SANS SECURITY AWARENESS

OUCH!

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers

Stop Die V(Ph)is(h)

Overzicht

E-mail- en berichtendiensten (zoals Skype, Twitter of Snapchat) zijn een van de voornaamste manieren waarop we communiceren. We gebruiken deze technologieën niet alleen dagelijks voor het werk, maar ook om in contact te blijven met vrienden en familie. Omdat zoveel mensen over de hele wereld afhankelijk zijn van deze technologieën, zijn ze uitgegroeid tot een van de primaire aanvalsmethoden die worden gebruikt door cyberaanvallers, een aanvalsmethode die phishing wordt genoemd. Leer wat phishing is en hoe u deze aanvallen kunt herkennen en stoppen, ongeacht of u op het werk bent of thuis.

Wat is Phishing

Phishing is een soort aanval waarbij u via e-mail of een berichtenservice wordt verleid om een actie uit te voeren die u niet zou moeten ondernemen, zoals klikken op een kwaadaardige link, uw wachtwoord delen of een geïnfecteerde e-mailbijlage openen. Aanvallers werken er hard aan om deze boodschappen overtuigend te maken en spelen in op je emotionele triggers, zoals urgentie of nieuwsgierigheid. Ze kunnen het doen lijken alsof het bericht van iemand of van iets komt dat u kent, zoals een vriend of een vertrouwd bedrijf dat u vaak gebruikt. Of misschien voegen ze zelfs logo's van uw bank toe of vervalsen ze het e-mailadres zodat het bericht legitiemer wordt. Aanvallers sturen deze berichten vervolgens naar miljoenen mensen. Zij weten niet wie het aas zal pakken, het enige dat ze weten is, hoe meer zij versturen des te groter de kans op slachtoffers.

Jezelf beschermen

In bijna alle gevallen is het openen en lezen van een e-mail of bericht prima. Om een phishing-aanval te laten werken, moeten de slechteriken je eerst verleiden om een actie uit te voeren. Gelukkig zijn er aanwijzingen dat een bericht een aanval is, hier zijn de meest voorkomende:

- Een enorm gevoel van urgentie, die "onmiddellijke actie" vereist voordat er iets verkeerds gebeurt, zoals dreigen met het sluiten van een account of u naar de gevangenis sturen. De aanvaller wil u haasten in het maken van een vergissing.
- Druk op u uitoefenen om het beleid of de procedures op uw werk te omzeilen of te negeren.
- Een enorm gevoel van nieuwsgierigheid, 'te mooi om waar te zijn' (nee, je hebt niet de loterij gewonnen)
- Een algemene aanhef zoals "Beste klant". De meeste bedrijven of vrienden die contact met u opnemen kennen uw naam.

- Zeer gevoelige informatie aanvragen, zoals uw creditcardnummer of wachtwoord of andere informatie die de legitieme afzender al zou moeten weten.
- Het bericht zegt dat het afkomstig is van een officiële organisatie, maar heeft een slechte grammatica of spelling of maakt gebruik van een persoonlijk e-mailadres zoals @gmail.com.
- Het bericht komt van een officiële e-mail (zoals uw baas), maar heeft een Reply-To-adres dat naar iemands persoonlijke e-mailaccount gaat.
- U ontvangt een bericht van iemand die u kent, maar de toon of de bewoording klinkt gewoon niet zoals hij of zij. Als u achterdochtig bent, belt u de afzender om te controleren of deze het bericht heeft verzonden. Het is voor een cyberaanvaller gemakkelijk om een bericht te maken dat van een vriend of collega afkomstig lijkt te zijn.

Uiteindelijk is gezond verstand je beste verdediging. Als een e-mail of bericht vreemd, verdacht of te mooi lijkt om waar te zijn, kan het een phishing-aanval zijn.

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 3.600 medewerkers. In 2015 realiseerde Cegeka Groep een omzet van 368 miljoen euro. Bezoek www.cegeka.com voor meer informatie.

Gastredacteur

Tonia Dudley ontwikkelt en voert sinds 2011 beveiligingsbewustwordingsprogramma's uit, waaronder het opzetten van een bekroond phishing-trainingsprogramma. U kunt haar vinden op www.linkedin.com/in/toniadudley.

Hulpmiddelen

Social Engineering:	https://www.sans.org/u/Cb1
Anderen helpen zichzelf te beschermen:	https://www.sans.org/u/Cb6
Email Do's and Don'ts:	https://www.sans.org/u/Cbg
CEO fraude:	https://www.sans.org/u/Cbl
OUCH! Vertalingen en archieven:	https://www.sans.org/u/Cbq

License