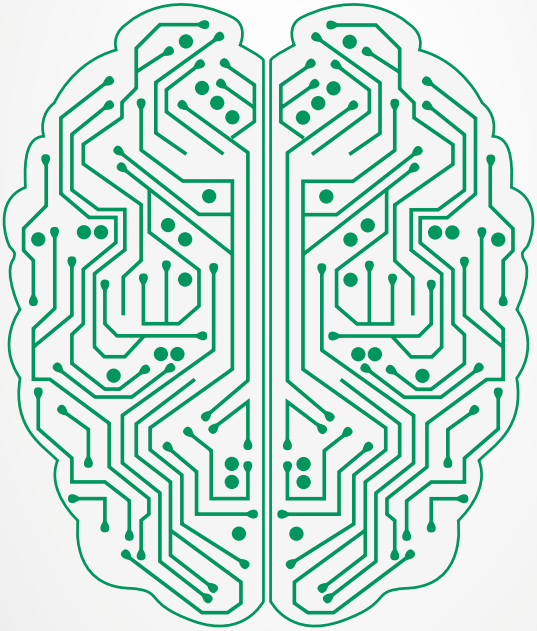
CEO-BETRUG

SCHÜTZEN SIE IHR UNTERNEHMEN UND SICH SELBST!



IHR GESPRÄCHSPARTNER IST VIELLEICHT NICHT DER, FÜR DEN ER SICH AUSGIBT

BGL
BNP PARIBAS

Die Bank für eine Welt im Wandel

Was ist „CEO-Betrug"?

Unter CEO-Betrug oder Social Engineering versteht man die Kunst, seinem Gesprächspartner auf **betrügerische Weise durch Manipulationstechniken nützliche Informationen zu entlocken**, um auf diese Weise **Geld zu entwenden**.

WAS UNTERNEHMEN BEFÜRCHTEN MÜSSEN

- Ausführung einer Überweisung auf das Konto von Betrügern
- Identitätsmissbrauch
- Datendiebstahl

„Ich vertrauen Ihnen." „Ich spreche mit Ihnen als Ihr Geschäftsführer." „Ich werde Ihnen nie vergessen, dass Sie mir geholfen haben." „Dies ist eine Anweisung!" „Enttäuschen Sie mich jetzt nicht..." „Es wird Ihnen honoriert." „Sprechen Sie mit niemandem darüber." „Dieses Projekt ist absolut vertraulich." „Diese Sache ist von äußerster Wichtigkeit." „Helfen Sie uns, die Betrüger zu überführen, indem Sie diese Überweisung ausführen!"

Wie die Betrüger vorgehen

1 BESCHAFFUNG VON INFORMATIONEN

Der Betrüger nimmt Kontakt mit dem Unternehmen auf und **beschafft sich Informationen** über die Organisation, ihre Projekte, ihre Verfahren und Schlüsselpersonen in der Finanzabteilung.

2 IDENTITÄTSMISSBRAUCH UND WAHL DES OPFERS

Der Betrüger gibt sich als **eine einflussreiche Person im Unternehmen (Geschäftsführer, Vorstandsmitglied)** oder Geschäftspartner aus und kontaktiert auf der Grundlage der gesammelten Informationen einen Mitarbeiter des Unternehmens, der zur Ausführung von Zahlungen berechtigt ist (Zielperson).

3 DRUCKAUSÜBUNG

Der Betrüger erteilt die Anweisung, **dringend die Zahlung** einer beträchtlichen Summe auf ein dem Opfer unbekanntes Konto, zumeist **im Ausland**, vorzunehmen. Möglicherweise verlangt er auch die **Änderung des IBAN-Kontos**, auf das die Zahlung einer Rechnung erfolgen soll.

4 MANIPULATION

Als guter Schauspieler und Manipulator setzt der Betrüger **autoritäres Verhalten** ein, **hebt die Kompetenz der Zielperson hervor** und betont die erforderliche Diskretion bzw. Geheimhaltung.

5 AUSFÜHRUNG DER ZAHLUNGSANWEISUNG

Die manipulierte Person steht stark unter Druck, erteilt der Bank aber **unter absoluter Geheimhaltung eine Zahlungsanweisung**. Der Betrüger fordert mit Nachdruck eine Ausführungsbestätigung.

6 NEUER VERSUCH

Schlägt der Betrugsversuch fehl, kann der Betrüger, der auf dieses Szenario vorbereitet ist, sich **als Ermittler der Kriminalpolizei ausgeben und verlangen, dass die Überweisung im Rahmen der Ermittlungen ausgeführt werden soll**. Damit ist er am Ziel.

Gut zu wissen

Das vorstehend beschriebene Vorgehen ist das gängigste Verfahren. Die Methoden, mit denen die Betrüger Ihnen Informationen und Geld entlocken wollen, sind allerdings zahlreich. Bleiben Sie wachsam!

85% der gesammelten Informationen über die Zielperson stammen aus **öffentlich zugänglichen Quellen** (Internet, Presse,...) oder ergeben sich durch Auskünfte des unmittelbaren Umfeldes.

Telefon und **E-Mails** sind die bevorzugten Kanäle der Betrüger, die wertvollen Informationen lassen sich jedoch auch **auf anderen Wegen beschaffen**.

20% der Betrugsversuche durch Social Engineering erfolgen über **manipulierte Internetseiten** und **gefälschte E-Mail-Adressen** von Personen und Behörden.

Um glaubwürdig zu wirken, zögern die Betrüger keinen Moment, eine Fülle an Informationen Preis zu geben, die sie auf betrügerische Weise erworben haben. Sie verschicken **sogar vermeintlich offizielle Bestätigungsmails von gefälschten E-Mail-Absenderadressen**.

Anfangs ging es bei dieser Betrugsmasche um recht hohe Summen. Da Unternehmen und Banken vorsichtiger geworden sind, versuchen die Betrüger es nun **mit niedrigeren Beträgen**, um nicht aufzufliegen.

Wie kann ich mich vor einem Angriff schützen?

- **Legen Sie Ihre Daten nicht offen** – weder an öffentlich zugänglichen Plätzen (z. B. im Zug), auf Internetseiten, in sozialen Netzwerken noch in Ihrem Unternehmen: Sichern Sie den Zugriff auf vertrauliche Dokumente, vergewissern Sie sich, dass Ihre digitalen Geschäftsdaten die Festplatten des Unternehmens nicht verlassen.
- Richten Sie **interne Verfahren** ein, die ein Vier-Augen-Prinzip ermöglichen und den Zugang zu sensiblen Daten einschränken.

- **Sensibilisieren Sie Ihre Mitarbeiter,** vor allem aus der Buchhaltung und der Finanzabteilung.
- **Klicken Sie in E-Mails** oder im Internet nicht **auf Links unbekannter Herkunft.**
- Sie kennen Ihren Gesprächspartner nicht? **Dann bitten Sie ihn um nähere Angaben** zu seiner Identität und seinem Unternehmen, fragen Sie ihn, woher er Ihre Kontaktdaten hat.

Was soll ich im Falle einer ungewöhnlichen Anfrage tun?

Betrüger geben nicht auf. Sie scheuen nicht davor zurück, verschiedene Personen anzurufen und mehrere Identitäten vorzutäuschen, um ihr Ziel zu erreichen.

- **Stellen Sie sich die richtigen Fragen** zu den Gründen für diesen Anruf.
- **Lassen Sie sich nicht unter Druck setzen** und behalten Sie gegenüber einem einschüchternden Gesprächspartner einen kühlen Kopf. Falls nötig, ziehen Sie einen Kollegen oder eine verantwortliche Person hinzu.
- **Vertrauen Sie auf Ihr Bauchgefühl:** Wenn Ihnen eine Anfrage verdächtig vorkommt, dann ist sie es wahrscheinlich auch!
- **Prüfen Sie die Legitimation des Anrufers** indem Sie ihn unter einer im Telefonverzeichnis erfassten Nummer zurückrufen.
- **Seien Sie vorsichtig,** wenn eine Anfrage mit Nachdruck, hoher Dringlichkeit bzw. Vertraulichkeit an Sie gerichtet wird und die internen Verfahren dabei nicht eingehalten werden.
- **Seien Sie misstrauisch** bei jeder ungewöhnlichen Überweisung, die Sie unterschreiben oder gegenzeichnen sollen, wenn diese in ein Land geht, in dem das Unternehmen geschäftlich nicht tätig ist.

Hat sich ein Betrugsfall bestätigt, informieren Sie **unverzüglich** Ihren Vorgesetzten und alarmieren Sie die Bank.

Die Bank verfügt über zahlreiche Maßnahmen, um derartige betrügerische Angriffe abzuwehren, aber Ihre Wachsamkeit ist für die Effizienz dieser Maßnahmen entscheidend.

Schärfen Sie das Bewusstsein Ihrer Mitarbeiter und bleiben Sie vor allem wachsam!

UNSERE ZWEIGSTELLEN IN LUXEMBURG-STADT

Bonnevoie
Cloche d'Or
Gare
Grand-Rue
Kirchberg Europe
Kirchberg Siège social
Limpertsberg
Merl-Belair
Merl-Jardins de Luxembourg
Royal Monterey

UNSERE ZWEIGSTELLEN IN LUXEMBURG

Bascharage Kordall
Bereldange
Bettembourg
Clervaux
Diekirch
Differdange
Dudelange
Echternach
Esch Belval
Esch Benelux
Esch Centre
Ettelbruck
Grevenmacher
Howald
Junglinster
Larochette
Mamer
Mersch
Mondorf-les-Bains
Niederanven
Pétange
Redange-sur-Attert
Remich
Schifflange
Steinfort
Strassen
Tétange Käldall
Vianden
Wasserbillig
Weiswampach
Wiltz

KONTAKTIEREN SIE UNS

(+352) 42 42-2000 **info@bgl.lu** **bgl.lu**

BGL BNP PARIBAS S.A.
50, avenue J.F. Kennedy – L-2951 Luxembourg
R.C.S. Luxembourg : B 6481

BGL BNP PARIBAS S.A. (50, avenue J.F. Kennedy, L-2951 Luxembourg. R.C.S. Luxembourg : B 6481) Marketingmitteilung Juli 2016

BGL BNP PARIBAS

Die Bank für eine Welt im Wandel