OUCH!

SANS SECURITY AWARENESS

Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers

Aanvallen en oplichting door middel van telefoongesprekken

Overzicht

Als je aan cybercriminelen denkt, denk je waarschijnlijk aan een kwaadaardig brein achter een computer die geavanceerde aanvallen op het internet uitvoert. Hoewel veel van de huidige cybercriminelen technologieën zoals e-mail of instant messaging gebruiken, gebruiken ze ook de telefoon om hun slachtoffers te misleiden. Er zijn twee grote voordelen aan het gebruik van een telefoon. Ten eerste zijn er, in tegenstelling tot e-mail, minder beveiligingstechnologieën die telefoongesprekken monitoren en een aanval kunnen detecteren en stoppen. Ten tweede is het voor hen veel gemakkelijker om emoties over te brengen via de telefoon, waardoor het waarschijnlijker is dat ze hun slachtoffers kunnen bedriegen. Laten we leren hoe we deze aanvallen kunnen herkennen en stoppen.

Hoe werken aanvallen via de telefoon?

Het begint met begrijpen waar deze aanvallers op uit zijn. Meestal willen ze geld, informatie of toegang tot de computer (of alle drie). Ze doen dit door je te laten doen wat ze willen. De aanvallers bellen mensen over de hele wereld, waardoor situaties ontstaan die zeer urgent lijken. Ze willen je uit balans krijgen door je te laten schrikken, zodat je niet helder denkt, en dan overhaast een fout laten maken. Enkele van de meest voorkomende voorbeelden zijn:

De beller doet zich voor als zijnde van de belastingdienst van de overheid en doet het voorkomen alsof je onbetaalde belastingen hebt. Ze leggen uit dat als je deze belastingen niet meteen betaalt je naar de gevangenis gaat en leggen zo druk op om de belastingen direct te betalen met een creditcard via de telefoon. Dit is een oplichting, veel belastingafdelingen, waaronder de IRS, bellen of e-mailen nooit mensen. Alle officiële fiscale kennisgevingen worden per gewone post verzonden.

De beller doet alsof hij van Microsoft Tech Support is en legt uit dat jouw computer is geïnfecteerd. Als ze je ervan overtuigen dat je geïnfecteerd bent, zetten ze je onder druk om hun software te kopen of ze toegang op afstand te geven tot je computer. Microsoft belt je niet thuis.

Je krijgt een automatisch voicemailbericht dat je bankrekening is geannuleerd en dat je een nummer moet terugbellen om het opnieuw te activeren. Wanneer je belt, krijg je een geautomatiseerd systeem dat vraagt om je identiteit te bevestigen en allerlei persoonlijke vragen stelt. Dit is echter niet de bank, ze registreren gewoon alle informatie voor identiteitsfraude.

Bescherm jezelf

De grootste verdediging die je hebt tegen telefonische aanvallen ben jij zelf. Houd deze dingen in gedachten.

Telkens als iemand je belt en een enorm gevoel van urgentie creëert en hij oefent druk op je uit om iets te doen, wees dan uiterst alert. Zelfs als het telefoongesprek op het eerste gezicht in orde lijkt, maar dan vreemd begint te voelen, kun je op elk moment stoppen en "nee" zeggen.

Als je denkt dat een telefoongesprek een aanval is, hoef je alleen maar op te hangen. Als je wilt bevestigen of het telefoongesprek legitiem was, ga dan naar de website van de organisatie (zoals de bank) en bel het telefoonnummer van de klantenservice direct zelf op. Zo weet je dat je met de echte organisatie praat.

Vertrouw nooit op Caller-ID, criminelen zullen vaak het nummer van de beller manipuleren zodat het lijkt alsof het afkomstig is van een legitieme organisatie of vanuit hetzelfde netnummer als je eigen telefoonnummer.

Laat een beller nooit de tijdelijke controle over jouw computer overnemen of je verleiden tot het downloaden van software. Dit is hoe slechteriken een computer kunnen besmetten.

Als je een telefoontje krijgt van iemand die je niet persoonlijk kent, laat het dan direct naar voicemail gaan. Op deze manier kun je onbekende gesprekken op je eigen tijd bekijken. Nog beter, op veel telefoons kun je dit standaard inschakelen met de functie "Niet storen".

Bedrog en aanvallen via de telefoon nemen toe. Jij bent zelf de beste verdediging die je hebt bij het detecteren en stoppen hiervan.

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

Jen Fox *levert diensten op het gebied van veiligheidsbewustzijn, social engineering en risicobeoordeling als Sr. Security Consultant at All Covered. Zoek Jen op Twitter als* @j_fox.

Bronnen

Consumenteninformatie over identiteit, privacy en online beveiliging:
https://www.consumer.ftc.gov/topics/privacy-identity-online-security
Meld een telefoonscam (in de VS): https://www.ftccomplaintassistant.gov/#crnt
Social Engineering: https://www.sans.org/u/Fi5