Uit de praktijk: resultaten en leerpunten van twee gedragsexperimenten om cyberveiligheid te vergroten

Amber van Druten, Karin Bongers & Michelle Ancher

3 november 2022

Inhoud

Gedragsexperiment 1 (EZK)

- Doelgroep: brede mkb
- Interventie:
  phishingmail & feedback

Gedragsexperiment 2 (JenV)

- Doelgroep: mkb-metaal
- Interventie:
  campagne & digitaal meldpunt

Doel:
Cyberweerbaarheid
mkb vergroten

Amber van Druten
Ministerie van EZK

Karin Bongers
Inspire to Act

Michelle Ancher
Haagse hogeschool

Grootschalig phishingexperiment onder mkb’ers

Phishing heeft grote impact op het MKB

- Aantal geregistreerde cybercrime incidenten fors gestegen (Politie, 2021)
- Veel cyberaanvallen beginnen met een gebruiker die op een phishingmail klikt
- Mkb vaak onderdeel van keten (Cyber Security Assessment Netherlands, 2021)

- Kennis over kenmerken van phishing kan klikken voorkomen…

  …Maar ervaring met phishing is effectiever (Norris et al., 2019; Baillon et al., 2019)

MKB phishingtest

- Onderzoeksvragen:
  1) Is een phishingtest een effectieve methode om de cyberweerbaarheid van het mkb te vergroten?
  2) Hangt dit effect af van het tijdsinterval waarmee de phishingtest plaatsvindt?

- Samenwerking tussen:

Ministerie van Economische Zaken en Klimaat

digital trust center.

RPC
Regionaal Platform Criminaliteitsbeheersing Noord-Holland
Partners in veilig ondernemen

Erasmus University Rotterdam

Proces

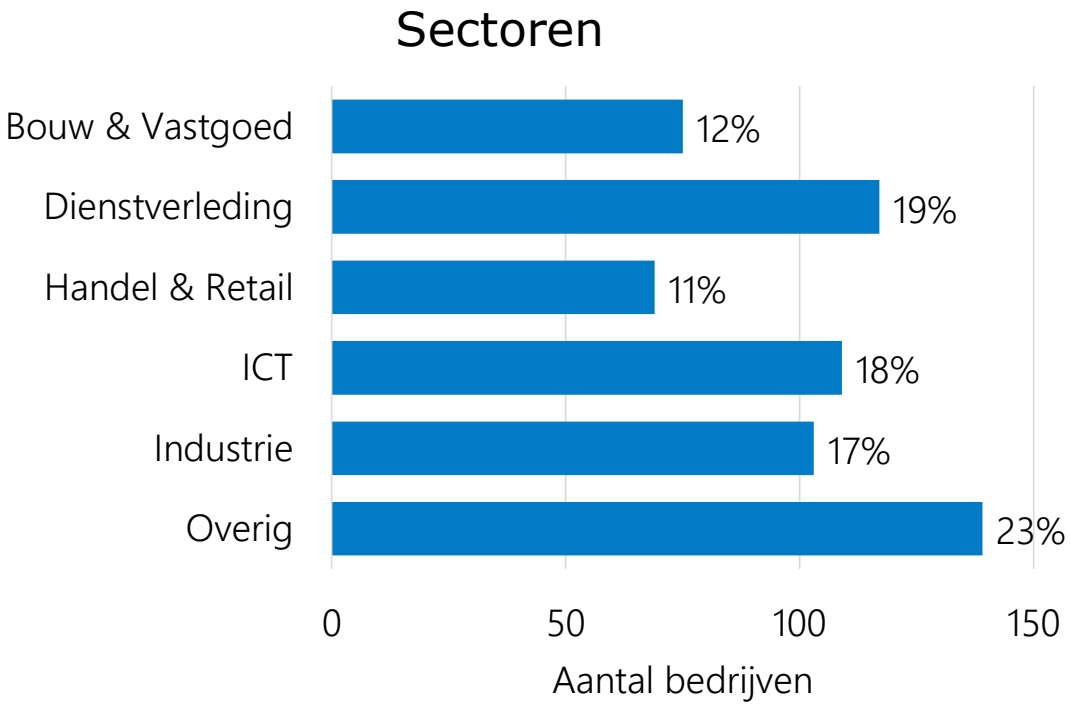
- **667 bedrijven 33.016 medewerkers**
- Formaliseren deelname met overeenkomsten
- Vragenlijst bedrijven
- Randomisatie: sector, aantal medewerkers, IT-beveiliging

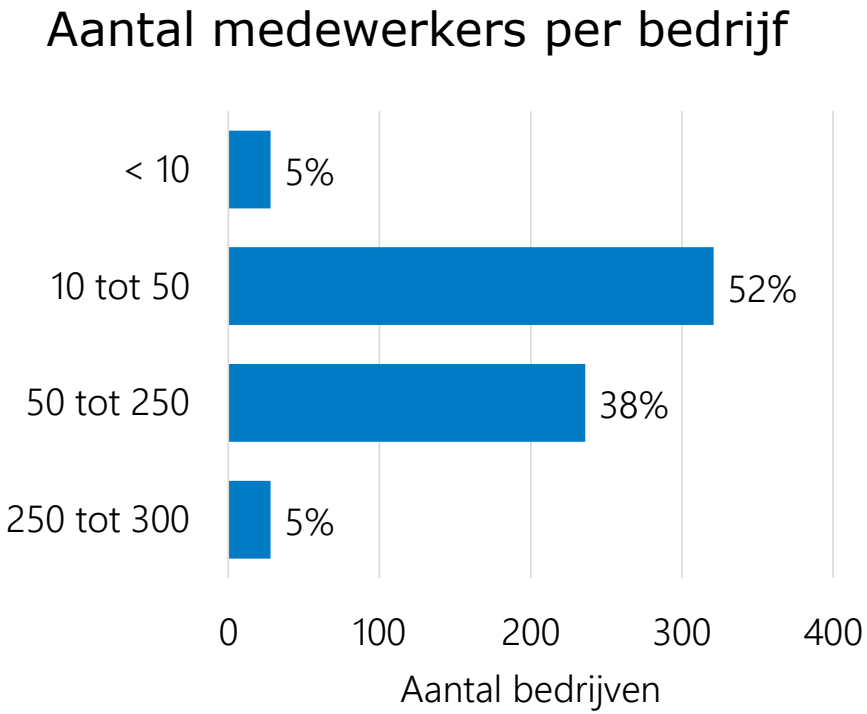
- Voorkomt dat mail in spambox komt

- Twee phishingmails per bedrijf
- **Tijdsinterval verschil**
- **Feedback** na het klikken op phishingmail
- Vragenlijst medewerkers

- Belangrijkste variabele: **klikgedrag**
- Anoniem rapport en vragenlijst per bedrijf
- Beleidsrapportage

650+ bedrijven, 33.000+ medewerkers





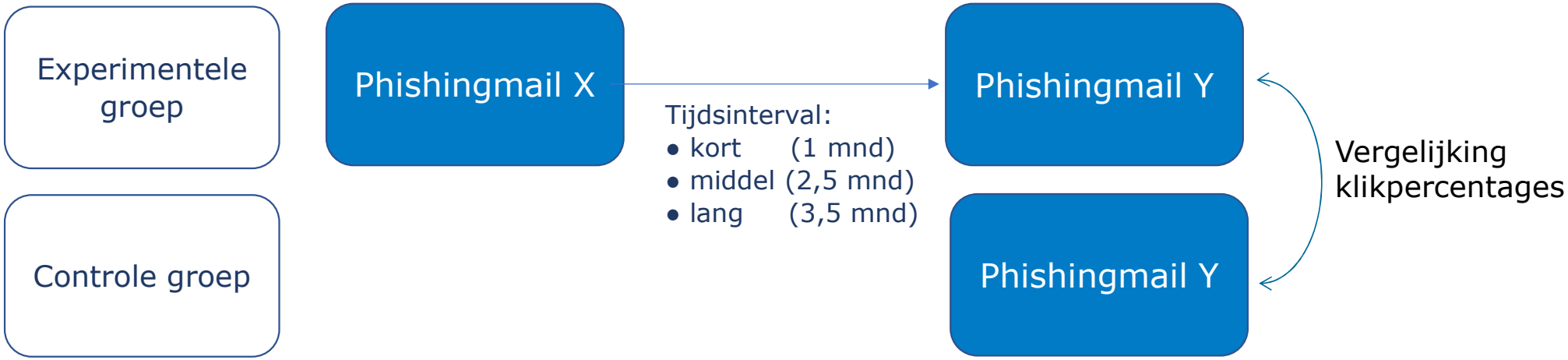
Opzet experiment (RCT)

- Vier onderzoeksgroepen:
  Willekeurig verdeeld obv bedrijfsgrootte, sector en IT-beveiliging

- Drie verschillende mails:

- Data:
  - Phishingtest (o.a. wel/niet klikken op onbetrouwbare link in phishingmail)
  - Vragenlijst medewerkers (na elke phishingtest)
  - Vragenlijst bedrijven vooraf en achteraf

Effectmeting phishingtest



Voorbeeld phishingmail

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

Voorbeeld feedbackpagina

1. **Onjuist of niet bestaand e-mailadres van de afzender**
   Vraag je altijd af: Wie is de afzender? Vertrouw je de e-mail van deze afzender? Klopt het e-mailadres? Bestaat dit bedrijf?
2. **Gebruik van een algemene aanhef**
   Een algemene aanhef kan wijzen op phishing. Maar let op! Ook als je naam in de aanhef staat, kan je worden bedrogen.
3. **Vraag om onmiddellijke actie**
   Een dringende vraag is vaak een signaal van phishing. Meestal gaat dit gepaard met een dreigende boodschap.
4. **Verdachte URL in de link**
   Meestal kun je zien of een link naar een verdachte website leidt. Beweeg daarvoor je muis over de link (niet klikken!). Het klikken op links in verdachte e-mails kan bijvoorbeeld leiden tot installatie van malware of ransomware.
5. **Te mooi om waar te zijn**
   Klinkt een aanbod te mooi om waar te zijn? Waarschijnlijk is het dat ook.

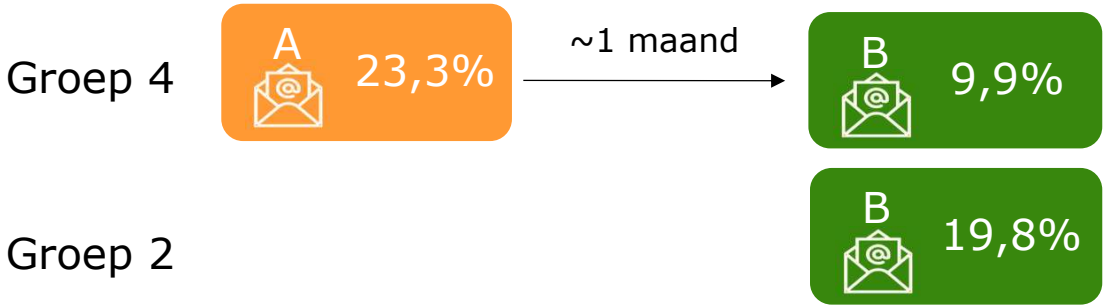
   Morgen ontvang je van de afzender invitation@survio.com een e-mail met het verzoek om anoniem een korte vragenlijst in te vullen.

Resultaten

22% van medewerkers klikt op onbetrouwbare link in generieke phishingmail

Effectiviteit van phishingtest

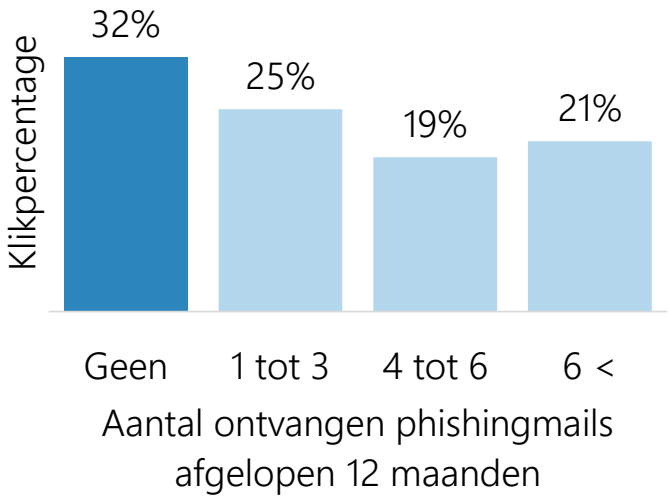
- Korte termijn (~1 maand): significant verschil



- Middellange termijn (~2,5 maand): geen significant verschil
- Lange termijn (~3,5 maand): geen significant verschil

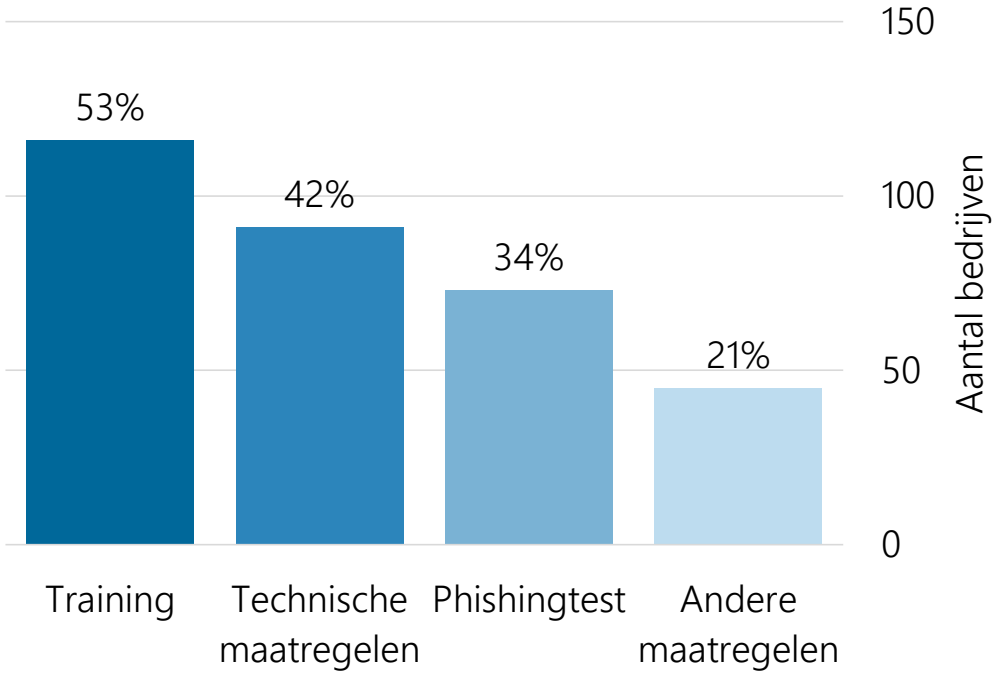
Klikgedrag & individuele eigenschappen

- Mannen klikken vaker dan vrouwen
- Medewerkers die de afgelopen 12 maanden géén phishingmail hebben ontvangen klikken vaker
- Risicozoekende medewerkers klikken vaker én hebben meeste baat bij phishingtest



Vervolg MKB Phishingtest

- 72% van plan maatregelen te nemen vergroten cyberweerbaarheid
- Na een jaar: Vragenlijst en groepsgesprek over daadwerkelijk uitvoeren maatregelen



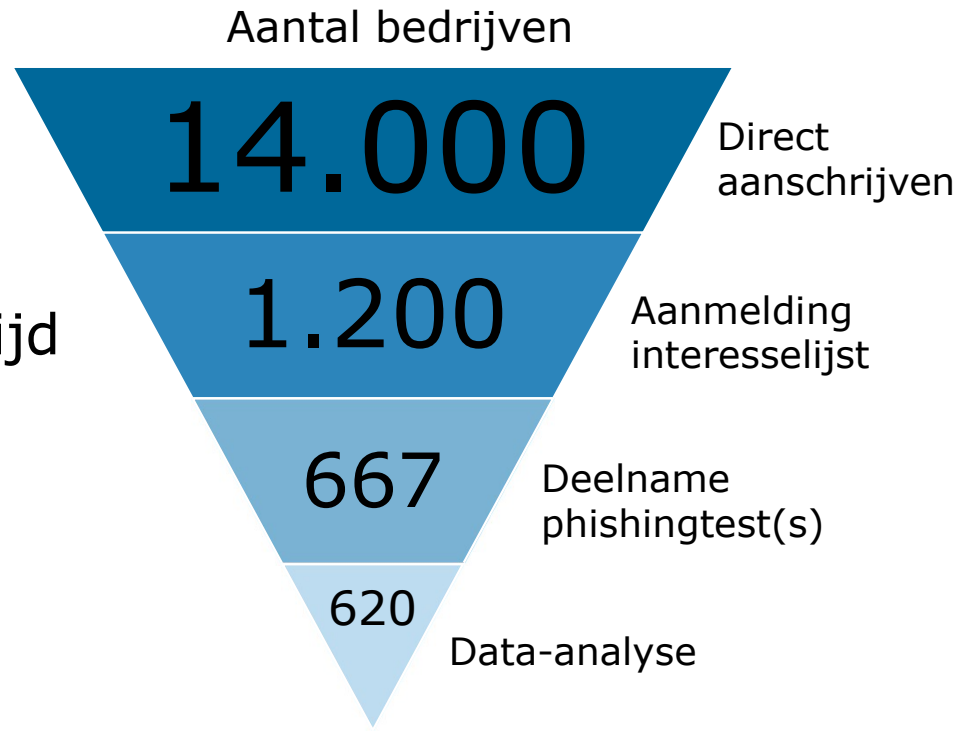
Conclusies

- ✓ Mkb is kwetsbaar voor phishing; 22% valt voor phishingtest
- ✓ Er zijn aanwijzingen voor een effect van een phishingtest op de korte termijn, maar niet op de (middel)lange termijn
- ✓ Risicozoekende mensen hebben meeste baat bij een phishingtest
- ✓ MKB Phishingtest is op zichzelf een manier om urgentie en cyberweerbaarheid binnen het mkb te vergroten

Zie BIN NL voor volledige rapportage

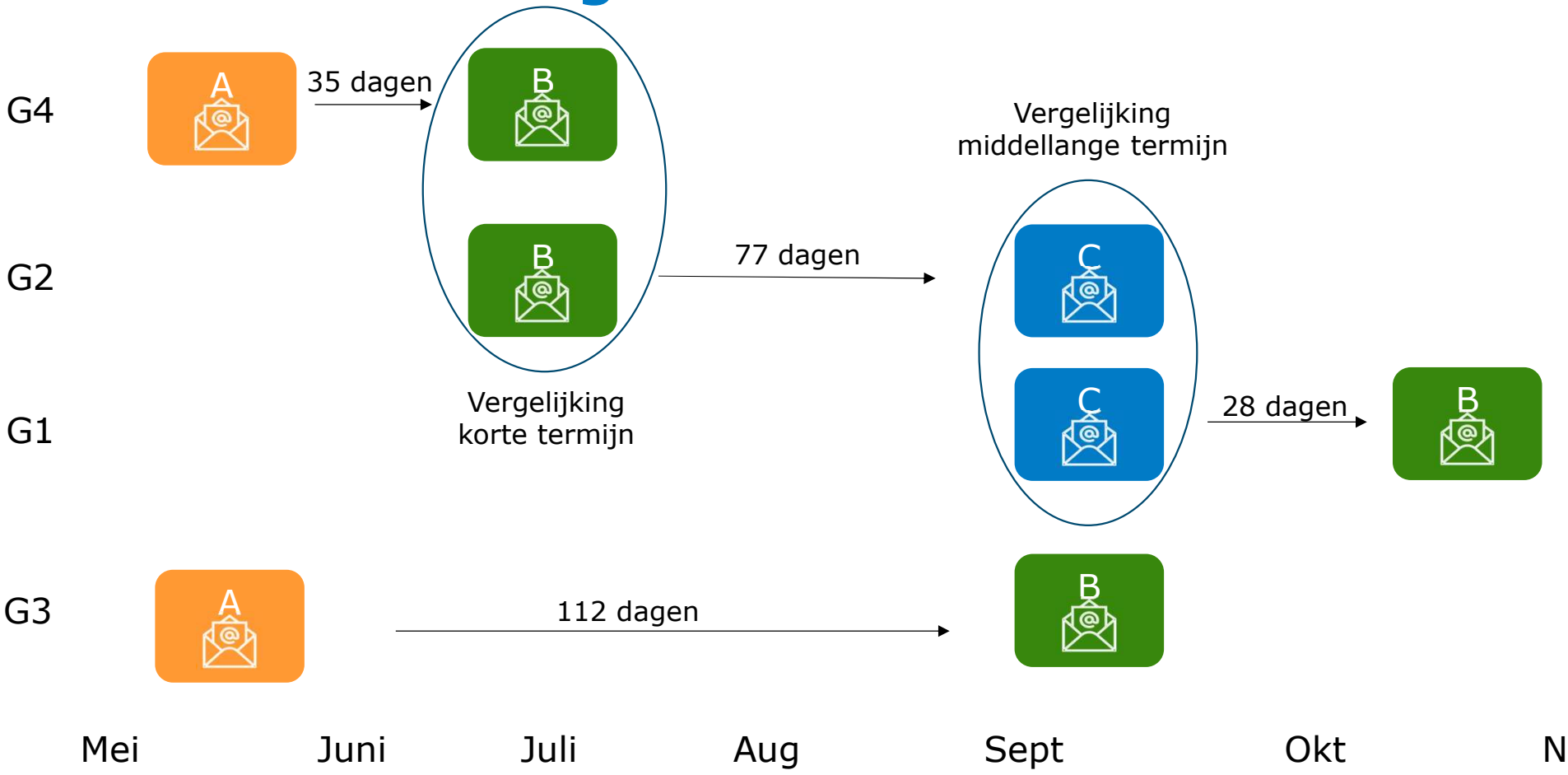
Geleerde lessen

- Mkb is lastig te bereiken doelgroep, direct aanschrijven meest effectief
- Werving & formalisering kost (veel!) tijd
- Onvoorziene zaken: URL-scanners



Vragen?

Onderzoeksdesign



Cyberweerbaarheid in mkb

Dag van Gedrag 2022

Inspire to act
Voor het effectief veranderen van gedrag

DE HAAGSE HOGESCHOOL

Proeftuin

Doel

Risico op slachtofferschap van cybercriminaliteit in mkb verkleinen.

Doelgroep

Medewerkers van mkb-metaal

Doelgedragingen

1. Medewerkers klikken niet op een link in verdachte emails.
2. Medewerkers melden verdachte emails bij een intern meldpunt.

Gedragsanalyse

Inzichten uit gedragsanalyse

Management

- Geen duidelijk beleid/regels
- Er is geen duidelijk intern meldpunt
- Leidinggevenden bespreken cyberveilig gedrag niet in overleggen

Medewerkers

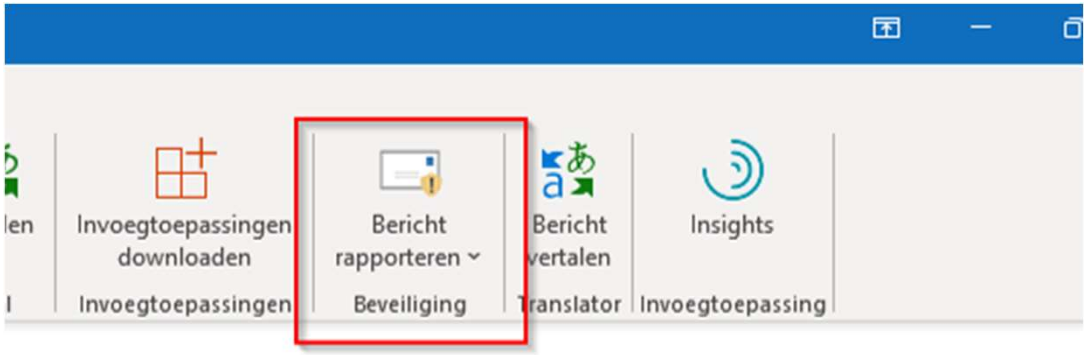
- Medewerkers klikken op de automatische piloot op links in emails
- Ver-van-mijn-bed
- Gedoe, willen gewoon aan het werk

Gedragsinterventie

Gedragsinterventie

Interventieonderdelen

1. Instellen intern meldpunt
   (bv. cybermeldpunt@*naam-mkb-metaalbedrijf*.nl)
2. Digitale meldknop in outlook
3. Handreiking voor leidinggevenden



Tips voor leidinggevenden

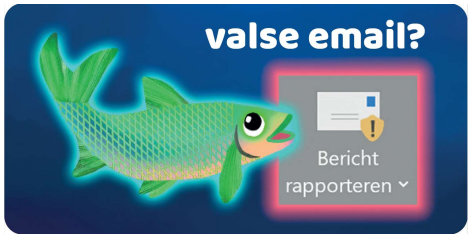
Om ons bedrijf tegen cybercriminaliteit te beschermen is het belangrijk om over cyberveiligheid te praten met onze medewerkers. Hieronder staan een paar tips die stimuleren dat medewerkers alert zijn en actie ondernemen als zij verdachte berichten ontvangen.

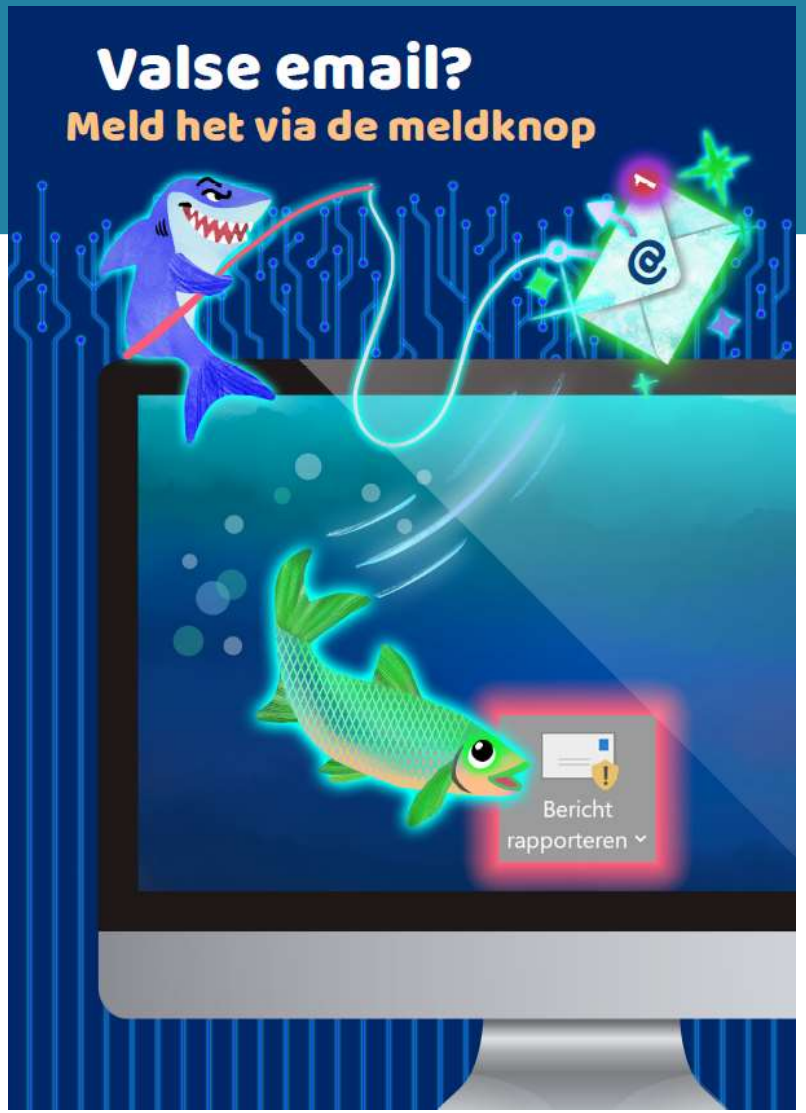
- Benadruk regelmatig in teamoverleggen dat je het belangrijk vindt om het bedrijf te beschermen tegen cybercriminaliteit. Geef aan dat medewerkers hierbij kunnen helpen door verdachte berichten te melden bij het interne cybermeldpunt.
- Vertel het aan medewerkers als er veel gemeld wordt bij het cybermeldpunt. Dit stimuleert andere medewerkers om ook verdachte berichten te gaan melden.
- Geef aan dat als medewerkers op een link hebben geklikt in een verdachte mail, het heel belangrijk is om het zo snel mogelijk te melden bij het interne cybermeldpunt. Gelukkig is het niet altijd heel ernstig.
- Sta open voor vragen van medewerkers over cyberveiligheid. Het geeft niet als je het antwoord niet weet. Verwijs medewerkers met vragen door naar het interne cybermeldpunt.

Gedragsinterventie

Interventieonderdel

4. Grote poster
5. Kleine poster
6. 3D Sticker



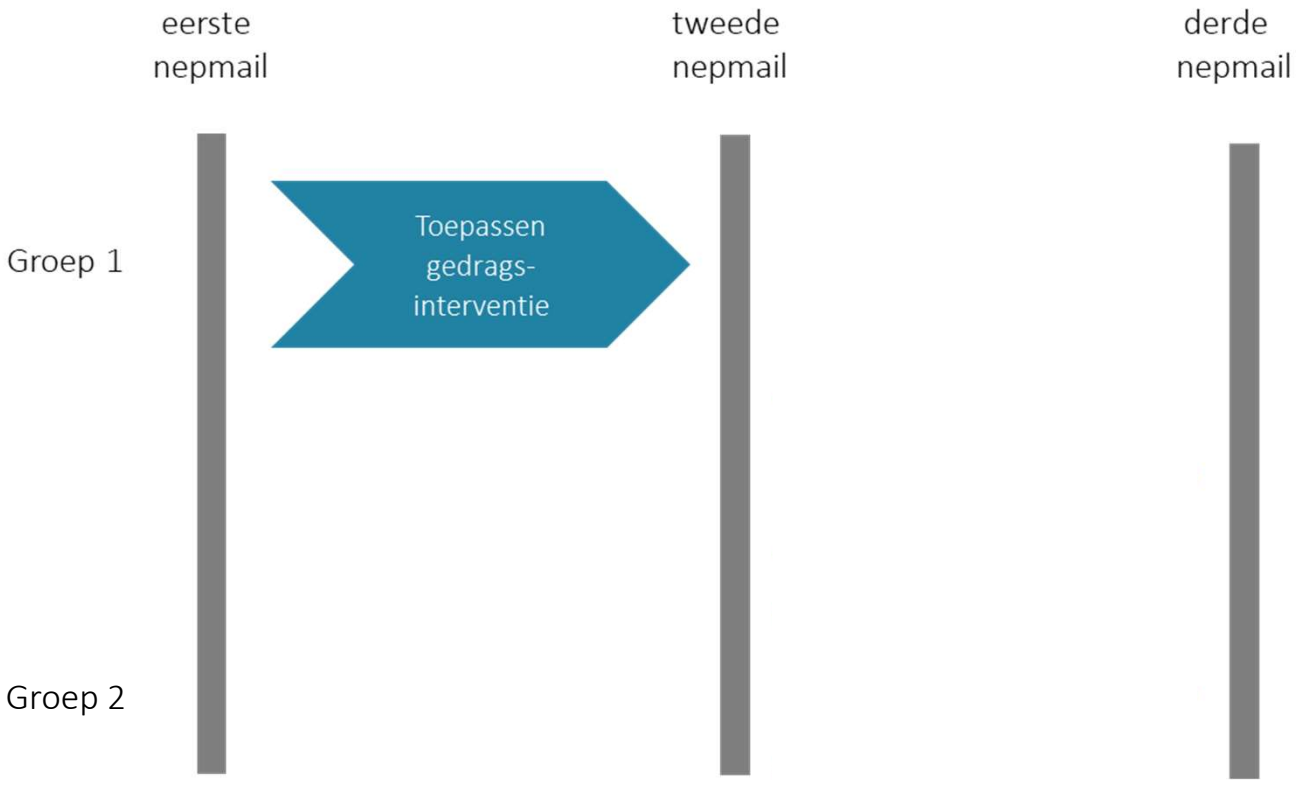


Gedragstechnieken

	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				✓		

Onderzoeksopzet

Onderzoeksdesign



Wat meten we?

Afhankelijke variabelen

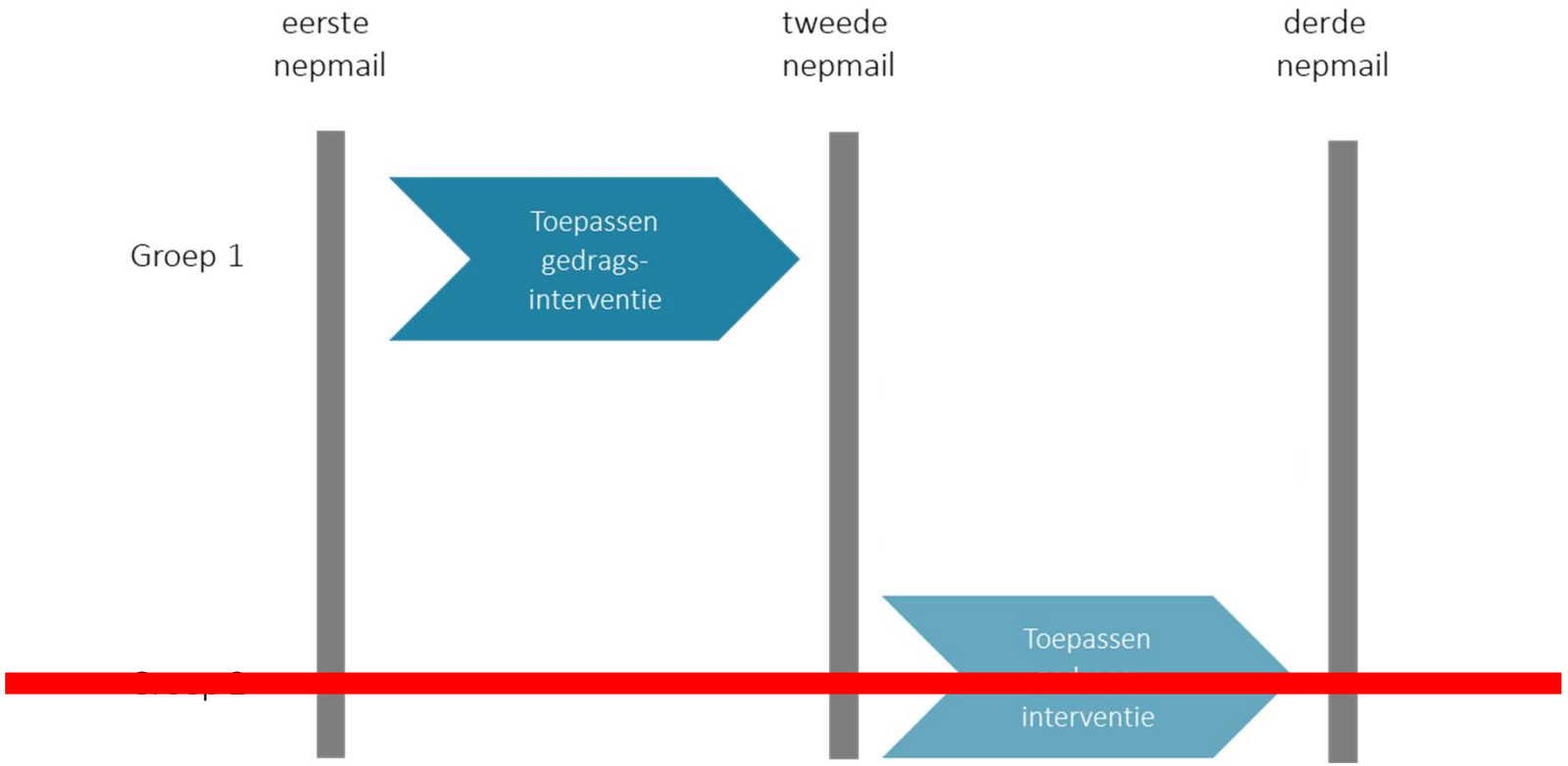
- Aantal meldingen bij cybermeldpunt (van mail 1, 2 en 3)
- Aantal keren dat er op de link geklikt wordt (in mail 1, 2 en 3)

Belevingsonderzoek

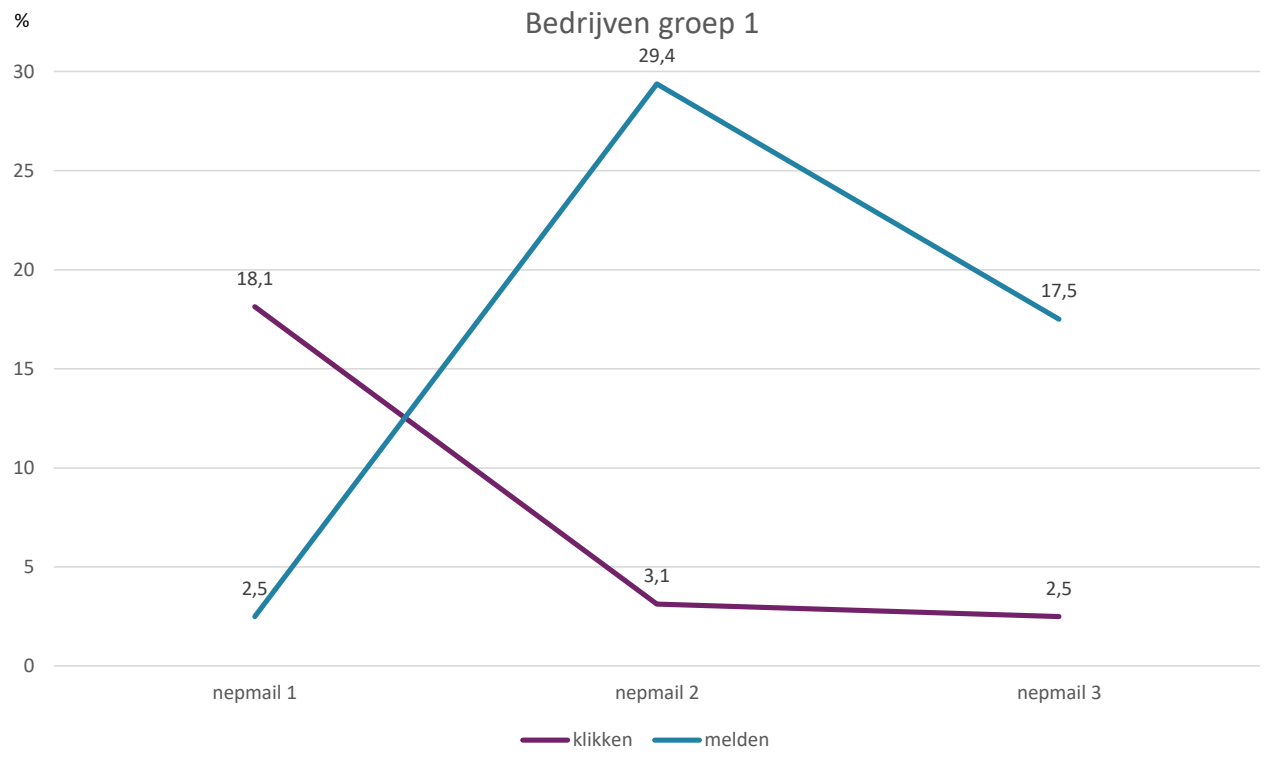
- Online vragenlijst

Resultaten

Missing data



Meld- en klikgedrag



Belevingsonderzoek

Bevindingen

- Bijna tweederde van de meldingen worden gedaan via de meldknop.
- Medewerkers zijn positief over de interventieonderdelen en interventie als geheel.
- Er wordt vaker over cyberweerbaarheid gesproken in het teamoverleg.
- Medewerkers geven aan alerter te zijn op valse e-mails.

Geleerde lessen en aanbevelingen

Geleerde lessen

Veel technische obstakels!

- Oudere versies software, waardoor meldknop installeren niet lukte
- Mails die ondanks whitelisten toch in spamfolder belanden (wat natuurlijk voor cyberveiligheid heel goed is!)

Bedrijven zijn ‘onbewust onbekwaam’

- Bedrijven hebben weinig affiniteit met onderzoek doen.
- Bedrijven hebben weinig affiniteit met gedragsinzichten.

Aanbevelingen

Technische controle vooraf

- Bij de aanmelding van bedrijven meteen controleren op de compatibiliteit van de software van de bedrijven met de technische vereisten voor de installatie van de meldknop.
- Bij elke nepmail eerst testen of de nepmails goed aankomen bij de bedrijven.

Goede procesbegeleiding

- Draaiboek maken voor elk bedrijf en met verantwoordelijke bespreken.
- Regelmatig contact houden met verantwoordelijke over voortgang.

digitaltrustcenter.nl/campagnematerialen-phishing

Inspire to act

DE HAAGSE HOGESCHOOL

MKB Nederland

Ministerie van Justitie en Veiligheid

digital trust center.

Michelle Ancher
m.ancher@hhs.nl

Docent-onderzoeker
Lectoraat Cybercrime en Cyber resilience
The Hague University of Applied Sciences

In de huid kruipen van de cybercrimineel

Hoe zelf ervaren helpt om weerstand te bieden en de (cyber)inhoud beter over te brengen

Cialdini

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

Phishing of echt?

We hebben je antwoord nodig.

Afmelden

bol.com

Beste ,

Uit de evaluatie van deze maand is gebleken dat je het geschenk dat we voor je gereserveerd hebben niet besteld hebt. Heb je vandaag tijd? Morgen is de laatste dag (zaterdag, 15 oktober). Het zal niet meer dan 30 seconden in beslag nemen.

Wanneer u op de onderstaande link klikt, wordt u direct doorgestuurd naar onze bestelpagina, waar u uw leveringsinformatie kunt invullen en de verzendkosten kunt betalen.

Pakketinformatie:
Bevat: Wachten op bevestiging
Klant:
Klant-id: @
Status: Beperkt aanbod
Jouw prijs: 0 eur
Verzendkosten: 0-2 eur

Ga door naar de bestelpagina

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Phishing of echt?

Gelieve uw bestelgegevens te controleren

Bol.com <klantenservicebol@outlook.com>
To: Michelle Ancher <m.j.ancher@hotmail.com>

bol.com

Beste M. Ancher,

Bedankt voor de aankoop van een huishoudelijk artikel op bol.com. Wij hebben uw betaling via het rekeningnummer eindigend op ...437 in goede orde ontvangen.

Wilt u zo vriendelijk zijn uw bestelgegevens te controleren via deze link:
controleer bestelgegevens

Bol.com

Ga door naar de bestelpagina

Afmelden

THE HAGUE
UNIVERSITY OF
APPLIED SCIENCES

Phishing of echt?

Van: "International Card Services" <noreply@service.icscards.nl>
Onderwerp: Herinnering: u heeft nog 10 dagen om uzelf te identificeren
Datum: 11 oktober 2021 12:49:42 CEST
Aan: [redacted]

ICS VISA
INTERNATIONAL CARD SERVICES

Voorkom blokkade: identificatie nodig

Geachte mevrouw [redacted]

U heeft een of meer Card(s) van International Card Services (ICS). Om uw Card(s) te kunnen blijven gebruiken, is het nodig dat u zich online identificeert vóór 21 oktober 2021. We hebben u hierover een brief en een herinnering gestuurd. Maar wij hebben uw online identificatie nog niet ontvangen. Daarom ontvangt u nu deze tweede herinnering.

Hoe weet u dat deze e-mail te vertrouwen is?
Goed dat u hierop let. Deze e-mail gaat over uw Card waarvan het 16-cijferige Card-nummer eindigt op [redacted]
Twijfelt u toch of deze e-mail echt van ICS komt? Bel dan met het vertrouwde telefoonnummer dat achter op uw Card staat.

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Vragenlijstonderzoek: Online consumentengedrag

Beste deelnemer,

Voor je ligt een korte vragenlijst van de Haagse Hogeschool (HHs) over online aankoopgedrag. De resultaten worden gebruikt in het kader van een grootschalig onderzoek naar online consumentengedrag. Inmiddels hebben al meer dan 2.000 mensen de vragenlijst ingevuld. Onder de deelnemers worden op 8 november 2022, boekenbonnen verloot.

Het invullen van de vragenlijst zal ongeveer 5 minuten van je tijd in beslag nemen. Er wordt betrouwbaar met je persoonlijke gegevens omgegaan. Deze worden niet met derden gedeeld of openbaar gemaakt, in welke vorm dan ook.

Mocht je nog vragen of opmerkingen hebben over het onderzoek, of kennis willen nemen van de resultaten, neem dan contact met mij op via m.slot@hhs.nl.

Alvast hartelijk dank voor uw deelname.
Met vriendelijke groet,

Drs. M. Slot, Opleiding Communicatie

Vul hier ajb je e-mailadres in. Deze wordt eenmalig gebruikt voor terugkoppeling van de eventueel gewonnen prijs.
.....

Omcirkel bij vraag 1 t/m 3 het antwoord dat op jou van toepassing is.

1.Heb je afgelopen 6 maanden online aankopen gedaan?
O Ja
O Nee

2.Bij welke webshop heb je je laatste aankoop gedaan?
O H&M
O bol.com
O Wehkamp
O Amazon.com
O anders……

3.Wat voor type product heb je aangeschaft?
O kleding
O boek, tijdschrift
O elektronica
O huishoudelijk product
O meubilair
O anders……

4.Vul hier ajb de ontbrekende tekens van je bankrekeningnummer in (want dit is nodig voor correcte verwerking van de gegevens). Let op: het gaat uit privacy overwegingen, om slechts enkele tekens.

□□XX □□□□ XXXXXXX□ □□

Junger, Montoya en Overink (2016) ‘Priming and warmings are not effective to prevent social engineering attacks’.

Spearphishing mail

Gelieve uw bestelgegevens te controleren

Bol.com <klantenservicebol@outlook.com>
To: Michelle Ancher <**m.j.ancher@hotmail.com**>

bol.com

Beste **M. Ancher**,

Bedankt voor de aankoop van een **huishoudelijk artikel** op **bol.com**. Wij hebben uw betaling via het rekeningnummer eindigend op **...437** in goede orde ontvangen.

Wilt u zo vriendelijk zijn uw bestelgegevens te controleren via deze link:
controleer bestelgegevens

Bol.com

Ga door naar de bestelpagina

Afmelden

THE HAGUE UNIVERSITY OF APPLIED SCIENCES

Counteren phishing

- Check links (mouse over)

- Kloppen naam en e-mailadres van de afzender?
- Algemene aanhef versus gepersonificeerd
- Wees alert op beinvloedingstechnieken: bijvoorbeeld hulp afwijzen
- Bel ipv klik
- Check bijvoorbeeld: https://www.fraudehelpdesk.nl/actueel/valse-emails/

of https://veiliginternetten.nl/

THE HAGUE UNIVERSITY OF APPLIED SCIENCES