uit verschillende artikelen zoals een extra beeldscherm, tablet, noise cancelling koptelefoon, draadloze oordopjes, printer, bureau of bureaustoel etc., in aanvulling op de artikelen die je mogelijk al hebt gekregen.

Kies vandaag vóór 22:30 jouw (thuis)werkartikelen uit op onze productenpagina, dan wordt jouw bestelling morgen verzonden.

Met vriendelijke groet,

Merel Peters
Werkplekcomfort.nl

werkplekcomfort.nl

Feedbackpagina

G. Vragenlijst bedrijven vooraf

Q1.1 Onder welke sector valt uw bedrijf?

- Bouw en Vastgoed
- Communicatie en Media
- Consultancy
- Energiebedrijven
- Facilitaire dienstverlening
- Fast Moving Consumer Goods
- Financiële dienstverlening
- Gezondheidszorg en welzijnszorg
- Handel en retail
- Horeca, Recreatie, Toerisme en Cultuur
- Industrie
- Informatie en Communicatie Technologie (ICT)
- Intermediairs
- Juridische dienstverlening
- Land- en tuinbouw
- Onderwijs en Onderzoek
- Overheid en semi-overheid
- Technische dienstverlening
- Telecommunicatie
- Transport en Logistiek
- Detailhandel
- Overig

Q1.2 Uit hoeveel werknemers bestaat uw bedrijf?

- Minder dan 10 werknemers
- 10 tot 50 werknemers
- 50 tot 250 werknemers
- Anders namelijk,….[open]

Q1.3 In hoeverre ervaart u door COVID-19 verandering in uw bedrijfsactiviteiten?

- Veel minder druk
- Minder druk
- Geen verandering
- Drukker
- Veel drukker
- Weet ik niet

Q1.4 Hoeveel procent van uw werknemers werkte er vóór COVID-19 op kantoor?

- [open antwoord met getal tussen 0 en 100%]

Q1.5 Hoeveel procent van uw werknemers werkt momenteel op kantoor?

- [open antwoord met getal tussen 0 en 100%]

Q1.6 De bedrijfsprocessen binnen mijn bedrijf zijn volledig afhankelijk van internet en computers

- Zeer eens
- Eens
- Neutraal
- Oneens
- Zeer oneens

- Weet ik niet/ geen mening

Q1.7 Is de IT-beveiliging binnen uw bedrijf uitbesteed?
- Ja, de IT-beveiliging is volledige uitbesteed
- Ja, de IT-beveiliging is deels uitbesteed
- Nee, de IT-beveiliging is volledig in eigen beheer

Q1.8 Maakt uw bedrijf gebruik van een Cloudservice?
- Ja
- Gedeeltelijk
- Nee

Q1.9 Hoe regelmatig worden er back-ups gemaakt?
- Dagelijks
- Wekelijks
- Maandelijks
- Jaarlijks
- Er worden geen back-ups gemaakt

Q1.10 Zijn er binnen uw bedrijf beleidsafspraken gemaakt voor het gebruik van internet (bijvoorbeeld met een inlogprocedure)?
- Ja
- Nee

H. Vragenlijst bedrijven achteraf

Q2.1 Hoe heeft u de MKB Phishingtest ervaren?

- Zeer nuttig
- Nuttig
- Neutraal
- Nutteloos
- Zeer nutteloos
- Weet ik niet/ geen mening

Q2.2 Bent u van plan om komende periode maatregelen te nemen om uw weerbaarheid tegen phishing te vergroten?

- Ja
- Nee

[Vraag Q2.3 en Q2.4 alleen getoond indien antwoord 'ja' op Q2.2]

Q2.3 Welke maatregelen bent u van plan om te nemen om uw weerbaarheid tegen phishing te vergroten? [meerdere antwoorden mogelijk]

- Een training geven aan werknemers over cybersecurity
- (Vaker) een phishing test uitvoeren
- Technische maatregelen
- Anders, namelijk [open]

Q2.4 Stel dat u een phishing test wil gaan uitvoeren. Hoe wilt u dit organiseren?
[meerdere antwoorden mogelijk]

- Ik overweeg om zelf een phishing test uit te voeren
- Ik overweeg om mee te doen aan een collectieve inkoop voor het uitvoeren van een phishing test (bijvoorbeeld door uw brancheverenigingen)
- Ik overweeg om de phishing test uit te laten voeren door een cybersecurity bedrijf
- Weet ik niet/ geen mening

Q2.5 De MKB Phishingtest is onderdeel van een breder onderzoek over cybersecurity in het mkb. Mogen het Regionaal Platform Criminaliteitsbeheersing (RPC) en Digital Trust Center (DTC, onderdeel van het ministerie van Economische Zaken en Klimaat) u benaderen in het geval van een vervolgonderzoek?

- Ja, ik geef toestemming
- Nee, ik geef geen toestemming

Q2.6 Heeft u nog aanvullende opmerkingen over de MKB Phishingtest?
[open antwoord]

I. Vragenlijst medewerkers na elke phishingmail

Q3.1 Heeft u een mail ontvangen van "domeinnaam desbetreffende phishingmail"?

- Ja
- Nee

Q3.2 Bent u van te voren door uw werkgever op de hoogte gesteld van deze phishing test?

- Ja
- Nee

Q3.3 Bent u vóór het openen van de phishingmail gewaarschuwd door een collega die de phishingmail reeds had gezien?

- Ja
- Nee

Q3.4 Waar werkte u toen u de phishingmail ontving?

- Op kantoor
- Vanuit huis
- Openbare plek
- Onderweg
- Weet ik niet/ geen antwoord

Q3.5 Bent u in het verleden (met uitzondering van de mail van "domeinnaam desbetreffende phishingmail") ooit slachtoffer geworden van een phishingmail?

- Ja
- Nee

Q3.6 Hoeveel phishingmails denkt u de afgelopen 12 maanden te hebben ontvangen op uw werkmail?

- Geen
- 1-3 phishingmails
- 3-5 phishingmails
- Meer dan 5 phishingmails

Q3.7 Mijn kennis over digitale en online veiligheid is…

- Zeer beperkt
- Beperkt
- Redelijk
- Goed
- Zeer goed

Q3.8 Wat is uw geslacht?

- Man
- Vrouw
- Anders

Q3.9 Wat is uw leeftijd?

- Jonger dan 18
- 18-24 jaar
- 25-29 jaar
- 30-34 jaar
- 35-39 jaar
- 40-44 jaar

- 45-49 jaar
- 50-54 jaar
- 55-59 jaar
- 60-64 jaar
- 65 jaar of ouder

Q3.10 In hoeverre bent u in het algemeen bereid of niet bereid om risico's te nemen?
Gebruik alstublieft een schaal van 0 tot 10, waarbij 0 betekent "totaal niet bereid om risico's te nemen" en een 10 betekent dat u "zeer bereid bent om risico's te nemen".

- [schaal met 0 tot 10]

Q3.11 In hoeverre bent u bereid om iets op te geven dat vandaag voordelig is voor u, om er dan in de toekomst meer van te kunnen profiteren?
Gebruik alstublieft een schaal van 0 tot 10, waarbij 0 betekent "totaal niet bereid zijn om vandaag iets op te geven om er meer van te profiteren de toekomst "en een 10 betekent dat u" zeer bereid bent om vandaag iets op te geven om er in de toekomst meer van te profiteren "

- [schaal met 0 tot 10]

Q3.12 In hoeverre gaat u ervan uit dat mensen alleen de beste intenties hebben?
Gebruik alstublieft een schaal van 0 tot 10, waarbij 0 betekent "Ik ga er nooit van uit dat mensen alleen de beste intenties hebben" en een 10 betekent "Ik ga er altijd van uit dat mensen alleen de beste intenties hebben"

- [schaal met 0 tot 10]

J. Regressiemodel phishing experiment

Enkele bedrijven zijn geëxcludeerd van de data analyse (zie hoofdstuk 3.1 voor toelichting).

Toelichting variabelen:

- *Experience A*. Het effect van phishingmail A op de korte termijn (vergelijking kliks van mail B tussen groep 2 en 4)
- *Proxy LT. Exp A*. Een benadering van het effect van phishingmail A op de lange termijn (vergelijking kliks van mail B tussen groep 1 en 2)
- *Exp. B*. Het effect van phishingmail B op de middellange termijn (vergelijking kliks van mail C tussen groep 1 en 2)
- *Proxy Exp. C*. Een benadering van het effect van phishingmail C op de korte termijn (vergelijking kliks van mail B tussen groep 1 en 2)

	Model 1 (Basis)	Model 2 (Vragenlijst)
Experience A	-0.10 +	-0.10
	(0.06)	(0.06)
Proxy LT. Exp. A	-0.05	-0.05
	(0.06)	(0.07)
Exp. B	0.03	0.00
	(0.06)	(0.08)
Proxy Exp. C	-0.04	-0.00
	(0.06)	(0.08)
E-mail A	0.23 ***	0.17 **
	(0.02)	(0.05)
E-mail B	0.20 ***	0.13 *
	(0.05)	(0.06)
E-mail C	0.22 ***	0.20 **
	(0.04)	(0.07)
Recalls receiving mail		0.08 ***
		(0.02)
Was informed		-0.02
		(0.02)
Colleague told		-0.08 ***
		(0.02)
Past victim phishing		-0.02
		(0.01)
Recalls no phishing last month		0.04 **
		(0.01)
Female		-0.04 +
		(0.02)
Age		-0.00
		(0.00)
Risk Preference		0.05 *
		(0.03)
Time Preference		0.04
		(0.03)
Trust Preference		0.02
		(0.02)
N	62680	10489
R2	0.20	0.26

Standard errors are heteroskedasticity robust. *** p < 0.001; ** p < 0.01; * p < 0.05; + p < 0.1.

K. Regressiemodel interactie-effect ervaring en risicoperceptie

Enkele bedrijven zijn geëxcludeerd van de data analyse (zie hoofdstuk 3.1 voor toelichting).

Toelichting variabelen:

- *Experience A*. Het effect van phishingmail A op de korte termijn (vergelijking kliks van mail B tussen groep 2 en 4)
- *Proxy LT. Exp A*. Een benadering van het effect van phishingmail A op de lange termijn (vergelijking kliks van mail B tussen groep 1 en 2)
- *Exp. B*. Het effect van phishingmail B op de middellange termijn (vergelijking kliks van mail C tussen groep 1 en 2)
- *Proxy Exp. C*. Een benadering van het effect van phishingmail C op de korte termijn (vergelijking kliks van mail B tussen groep 1 en 2)

	Model 3 (Interaction)
Experience A	-0.03
	(0.07)
Proxy Long-term Experience. A	-0.03
	(0.07)
Experience B	0.01
	(0.08)
Proxy Experience C	0.02
	(0.08)
E-mail A	0.20 ***
	(0.02)
E-mail B	0.15 **
	(0.05)
E-mail C	0.24 ***
	(0.06)
Risk Preference	0.11 ***
	(0.02)
Risk Preference * Experience A	-0.12 **
	(0.04)
N	14748
R2	0.24

Standard errors are heteroskedasticity robust. *** p < 0.001; ** p < 0.01; * p < 0.05; + p < 0.1.