Waarom we nog steeds in valse e-mails trappen

*Phishing heeft een indrukwekkende evolutie doorgemaakt. Het is niet langer miljoenen e-mails verzenden in de hoop een nieuw slachtoffer aan de haak te slaan. Net als zoveel cybercriminaliteit heeft phishing zich ongelooflijk ontwikkeld (en vereist daarmee een even verfijnde respons).*

Cijfers van Sophos hebben aangetoond dat phishingmails week in, week uit organisaties tracht te misleiden. Het is een continue aanval op het bedrijfsleven: 41% van de organisaties ervaart phishing-aanvallen dagelijks (of vaker) en meer dan driekwart (77%) ervaart minstens één keer per maand een phishing-aanval. Misschien wel het meest verontrustend is dat ongeveer 30% van deze phishing-e-mails wordt geopend, waaruit blijkt dat het cybercriminelen, ondanks bewustzijnsprogramma’s en trainingen, nog steeds lukt om personen te misleiden.

Inzicht in hun manier(en) van handelen is van groot belang. Sophos heeft inzicht in welke soorten e-mails het beste werken, wie het meest onder vuur wordt genomen alsmede de beste (combinatie van) technologieën en trainingen om een ​​organisatie te beveiligen. We kunnen bijvoorbeeld aantonen dat boekhouding en financiën de meest doelgerichte afdelingen zijn. Maar gezien het feit dat administratie en management op de voet volgen, is er een duidelijke behoefte om beschermende technologieën te combineren met op maat gemaakte, specifieke trainingen die de rollen van mensen weerspiegelt.

Om de woorden van John Shier van Sophos aan te halen:

*“Omdat de kwaliteit van phishing-e-mails is verbeterd, is het belangrijk te onthouden dat sommige ontvangers voor de gek worden gehouden. Gebruikers vormen de eerste verdedigingslinie tegen een succesvolle phishing-aanval. Hoewel educatie een belangrijk onderdeel is van het veilig houden van een organisatie, geldt dit ook voor de mogelijkheid van de gebruiker om verdachte phishing-pogingen te melden. Maak het eenvoudig en zonder consequenties voor uw gebruikers om aanvallen te melden, zelfs als ze zijn misleid. Het systeem voor vroegtijdige waarschuwing is cruciaal voor elke organisatie die snel en resoluut wil reageren op een phishingaanval.”*

Een rapport over Sophos’ bevindingen is **hier** te vinden. Als je deze informatie wilt bespreken of de impact van phishing verder zelf wilt onderzoeken (en waarom en hoe mensen er nog steeds voor vallen), kan ik je in contact brengen met de Sophos-specialisten in België of in Londen. Tevens hebben we een gratis antiphishing toolkit en onze whitepaper 'Don’t take the bait’ om er een ​​sterk en goed onderbouwd artikel over te schrijven.