# 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.

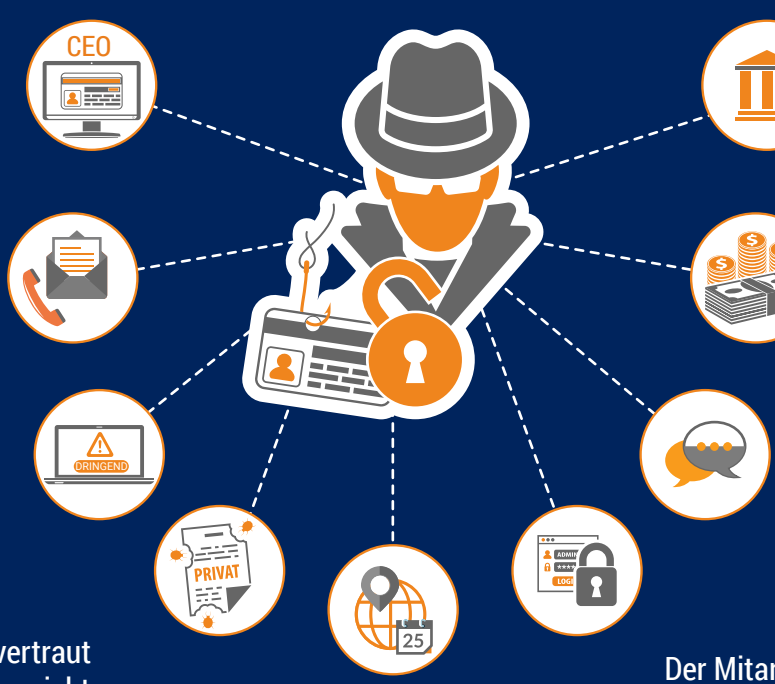
## WIE FUNKTIONIERT ES?

Ein Betrüger, der sich als hochrangige Person des Unternehmens (z.B. CEO oder CFO) ausgibt, ruft an oder schreibt eine E-Mail.

Er verfügt über gute Kenntnisse über die Organisation.

Er verlangt eine dringende Zahlung.

Er benutzt Begriffe wie: 'vertraulich', 'Die Firma vertraut Ihnen', 'ich bin momentan nicht verfügbar'.




Er nimmt Bezug auf eine sensible Situation (z.B. Steuerprüfung, Fusion, Akquisition).

Oftmals handelt es sich um internationale Zahlungen, die an Banken ausserhalb Europas gehen.

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

Instruktionen bezüglich des weiteren Vorgehens werden später über eine dritte Person oder über E-Mail bekanntgegeben.

Der Mitarbeiter wird angehalten, den regulären Autorisierungsprozess zu umgehen.

## WAS SIND DIE ANZEICHEN?

- Unaufgeforderte(r) E-Mail/Telefonanruf
- Direkter Kontakt zu einer hochrangigen Person, mit der Sie normalerweise nicht in Kontakt stehen
- Bitte um absolute Vertraulichkeit
- Druck und ein Gefühl der Dringlichkeit
- Ungewöhnliche Anfrage im 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.**

Ermutigen 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** für die Behandlung von CEO-Betrug.

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

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 mit sensiblen Daten oder Geldüberweisungen betraut sind.

Bei Zweifeln an einer Zahlung, **fragen Sie einen kompetenten Kollegen.**

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

**Beschränken Sie Informationen und gehen Sie vorsichtig** mit sozialen Medien um.

**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 | Bundeskriminalamt | bankenverband | #CyberScams