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 mots de passe ou codes TAN à quiconque, même à un administrateur système ou à un supérieur. Votre mot de passe vous appartient, et il n’appartient qu’à vous !
- restez méfiant lorsque vous êtes sollicité par courriel ou par téléphone. 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 n’ont qu’un seul et même objectif, celui 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/) comme Facebook, Xing, Instagram etc. 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.

Que faire concrètement pour se protéger ?

Il n’existe malheureusement pas de moyens techniques permettant de se protéger contre l’ingénierie sociale. Dans la mesure où les escrocs jouent sur la nature humaine, sur ses qualités et ses défauts, comme la disponibilité et serviabilité, la peur, la bonne foi, la naïveté etc., il est très difficile de reconnaître une attaque de Social Engineering et par conséquent de s’en défendre.

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. En situation, 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 doute, informez votre banque

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/) les coordonnées de votre banque.

Exemples d'attaques par Social Engineering

- Une personne essaye d'obtenir l'accès à votre habitation ou au sein de votre entreprise en se faisant passer pour un technicien (par ex. d'une compagnie téléphonique, d'une centrale électrique, etc.).
- 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).
- Un pseudo-informaticien se présente sur votre lieu de travail, soi-disant pour effectuer la maintenance de votre ordinateur.
- 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 ou Social Engineering est une méthode d'espionnage répandue visant à accéder à des données confidentielles. La cible de l'attaque est toujours la personne humaine et il n'existe aucun moyen technique de s'en prémunir. La seule façon de vous protéger est donc d'écouter votre bon sens.