OUCH! | September 2019

De maandelijkse Security Awareness nieuwsbrief voor jou!

Oplichting via Social Media

Overzicht

Velen van ons hebben phishing-e-mailaanvallen ontvangen, zowel op het werk als thuis. Dit zijn e-mails die er legitiem uitzien, zoals van jouw bank, jouw baas of jouw favoriete online winkel. Deze e-mails zijn echter in werkelijkheid een aanval, een poging om je te dwingen een actie te ondernemen die je niet moet ondernemen, zoals het openen van een geïnfecteerde e-mailbijlage, het delen van je wachtwoord of het overmaken van geld. De uitdaging is dat hoe slimmer wij worden in het spotten en stoppen van deze e-mailaanvallen, des te meer cybercriminelen andere manieren zullen proberen om contact op te nemen en mensen te bedriegen.

Pogingen om mensen te bedriegen of voor de gek te houden kunnen plaatsvinden via bijna elke vorm van communicatie die je gebruikt, van Skype, WhatsApp en Slack tot Twitter, Facebook, Snapchat, Instagram of zelfs gaming apps. Communicatie via deze platforms of kanalen kan informeler of betrouwbaarder aanvoelen, en dat is precies de reden waarom aanvallers ze gebruiken om anderen voor de gek te houden. Bovendien is het met de huidige technologieën veel gemakkelijker geworden voor elke aanvaller, waar ook ter wereld, om zich voor te doen alsof hij of zij iets of iemand is die hij of zij wil. Het is belangrijk om te onthouden dat alle communicatie die op je pad komt, misschien niet is zoals het lijkt en dat mensen niet altijd zijn wie ze lijken te zijn.

Hoofdpunten

Hier zijn de meest voorkomende aanwijzingen dat het bericht dat je net hebt ontvangen of het bericht dat je zojuist hebt gelezen een aanval kan zijn.

Spoedeisendheid: Een bericht dat een gevoel van urgentie heeft dat “onmiddellijke actie” vereist voordat er iets ergs gebeurt, zoals dreigen met het sluiten van een account of je naar de gevangenis sturen. De aanvaller wil jou opjagen om een fout te maken.

Druk; Druk op je uitoefenen om beleid of procedures op het werk te omzeilen of te negeren.

Nieuwsgierigheid: Een sterk gevoel van nieuwsgierigheid of iets dat te mooi is om waar te zijn. Nee, je hebt de loterij niet gewonnen.

Sensibel: Een verzoek om zeer gevoelige informatie, zoals je creditcardnummer of wachtwoord, of informatie die je gewoon niet gemakkelijk kunt delen.

Officiële berichten: Het bericht zegt dat het afkomstig is van een officiële organisatie, maar heeft een slechte grammatica of spelling. De meeste overheidsorganisaties zullen geen gebruik maken van sociale media voor officiële communicatie. Als je niet zeker weet of het bericht legitiem is, bel dan de organisatie terug, maar gebruik een vertrouwd telefoonnummer, zoals dat van hun website.

Imitatie: Je ontvangt een bericht van een vriend of collega, maar de toon of formulering klinkt gewoon niet zoals zij. Als je achterdochtig bent, bel dan de afzender op om te controleren of hij/zij het bericht heeft verzonden. Het is gemakkelijk voor een cyberaanvaller om berichten te maken die van iemand die je kent lijken te zijn. In sommige gevallen kunnen ze een account van je vriend overnemen, zich dan voordoen als je vriend en je bereiken. Wees je vooral bewust van sms'jes, Twitter en andere vormen van korte berichten, wat moeilijker is om een gevoel van de persoonlijkheid van de afzender te krijgen.

Jij bent de beste verdediging tegen zwendel, oplichterij en dergelijke aanvallen. Als een bericht vreemd of verdacht lijkt, negeer of verwijder het dan gewoon, of als het van iemand is die je persoonlijk kent, bel de persoon om te bevestigen dat het echt verstuurd is.

Over Cegeka Groep

Cegeka is een onafhankelijke ICT–dienstverlener die klanten in heel Europa helpt met hun digitale transformatie, agile ontwikkeling, trusted cloudoplossingen en 24/7 managed services. Cegeka heeft vestigingen in België, Duitsland, Frankrijk, Italië, Nederland, Luxemburg, Oostenrijk, Polen, Roemenië, Slowakije en Tsjechië. Cegeka heeft meer dan 4.200 medewerkers. In 2018 realiseerde Cegeka Groep een omzet van 512 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Dr. Jessica Barker *(@drjessicabarker) is een koploper op het gebied van de menselijke kant van cyberveiligheid. Ze is co-CEO van Cygenta, waar ze haar passie voor het positief beïnvloeden van cybersecurity bewustzijn, gedrag en cultuur over de hele wereld volgt. Ze is de voorzitter van ClubCISO en een populaire keynote speaker.*

Bronnen

Social Engineering:	https://www.sans.org/u/Uz6
Phone Call Scams:	https://www.sans.org/u/Uzb
Stop That Phish:	https://www.sans.org/u/Uzg
Personalized Scams:	https://www.sans.org/u/Uzl