AUMATICS PHISHING CAMPAGNE

TEST JEZELF

aumatics

Onze campagne tegen phishing: no pain, no gain

Lemy Nguyen en Lennert Hut, Aumatics

De firewall kan netjes zijn geüpdatet en de virusscanner is misschien net nieuw. Maar keer op keer blijkt uit Aumatics' campagnes tegen phishing: als jij of je collega's niet alert zijn, zet je met één e-mail de veiligheid van het bedrijfs-netwerk op het spel. Hoe ver komen phishingmails binnen jouw organisatie?

Phishing is de meestgebruikte methode voor aanvallers om binnen te komen in jouw bedrijf. De simpele reden hiervoor: omdat het de meest effectieve methode is. Het is vrij gemakkelijk om te scoren met phishing, de opbrengst is vaak groot. Niet onbelangrijk: het werkt, omdat het gebruik maakt van de toe-name van het aantal berichten en notificaties op de werkplek.

Nog veel vaker dan een paar jaar geleden ontmoeten we elkaar in online meetings en andere online communicatiemiddelen. Kwaadwillenden liften met succes mee met die trend. Door lockdowns en thuiswerken in coronatijd steeg het aantal phishing-sites in 2021 met 27% (Sidn.nl).

Ga er dus maar vanuit: ook jouw Inbox wordt niet overgeslagen. En in zo'n 92% van de gevallen zoeken aanvallers naar persoonlijke gegevens. Jouw naam, nummers en wachtwoorden, aldus IT Security partner Kasaya. Zodat ze ermee aan de haal kunnen gaan.

Phishing van bank, loterij of pakketbezorger?

Dat gebeurt soms op een lachwekkend doorzichtige manier (hallo, rijke Nigeriaanse prins). Maar: steeds vaker op heel listige manier. Bijvoorbeeld door opvallend goed nagemaakte e-mails van een bank of loterij. Of een pakketbezorger die je vraagt om te bevestigen dat je een pakketje wil ontvangen. Toevallig, je zat er net op te wachten, toch?

Wat we ook vaker zien is dat IT Security zelf het onderwerp wordt. Bijvoorbeeld doordat jou wordt wijsgemaakt dat er een verdachte e-mail is aangetroffen in je Inbox. Of je even kunt klikken om te controleren of het echt zo is.

Het gevaar komt dus uit veel verschillende richtingen en in vele variaties. Ze hebben meestal wel een overeenkomst: zij schieten met hagel. Immers, hoe meer je mailt als verzender met kwade bedoelingen, des te groter de kans op succes. Bekijk phishingmails met deze kennis in het achterhoofd en je ziet opeens een stuk meer.

De link als lokaas

‘Echte’ organisaties zoals jouw bank of een pakketbezorger laten dit zoveel mogelijk zien. Bijvoorbeeld door duidelijk aan te geven hoe en op welke manier ze met jou communiceren. Zo kunnen banken je best mailen. Hoe belangrijker de e-mail, des te groter de kans dat ze laten zien dat ze jou echt bedoelen. Bijvoorbeeld door je aan te spreken bij je echte naam of andere informatie te tonen die aantoont het een gerichte actie is. Dus geen privacygevoelige informatie. En ze vragen al helemaal niet om pincodes. Nooit.

Wat wij steeds vaker zien is er dat er een actie wordt gevraagd, maar dat die actie is losgekoppeld van de e-mail. In de e-mail houdt de afzender het dan bij met alleen een mededeling of verzoek. Het grote voordeel hiervan: er staat geen link in de e-mail.

Over links gesproken. De link in de e-mail is dé sleutel voor succes voor aanvallers. Het is de wolf in schaapskleren van online communicatie. De link en het verhaal eromheen zijn niet wat ze beweren te zijn.

Opmerking vooraf over onze phishingcampagne

Bij onze campagnes tegen phishing zetten wij hier op in. Onze klanten maken zich terecht zorgen over de IT Security van hun organisatie. En als het goed is, zien ze dat hun IT Security staat of valt met de weerbaarheid op de werkvloer.

Die kennis komt niemand aanwaaien. Phishing kun je herkennen, maar alleen als je weet waar je op moet letten. Je kunt van jezelf vinden dat je alert bent, maar je moet de momenten doorhebben en de door aanvallers gebruikte methodes. Onze klanten vragen ons dan om een phishingcampagne. Wij sturen in een afgesproken periode door ons ontworpen e-mails. Dat zijn mock-ups, dus imitaties van phishingmails.

Dat kunnen gemakkelijke e-mails zijn. Bijvoorbeeld met de mededeling dat je *honderdmiljoenmiljard* euro kan bijschrijven als je 1 keer klikt. Maar ook e-mails die bijna niet te onderscheiden zijn van echte e-mails. Denk je dat je daar ook niet intuint? We dagen je graag uit in deze white paper. En als je inderdaad zo scherp oplet: gefeliciteerd. Maar alvast een belangrijke opmerking vooraf: als je collega niet net zo scherp is, ben je nog nergens. Één verkeerde klik is immers voldoende.

Wat de reactie van onze klanten op onze phishingcampagne ook is, wij brengen na verzending nauwkeurig in kaart wat de resultaten zijn. Werd er (massaal) geklikt op de poging tot phishing? Hoe komt dat? En hoe voorkomen we dit, als het er om spant?

Ready?

Tijd voor een demonstratie. We beginnen meestal gemakkelijk. Eentje uit de categorie ‘afbeelding in lage resolutie met spelfouten’, compleet met link naar slechte opgemaakte inlogpagina.

Zie de volgende pagina!

Niveau 1, *the obvious*

Email Template

Beste [first_name] [last_name],

Wij van American Express geven terug aan onze gemeenschap. Wij ondersteunen Bitcoin en wij vinden dat u dat ook zou moeten doen!

Alle Bitcoin die naar deze link wordt verzonden, wordt verdubbeld naar u teruggestuurd!

REAGEER DIRECT!!

De link is 12 uur geldig.

Met vriendelijke groet,

American Express

De bovenstaande voorbeeldmail zou linken naar de volgende webpagina:

Landing Page

aumatics

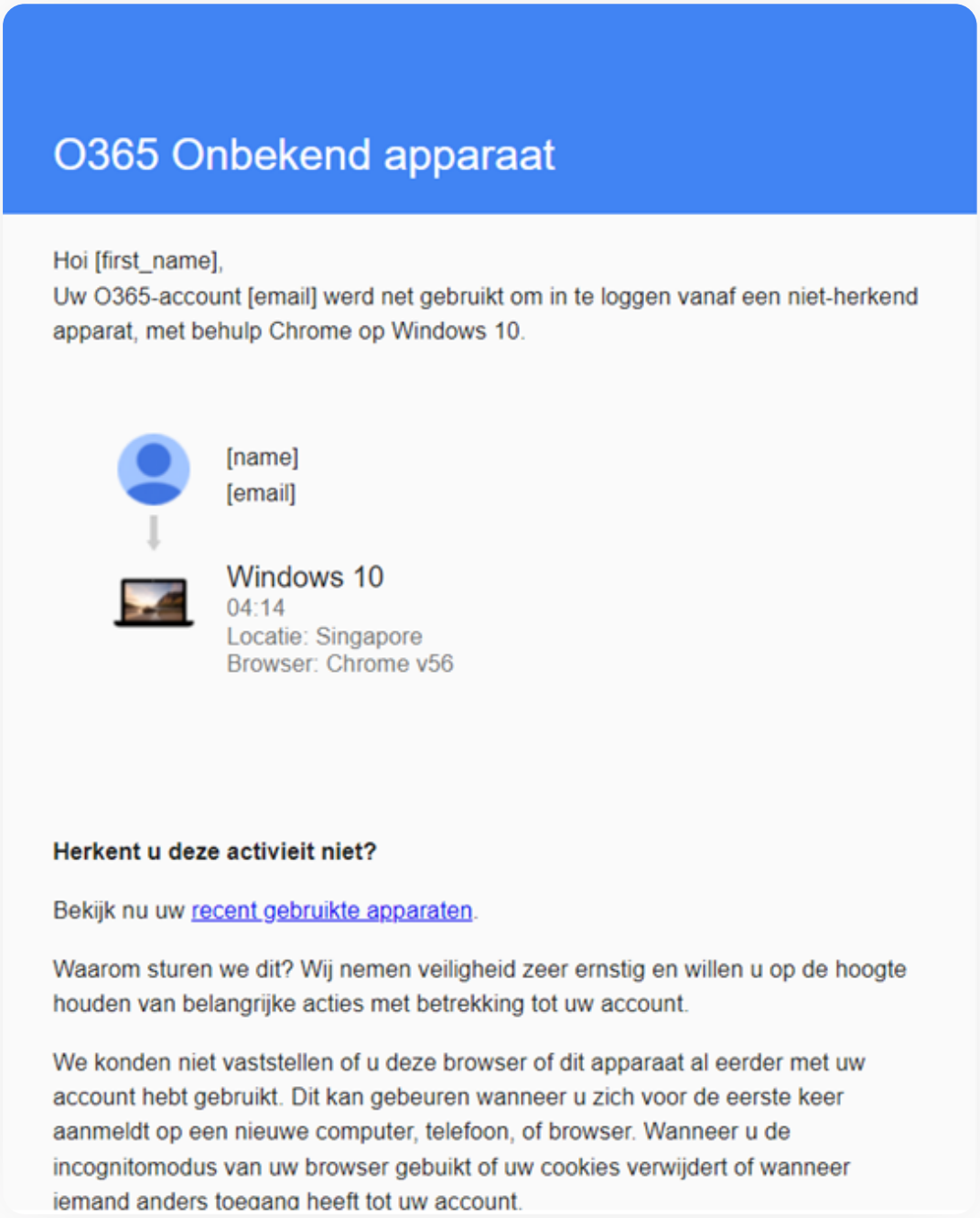
En?...

Hier zou je nooit op klikken, toch? En inloggen doe je al helemaal niet, toch?

Maar daarna wordt het moeilijker. Bijvoorbeeld omdat je een melding binnenkrijgt die prima past in de ‘normale’ stroom mails die je op een dag voor de kiezen krijgt. Ze vallen niet op en om die reden doen deze phishingmails geen beroep op je alertheid.

Waardoor ze wel opvallen? Bekijk onderstaande phishingmail zelf. We zeggen er wel bij: je weet nu al dat iets fishy is aan deze berichten. Hoe zou het in de praktijk gaan, als je dit bericht aantreft naast de 863 andere berichten in je inbox?

Niveau 2: het wordt al moeilijker



O365 Onbekend apparaat

Hoi [first_name],
Uw O365-account [email] werd net gebruikt om in te loggen vanaf een niet-herkend apparat, met behulp Chrome op Windows 10.

[name]
[email]

Windows 10
04:14
Locatie: Singapore
Browser: Chrome v56

Herkent u deze activieit niet?

Bekijk nu uw recent gebruikte apparaten.

Waarom sturen we dit? Wij nemen veiligheid zeer ernstig en willen u op de hoogte houden van belangrijke acties met betrekking tot uw account.

We konden niet vaststellen of u deze browser of dit apparaat al eerder met uw account hebt gebruikt. Dit kan gebeuren wanneer u zich voor de eerste keer aanmeldt op een nieuwe computer, telefoon, of browser. Wanneer u de incognitomodus van uw browser gebuikt of uw cookies verwijdert of wanneer iemand anders toegang heeft tot uw account.

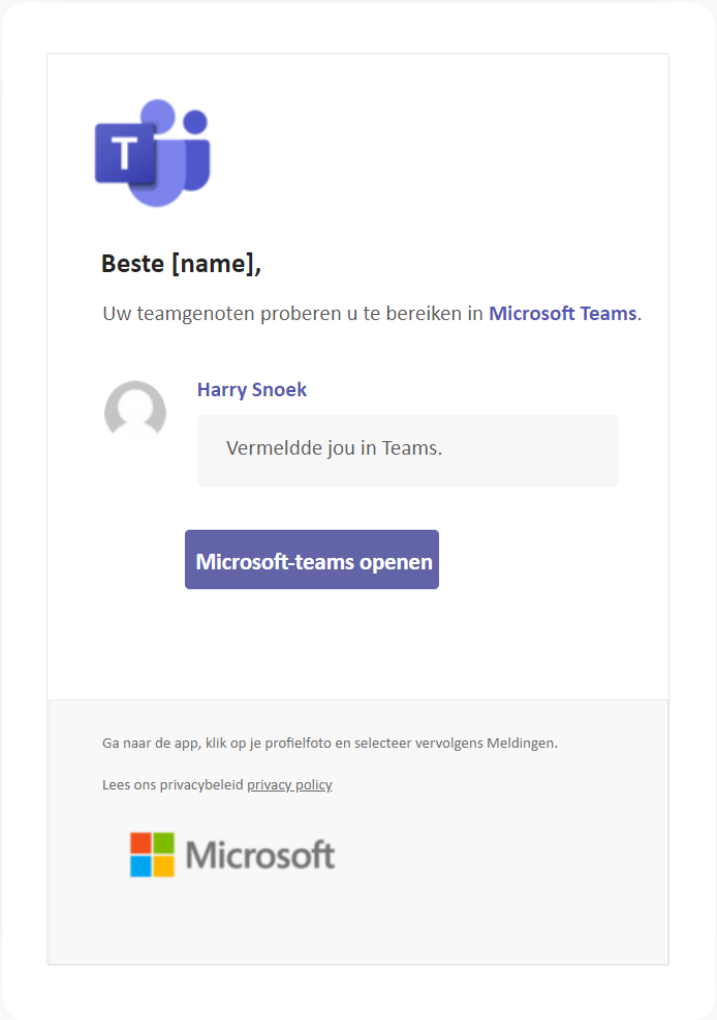
Opmerking: Tussen de haakjes zou je dan gewoon je eigen naam lezen. Om die reden zou de mail niet door de mand moeten vallen. Maar van deze weet je dus nu al dat het foute boel is...

Om welke reden valt deze mail wél door de mand? De tip die wij hier willen geven; de alarmbellen moeten afgaan met één enkele aanwijzing. Die aanwijzing zit in bovenstaande bericht niet in de inhoud. Het verzendadres bevat wel het woord Microsoft, maar is afkomstig van het domein online-account.info, dus het adres na '@'. Die website is onbekend terrein. Bij jou als gebruiker. En als het om phishing gaat, moet onbekend ook onbemind maken. Tenminste, als het goed is.

Niveau 3: nog bij de les?

Onderstaand voorbeeld is onze laatste. De spreekwoordelijk klap op de vuurpijl voor phishing. Het venijnige van deze phishingmail is namelijk dat je je helemaal niet realiseert dat ook dit phishing kan zijn. Het lijkt meer op een gesprek in Teams. Daarnaast gaan door de gebruikte foto's de alarmbellen niet af. Ook niet doordat jouw eigen naam wordt gebruikt.

We introduceren hiermee namelijk een bijzondere vorm van phishing. Deze vorm van phishing noemen we Spear Phishing. Denk je alle gevallen van klassieke phishing te kennen? Dit is echt next level. Spear Phishing verschilt ten opzichte van andere phishing mails doordat het niet onpersoonlijk is. Ze hebben jou op de korrel. Jij bent als aangemerkt als doelwit. Omdat je extra waardevolle data in bezit hebt. Of omdat je een gemakkelijk slachtoffer bent.



Wij voegen er aan toe: misschien ook omdat je jezelf tot gemakkelijk slachtoffer hebt gemaakt. Door iets te veel persoonlijke informatie online te zetten. Wat ook gewoon kan, is dat je net als velen van ons zonder het te weten ooit slachtoffer bent geweest van 'digitale huisvredebreuk.' En die gegevens nu worden ingezet voor een nieuwe malafide actie.

Wat de aanleiding ook was, de uitvoering bij Spear Phishing is meestal overtuigend. Hoe doen aanvallers dat? Door zoveel mogelijk privédetails te verzamelen en te combineren tot een overtuigende e-mail. Door de focus op jou als persoon, kan dit echt heel waarheidsgetrouwe pogingen opleveren. Daarnaast haakt dit voorbeeld aan bij een nieuwe trend in phishing. We zien namelijk steeds vaker dat social media-accounts een dankbare bron van kennis zijn voor kwaadwillenden. Zij profiteren van onze behoefte om persoongegevens te delen en tegelijkertijd maken ze misbruik van de communicatiekanalen van social media accounts.

Ook bij dit voorbeeld geldt: tussen haakjes en in het fotokader zou je de juiste naam en bijbehorende foto zien van jouw collega

Zou jij klikken? En als je het laatste voorbeeld terecht niet vertrouwde; zouden je collega's er wel in tuinen? Nee? En als je een herinnering van een dergelijk verzoek linkverzoek krijgt zoals hieronder?

Ook bij dit voorbeeld geldt: tussen haakjes en in het fotokader, zou je de juiste naam en bijbehorende foto zien.

De organisatorische kant van het verhaal. Net zo belangrijk.

Hoe lastig vond je de voorbeelden? En hoeveel van je collega's hebben geklikt? De impact van de laatste vraag op jouw organisatie kan niet worden onderschat. Het gaat er namelijk niet alleen om dat jij alert genoeg bent, of zoals wij dat noemen, of jij genoeg *awareness* hebt. De effectiviteit hiervan staat of valt namelijk met het gedrag van álle gebruikers op het bedrijfsnetwerk. En om nog specifieker te zijn; het gedrag van de zwakste schakel. Het is dus zaak om alle kennis die wij delen in dit white paper te laten landen bij iedereen binnen je organisatie. En dan op zo'n manier dat er een algeheel basisniveau van awareness tegen phishing bestaat.

Wij maken ons geen illusies. Je zult daar meer voor nodig hebben dan een white paper. Fijn dat je zo aandachtig leest, maar wij realiseren ons dat anderen minder aandacht hebben. Helaas, zeggen we erbij.

Wat is de oplossing? Op welke manier dringt het wel door bij iedereen dat phishing een van de meest gevaarlijke bedreigingen is voor IT Security?

Het antwoord is: security-awareness tegen phishing is ook een organisatorische opgave. Omdat het iedereen binnen een organisatie aangaat. Maar ook omdat in alle geledingen van een organisatie phishing kan toeslaan. Iedereen ontvangt e-mail en vervalsingen die soms zo slecht te herkennen zijn, dat in beginsel iedereen erin kan trappen. Om die reden is het noodzakelijk om dit onderwerp grondig aan te pakken. En om er de tijd voor te nemen.

Oefen, analyseer, herhaal

Ons voorstel is om phishing aan te pakken aan de hand van een gestructureerd plan van aanpak dat je in overleg wegzet in de tijd. Na de vastgestelde periode analyseer je samen met ons wat de resultaten zijn en herhaal je onderdelen van de training die lastig zijn gebleken voor collega's.

Die cyclus noemen we Plan-Do-Check-Act en leggen we je graag uit. Met deze aanpak neem je je collega's mee in de harde werkelijkheid van phishing én bouw je zelflerend vermogen in. Wij deden dat onlangs voor een organisatie en de resultaten bleven niet uit.

Je moet namelijk een lange adem hebben om phishing buiten de poort te houden. Waarom? Neem deze overwegingen mee:

Verloop
In een organisatie van enige omvang speelt verloop onder het personeel een grote rol. Collega's die kennis hebben over phishing gaan uit dienst; nieuwe collega's schuiven aan en weten dikwijls weinig over preventie.

Stay up to date
De wereld verandert, phishing ook. Aangehaakt blijven bij phishing anno nu is noodzakelijk

Prioriteit
Hou de prioriteit hoog. Zodra je stopt met een phishingcampagne en awarenesstraining, wordt de aandacht minder en de prioriteit gaat op een laag pitje. Zul je net zien dat een collega dan er dan net intuint.

Vier aanbevelingen

Als je goed hebt gelezen, merk je dat dit voornamelijk organisatorische zaken zijn. Het begint met het voornemen om phishing serieus te nemen. Dat doen onze klanten bijvoorbeeld door ons in de arm te nemen voor een phishing-campagne.

Dat werkt zo. Aumatics verstuurt dan op afstand regelmatig een phishingmail. Wij houden bij wat er gebeurt met deze mail(campagne). De bevindingen en leerpunten delen wij met de opdrachtgever. Vervolgens adviseren wij wat, waar en op welke manier de organisatie weerbaarder kan worden gemaakt, volgens de methode die we hierboven al beschreven.

Als IT-partner kijken wij daarbij van nature naar techniek. Maar niet uitsluitend. Het niveau van weerbaarheid is een mix van technische én organisatorische maatregelen. Vier aanbevelingen hiervoor:

1

Goede infrastructuur

Richt de infrastructuur van het bedrijfsnetwerk zo in dat de kans op een geslaagde phishingmail zo klein mogelijk is. Zorg bijvoorbeeld voor waarschuwingen bij e-mail van onbekenden en sta niet zomaar toe dat er wordt geklikt op dit soort e-mails.

2

Een actieplan

Denk na over het ‘Wat-als-scenario’. Ooit, op een dag, gaat er toch geklikt worden op een phishingmail binnen jouw organisatie. Wat gebeurt er dan? Ligt er een scenario op de plank om meer schade te voorkomen? Zogenoemde mitigerende maatregelen kunnen veel schade voorkomen. Vraag ons gerust naar de belangrijkste.

3

Techniek

Techniek weert phishing zoveel mogelijk met een spamfilter aan de voorkant. Aan de achterkant zijn het vooral de organisatorische maatregelen die de problemen voorkomen. Laat je werknemers een online webinar volgen ter preventie. Zo leren jij en je collega's alle verschijningsvormen van phishing kennen. Doe dit structureel en maak het bijvoorbeeld onderdeel van de introductie bij nieuwe collega's. Door de PDCA (Plan-Do-Check-Act) cyclus voorkom je eenmalige acties die snel weer verdwijnen en weinig waardevol zijn. Stel bijvoorbeeld in het jaar een moment vast waarop deze PDCA-cyclus tegen phishing begint en je de gebruikte technologische maatregelen evalueert. Benieuwd hoe phishingmails eruit zien die momenteel de ronde doen? De Fraudehelpdesk.nl (klik gerust ;-)) inventariseert doorlopend welke phishingmails nu rondgaan en toont ze. Waardevol oefenmateriaal, dat je gerust kan inzetten voor jou en je collega's!

4

Wachtwoordmanager

Maak gebruik van een wachtwoordmanager. Deze heeft een handige invuloptie voor alle wachtwoorden. Het bijhouden van alle ontelbare wachtwoorden is namelijk niet meer te doen. Dat weet jij, dat weten wij. Al helemaal niet met de hoge eisen van vandaag de dag. Een hoofdletter, speciaal teken, leesteken, cijfer, *we feel your pain*. Een wachtwoordmanager vult wachtwoorden zelf in vanuit de veilige kluis. Maar er is meer: door het gebruik van een wachtwoordmanager wordt je gewaarschuwd als je op malafide sites terechtkomt. De wachtwoordmanager controleert namelijk daarnaast of het adres van de inlogsite overeenkomst met wat er is vastgelegd. Is er geen match? Dan biedt Keeper niet aan om de inlognaam en wachtwoord in te vullen. Verwachtte je dit wel, omdat je denkt dat je op de juiste site bent? Dan moeten alle alarmbellen bij je afgaan. Interesse in deze quick win beveiligingsmaatregel, die meteen ook het leven gemakkelijker maakt? Probeer Keeper Wachtwoordmanager.

Het ontregelende aan een phishingcampagne

Nog een laatste aandachtspunt, met name over het menselijke aspect. De organisatie kan zijn ingelicht dat er een phishingcampagne aankomt. Maar verzeker je ervan dat ze de impact ervan ook doorhebben. Een phishingmail gaat normaal gesproken naar veel collega's in een keer. En uit eigen ervaring kunnen wij zeggen dat een geslaagde phishingmail vanuit Aumatics een echte onruststoker kan zijn.

Verzeker je er dus van dat de IT-afdeling of Service Desk realiseren dat ze na verzending aan de bak kunnen. Er zullen veel vragen komen van collega's, die terecht vinden dat er een luchtje zit aan de mail. Zij kunnen dan worden gerustgesteld. En: ze kunnen gefeliciteerd worden dat ze zo alert zijn. Maar dan moeten de betrokkenen wel op de hoogte zijn van het verzendmoment en de mogelijke impact.

Live and let live

Dit zeggen wij vanuit Aumatics niet zomaar. Het voorkomen van phishing is voor een groot deel een technisch verhaal. Maar jij en jouw collega's zijn de ontvangers. Reacties op de mail kunnen verschillen. Het kan dus ook zijn dat collega's not amused zijn, hoewel ze wisten dat dit eraan zat te komen. Want het was al zo druk. En wat als ik per ongeluk heb geklikt? Krijg ik dit te horen tijdens mijn functioneringsgesprek? Dat soort vragen kunnen op je af komen.

De antwoorden zul je als opdrachtgever zelf moeten opstellen vooraf. Zo blijft het zicht op de bedoeling van een campagne helder. Iedereen kan het slachtoffer worden van phishing, dus het is geen zaak van individuen. Een organisatie als geheel wapent zich tegen de weerbarstige realiteit van phishing.

Gebeurt het jou? Of je collega? Dan heb je het succes van een campagne bewezen. Uiteindelijk is er niets aan de hand.

Maar stel je voor dat het een echte phishingmail was. Wacht jij af tot het moment daar is? Of ben je het liever voor?

Wil jij écht aan de slag met phishing?

Benieuwd hoe ver jij en jouw collega's komen in een phishingcampagne van Aumatics? Laat het weten op Aumatics.nl en voorkom dat echte aanvallers vat krijgen op jouw bedrijfsnetwerk.

Vraag advies