

Sicher. Ihre Landespolizei



Schütze dich vor Cybercrime Die Maschen der Betrüger



SCHOCKANRUF



Unbekannte Nummer
+423 2713456

„Ihr Sohn hatte
einen schweren Unfall!
Zahlen Sie jetzt,
sonst wird er bestraft!“



Handeln Sie
sofort!

Was ist
wirklich
passiert?



Vorgehen der Betrüger?

- Betrüger täuschen völlig unerwartet eine Notsituation vor und erzeugen damit einen Schock.
- Betrüger verlangen persönliche Daten und Geld.
- Druck oder Angst, damit Sie schnell handeln.

Was soll ich tun?

- Misstrauisch sein bei unerwarteten Anrufen!
- Bei Zweifel: auflegen und keine Daten preisgeben
- Umgehend mit Bank Kontakt aufnehmen und Rückforderung von allfälligen Zahlungen einleiten.
- Sich jemandem anvertrauen / Anzeige erstatten

FALSCHER POLIZIST



Anruf

Polizei

+423 2345678

„Ihre Daten wurden missbraucht!
Wir müssen Ihr Geld
und Ihre Wertsachen
in Sicherheit bringen.“



Ablehnen



Annehmen



**Vertraulich!
Auflegen verboten!**

Klingt
ernst...
aber stimmt
das?



Vorgehen der Betrüger?

- Betrüger täuschen völlig unerwartet eine glaubwürdige Notsituation vor.
- Geld oder Schmuck soll in Sicherheit gebracht werden, meist Abholung durch Betrüger.
- Druck oder Angst, damit Sie schnell handeln.

Was soll ich tun?

- Misstrauisch sein bei unerwarteten Anrufen.
- Bei Zweifel: auflegen und echte Polizei kontaktieren
- Keine persönlichen Daten oder Codes weitergeben!
- Sich jemandem anvertrauen / Anzeige erstatten

BETRÜGERISCHER TECHNISCHER SUPPORT



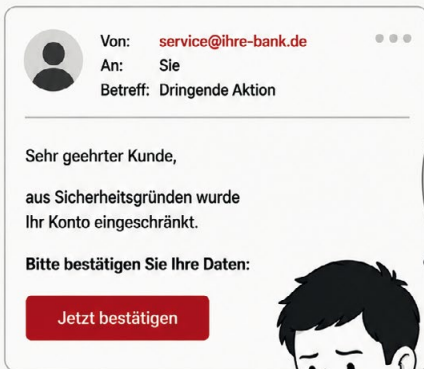
Vorgehen der Betrüger?

- Plötzliche Sicherheitswarnung mit Aufforderung, angegebene Support-Nummer anzurufen.
- Ziel ist die Fernsteuerung Ihres Computers.
- Betrüger versuchen, Zahlungen zu erfassen und unter Vorwand durch Sie freigeben zu lassen.

Was soll ich tun?

- Misstrauisch sein! Bei Zweifel: auflegen!
- Keine Fernsteuerungen auf Computer zulassen!
- Passwörter ändern
- Sich jemandem anvertrauen / Anzeige erstatten

PHISHING



Vorgehen der Betrüger?

- Betrüger verleiten Opfer zur Eingabe von vertraulichen Daten, z.B. Passwort.
- Von Interesse sind E-Mail-Konten, E-Banking-Zugänge oder Kreditkarteninformationen

Was soll ich tun?

- Misstrauisch sein, wenn Passwort verlangt wird!
- Keine Links aus E-Mails anklicken! Stattdessen Adresse direkt im Browser eintippen.
- Unterschiedliche Passwörter für unterschiedliche Internet-Dienste, regelmässig ändern.

CEO-FRAUD



Von: John Doe (Geschäftsführer)
An: Sie
Betreff: Dringend – vertrauliche Zahlung



Hallo,

ich bin gerade in einer Besprechung und habe nur kurz Zeit.

**Bitte veranlassen Sie umgehend eine Zahlung
in Höhe von 28.500,00 € auf folgendes Konto:**

Empfänger: Strategic Consulting GmbH
IBAN: DE45 7002 0270 0033 1234 56
Verwendungszweck: Projekt Phoenix

Die Zahlung ist eilig und vertraulich.

Keine Rückfragen.

Danke!

John Doe



Vorgehen der Betrüger?

- Wichtiger Auftrag des Firmen-Chefs.
- Dringende und geheime Anweisung, eine grosse Zahlung auszuführen.
- Firmen-Chef sei ausser Haus oder an einer Sitzung, Rückfragen seien nur per E-Mail möglich.

Was soll ich tun?

- Skeptisch sein bei unerwarteten Zahlungsaufträgen
- Nicht per E-Mail, sondern persönlich oder telefonisch bei echtem Firmen-Chef nachfragen.
- Sich jemandem anvertrauen / Anzeige erstatten

BEC | BUSINESS E-MAIL COMPROMISE

E-Mail gefälscht.
Kontodaten manipuliert.
Geld weg.



Von: rechnung@lieferant-gmbh.com
An: buchhaltung@ihrefirma.ch
Betreff: Zahlungsinformationen aktualisiert



Guten Tag,
aufgrund einer Änderung unserer Bankverbindung
bitten wir Sie, zukünftige Zahlungen auf
folgendes Konto zu überweisen:

IBAN: CH48 3000 5234 1234 5678 9

BIC: BCOLCH2LXXX

Kontoinhaber: Lieferant GmbH

Vielen Dank.
Ihr Lieferant GmbH



Vorgehen der Betrüger?

- Anweisung einer vermeintlichen Partner-Firma.
- Scheinbar habe sich die Konto-Nummer geändert, Rechnung lautend auf ein neues Konto.
- Oft weit zurückliegendes Ereignis, auf das sich die Rechnung bezieht.

Was soll ich tun?

- Skeptisch sein bei unerwarteten Kontoänderungen oder Rechnungen zu weit zurückliegenden Anlässen
- Umgehend mit Bank Kontakt aufnehmen.
- Sich jemandem anvertrauen / Anzeige erstatten

BETRUG MIT VERKAUFSANZEIGEN



Vorgehen der Betrüger?

- Gefälschte Webseiten
- Scheinware: Vorauszahlung ohne Lieferung
- Scheinkäufer: Anfrage der Kreditkarten-Daten, um Gutschrift zu tätigen, stattdessen Abbuchung

Was soll ich tun?

- Nur auf vertrauenswürdigen Plattformen kaufen! Referenzen und Betrugswarnungen lesen.
- Umgehend mit Bank Kontakt aufnehmen und Rückforderung der Zahlung einleiten.
- Sich jemandem anvertrauen / Anzeige erstatten

ROMANCE SCAM



Vorgehen der Betrüger?

- Gefälschtes Profil von irgendwo auf der Welt
- Regelmässiger Kontakt über längeren Zeitraum mit viel Schmeicheleien. Besuch ist das Ziel.
- Kurz vor Besuch: Notsituation, Geld wird verlangt.

Was soll ich tun?

- Kontakt zu einer Internet-Bekannntschaft abbrechen, wenn Geld oder Güter verlangt werden!
- Keine Pakete oder Zahlungen annehmen
- Umgehend mit Bank Kontakt aufnehmen
- Sich jemandem anvertrauen / Anzeige erstatten

ONLINE-ANLAGEBETRUG



Vorgehen der Betrüger?

- Werbeanzeigen im Internet mit gefälschten Videos von prominenten Personen
- Hohe Gewinnversprechen, häufig vorgetäuschte Anlagen in Kryptowährungen
- Gehandelt wird nie und das Geld ist verloren.

Was soll ich tun?

- Vorsicht bei hohen Gewinnversprechen
- Skeptisch sein bei Anfragen unbekannter Personen
- Umgehend mit Bank Kontakt aufnehmen
- Sich jemandem anvertrauen / Anzeige erstatten

MONEY & PACKAGE MULES



Vorgehen der Betrüger?

- Geld über eigenes Konto empfangen und in anderer Form weiterleiten
- Pakete empfangen, unpacken und weiterschicken.
- Provision darf direkt behalten werden.

Was soll ich tun?

- Misstrauisch sein bei «Geld ohne Aufwand»
- Bankkonten nie Dritten zur Verfügung stellen
- Keine Gelder oder Pakete weiterleiten
- Kontakt zu Betrügern abbrechen.
- Sich jemandem anvertrauen / Anzeige erstatten

CYBERMOBBING



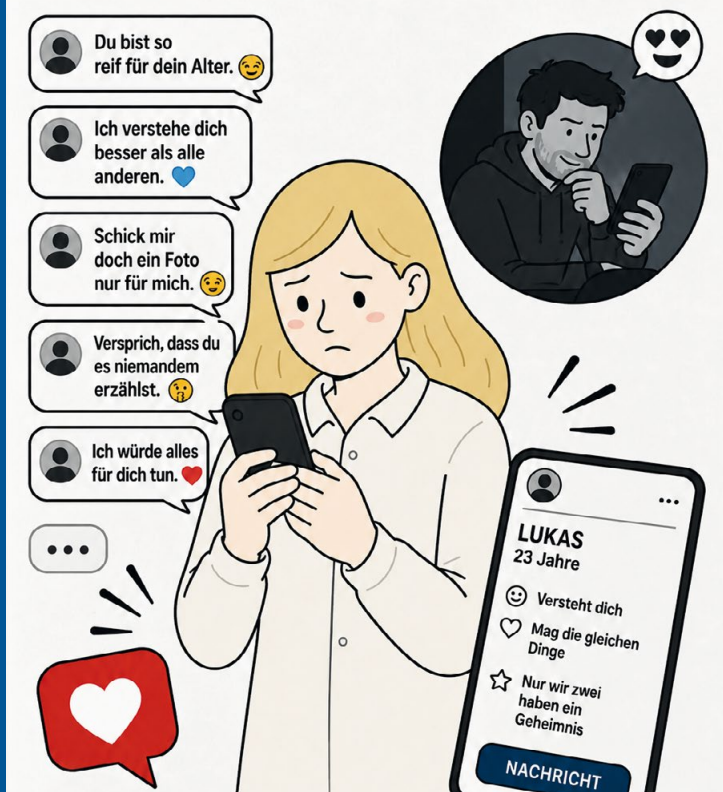
Vorgehen der Betrüger?

- Erstellen von beleidigenden Fake-Profilen
- Verbreitung falscher Informationen / Gerüchten
- Verbreitung von peinlichen, verfälschten, freizügigen oder pornographischen Medien

Was soll ich tun?

- Nicht reagieren, Täter blockieren.
- Privatsphäre schützen, Datenschutzeinstellungen auf Mobiltelefon oder PC überprüfen.
- Thema Cybermobbing ansprechen
- Sich jemandem anvertrauen / Anzeige erstatten

GROOMING



Vorgehen der Betrüger?

- Gezielte Kontaktaufnahme von Erwachsenen mit Minderjährigen in Sozialen Medien
- Erlangung von Vertrauen mit Schmeicheleien, Geschenken, Aufmerksamkeit, etc.
- Missbrauchsabsicht

Was soll ich tun?

- Nicht reagieren, Täter blockieren.
- Privatsphäre schützen, Datenschutzeinstellungen auf Mobiltelefon oder PC überprüfen.
- Sich jemandem anvertrauen / Anzeige erstatten

SEXTORTION



Ich habe deine Bilder.
Wenn du nicht zahlst,
schicke ich sie an alle!



Zahlen Sie jetzt,
sonst geht alles
viral!



Zahlung nur in
Bitcoin!



Was soll ich
jetzt tun?



Vorgehen der Betrüger?

- Anfragen von unbekannten attraktiven Personen.
- Verleitung zu Videochat und zu Handlungen
- Erpressung mit Bildmaterial

Was soll ich tun?

- Keine Kontakte mit Personen, die man nicht aus dem realen Leben kennt
- Sich bewusst machen, dass Aufzeichnung eines Videochats möglich ist
- Nicht auf Forderungen der Betrüger eingehen
- Sich jemandem anvertrauen / Anzeige erstatten

RANSOMWARE



Vorgehen der Betrüger?

- Begriff kommt von Ransom (Lösegeld) und Software
- Angriffsziele sind meist Unternehmen. Betrüger suchen eine Zugangsmöglichkeit.
- Mehrstufig: Daten stehlen, dann verschlüsseln

Was soll ich tun?

- Alle Zugänge zum Unternehmen schützen!
- Updates, Backup, etc.
- Kein Lösegeld bezahlen, keine kriminellen Netzwerke unterstützen!
- IT-Dienstleister kontaktieren / Anzeige erstatten

**Landespolizei des
Fürstentums Liechtenstein**

Gewerbeweg 4

LI-9490 Vaduz

T +423 236 71 11

info@landespolizei.li

www.landesspolizei.li