Police cantonale Fribourg
Police de sûreté
Brigade financière
Case postale 160
1763 Granges-Paccot

bfi@fr.ch
Téléphone 026 304 17 19
www.policefr.ch

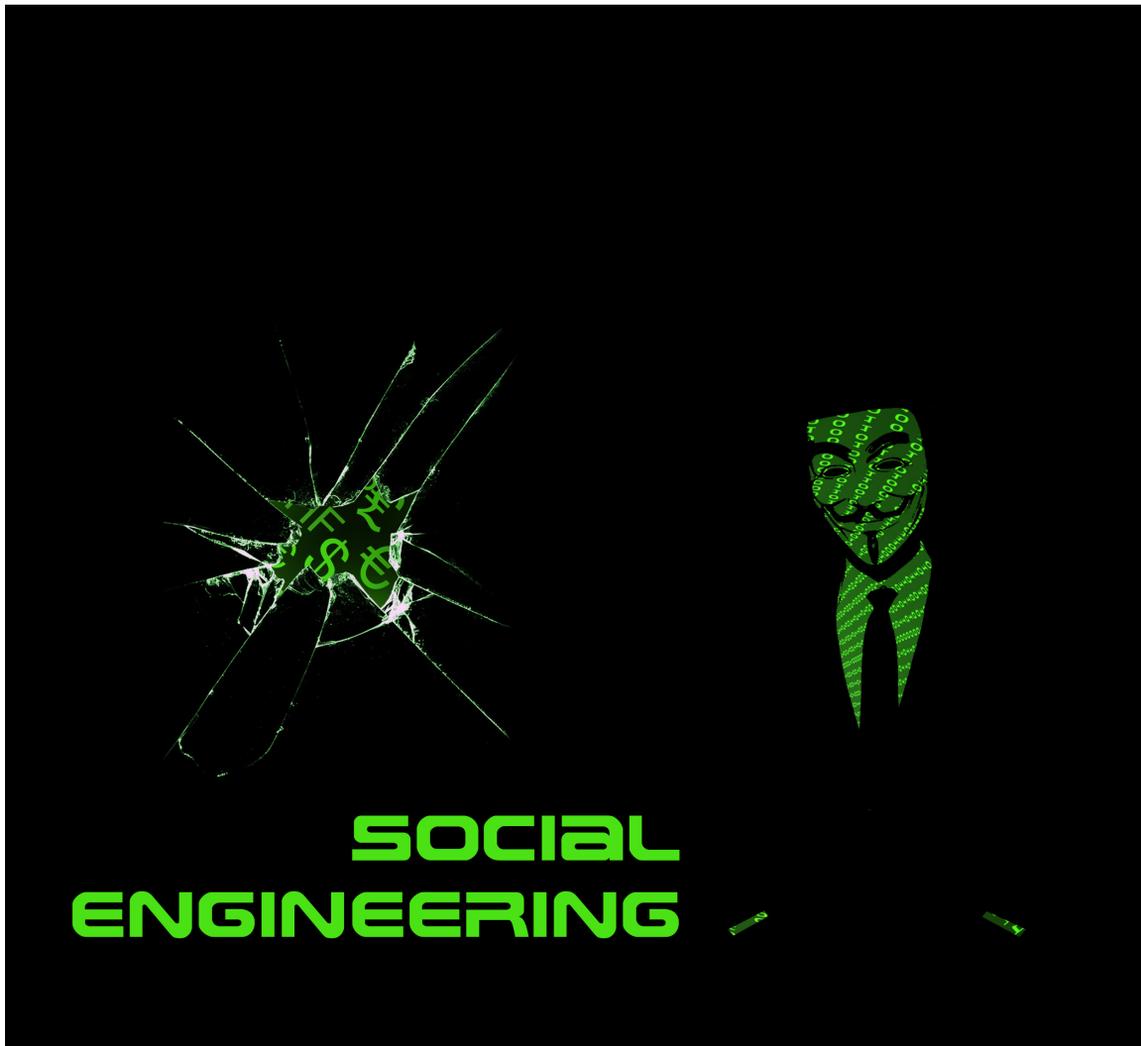
Source : Police cantonale bernoise

ETAT DE FRIBOURG
STAAT FREIBURG

Police cantonale POL
Kantonspolizei POL

POLICE

Arnaque au président (PDG)
Attention, vigilance accrue !



SOCIAL ENGINEERING

Définition

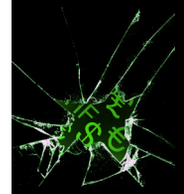
Le terme «social engineering», aussi appelé «ingénierie sociale», consiste à instrumentaliser des personnes afin de contourner les dispositifs de sécurité d'une entreprise. Le but est d'amener les personnes visées à effectuer des transferts d'argent, à trahir des secrets ou à divulguer des informations confidentielles.

Le social engineering se base sur la force de persuasion et se sert de la crédulité des victimes. Les malfrats se font passer pour un supérieur hiérarchique (ex : directeur, membre du conseil d'administration, etc.), un avocat/notaire, un agent d'assurance, un employé de régie ou un partenaire commercial.

Méthode des escrocs

Les procédés utilisés par ce type de délinquants respectent souvent les schémas suivants :

- **Une première phase d'approche :** par courriel ou par téléphone, afin de gagner la confiance de la victime.
- **Une mise sous pression :** par une demande de transaction unique, sortant de la procédure ordinaire, en prétextant un souci de discrétion, de sécurité, en feignant une situation d'urgence, un besoin de liquidités, en faisant croire à une opportunité d'affaires attractive, à un changement de fiduciaire ou de régie, etc.
- **Une diversion :** par une phrase ou une situation dont le but est de conforter la personne visée dans un sentiment d'apparente sécurité, afin que son attention soit attirée ailleurs (louanges, compliments, promesses, etc.).



Variante du social engineering : le «e-mail phishing / hacking»

L'auteur pirate la boîte e-mail (phishing ou hacking), recherche et collecte les informations utiles pour lui dans le carnet d'adresse et la correspondance. Ces dernières serviront à la prise de contact avec la future victime. L'auteur utilise notamment l'adresse e-mail piratée et se fait ainsi passer pour le réel expéditeur du courriel envoyé auprès du destinataire. Des documents falsifiés comme des ordres de virement, factures, etc. serviront de justificatifs pour déclencher les transactions délictueuses.

Recommandations – Pas de clic précipité et irréfléchi !

- Chaque transaction doit faire l'objet d'une justification écrite (contrat, assurance-vie, etc.).
- En cas de doute, chercher le contact personnel (direction, compagnie d'assurances, etc.).
- Ne jamais se laisser mettre sous pression.
- Ne jamais transgresser les règles de sécurité internes, ni violer les règles de confidentialité (sous prétexte d'une urgence).
- Respecter le processus interne en cas de transaction d'argent (hiérarchie, compétence, consultation, principe des «quatre yeux», signature collective).
- Ne jamais utiliser le bouton «répondre» à un courriel douteux, mais faire un nouveau courriel. L'adresse électronique de l'auteur est une «contrefaçon» qui est souvent quasi identique à l'originale. Ne jamais ouvrir les fichiers attachés douteux.
- Avertir et sensibiliser les victimes potentielles, comme le service-comptabilité par exemple.
- En cas de doute, vérifier l'origine d'un courrier électronique.
- Mettre en place, si possible, un trafic sécurisé ou certifié des courriels.

ANNONCEZ SANS TARDER LES CONSTATATIONS SUSPECTES À LA POLICE AU NUMERO 117 !