CEO/BUSINESS E-MAIL BETRUG (CEO-BETRUG)

CEO-Betrug tritt auf, wenn ein Mitarbeiter, der zur Ausführung von Zahlungen berechtigt ist, dazu verleitet wird, eine gefälschte Rechnung zu bezahlen oder eine nicht autorisierte Transaktion von einem Geschäftskonto vorzunehmen.

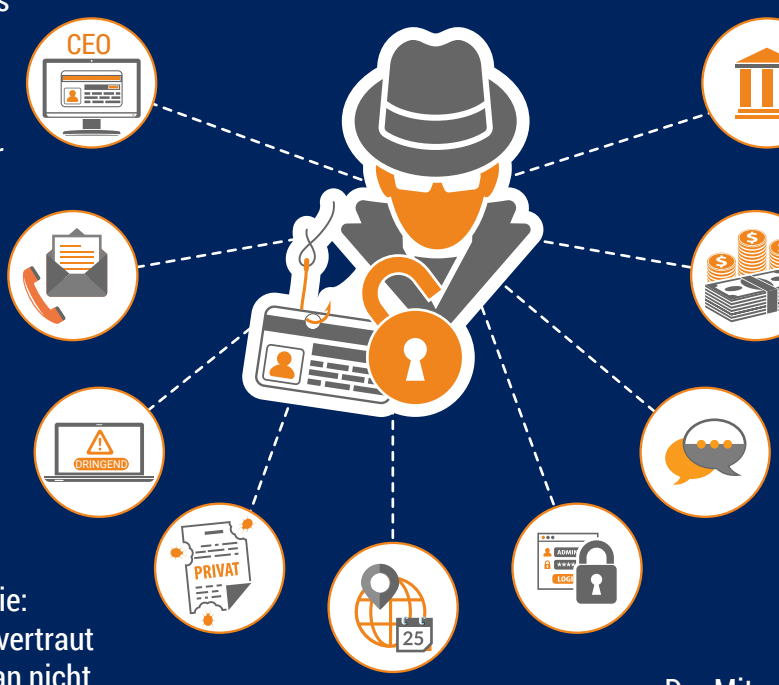
WIE FUNKTIONIERT ES?

Die Betrüger, die sich als hochrangige Personen des Unternehmens (z.B. CEO oder CFO) ausgeben, rufen an oder schreiben eine E-Mail.

Sie verfügen über gute Kenntnisse über die Organisation.

Sie verlangen eine dringende Zahlung.

Sie benutzen Begriffe wie: 'Vertraulich', 'Die Firma vertraut Ihnen', 'Ich bin momentan nicht verfügbar'.



Es handelt sich oftmals um internationale Zahlungen, die an Banken ausserhalb Europas gehen.

Der Mitarbeiter transferiert Geld auf ein Konto, das durch den Betrüger kontrolliert wird.

Instruktionen bezüglich das weitere Vorgehen werden später über eine Drittperson oder über E-Mail bekanntgegeben.

Der Mitarbeiter wird angehalten, den regulären Autorisierungsprozess zu umgehen.

Sie nehmen Bezug auf eine sensible Situation (z.B. Steuerprüfung, Fusion, Akquisition).

WAS SIND DIE ANZEICHEN?

- Ungewöhnliche(r) E-Mail/Telefonanruf
- Direkter Kontakt zu einer leitenden Person, mit der Sie normalerweise nicht in Kontakt stehen
- Bitte um absolute Vertraulichkeit
- Druck und ein Gefühl der Dringlichkeit
- Ungewöhnliche Anfrage in Widerspruch zu internen Verfahren.
- Drohungen oder ungewöhnliche Schmeicheleien/Belohnungsversprechen

WAS KÖNNEN SIE TUN?

ALS UNTERNEHMEN

Nehmen Sie die Risiken ernst und stellen Sie sicher, dass **die Mitarbeiter ebenfalls informiert und sensibilisiert sind.**

Bestärken Sie Ihre Mitarbeiter, **Zahlungsanfragen mit Vorsicht zu behandeln.**

Implementieren Sie interne Protokolle für Zahlungen.

Implementieren Sie ein Verfahren zur Überprüfung der Rechtmässigkeit von Zahlungsaufträgen, die per E-Mail eingehen.

Implementieren Sie **Meldeverfahren bei Verdacht** auf CEO-Betrug.

Überprüfen Sie die auf Ihrer Unternehmenswebseite veröffentlichten Informationen, **schränken Sie diese ein und zeigen Sie Vorsicht** in Bezug auf soziale Medien.

Führen Sie technische **Sicherheitsupdates und -upgrades durch.**

Kontaktieren Sie bei Betrugsversuchen immer die Polizei, auch wenn Sie kein Opfer des Betrugs wurden.

ALS MITARBEITER

Halten Sie sich strikt an die Sicherheitsverfahren für Zahlungen und Beschaffungen. **Überspringen Sie keine Schritte und geben Sie bei Druck nicht nach.**

Überprüfen Sie immer die E-Mail Adressen, wenn Sie sensible Daten oder Geldüberweisungen verarbeiten.

Bei Zweifeln an einer Zahlung, **fragen Sie den zuständigen Kollegen.**

Öffnen Sie nie verdächtige Links oder Anhänge, die Sie über E-Mail erhalten. Seien Sie besonders vorsichtig, wenn Sie Ihre privaten E-Mails auf dem Geschäftscomputer abrufen.

Beschränken Sie Informationen und sind vorsichtig in Bezug auf soziale Medien.

Vermeiden Sie es, Informationen über die Hierarchie, Sicherheit oder Verfahren der Firma zu teilen.

Wenn Sie eine verdächtige E-Mail oder einen verdächtigen Anruf erhalten, informieren Sie immer Ihre IT-Abteilung.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | .BK BUNDESKRIMINALAMT | WKO BANK · VERSICHERUNG

#CyberScams

ANLAGEBETRUG

Häufig beinhaltet Anlagebetrug lukrative Investitionsmöglichkeiten wie Aktien, Anleihen, Krypto-Währungen, seltene Metalle, Investitionen in Grundeigentum im Ausland oder alternative Energien.

WAS SIND DIE ANZEICHEN?

- Ihnen wird eine schnelle Rendite versprochen und versichert, dass die Investition sicher ist.
- Das Angebot ist nur für begrenzte Zeit verfügbar.
- Sie erhalten wiederholt unaufgeforderte Anrufe.
- Das Angebot steht nur Ihnen zur Verfügung und Sie werden gebeten, es nicht weiterzugeben.

WAS KÖNNEN SIE TUN?

- **Lassen Sie sich immer unabhängig beraten,** bevor Sie Geld übergeben oder eine Investition tätigen.
- **Lehnen Sie unangekündigte Anrufe** im Zusammenhang mit Investitionsmöglichkeiten ab.
- **Seien Sie misstrauisch** gegenüber Angeboten, die eine sichere Investition, garantierte Erträge und hohe Gewinne versprechen.
- **Vorsicht vor zukünftigen Betrugsversuchen.** Wenn Sie bereits Opfer sind, werden die Betrüger Sie wahrscheinlich wieder ins Visier nehmen oder Ihre Daten an andere Kriminelle verkaufen.
- **Kontaktieren Sie** bei Verdacht **die Polizei.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | .BK BUNDESKRIMINALAMT | WKO BANK · VERSICHERUNG | #CyberScams

RECHNUNGSBETRUG

WIE FUNKTIONIERT ES?

- Ein Unternehmen wird von jemandem kontaktiert, der vorgibt, einen Lieferanten/Dienstleister/Kreditgeber zu vertreten.
- Eine Kombination von Kontaktmöglichkeiten kann verwendet werden: Telefon, Brief, E-Mail, etc.
- Der Betrüger verlangt, dass die Bankverbindung (also die Bankverbindungsdetails des Zahlungsempfängers) für die Zahlung zukünftiger Rechnungen geändert wird. Das vorgeschlagene neue Konto wird vom Betrüger kontrolliert.

WAS KÖNNEN SIE TUN?

ALS UNTERNEHMEN

Stellen Sie sicher, dass die **Mitarbeiter über diese Art von Betrug informiert** sind und wissen, wie sie ihn vermeiden können.

Führen Sie einen **Prozess zur Überprüfung** der Rechtmässigkeit von Zahlungsaufträgen ein.

Instruieren Sie die verantwortlichen Mitarbeiter, dass Rechnungen vor der Bezahlung **immer auf Unregelmässigkeiten zu prüfen sind.**

Überprüfen Sie die auf Ihrer Unternehmenswebseite **veröffentlichten Informationen,** insbesondere Verträge und Lieferanten. Instruieren Sie Ihre Mitarbeiter, was sie über das Unternehmen in sozialen Medien teilen dürfen.

ALS MITARBEITER

Überprüfen Sie alle Anfragen, die angeblich von Ihren Gläubigern stammen, insbesondere wenn diese Sie bitten, ihre Bankverbindung für zukünftige Rechnungen zu ändern.

Verwenden Sie nicht die auf dem Brief/Fax/E-Mail angegebenen Kontaktdaten, mittels welchem die Änderung beantragt wird. Verwenden Sie stattdessen solche aus **vorheriger Korrespondenz.**

Bestimmen Sie **einheitliche Ansprechpartner** bei Unternehmen, an die Sie regelmässig Zahlungen leisten.

Beschränken Sie die Informationen, die Sie über Ihren Arbeitgeber in sozialen Medien teilen.

Für Zahlungen ab einem bestimmten Schwellenwert sollte **ein Verfahren zur Bestätigung** des richtigen Bankkontos und Empfängers (z.B. ein Treffen mit dem Unternehmen) **eingerichtet werden**.

Wenn eine Rechnung bezahlt wurde, **senden Sie dem Empfänger eine E-Mail zur Information.** Geben Sie den Namen der begünstigten Bank und die letzten vier Ziffern des angegebenen Kontos an, um die Sicherheit zu gewährleisten.

! Wenden Sie sich bei Betrugsversuchen immer an die Polizei, auch wenn Sie nicht Opfer des Betrugs geworden sind.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | .BK BUNDESKRIMINALAMT | WKO BANK · VERSICHERUNG

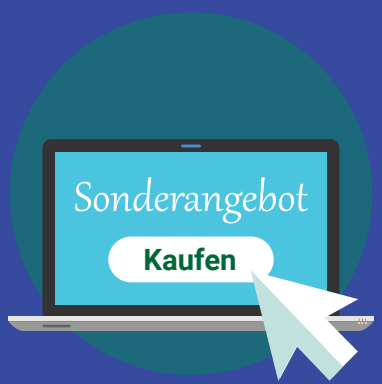
#CyberScams

ONLINE SHOPPING BETRUG

Online-Angebote sind oft lukrativ, aber Vorsicht vor Betrug ist geboten.

WAS KÖNNEN SIE TUN?

- **Verwenden Sie,** wenn möglich, **inländische Onlineshops -** allfällige Probleme lassen sich wahrscheinlich einfacher lösen.
- **Suchen & Recherchieren -** Überprüfen Sie die Bewertungen vor dem Kauf.
- **Verwenden Sie Kreditkarten -** Sie haben bessere Chancen, Ihr Geld zurückzubekommen.



- **Nutzen Sie für die Bezahlung nur einen sicheren Zahlungsdienst -** Wird nach einem Geldtransferservice oder einer Banküberweisung gefragt? Überlegen Sie es sich gut!
- Bezahlen Sie nur, wenn Sie mit einer **sicheren Internetverbindung** verbunden sind - Vermeiden Sie die Verwendung von kostenlosem oder offenem WiFi.
- **Bezahlen Sie nur mit einem sicheren Gerät** - Halten Sie Ihr Betriebssystem und Ihre Sicherheitssoftware auf dem aktuellen Stand.
- Hüten Sie sich vor Anzeigen, die aussergewöhnliche Angebote oder Wunderprodukte anpreisen - **Wenn es zu gut klingt, um wahr zu sein, ist es das wahrscheinlich auch!**
- Popup-Anzeigen, in denen steht, dass Sie einen Preis gewonnen haben? **Überlegen Sie es sich gut,** wahrscheinlich gewinnen Sie nur Schadsoftware.
- Falls das Produkt nicht ankommt, wenden Sie sich an den Verkäufer. Wenn Sie keine Antwort erhalten, **wenden Sie sich an Ihren Zahlungsdienstleister**.

Melden Sie jeden vermuteten Betrugsversuch der Polizei, auch wenn Sie nicht Opfer des Betrugs geworden sind.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | .BK BUNDESKRIMINALAMT | WKO BANK · VERSICHERUNG | #CyberScams

BANK PHISHING E-MAILS

Phishing bezeichnet betrügerische E-Mails, die die Empfänger dazu verleiten, persönliche, finanzielle oder sicherheitsrelevante Informationen preiszugeben.

WIE FUNKTIONIERT ES?

Diese E-Mails:

können identisch aussehen wie die Korrespondenz Ihrer aktuellen Bank.

kopieren Logos, Layout und Tonfall echter E-Mails.

verlangen das Öffnen eines Anhangs oder das Klicken auf einen Link.

vermitteln das Gefühl von Dringlichkeit.

WAS KÖNNEN SIE TUN?

- **Halten Sie Ihre Software auf dem neusten Stand,** inklusive Browser, Antivirusprogramm und Betriebssystem.
- Seien Sie speziell **wachsam**, wenn eine 'Bank' sensitive Informationen von Ihnen verlangt (z.B. Ihr E-Banking Passwort).
- **Schauen Sie die E-Mail genau an:** Vergleichen Sie die Adresse mit früheren echten Nachrichten Ihrer Bank. Achten Sie auf Schreibfehler und Grammatik.
- **Beantworten Sie verdächtige E-Mails nicht,** leiten Sie diese vielmehr unter manueller Eingabe der Adresse an die Bank weiter.
- **Klicken Sie nicht auf den Link oder öffnen Sie den Anhang nicht,** geben Sie die Adresse manuell im Browser ein.
- Im Zweifelsfall **schauen** Sie auf der Webseite Ihrer Bank nach oder rufen Sie Ihre Bank an.

Cyberkriminelle bauen darauf, dass die Menschen vielbeschäftigt sind; oberflächlich sehen diese gefälschten E-Mails echt aus.

#CyberScams

Aufgepasst bei mobilen Geräten! Es kann schwieriger sein, einen Phishing-Versuch auf Ihrem Mobiltelefon oder Tablet zu erkennen.

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

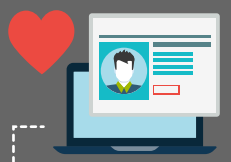
.BK BUNDESKRIMINALAMT

WKO BANK · VERSICHERUNG

ROMANTIK BETRUG

Betrüger nehmen ihre Opfer auf Online-Dating Webseiten ins Visier, nutzen aber auch soziale Medien oder E-Mail, um Kontakt aufzunehmen.

WAS SIND DIE ANZEICHEN?



Jemand, den Sie kürzlich online kennengelernt haben, täuscht starke Gefühle für Sie vor und bittet um private Chats.

Ihre Nachrichten sind oft schlecht geschrieben und vage.

Ihr Online-Profil stimmt nicht mit dem überein, was sie Ihnen sagen.

Möglicherweise bitten sie Sie, intime Bilder oder Videos von sich zu senden.

€€€

Zuerst gewinnen sie Ihr Vertrauen. Dann fragen sie Sie nach Geld, Geschenken oder Ihren Bank-/ Kreditkartendaten.

Wenn Sie das Geld nicht überweisen, versuchen sie Sie zu erpressen. Wenn Sie es überweisen, werden sie mehr verlangen.

SIND SIE EIN OPFER?

Schämen Sie sich nicht!
Stellen Sie sofort jeglichen Kontakt ein.
Behalten Sie wenn möglich sämtliche Kommunikation wie Chat-Nachrichten.
Erstatten Sie Anzeige bei der Polizei.
Melden Sie es der Webseite, auf der der Betrüger Sie erstmals kontaktiert hat.
Falls Sie Ihre Kontodaten angegeben haben, wenden Sie sich an Ihre Bank.

WAS KÖNNEN SIE TUN?

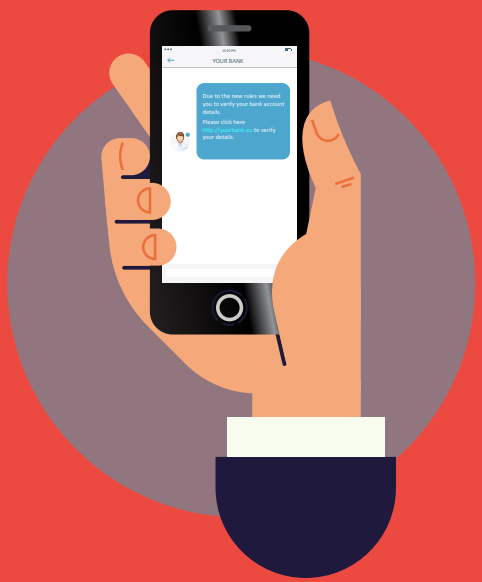
- **Seien Sie vorsichtig,** wie viele persönliche Daten Sie in sozialen Netzwerken oder auf Dating-Webseiten teilen.
- **Berücksichtigen Sie immer die Risiken.** Betrüger sind auf den renommiertesten Webseiten präsent.
- **Gehen Sie es langsam** an und stellen Sie Fragen.
- **Überprüfen** Sie Foto und Profil der Person, um zu sehen, ob das Material woanders verwendet wurde.
- **Achten Sie** auf Rechtschreib- und Grammatikfehler, Unstimmigkeiten in Geschichten sowie Ausreden, wie die Kamera funktioniere nicht.
- **Teilen Sie kein** kompromittierendes Material, mit dem Sie erpresst werden könnten.
- Wenn Sie sich persönlich treffen, **erzählen Sie Familie und Freunden,** wohin Sie gehen.
- **Hüten Sie sich vor Geldanfragen.** Senden Sie nie Geld oder geben Sie nie Kreditkarten-/Kontodaten oder Kopien von persönlichen Dokumenten weiter.
- Vermeiden Sie es, Vorauszahlungen zu tätigen.
- **Überweisen Sie kein Geld** für Andere: Geldwäscherei ist eine Straftat.

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | .BK BUNDESKRIMINALAMT | WKO BANK · VERSICHERUNG

#CyberScams

BANK PHISHING SMS

Smishing (eine Kombination der Wörter SMS und Phishing) ist der Versuch von Betrügern, persönliche, finanzielle oder sicherheitsrelevante Informationen mittels Textnachricht zu erlangen.



WIE FUNKTIONIERT ES?

Die Textnachricht wird Sie typischerweise auffordern, einen Link anzuklicken oder eine Telefonnummer anzurufen, um ihr Konto zu 'prüfen', 'aktualisieren' oder 'reaktivieren'. Aber...der Link führt zu einer gefälschten Webseite und die Telefonnummer zu einem Betrüger, der vorgibt das echte Unternehmen zu sein.

WAS KÖNNEN SIE TUN?

- **Klicken Sie nicht auf Links, Anhänge oder Bilder,** die Sie in unerbetenen Textnachrichten erhalten, ohne vorher den Absender zu überprüfen.
- **Keine Hast.** Nehmen Sie sich Zeit, die notwendigen Überprüfungen vorzunehmen, bevor Sie antworten.
- **Beantworten Sie nie Textnachrichten,** die die Eingabe Ihrer PIN, Ihres E-Banking Passwortes oder anderer Sicherheitsmerkmale verlangt.
- Wenn Sie vermuten, dass Sie einen Smishing-Text beantwortet und Ihre Bankdaten preisgegeben haben, **kontaktieren Sie sofort Ihre Bank.**

EUROPOL EC3 European Cybercrime Centre · EBF European Banking Federation · .BK BUNDESKRIMINALAMT · WKO BANK · VERSICHERUNG

#CyberScams

GEFÄLSCHTE BANK-WEBSEITEN

Bank Phishing E-Mails enthalten in der Regel Links, die Sie zu einer gefälschten Bank-Webseite führen, auf der Sie aufgefordert werden, Ihre finanziellen und persönlichen Daten einzugeben.

WAS SIND DIE ANZEICHEN?

Gefälschte Bank-Webseiten sehen nahezu identisch wie die Original-Webseiten aus. Solche Webseiten verfügen häufig über Popup-Fenster, die Sie auffordern, Ihre Bankdaten einzugeben. Echte Banken benutzen keine Popup-Fenster.

Diese Webseiten zeigen normalerweise Folgendes an:

Dringlichkeit: Sie werden keine solchen Nachrichten auf legitimen Webseiten finden.

Popup-Fenster: Sie werden häufig verwendet, um sensible Informationen von Ihnen zu sammeln. Klicken Sie nicht darauf und vermeiden Sie es, persönliche Daten über solche Fenster zu übermitteln.

Schlechtes Design: Seien Sie vorsichtig mit Webseiten, die Fehler in Design oder Rechtschreibung und Grammatik enthalten.

WAS KÖNNEN SIE TUN?

Klicken Sie nie auf Links, die in E-Mails enthalten sind und zur Webseite Ihrer Bank führen.

Geben Sie Links immer manuell ein oder verwenden Sie einen vorhandenen Link aus Ihrer Favoritenliste.

Verwenden Sie einen Browser, mit dem Sie **Popup-Fenster blockieren können.**

Wenn Sie etwas Wichtiges beachten müssen, werden Sie von Ihrer Bank darüber informiert, **wenn Sie auf Ihren Online-Account zugreifen.**

EUROPOL EC3 European Cybercrime Centre | EBF European Banking Federation | .BK BUNDESKRIMINALAMT | WKO BANK · VERSICHERUNG

#CyberScams

BANK VISHING ANRUFE

Vishing (eine Kombination der Wörter Voice und Phishing) ist Telefonbetrug. Die Betrüger verleiten ihre Opfer dazu, persönliche, finanzielle oder Sicherheitsinformationen bekanntzugeben oder Geld an sie zu überweisen.

WAS KÖNNEN SIE TUN?

- **Vorsicht** bei unbekannten Anrufern.
- **Verlangen Sie die Nummer des Anrufers** und sagen Sie, dass Sie zurückrufen.
- Um die Identität zu prüfen, **schlagen Sie die Telefonnummer der Organisation** nach und kontaktieren Sie diese direkt.
- **Verwenden Sie zur Überprüfung nicht die Ihnen mitgeteilte Telefonnummer** (diese könnte gefälscht sein).
- Betrüger finden persönliche Basisinformationen online (z.B. auf sozialen Medien). **Trauen Sie einem Anrufer nicht,** nur weil er solche Details kennt.
- **Geben Sie** die PIN Ihrer Kredit- oder Debitkarte oder Ihr E-Banking Passwort nicht bekannt. Ihre Bank wird nie nach diesen Details fragen.
- **Überweisen Sie kein Geld** auf deren Aufforderung auf ein anderes Konto. Ihre Bank wird das nie verlangen.
- Bei Verdacht auf einen betrügerischen Anruf, **melden Sie dies Ihrer Bank.**

EUROPOL EC3 European Cybercrime Centre

EBF European Banking Federation

.BK BUNDESKRIMINALAMT

WKO BANK · VERSICHERUNG

#CyberScams