Maandelijkse Security Awareness nieuwsbrief voor Computergebruikers

# CEO Fraude / BEC

## Wat is CEO Fraude / BEC?

Cyber aanvallers zijn voortdurend bezig met de ontwikkeling van een e-mailaanval genaamd CEO Fraude, of Business Email Compromise (BEC). Dit zijn gerichte e-mailaanvallen die hun slachtoffer overhalen een actie te ondernemen die ze niet zouden moeten ondernemen. In de meeste gevallen zijn de slechteriken op zoek naar geld. Wat deze aanvallen zo gevaarlijk maakt, is dat cyberaanvallers onderzoek doen naar hun slachtoffers voordat ze met hun aanval beginnen. Het is ook erg moeilijk voor beveiligingstechnologieën om deze aanvallen te stoppen omdat er geen geïnfecteerde e-mailbijlagen of kwaadaardige koppelingen zijn om te detecteren. Hier is hoe de aanval werkt.

De cyberaanvaller maakt gebruik van het internet om het beoogde slachtoffer en mensen met wie zij interacties hebben te onderzoeken. Bijvoorbeeld, wanneer ze zich zouden richten op jou dan onderzoeken ze wie jouw baas is op het werk of misschien een makelaar met wie je samenwerkt. De cyberaanvaller maakt dan een e-mail, doet alsof hij een van deze mensen is en stuurt de e-mail naar je toe. De e-mail is dringend en vereist dat je direct actie onderneemt, zoals het verwerken van een factuur, het wijzigen van wie je een betaling doet, of het overtuigen om te antwoorden met gevoelige documenten. De e-mail werkt door je onder druk te zetten om te doen wat zij willen. Hier zijn twee voorbeelden van hoe zo'n aanval zou kunnen werken."

**Wire Transfer:** Een cybercrimineel is uit op geld. Ze onderzoeken het bedrijf waarvoor je werkt en identificeren de personen die werken in crediteuren of iedereen die verantwoordelijk is voor het overmaken van geld. De misdadigers creëren en sturen een e-mail naar deze individuen die zich voordoet als hun baas of een senior executiv. In de e-mail staat dat er sprake is van een calamiteit en dat er direct geld moet worden overgeboekt naar een nieuwe bankrekening. De e-mail zet hen onder druk om een vergissing te maken en in werkelijkheid sturen ze geld naar de cybercrimineel.

**Belastingfraude:** Cybercriminelen zijn uit op persoonlijke informatie om te gebruiken voor belastingfraude. Een van de snelste manieren om dit te krijgen is het stelen van de informatie van alle medewerkers van een bedrijf. De cybercriminelen onderzoeken en identificeren wie er bij Human Resources werkt. Vervolgens sturen ze valse e-mails naar deze personen, en doen ze alsof ze een hogere leidinggevende of misschien iemand van juridische aard zijn. De e-mails creëren een dringend verhaal, dat de fiscale informatie over alle medewerkers meteen moet worden ingediend. De mensen van Human Resources denken dat ze de gevoelige documenten naar de leidinggevende sturen, terwijl ze ze in werkelijkheid naar een cybercrimineel sturen.

## Jezelf beschermen

Wat kun je doen om jezelf te beschermen? Gezond verstand is de beste verdediging. Hier zijn de meest voorkomende aanwijzingen om naar te zoeken.

**De e-mail is zeer kort en dringend (vaak slechts een paar zinnen) en de handtekening zegt dat de e-mail werd verzonden vanaf een mobiel apparaat.**

**Er is een sterk gevoel van urgentie, waardoor je onder druk wordt gezet om je werkgeversbeleid te negeren of te omzeilen. Volg altijd het beleid en de procedures met betrekking tot het werk, zelfs als de e-mail afkomstig lijkt te zijn van je baas of zelfs de CEO.**

**De e-mail is werkgerelateerd, maar gebruikt een persoonlijk e-mailadres, zoals @gmail.com of @hotmail.com.**

**De e-mail lijkt afkomstig te zijn van een senior leider, collega of leverancier met wie je werkt, maar de toon van het bericht klinkt niet zoals zij.**

**Deze instructies verschillen van de instructies die je al hebt ontvangen, zoals het aanvragen van onmiddellijke betaling op een andere bankrekening.**

Als je vermoedt dat je op het werk bent aangevallen, stop dan alle interactie met de aanvaller en meld dit aan je supervisor. Als je thuis bent benaderd of het slachtoffer bent geworden van een bankoverschrijving, meld deze dan onmiddellijk bij je bank en vervolgens bij de politie.

## 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

***Don Cavender*** *is een voormalig speciaal agent van de FBI met meer dan 22 jaar ervaring in digitaal forensisch onderzoek en cybercrime. Hij heeft zich recentelijk gericht op cybercriminele organisaties als BEC-coördinator van Washington DC. Hij geeft trainingen en doet onderzoek op het gebied van digitaal forensisch onderzoek en cyberonderzoek.* @don_cavender
https://www.linkedin.com/in/donald-cavender

## Bronnen

| | |
|---|---|
| Social Engineering: | https://www.sans.org/u/HE3 |
| Stop That Phish: | https://www.sans.org/u/HE8 |
| Stop That Malware: | https://www.sans.org/u/HEd |
| Lock Down Your Login: | https://www.sans.org/u/HEi |