PHISING
BINNEN HET MKB

“Één op de vijf medewerkers binnen het mkb klikt op een phishingmail.”

In deze folder staan vijf belangrijke tips om jouw bedrijf tegen phishingmails te beschermen.

1. WAT IS PHISHING?

Phishing is een vorm van digitale fraude waarbij cybercriminelen proberen persoonlijke gegevens of wachtwoorden te stelen. Ze doen dat vaak door mensen te misleiden door hen bijvoorbeeld onder tijdsdruk te zetten. Ook proberen zij informatie of geld van bedrijven te pakken te krijgen. Je hebt vast zelf ook wel eens een mailtje gehad dat zogenaamd van jouw bank afkomstig was? Een waarschuwing dat je bankpas geblokkeerd zou worden als je niet snel actie ondernam. Je wordt door de crimineel aangezet tot snel handelen omdat je dan niet helder nadenkt, maar vooral snel van de stress af wil zijn. Dat is wat criminelen graag ziet: snel doen wat zij willen. Maar er is een goede aanpak: vertraag, check en meld!

Pishing komt via verschillende kanalen zoals Whatsapp, SMS en mail op medewerkers van jouw bedrijf af. Het komt ook voor dat organisaties worden gebeld namens een zogenaamde ICT helpdesk of toeleverancier. Nu denk je waarschijnlijk 'Dat overkomt mijn bedrijf niet! Zo interessant zijn wij niet...'. Uit onderzoek blijkt dat de meeste ondernemers dat denken. Maar weet je dat niets minder waar is?

2. WAT IS HET RISICO?

Als jouw medewerker op een phishingmail klikt en mogelijk ook nog informatie prijsgeeft, dan loop je direct op twee manieren gevaar;

1. Je verliest geld en/of belangrijke bedrijfsinformatie.
2. Je geeft criminelen toegang tot je systemen voor het installeren van schadelijke software zoals gijzel- of spionagesoftware. Phishingmails zijn namelijk vaak een opstap voor cybercriminelen om verder te komen in het netwerk van je bedrijf. Eenmaal binnen proberen ze om bedrijfsprocessen in kaart te brengen om deze uit te buiten of te verstoren om het bedrijf te schaden of onder druk te zetten.

3. ZE SPELEN OP JE GEVOEL

Waarom trappen mensen in phishingmails? Criminelen verzinnen verhalen die je raken. Ze spelen in op je gevoel. De techniek die daarachter zit heet social engineering. Het is eigenlijk gewoon keiharde manipulatie. Zo wordt je bijvoorbeeld bang gemaakt. Bang om iets niet goed te doen of bang om iets kwijt te raken, zodat je snel handelt en niet nadenkt, als gevolg van de stress die je door hun verhaal ervaart.

• Als je een bericht ontvangt van de Belastingdienst of de Politie, ben je al gauw geneigd te doen wat er gevraagd wordt. Je zit namelijk niet te wachten op problemen dus maar snel die naheffing of boete betalen! Of toch maar wel inloggegevens afstaan nadat je op dat linkje hebben geklikt. Op deze manier kan je immers erger voorkomen! Als je in paniek bent, ga je gauw over tot handelen zonder de afzender te checken of de andere punten waaraan je een phishingmail kan herkennen.

• Schaarste en tijdsdruk zijn ook trucs die vaak door cybercriminelen wordt gebruikt. Zij brengen je graag in paniek door bijvoorbeeld het bericht dat je bankpas binnen twee dagen geblokkeerd wordt. Stel je voor dat je een bericht ontvangt dat je emailaccount geblokkeerd wordt terwijl je juist aan het wachten bent op een belangrijke mail van die ene klant met die grote order... Kan je je voorstellen dat je in de stress raakt? En laat nou net die stress een slechte raadgever zijn. Want je gaat vooral snel handelen en dat is precies wat criminelen willen!

Er zijn nog veel meer psychologische trucs die cybercriminelen uithalen met phishing. Wil je hier meer over weten? Zoek dan eens op 'cialdini principes' het zijn dezelfde principes als in de marketing worden gebruikt.

4. HOE HERKEN IK PHISHING?

De tijd waarin je een phishingbericht goed kon herkennen aan spelfouten is al wel enige tijd voorbij. Toch denken mensen nog vaak dat ze oplichting op die manier kunnen herkennen. In de werkelijkheid is het erg moeilijk om phishing te herkennen. Vooral wanneer berichten van bekende personen of organisaties af lijken te komen en namen en informatie bevatten die bekend zijn binnen het bedrijf. Dat heet spearphishing: een hele gerichte aanval op specifieke personen op basis van gedetailleerde kennis. Dat is echt heel lastig om te herkennen!

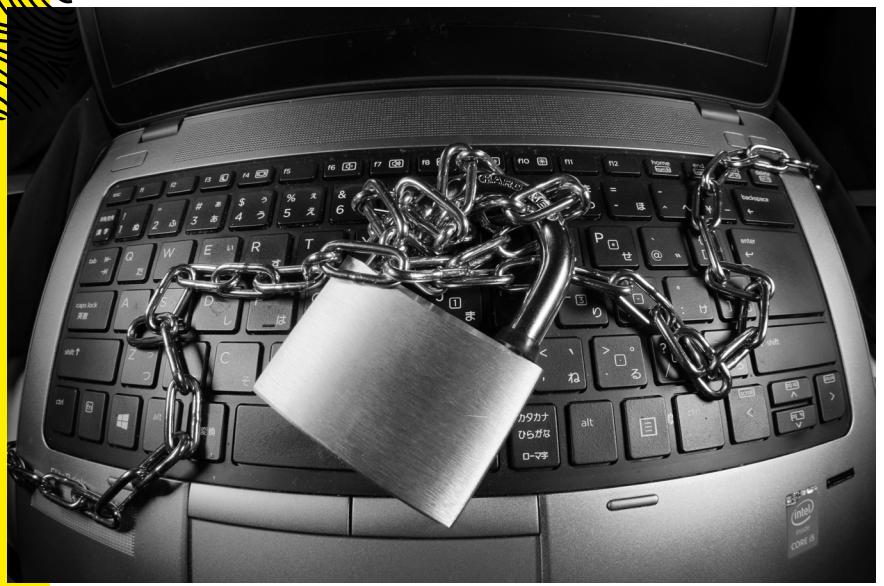
Doe jezelf een plezier en kijk eens naar de BINGO-kaart over phishingmails herkennen op Digital Trust Centre: https://www.digitaltrustcenter.nl/informatie-advies/phishing/hoe-herken-ik-een-phishing-e-mail

Er is ook een leuke quiz over het herkennen van phishing op https://www.digitaltrustcenter.nl/test-je-kennis-phishing
Het kan een inleiding zijn voor een gesprek over pishing met collega's binnen je bedrijf: praat hier eens over bij de koffie!
Een aantal voorbeelden van phishing waarmee het mkb vaak wordt geconfronteerd zijn:

1. **CEO-fraude:** bij deze vorm van phishing ontvangt iemand van jouw financiële administratie een berichtje van een crimineel die zich voordoet als een leidinggevende of iemand van de directie. Het bericht bevat vaak een verzoek om met spoed een grote betaling te doen.

2. **Consent phishing:** criminelen proberen met behulp van een toestemmingsverklaring van een (vaak bekende) applicatie toegang krijgen tot jouw account. Pop-ups van veel gebruikte applicaties worden bijvoorbeeld nagemaakt of je krijgt een e-mail over een zogenaamde wijziging van een applicatie. Als je op een link in dit bericht klikt - bijvoorbeeld om akkoord te gaan met de nieuwe voorwaarde - dan geef je de crimineel zonder dat je het weet toegang tot je account.

3. **Neptelefoontjes/helpdeskfraude:** Bij deze vorm van phishing ontvang je geen bericht, maar word je opgebeld. Criminelen doen zich bijvoorbeeld voor als bank- of helpdeskmedewerker. Er doet zich een zogenaamd probleem voor en om je te helpen zul je je inloggegevens moeten delen. Het kan ook zijn dat je wordt verleid om software op je computer te installeren zodat de medewerker kan meekijken en je zogenaamde probleem oplossen. Nooit doen!



Criminelen spelen steeds in op actuele thema's en bedenken steeds nieuwe verhalen. Het is dus belangrijk om goed op te hoogte te blijven van de nieuwste oplichtingstrucs die zij gebruiken. Op deze website staan de meest recente trucs: https://www.fraudehelpdesk.nl/. Ook kan je je snel en eenvoudig abboneren op de nieuwsbrief waarmee je elke maand bericht ontvangt over de nieuwste oplichtingspraktijken en trends daarin.

5. HOE BESCHERM IK MEZELF?

Zoals je al hebt gemerkt zijn cybercriminelen gewoon professionele oplichters. Toch zijn er wel degelijk dingen die jij kan doen om slachtofferschap van phishing te voorkomen! Wat kun je doen? Phishing tegengaan vereist zowel een technische- als een mensgerichte aanpak. Enerzijds kun je je werknemers trainen om phishingmails te herkennen; anderzijds zijn er ook technische maatregelen die je kan nemen.

1. **Bewustzijn en aandacht**
Wees je ervan bewust dat jij als mens gemakkelijk te beïnvloeden bent. De eerste stap is om op te merken dat je onder druk wordt gezet en snel wil handelen. Vertraag juist in deze situaties. Tip: Laat je medewerkers trainen om goed met deze dreiging om te kunnen gaan. En heb het hier eens per maand nog eens over om de alertheid te behouden.

2. **Email authenticiteit**
Installeer DMARC, DKIM of SPF. Dit zijn programma's die de herkomst van mails checken. Worden ze daadwerkelijk verzonden vanuit het domein dat in de mail staat? Een automatische check haalt veel ellende uit de lucht!

3. **Check de link!**
Is er een link in een e-mailbericht waar je op moet klikken? Daar kun je vaak al veel aan zien. Tip: Neem binnenkort vijf minuten in een teamoverleg om de tips hierover van de Fraudehelpdesk door te lopen.
https://www.fraudehelpdesk.nl/fraude/is-dit-een-vals-website-adres/. Ook bestaat de site www.checkjelinkje.nl waar je het adres van de link in kan voeren om deze te controleren!

4. **Bedenktijd**
Als je hebt opgemerkt dat je onder druk wordt gezet, dan is het van belang om bedenktijd in te bouwen. Door deze bedenktijd in te bouwen kan je eerst wat onderzoek doen en denken voordat je overgaat tot handelen.

5. **Vraag hulp**
Bel een bekende om even te overleggen. Laat hem/haar meekijken naar bijvoorbeeld een bericht. Iemand die wat meer afstand heeft tot het bericht kan er nuchter naar kijken en ziet misschien meer details.

6. TOCH GETROFFEN DOOR PHISHING?

Ieder bedrijf kan slachtoffer worden van een phishingbericht. Ga er dus vanuit dat het ook jou een keer overkomt. Dit is helemaal niet gek, omdat je als bedrijf met mensen nu eenmaal te beïnvloeden bent. Schaam je dus vooral niet dat het jouw bedrijf is overkomen!

Mocht jouw bedrijf slachtoffer zijn geworden, dan is het belangrijk om hierover te praten met elkaar. Laat medewerkers – ook als ze twijfelen – dit zo snel mogelijk melden bij bijvoorbeeld je ICT-leverancier of leidinggevende. Hoe sneller er een melding wordt gedaan, des te sneller kan er actie ondernomen worden om de schade te beperken!

Waak er ook voor dat deze mensen niet in een verder in een schuldgevoel terechtkomen. Ze schamen zich vaak al enorm. Maar de waarheid is dat het iedereen kan overkomen. Er is dus niks om je voor te schamen of medewerkers de schuld van te geven. Dit hoort vandaag de dag bij de risico's van het ondernemen! Dat geldt dus ook voor je medewerkers: bijvoorbeeld de medewerker van de financiële administratie die toch dat bedrag overmaakte na een mail vanaf een privé account ontvangen te hebben alsof het afkomstig was van de directeur zelf.

Doe bij slachtofferschap van phishing altijd aangifte bij de politie. Dat kost tijd maar met jouw aangifte weten zij wat er speelt, kunnen zij verdachten opsporen en help je andere ondernemers alert te zijn! Je kan de fraude ook online melden bij de Fraudehelpdesk. Zij kunnen dan andere ondernemers waarschuwen en zo veel ellende voorkomen.

Deze flyer is ontwikkeld in eem samenwerking tussen het Veiligheidsnetwerk Oost-Nederland en het lectoraat Maatschappelijke Veiligheid van de Hogeschool Saxion, onder financiering van de Citydeal Lokale Weerbaarheid Cybercrime in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid.