«Social Engineering» Information et prévention

Comment reconnaître une attaque de social engineering?

- En se faisant passer pour un technicien (par ex. d'une compagnie téléphonique, d'une centrale électrique, etc.), une personne essaye d'accéder à votre habitation ou à votre entreprise.
- Vous recevez un courriel vous demandant de cliquer sur un lien hypertexte vous invitant à ouvrir une session en saisissant votre identifiant et votre mot de passe, ou à révéler des informations personnelles («phishing» ou hameçonnage).
- Une personne vous appelle au téléphone sous le prétexte d'un sondage pour vous soutirer des informations confidentielles (ex: revenus, mesures de sécurité, etc.).
- Un pseudo-informaticien arrive sur votre lieu de travail, soit disant pour effectuer des travaux de maintenance sur votre PC.

Toutes ces attaques n'ont qu'un seul et même objectif, celui de soutirer des informations personnelles ou confidentielles (par ex. codes d'accès, identifiants, mots de passe, etc.), et ce à des fins criminelles.

Pour vous protéger,

- révélez le moins d'informations personnelles possible. En particulier sur les réseaux sociaux, tels que Facebook, Xing etc., mieux vaut divulguer le moins de données possible.
- En règle générale, il convient de ne JAMAIS communiquer votre mot de passe à d'autres personnes. Pas même à un administrateur système, ni à votre supérieur. Votre mot de passe vous appartient, et il n'appartient qu'à vous!
- Soyez méfiant lorsque vous êtes sollicité par email. Même des courriels provenant d'expéditeurs connus (amis) peuvent être falsifiés.

Social Engineering

L'ingénierie sociale ou social engineering est une méthode d'espionnage répandue visant à obtenir l'accès à des données confidentielles. La cible de l'attaque est toujours la personne humaine. Pour soutirer des informations confidentielles, les arnaqueurs exploitent très souvent la bonne foi, la serviabilité, mais aussi l'insécurité des personnes. Que ce soit par téléphone, en se faisant passer pour quelqu'un d'autre, ou par Internet (attaques par hameçonnage), ils sont prêts à tout pour obtenir ce qu'ils veulent.

En règle générale, la seule façon de se protéger est de s'armer de bon sens. Il est généralement utile de réfléchir sur les informations que l'on est amené à révéler et sur les personnes auxquelles on a affaire.

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-en immédiatement votre institut financier. Vous trouverez les coordonnées sur http://www.ebankingentoutesecurite.ch.

Pour en savoir plus: www.ebas.ch/socialengineering

«eBanking – en toute sécurité!» informe les utilisateurs des services de banque en ligne sur les questions de sécurité

eBanking en toute sécurité!

Le site Web **www.ebankingentoutesecurite.ch** vous informe gratuitement sur les mesures nécessaires à mettre en œuvre et les règles de comportement à adopter pour une utilisation sécurisée des applications e-banking.

Hochschule Luzern – Informatik
Campus Zug-Rotkreuz, Suurstoffi 41b
CH-6343 Rotkreuz