nlcom
SLIM IN ICT

NLcom Security Awareness Training

Supported by Webroot

De mens = de zwakste schakel in elke beveiliging

Hoe goed is uw bedrijf beschermd tegen cyberaanvallen, phishing, spam en malware? Een betere vraag is misschien wel; zijn uw medewerkers op de hoogte van deze gevaren en kennen zij hun rol hierin? In de praktijk krijgen uw medewerkers te maken met bijvoorbeeld een phishing e-mail. Herkennen uw medewerkers deze phishing e-mail of gaan ze er op in? Hopelijk heeft u er nog geen ervaring mee maar voorkomen is natuurlijk beter dan genezen. Met dit artikel willen we u graag informeren wat NLcom hierin voor u kan betekenen. Onderstaand een drietal nieuwsberichten over phishing.

“Google Docs-gebruikers getroffen door schadelijke nepmail.

Er gaat een nepmail rond die gebruikers laat inloggen bij Google Docs, waarmee ongemerkt toegang tot e-mails en contacten wordt gegeven. Een groot aantal van dit soort nepmails wordt op dit moment verspreid onder mensen met Google-accounts. Daarover schrijven verschillende media, waaronder Business Insider. De mail doet alsof iemand uit de contactenlijst van de gebruiker een Google Doc heeft gedeeld...”

***Bron**: NU.nl - Google Docs-gebruikers getroffen door schadelijke nepmail - https://www.nu.nl/internet/4666545/google-docs-gebruikers-getroffen-schadelijke-nepmail.html*

“Wachtwoorden 50.000 Snapchat-gebruikers gestolen via phishing in juli.

De wachtwoorden en gebruikersnamen van 50.000 Snapchat-gebruikers zouden in juli zijn gestolen bij een phishingaanval. Dat meldt The Verge op basis op interne e-mails van Snapchat die de nieuwssite in handen heeft. De gegevens werden opgeslagen in een openbare lijst op een phishingwebsite genaamd klkviral.org. Volgens ingewijden stuurden de kwaadwillenden een link naar gebruikers via een account dat eerder gehackt werd. Nadat erop de link geklikt werd, opende er een website die leek op het login-scherm van Snapchat. Als gebruikers vervolgens probeerden in te loggen met hun eigen gegevens, werden deze gestolen...”

***Bron**: NU.nl - Wachtwoorden 50.000 Snapchat-gebruikers gestolen via phishing in juli https://www.nu.nl/internet/5138270/wachtwoorden-50000-snapchat-gebruikers-gestolen-via-phishing-in-juli.html*

“Twee op drie mensen trapt in Twitter-phishingbot.

Een phishingbot van onderzoekers op Twitter is er in geslaagd twee op de drie mensen te misleiden. Dat vertellen de onderzoekers in een paper. De bot analyseert berichten van Twitter-gebruikers, om op basis daarvan gepersonaliseerde berichten te sturen. Bij phishing ontvangt een slachtoffer een bericht dat er uitziet als bijvoorbeeld een bericht van een bank, met een link naar een website. Gegevens die via de link worden verzonden, komen in handen van internetcriminelen...”

***Bron**: NU.nl - Twee op drie mensen trapt in Twitter-phishingbot https://www.nu.nl/tech/4303120/twee-drie-mensen-trapt-in-twitter-phishingbot.html*

Om datalekken te voorkomen is “bewustwording” het sleutelwoord. Met de NLcom Security Awareness Training geeft u uw werknemers de handvaten om vreemde situaties te signaleren en vervolgens de juiste keuzes te maken. Zorg dat uw medewerkers zich bewust zijn van hun rol in de interne ICT Security en een hoop ellende kan voorkomen worden.

Hoe werkt de NLcom Security Awareness Training (NSAT)?

Security functioneert alleen als uw medewerkers op de hoogte zijn van mogelijke gevaren en begrijpen wat hun rol hierin is. Het is van groot belang dat medewerkers begrijpen hoe hun eigen acties de totale beveiliging van het bedrijf op het spel kunnen zetten. Denk hierbij niet alleen aan het verlies van data maar zeker ook imagoschade en financiële schade.

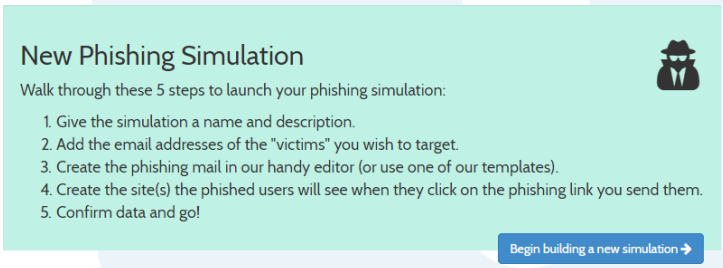
De NLcom Security Awareness Training bestaat uit verschillende online cursussen die medewerkers onder andere inzicht geeft in de werking van cybersecurity. Bepaalde groepen werknemers ontvangen een e-mail met bijvoorbeeld een hyperlink naar een opgezette phishing site. Deze e-mails lijken bijvoorbeeld van een bekende bank te zijn, of van een vaste leverancier. Als de medewerkers op de link in de e-mail klikken en gegevens achterlaten, wordt dit geregistreerd waarna ze een mededeling krijgen dat het nu een simulatie is maar het een gevaar had kunnen zijn. Vervolgens is het zaak de medewerker deel te laten nemen aan een online cursus om kennis op te doen. Alle stappen die een medewerker uitvoert worden geregistreerd en verwerkt in de rapportages. Met deze rapportages wordt de vooruitgang inzichtelijk en meetbaar.

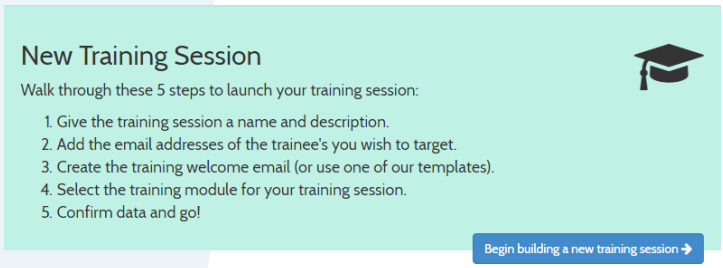
Video: NLcom Security Awareness Training Overview

Campagnes

Het uiteindelijke doel van NSAT is medewerkers zich bewust te laten worden van security in de breedste zin van het woord. Het is dus zaak de medewerkers te motiveren om de aangeleverde informatie zich eigen te maken en het te implementeren in hun dagelijkse werkzaamheden. Met dit doel voor ogen zijn er twee manieren om de eindgebruiker bewust te maken. Dit kan middels een simulatie van een mogelijk gevaarlijke situatie om vervolgens de training aan te bieden. Het is ook mogelijk de medewerkers eerst de training te laten doorlopen om vervolgens de stof te toetsen middels een phishing simulatie. Middels de simulatie wordt men zich bewuster van de gevaren en met de toevoeging van de training kan men leren waar men op moet letten. Wanneer men bewuster is zullen gevaarlijke situaties voorkomen worden.

Hoe bewust zijn uw medewerkers zich van security? Klikken uw medewerkers op alles wat ze zien? Meten is weten, en dat kan nu met NLcom Security Awareness Training.





Phishing Simulatie

Voorbeeld van een Phishing Simulatie: De doelgroep ontvangt een nagemaakte phishing e-mail met hierin een link. Zodra men op de link klikt komen ze in een fake login scherm en wordt naar persoonlijke gegevens gevraagd. Zodra deze worden ingevuld en “verzonden” wordt een melding getoond dat ze de fout in zijn gegaan. Deze stappen worden per eindgebruiker geregistreerd en gerapporteerd om de security awareness inzichtelijk te maken. Hier wordt vervolgens een rapportage van gemaakt en mogelijke vervolgstappen besproken om dit in de toekomst te voorkomen.

Training

Voorbeeld van een Training: De doelgroep ontvangt een e-mail met hierin de uitnodiging om deel te nemen aan de training. Het doel van deze e-mail is om de eindgebruikers te motiveren deel te nemen aan de training. De training is ook via een centrale plek beschikbaar te stellen via een URL. De medewerkers kunnen zich vervolgens registreren en deelnemen aan de training. Bij een nieuwe medewerker kan dit een standaard tool zijn om vanaf het eerste uur de bewustwording te trainen.

Rapportageonderdelen

Onderstaande onderdelen worden gelogd en gerapporteerd per campagne. Door de rapportages is snel duidelijk hoe iemand het heeft gedaan en waar in de organisatie nog verbeterpunten liggen.

In deze rapportages zijn onderstaande onderdelen opgenomen:

- Aantal verstuurde e-mails
- Aantal afgeleverde e-mails
- Aantal geopende e-mails
- Aantal geklikte links
- Aantal gestarte trainingen
- Aantal voltooide trainingen

Onderwerpen

De volgende onderwerpen zijn beschikbaar. NLcom is continue bezig met de doorontwikkeling van deze onderwerpen. Elk onderwerp informeert de eindgebruiker waarna de behandelde stof wordt getest in een korte quiz. Na het succesvol afronden van een onderwerp krijgt de eindgebruiker een digitaal certificaat. Afhankelijk van het bedrijf zijn bepaalde onderwerpen interessanter dan andere daar is dan ook zelf een keuze in te maken.

Algemeen

Understanding Cybersecurity	*10 min*
Understanding Malware	*8 min*
Working Safely and Securely	*10 min*
Avoid Phishers, Hackers and Social Engineers	*10 min*

Cybersecurity

Social Media Awareness	*5 min*
Phishing Awareness	*5 min*
Websites and Software	*5 min*
E-mail	*5 min*
Passwords	*5 min*
Physical Access	*5 min*

Als u interesse heeft in NLcom Security Awareness Training kunt u het beste contact opnemen met ons sales team via sales@nlcom.nl of +31 (0)43 350 01 90.