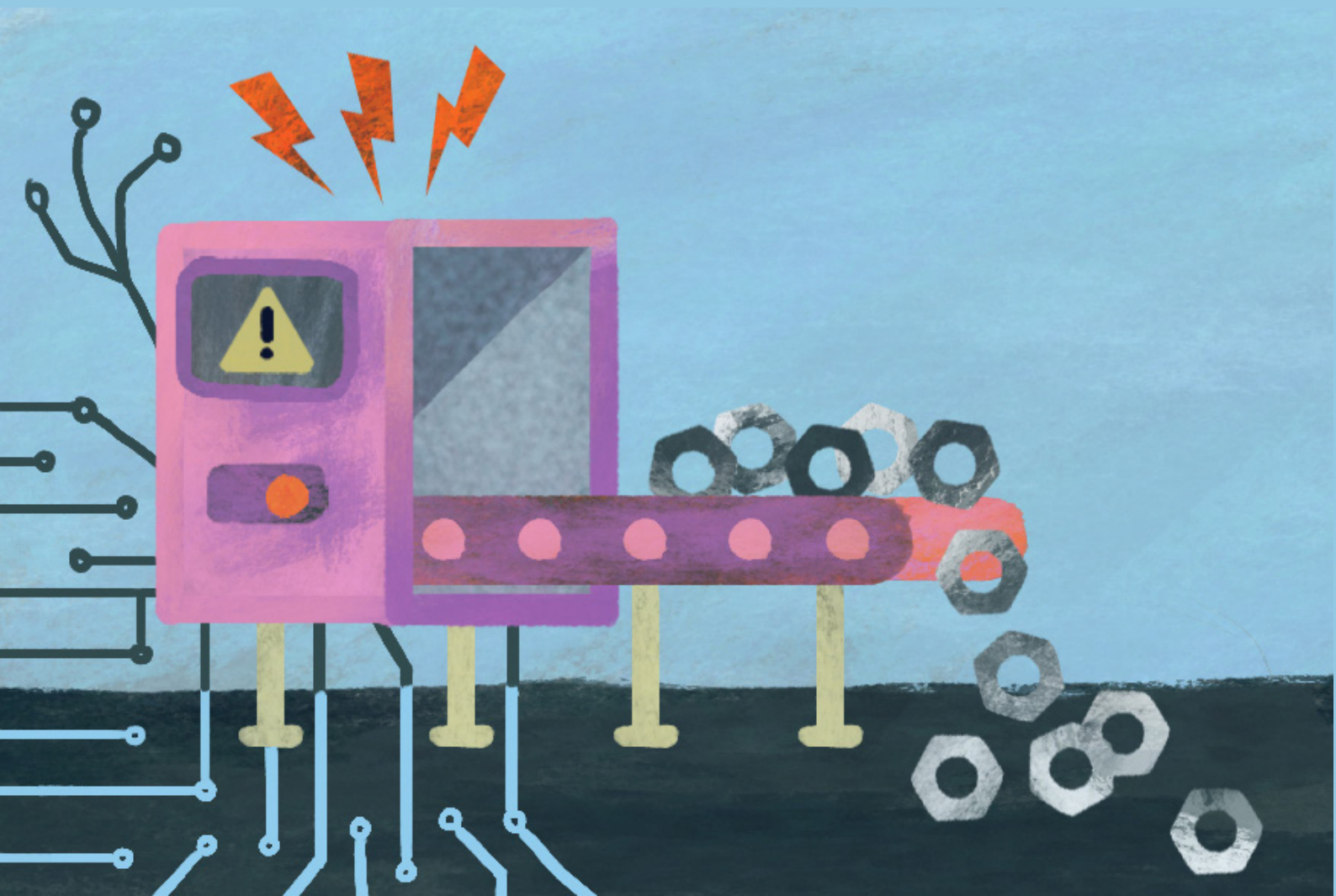
SAMENVATTING

ONTVANKELIJKHEID VOOR CYBERVEILIGHEID VERGROTEN BIJ ONDERNEMERS

Geanticipeerde spijt als gedragstechniek in nieuwsberichten



Samenvatting onderzoek Pilot 1

Aanleiding

Dit onderzoek 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. Dit document is een samenvatting van twee pilots die zijn uitgevoerd om de ontvankelijkheid van ondernemers met betrekking tot informatie over cyberveiligheid te vergroten.

Nieuwberichten Pilot 1

Pilot 1

De eerste pilot is uitgevoerd in samenwerking met de Koninklijke Metaalunie en Digital Trust Center (DTC). Via de Koninklijke Metaalunie zijn 3 nieuwsberichten verstuurd over cyberveiligheid; een standaardbericht; een bericht met geanticipeerde spijt techniek; en een met anti-neutralisatietechnieken.

Geanticipeerde spijtbericht

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. Hieronder staat het bericht, waarbij we inspelen op geanticipeerde spijt.

VOORBEELD

Geanticipeerde spijt

Laat cybercriminelen je bedrijf niet stilleggen en voorkom spijt

Stel je de chaos voor als cybercriminelen jouw bedrijfsproces stilleggen. Je operationeel proces ligt stil, je kunt niet leveren aan klanten en moet medewerkers naar huis sturen. En dan blijkt dat je dit had kunnen voorkomen. Hoe zou jij je voelen? Verklein dit risico en doe de cyberweerbaarheidsscan of geef je vóór 17 november op voor de gratis MKB Phishingtest. > Naar website Digital Trust Center.

Anti-neutralisatietechnieken

Uit eerder onderzoek blijkt dat mensen soms neutralisatietechnieken gebruiken voor het uitblijven van (moreel) gewenst gedrag of het vertonen van ongewenst gedrag. Voorbeelden hiervan op het gebied van cyberveiligheid zijn: ‘Ze komen toch niet bij ons, want er valt bij ons niets te halen’ of ‘Ze komen toch niet bij ons, want wij zijn maar een klein bedrijf’. Door in communicatie anti-neutralisatietechnieken te gebruiken, haal je de rationaliseringen onderuit, waardoor mensen zich meer geneigd voelen om in actie te komen. Hieronder staat het bericht, waarbij we gebruik maken van anti-neutralisatietechnieken.

VOORBEELD

Anti-neutralisatietechnieken

Er is geen enkel excuus om je deur open te laten staan voor cybercriminelen

Denk jij dat jouw bedrijf niet interessant is of te klein voor cybercriminelen? Dat er niets te halen valt? Ten onrechte: het maakt niet uit hoe groot je bent, maar hoe makkelijk cybercriminelen binnenkomen. Neem je verantwoordelijkheid en doe de cyberweerbaarheidsscan of geef je vóór 17 november op voor de gratis mkb-phishingtest > Naar website Digital Trust Center.

Standaardbericht

Om te toetsen of bovenstaande berichten effectief zijn in het ontvankelijk maken van mkb-ers voor informatie over cyberveiligheid, hebben we ook een standaardbericht (controle bericht) ontwikkeld, zie hieronder. In dit standaardbericht hebben we taal en jargon gebruikt die normaliter ook gebruikt worden in berichten over cyberveiligheid in de metaalsector.

VOORBEELD

Standaarbericht

Vergroot de cyberweerbaarheid op de werkvloer

Maar liefst één op de vijf metaalbedrijven is de laatste jaren slachtoffer geworden van een cyberincident. De gevolgen zijn vaak groot: directe financiële schade, het verlies van gegevens, imagoschade en tijdverlies. Hoe cyberproof is jouw bedrijf? Doe de cyberweerbaarheidsscan of geef je vóór 17 november op voor de gratis mkb-phisingtest. > Naar website Digital Trust Center.

Nieuwberichten Pilot 2

Pilot 2

Om de effectiviteit van de gedragstechnieken nogmaals te onderzoeken, hebben we een tweede pilot uitgevoerd in samenwerking met de Kamer van Koophandel (KvK) met een grotere steekproef. Deze pilot heeft een vergelijkbare opzet als de eerste pilot. Via de KvK zijn ook 3 nieuwsberichten verstuurd over cyberveiligheid; een standaardbericht; een bericht met geanticipeerde spijt techniek; en een met anti-neutralisatietechnieken.

Nieuwberichten

Hiernaast staan de drie nieuwsberichten.
Bij elk bericht is hetzelfde plaatje geplaatst.

VOORBEELD

Geanticipeerde spijt

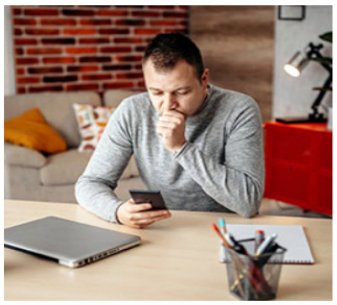
Cybercrime is overal: ontdek hoe kwetsbaar jouw bedrijf is

Met 1 verkeerde muisklik word je geraakt door cybercrime en staat je bedrijf volledig stil. Zonde, want dit had je kunnen voorkomen. Hoe groot is jouw risico op een cyberincident is en hoe bescherm je jouw bedrijf?

Ontdek het hier

VOORBEELD

Anti-neutralisatietechnieken



Cybercrime treft alleen grote bedrijven? Dit is niet waar

Niet alleen grote bedrijven maar ook jij kan slachtoffer worden van cybercrime. Hoe groot is jouw risico op een cyberincident en hoe bescherm je jouw bedrijf?

Ontdek het hier

VOORBEELD

Standaard bericht

Ontdek hoeveel risico je bedrijf loopt op cybercrime

Met de Risicoklassenindeling zie je binnen een aantal kliks hoe groot de kans is dat je slachtoffer wordt van cybercrime. En ontdek je hoe je jouw bedrijf beschermt.

Lees meer

Pilotopzet

Methode

De berichten werden via de wekelijkse digitale nieuwsbrief van de Koninklijke MetaalUnie verspreid onder hun leden. In overleg met de Koninklijke Metaalunie hebben we de regio's verdeeld over de drie groepen: standaardbericht; anti-neutralisatie-bericht; en geanticipeerde spijtbericht. In de nieuws-berichten stond een link naar een landingspagina op de website van het DTC.

Afhankelijke variabele

De afhankelijke variabele is het aantal keren dat er op de link in het nieuwsbericht is geklikt.

Hypothese

We verwachten dat leden die de nieuwsberichten met gedragstechnieken hebben ontvangen (experi-mentele nieuwsberichten) vaker op de link klikken dan leden die het standaard nieuwsbericht hebben ontvangen (controle nieuwsbericht).

Resultaten en conclusie

We vinden geen significante verschillen tussen de drie berichten. De gedragstechnieken lijken geen effect te sorteren op de ontvankelijkheid van mkb-ers voor cyberveiligheid. Toch kunnen we dat niet met zekerheid concluderen, aangezien het totaal aantal mensen dat op de link klikt te laag is om effectiviteit aan te kunnen tonen.

Resultaten en conclusie

Resultaten

Leden die het bericht met geanticipeerde spijt techniek ontvangen, klikken significant vaker op de link in de nieuwsbrief dan leden die het standaardbericht ontvangen. Dit bericht leidt overall tot 29% meer kliks dan het standaardbericht. Bij mkb-ers leidt het tot 22% meer kliks; bij zzp-ers tot 30% meer kliks en bij starters tot 41% meer kliks dan het standaardbericht. Er is geen verschil tussen het bericht met anti-neutralisatie technieken en het standaardbericht.

Leden die de standaardversie van het interviewverslag ontvangen, klikken vaker op de link naar de Risicoklassenindeling digitale veiligheid dan leden die het interviewverslag met anti-neutralisatietechnieken ontvangen en leden die het interviewverslag met geanticipeerde spijt techniek ontvangen.
Het standaardverslag van het interview leidt tot 41% meer kliks naar de landingspagina van het DTC dan het interviewverslag met anti-neutralisatie technieken; en tot 59% meer kliks dan het interviewverslag met geanticipeerde spijt.

Conclusie

- Inspelen op geanticipeerde spijt in een nieuwsbericht is effectief om ondernemers ontvankelijk te maken voor informatie over cyberveiligheid. Dit geldt zowel voor mkb-ers, zzp-ers als starters. Het leidt respectievelijk tot 22%, 30% en 41% meer kliks dan een standaard nieuwsbericht. Overall leidt het tot 29% meer kliks dan een standaard nieuwsbericht.

- Anti-neutralisatietechnieken in een nieuwsbericht hebben geen effect op ontvankelijkheid.

- Inspelen op geanticipeerde spijt en anti-neutralisatietechnieken zijn niet effectief in het interviewverslag. Integendeel: de standaardversie van het interviewverslag leidt tot resp. 59% en 41% meer kliks.