CEO fraude

Beter voorkomen dan betalen

CERT.be

31 juli 2017

TLP: WHITE

CERT.be
The Federal Cyber Emergency Team

CENTRE FOR CYBER SECURITY BELGIUM

Inhoudstafel

1 WAT IS CEO FRAUDE?

CEO fraude is een vorm van oplichting waarbij cybercriminelen de financiële afdeling van een onderneming contacteren met de vraag een belangrijke betaling uit te voeren. De oplichters nemen de identiteit aan van de CEO, CFO of een vertrouwde persoon binnen het bedrijf en vragen een medewerker van de financiële afdeling om een dringende betaling uit te voeren. Omdat de werknemer in de veronderstelling is dat de vraag van het hoger management komt, is de kans reëel dat de betaling effectief wordt uitgevoerd.

Als de fraude niet binnen de 24 uur aan het licht komt, is het zeer moeilijk of zelfs onmogelijk om het geld te recupereren. Voorkomen is dus beter dan betalen.

Deze vorm van cybercriminaliteit is niet nieuw, maar CERT.be krijgt steeds meer meldingen van pogingen tot CEO fraude. Gelukkig zijn medewerkers vaak alert genoeg om correct te reageren en de overschrijving niet uit te voeren. Helaas lukt de fraude soms wel, en dan kunnen de verliezen voor ondernemingen in de miljoenen euro oplopen.

Tussen juni 2015 en januari 2016 rapporteerde de FBI een verhoging van 1300% in verliezen voor ondernemingen door dit type van fraude; in totaal 3 miljard dollar. In België betaalde een bank 70 miljoen euro aan onbekende criminelen. Ook Google en Facebook waren slachtoffer met verliezen tot 100 miljoen dollar. Zowel grote als kleine bedrijven worden geviseerd.

Lees hier hoe u CEO fraude kan herkennen en voorkomen, en wat u moet doen als uw onderneming toch slachtoffer van deze oplichting werd.

2 HOE WERKT CEO FRAUDE PRECIES?

Verkenningsfase

Net zoals een inbreker vooraf de zwakke plekken van een woning zoekt en de gewoontes van de bewoners observeert, zal een cybercrimineel zo veel mogelijk informatie proberen te verkrijgen over de onderneming.

Onder een valse identiteit probeert de oplichter de volgende informatie te ontfutselen:

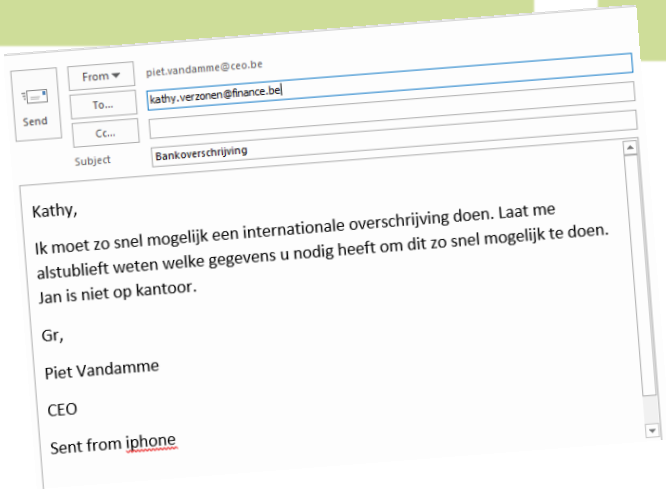
- de identiteit van de medewerkers die bevoegd zijn om aanzienlijke betalingen uit te voeren,
- de interne betalingsprocessen (procedures, accountnummers en balansinformatie, enz.),
- de leveranciers of klanten van het bedrijf.

Dit kan telefonisch gebeuren, via een vervalst e-mailadres of gewoon door gegevens online op te zoeken.

Uitvoeringsfase

Zodra de cybercrimineel voldoende informatie in handen heeft, is hij klaar om de oplichting **uit te voeren**. Dit verloopt als volgt:

- De onderneming wordt per e-mail of telefonisch gecontacteerd door de oplichter die zich voordoet als CEO, CFO of een andere contactpersoon die gekend is in de onderneming.
- Om het gevoel van legitimiteit te vergroten, gebruikt de oplichter soms ook andere valse identiteiten zoals die van een advocaat, de voorzitter van de raad van bestuur of een klant.
- De oplichter vraagt om een belangrijke overschrijving te doen. De opdracht wordt voorgesteld als uiterst belangrijk, dringend of geheim, met de bedoeling bestaande procedures te omzeilen of om te kunnen rekenen op een snelle en vertrouwelijke afhandeling.
- De medewerker die gelooft dat deze vraag legitiem is, zal de betaling naar de rekening van de oplichter uitvoeren.



3 HOE HERKENNEN?

De kans is groot dat het om CEO fraude gaat wanneer er **ongewone transacties** gevraagd worden, met **ongebruikelijke redenen**, in **uitzonderlijke omstandigheden** en met zeer **hoge bedragen**.

Wees extra aandachtig

- als iemand om geheimhouding vraagt,
- als er aangedrongen wordt op urgentie,
- als de vraag via een onbekend e-mailadres of telefoonnummer gesteld wordt,
- bij ongewone druk om gevoelige informatie te geven of om een betaling te doen,
- bij overschrijvingen naar onbekende bankrekeningen,
- bij aanvragen op vrijdagavond of net voor een feestdag,
- bij wijzigen van de betalingsgegevens van een leverancier.

4 HOE VOORKOMEN?

CEO fraude heeft weinig kans op slagen als ondernemingen de juiste maatregelen nemen.

Management

- Zorg ervoor dat de betalingsprocessen duidelijk zijn en goed gevolgd worden.
- Zorg voor duidelijke procedures om betalingsoverdrachten of gevoelige informatieverzoeken te verifiëren, vooral deze via e-mail.
- Informeer medewerkers en zorg dat ze een goede training hebben zodat ze de oplichting snel herkennen en adequaat reageren.

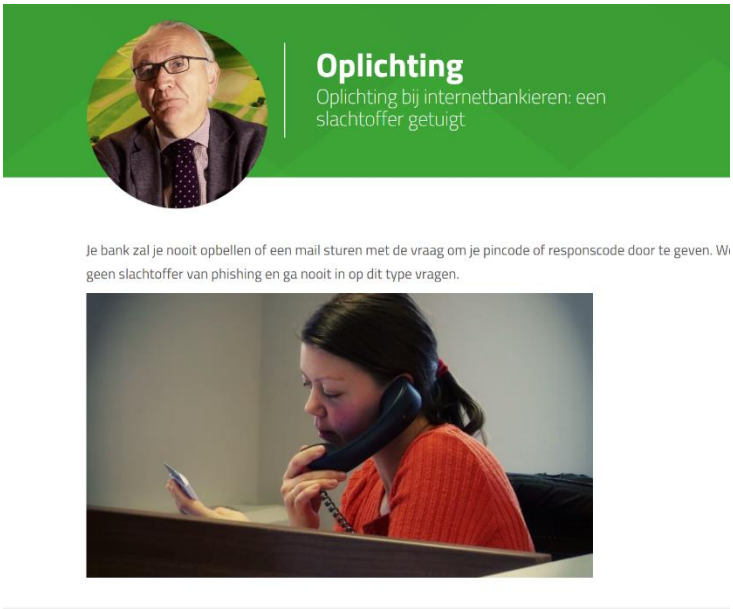
Medewerkers

- Klik nooit op een bijlage of een link in een e-mail die u niet volledig vertrouwt.
- Pas beveiligings- en betalingsregels strikt toe. Bijvoorbeeld: betalingen vanaf een bepaald bedrag door meerdere medewerkers laten ondertekenen.
- Beschrijf nooit aan onbekenden hoe betalingen in uw onderneming gebeuren. Hou deze procedures voor intern gebruik.
- Controleer of e-mailadressen correct zijn.
- Neem contact op met de aanvrager via een ander telefoonnummer of e-mail dan dat verstrekt is, om er zeker van te zijn dat dit de echte aanvrager is. Gebruik bv. *forward*, i.p.v. *reply*.

5 SLACHTOFFER VAN CEO FRAUDE?

- Waarschuw de verantwoordelijke van uw onderneming.
- Waarschuw de organisaties of personen van wie de identiteit gebruikt wordt, bv. als er een valse e-mail van een financiële instelling gebruikt werd, kunt u melden dat er valse e-mails in hun naam verstuurd worden.
- Als de overschrijving al uitgevoerd is, neem dan onmiddellijk contact op met uw bank om de betaling stop te zetten.
- CEO fraude is een strafbaar feit. U kunt dit aangeven bij de politie.

Getuigenis



6 MEER INFO

Safeonweb

Cybersecurity- Gids voor de KMO

Deze gids van het CCB voor KMO's geeft een uitvoerig overzicht over basis- en meer geavanceerde cyberveiligheidsmaatregelen.

Cyber Security KIT

De Cyber Security KIT werd ontwikkeld door de Cyber Security Coalition en het Centrum voor Cybersecurity Belgium voor KMO's en andere organisaties om het cybersecurity bewustzijn te helpen verhogen.

Volgende thema's komen aan bod:

- Hoe maak ik een sterk wachtwoord?
- Hoe herken ik phishing mails?
- Hoe sterk ik mij tegen social engineering?

Deze toolkit kan gratis gedownload worden in NL en FR op de website van de Cyber Security Coalition.

7 CONTACT

CERT.be
Federal Cyber Emergency Team
Wetstraat 16
1000 Brussel
info@certbe

Centrum voor Cybersecurity België
Wetstraat 16
1000 Brussel
info@ccb.belgium.be

Disclaimer

Verantwoordelijke uitgever

Centrum voor Cybersecurity België
M. De Bruycker, Directeur
Wetstraat, 16
1000 Brussel

Wettelijk depot

D/2017/14828/001