De maandelijkse Security Awareness nieuwsbrief voor jou!

Oplichting op maat

Overzicht

Cybercriminelen blijven nieuwe en creatieve manieren bedenken om mensen voor de gek te houden. Een nieuw soort oplichting wint aan populariteit - oplichting op maat. Cybercriminelen vinden of kopen informatie over miljoenen mensen en gebruiken die informatie om hun aanvallen te personaliseren. Hieronder laten we je zien hoe deze oplichting werkt en nemen we je mee langs een veelvoorkomend voorbeeld. Hoe meer je weet over deze oplichterij, hoe makkelijker het voor jou is om ze op te sporen en te stoppen.

Hoe werkt het?

E-mail- of telefoonoplichterij is niet nieuw, cybercriminelen proberen al jaren mensen voor de gek te houden. Voorbeelden hiervan zijn de “You Won the Lottery” of de beruchte Nigeriaanse Prins oplichting. In deze traditionele oplichterspraktijken weten cybercriminelen echter niet op wie ze zich richten. Ze creëren eenvoudigweg een generieke boodschap en sturen deze naar miljoenen mensen. Omdat deze oplichting zo generiek is, zijn ze meestal gemakkelijk te herkennen. Een gepersonaliseerde oplichterij is anders, de cybercriminelen doen eerst onderzoek en maken een bericht op maat voor elk beoogd slachtoffer. Dit doen ze door het vinden of kopen van een database met namen, wachtwoorden, telefoonnummers of andere gegevens van mensen. Dit soort informatie is gemakkelijk beschikbaar dankzij alle websites die zijn gehackt. Het is ook algemeen beschikbaar op social media sites en in openbare overheidsdossiers. De criminelen richten zich dan op iedereen over wie ze informatie hebben.

Een veel voorkomende truc die cybercriminelen gebruiken is angst of afpersing om jou te dwingen om aan hen geld te betalen. De aanval werkt als volgt. Ze vinden of kopen informatie over mensen die gebruikersnamen en wachtwoorden van gehackte websites. Ze vinden jouw accountinformatie in zo’n database en sturen jou (en iedereen in de database) een e-mail met wat persoonlijke gegevens over jou, inclusief het originele wachtwoord dat je op de gehackte website hebt gebruikt. De crimineel verwijst naar het wachtwoord als “bewijs” dat jouw computer of apparaat is gehackt, wat natuurlijk niet waar is. De crimineel beweert dan dat terwijl zij je computer hebben gehackt, zij je ook hebben betrapt op het online bekijken van pornografie. De e-mail dreigt dan dat als je hun afpersingskosten niet betaalt, zij met je familie en vrienden bewijs zullen delen van pijnlijke online activiteiten.

De valkuil is, in bijna elke situatie zoals deze heeft de cybercrimineel jouw systeem nooit gehackt. Ze weten zelfs niet eens wie je bent of welke websites je hebt bezocht. De oplichter probeert eenvoudigweg de weinige persoonlijke gegevens die ze over je hebben te gebruiken om je bang te maken zodat je gelooft dat ze jouw computer of apparaat hebben gehackt, en

om je te verleiden tot het betalen van geld. Vergeet niet, slechteriken kunnen dezelfde technieken ook gebruiken voor een telefoongesprek scam.

Wat kun je doen?

Besef dat dergelijke e-mails of telefoongesprekken een oplichterij zijn. Het is vanzelfsprekend om bang te zijn als iemand persoonlijke informatie over je heeft. Denk er echter aan dat de afzender liegt. De aanval is een onderdeel van een geautomatiseerde massacampagne, niet een poging om je direct te benaderen. Het wordt steeds gemakkelijker voor cybercriminelen om vandaag de dag persoonlijke informatie te vinden of te kopen, dus verwacht in de toekomst meer persoonlijke oplichting zoals deze. Enkele aanwijzingen om te zoeken.

- **Wanneer je een zeer dringende e-mail, bericht of telefoontje ontvangt, moet je erg argwanend zijn. Als iemand emoties zoals angst of urgentie gebruikt, proberen ze je te dwingen een misstap te maken.**
- **Wanneer iemand betaling eist in BitCoin, cadeaubonnen of andere niet-traceerbare methoden**
- **Wanneer je een verdachte e-mail krijgt, zoek dan op Google om te zien of andere mensen soortgelijke aanvallen hebben gemeld.**

Uiteindelijk is gezond verstand de beste verdediging. Wij raden echter ook aan om altijd een uniek, lang wachtwoord te gebruiken voor elk van je online accounts. Kun je niet al je wachtwoorden onthouden? Gebruik een wachtwoordmanager. Maak bovendien waar mogelijk een verificatie in twee stappen mogelijk.

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

Lenny Zeltser *is een cybersecurity veteraan. Hij bouwt anti-malware oplossingen bij Minerva Labs en geeft les aan het SANS instituut. Zijn ervaring omvat ook managed security services en consulting. Volg hem op zeltser.com/blog en op Twitter @lennyzeltser.*

Bronnen

Social Engineering:	https://www.sans.org/u/MUU
Stop That Phish:	https://www.sans.org/u/MUZ
Search Yourself Online:	https://www.sans.org/u/MV4
Password Manager:	https://www.sans.org/u/MV9