Kantonspolizei Freiburg
Kriminalpolizei
Finanzbrigade
Postfach 160
1763 Granges-Paccot

bfi@fr.ch
Telefon 026 304 17 19
www.polizeifr.ch

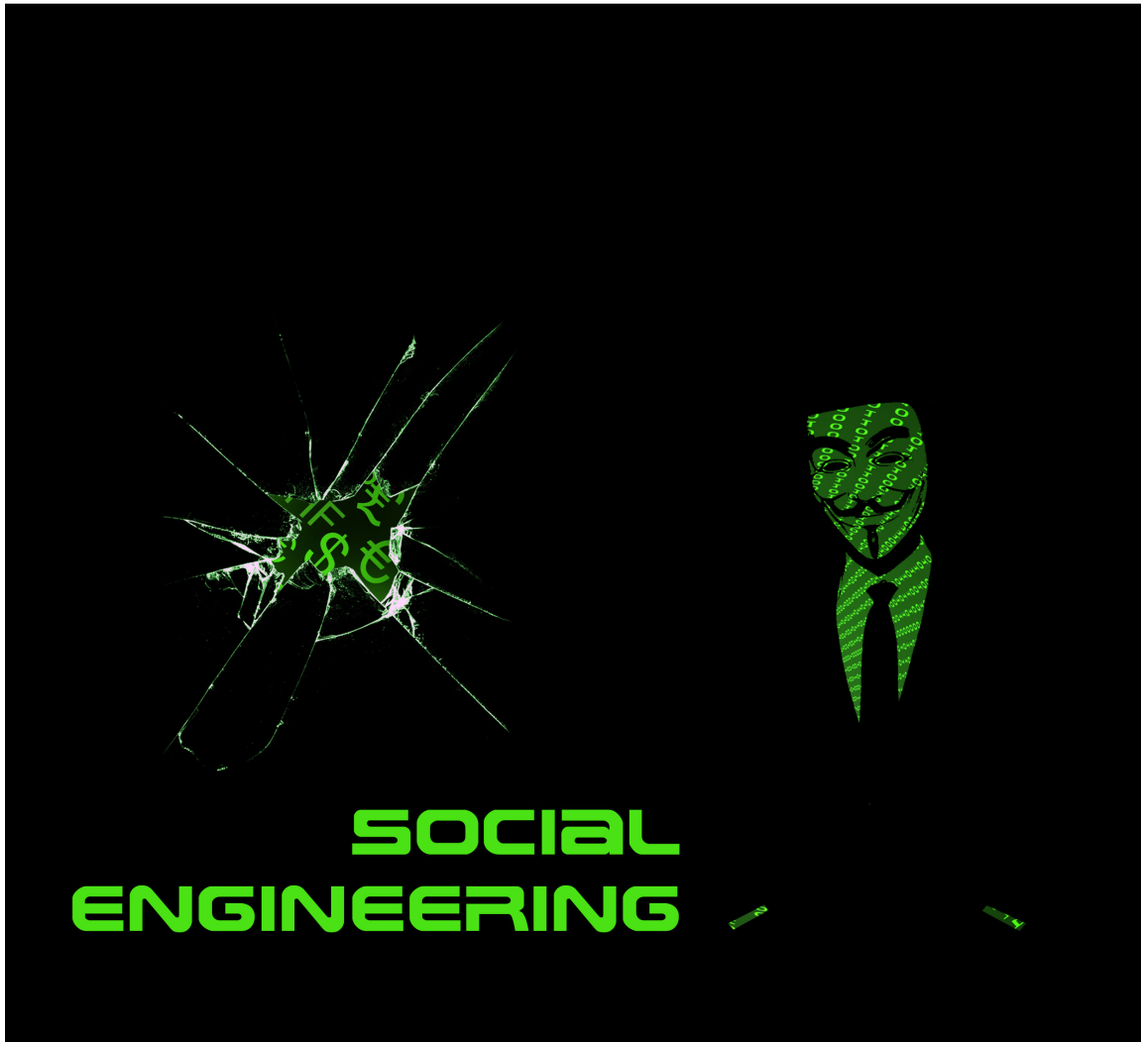
Quelle : Kantonspolizei Bern

ETAT DE FRIBOURG
STAAT FREIBURG

Police cantonale POL
Kantonspolizei POL

POLICE

Beabsichtigter CEO-Betrug verlangt hohe Aufmerksamkeit



SOCIAL ENGINEERING

Definition

Der Begriff Social Engineering, auch als „soziale Manipulation" bezeichnet, meint das Instrumentalisieren von Personen, um u.a. Sicherheitsdispositive zu umgehen. Man hofft damit, Menschen dazu zu bringen, Geldüberweisungen zu tätigen, Geheimnisse zu verraten oder vertrauliche Informationen preiszugeben.

Social Engineering basiert auf Überzeugungskraft und Ausnutzung der Gutgläubigkeit. Die in böser Absicht handelnde Person gibt sich als hierarchisch höher positionierte Person (Direktor, Verwaltungsratsmitglied, usw.) oder bspw. als Anwalt/Notar, Mitarbeiter einer Versicherung, einer Hausverwaltung oder eines Geschäftskunden aus.

Vorgehensweise der Betrüger

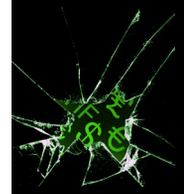
- **Eine erste Annäherungsphase:** per E-Mail oder Telefon, um das Vertrauen der Person zu gewinnen.
- **Unter Druck setzen:** um ein schnelles, unübliches, von Gewohnheiten abweichendes Handeln zu verlangen (unter dem Vorwand der Sicherheit, der Diskretion, dem Vortäuschen einer Notsituation, eines Liquiditätsbedarfs, einer vermeintlich attraktiven Geschäftsmöglichkeit, einer Verlagerung der Buchhaltung, einer Änderung der Hausverwaltung usw.).
- **Mit Ablenkung:** ein Satz oder eine Situation, welcher/welche der im Fokus stehenden Person eine vermeintliche Sicherheit vermittelt, um zu verhindern, dass er sich auf die Drucksituation konzentriert (Lob, Komplimente, Versprechungen, Bestätigungen usw.).

Sonderform des Social Engineering ist das E-Mail Phishing / Hacking

Der Zugang zum E-Mail-Account wird durch Phishing oder Hacking erlangt. Einmal in den Account eingedrungen, werden E-Mails gelesen, kontrolliert und die Informationen zu Kontaktaufnahmen verwendet. Dabei wird die E-Mailadresse des gehackten Accounts missbräuchlich als Absender verwendet. Mit zusätzlichen, gefälschten Urkunden, Zahlungsaufträgen usw., wird die betrügerische Zahlung oder die Täuschung erwirkt.

Empfehlungen – keine schnellen, unbedachten Clicks!

- Jede Überweisung bedingt eine Rechtfertigung (Vertrag, Lebensversicherung usw.).
- Im Zweifelsfall persönlichen Kontakt suchen (Direktion, Versicherungsgesellschaft usw.).
- Nie unter Druck setzen lassen.
- Nicht gegen übliche firmeninterne Sicherheitsregeln verstossen und Vertraulichkeitsregeln verletzen (unter der falschen Annahme eines Notfalls).
- Sicherstellen der Prozessabläufe bei Geldtransaktionen (Hierarchie, Kompetenz, Rückfragen, Vier-Augenprinzip, Kollektivunterschrift).
- Nie den Knopf „Antworten" bei derartigen E-Mails benutzen, sondern konsequent eine neue E-Mail erfassen. Die elektronische Adresse des Täters ist eine „Fälschung", die optisch oft sehr nahe beim Original ist. Keine dubiosen Anhänge öffnen.
- Potentiell betroffene Mitarbeiter, insbesondere die Buchhaltung, informieren und sensibilisieren.
- Die Herkunft einer elektronischen Post im Zweifelsfall überprüfen.
- Mailverkehr nach Möglichkeit verschlüsselt oder über Zertifikate führen.



MELDEN SIE VERDÄCHTIGE VORKOMMNISSE UNVERZÜGLICH DER POLIZEI UNTER DER NUMMER 117!