

L'ingénierie sociale (Social Engineering)

Pour soutirer des informations confidentielles, les arnaqueurs exploitent très souvent la bonne foi, la disponibilité, mais aussi l'insécurité des personnes. Faux appels, faux policiers, faux courriels... Quelque soit le subterfuge utilisé, les attaques d'ingénierie sociale ont toujours pour cible l'être humain. La meilleure protection reste donc une bonne dose de « bon sens ».

Pour vous protéger contre les attaques d'ingénierie sociale...

- révélez le moins d'informations personnelles possible. Sur les réseaux sociaux en particulier, il convient de faire preuve de la plus grande réserve.
- ne communiquez jamais vos mots de passe ou vos codes – tels que vos codes NIP de cartes ou vos données d'accès à Online Banking, à quiconque. Vos données d'accès ou codes NIP vous appartiennent, et ils n'appartiennent qu'à vous !
- restez méfiant lorsque vous êtes sollicité par courriel ou par téléphone – en particulier lorsque l'on exerce une pression sur vous. Ne vous fiez pas aveuglément à un nom d'expéditeur qui vous semble familier ou à un numéro apparemment connu car ils pourraient avoir été falsifiés !

Les attaques d'ingénierie sociale ont souvent pour objectif de vous soutirer des informations personnelles ou confidentielles (par ex. : codes d'accès, identifiants, mots de passe, etc.), et ce à des fins criminelles.

La première étape consiste à réunir le plus d'informations possible sur la victime. Car c'est grâce à ces informations que les escrocs parviendront ensuite à abuser de sa confiance. L'arnaqueur peut par exemple se faire passer auprès de vous pour une personne de votre cercle de connaissances.

Et dans cette chasse à l'information, Internet s'avère un outil idéal. Les [réseaux sociaux](https://www.ebas.ch/fr/les-reseaux-sociaux/) (https://www.ebas.ch/fr/les-reseaux-sociaux/) comme Facebook, LinkedIn, Instagram & Cie, sont de véritables mines d'informations. Une fois munis de toutes ces données, les escrocs peuvent entrer en contact avec leurs victimes et leur tenir un discours très crédible.

En règle générale, la seule façon de se protéger est de s'armer de bon sens dès lors que l'on a affaire à des inconnus, mais aussi à des personnes (apparemment) connues. Bien souvent, il convient également de réfléchir sur la nature des informations que l'on s'apprête à révéler, et sur la personne à laquelle elles sont destinées.

En cas de soupçon, mettez fin à la communication

Si l'on vous contacte de manière inattendue ou si quelque chose vous semble suspect de manière générale, ne divulguez pas d'autres informations et mettez fin à la communication. Si vous avez le moindre doute concernant vos opérations de banque en ligne, ne révélez rien et informez immédiatement votre institut financier. Vous trouverez [ici](https://www.ebas.ch/fr/partenaires/) (https://www.ebas.ch/fr/partenaires/) les coordonnées de votre banque.

Exemples d'attaques par Social Engineering

- Vous recevez un courriel dans lequel on vous demande de cliquer sur un lien pour vous identifier ou communiquer des informations personnelles vous concernant.
- Une personne vous appelle au téléphone dans le cadre d'un sondage et vous pose une série de questions concernant par exemple vos revenus, les mesures de sécurité que vous adoptez à l'ordinateur, etc.).
- Un escroc vous envoie un courriel en falsifiant le nom de l'expéditeur et se fait passer pour une personne connue (avec si possible un malware en pièce jointe).
- Vous recevez un e-mail de votre supérieure ou supérieur hiérarchique vous priant d'effectuer un paiement urgent.
- Un pseudo-informaticien se présente sur votre lieu de travail, soi-disant pour effectuer la maintenance de votre ordinateur.
- Une personne se fait passer pour un technicien (p. ex. d'une compagnie téléphonique, d'un fournisseur d'électricité, etc.) et tente ainsi d'accéder à votre ordinateur, votre maison ou votre entreprise.
- Les attaques d'ingénierie sociale peuvent aller très loin, au point que certaines personnes postulent pour des postes au sein d'une entreprise dans l'intention de voler plus tard certaines informations.

L'ingénierie sociale est une méthode par laquelle les pirates utilisent des astuces psychologiques ciblées pour manipuler les gens dans le but d'obtenir des informations sensibles ou de déclencher un comportement particulier. Pour ce faire, la confiance, la pression ou la tromperie sont sciemment utilisées. La manipulation passe souvent inaperçue et peut en principe toucher n'importe qui. Il est donc important de faire preuve de vigilance et de protéger ses données personnelles.



«Ça avait l'air tellement urgent que je n'ai pas réfléchi...»

Toutes les histoires qui commencent comme ça finissent mal.
Si vous recevez une demande inattendue ou qui vous semble suspecte, mettez fin à la communication.
Informez-vous et évitez les arnaques. www.ebas.ch

eBanking en toute sécurité!
by Hochschule Luzern