**Cyberingénierie sociale**

**L’ingénierie sociale**, dans le contexte de la sécurité de l’information, consiste à manipuler psychologiquement des gens pour leur faire faire quelque chose ou leur faire divulguer des informations confidentielles. C’est le type d’escroquerie basé sur l’abus de confiance dans le but de recueillir des informations, frauder, accéder à un système ; il est différent d’une escroquerie traditionnelle en ce qu’il est souvent l’une des nombreuses étapes d’un système de fraude plus complexe.

Le terme d’« ingénierie sociale » en tant qu’acte de manipulation psychologique est également associé aux sciences sociales, mais sa pratique a pris de l’ampleur parmi les professionnels de l’informatique et de la sécurité de l’information.

Toutes les techniques d’ingénierie sociale sont basées sur des caractéristiques spécifiques de la prise de décision humaine connues sous le nom de biais cognitifs. Ces biais, parfois appelés « bugs dans le hardware humain » sont exploités sous différentes formes afin de créer des techniques d’attaque dont certaines sont citées ci-dessous. Les attaques utilisées dans l’ingénierie sociale peuvent servir à voler des informations confidentielles des employés. Le plus fréquemment, l’ingénierie sociale utilise le téléphone. Des malfaiteurs peuvent se faire passer pour des exterminateurs de nuisibles, des pompiers ou des techniciens pour voler les secrets d’une entreprise en toute discrétion.

Par exemple, un individu pénètre dans un bâtiment et affiche un communiqué semblant officiel sur le panneau d’affichage de l’entreprise informant du changement de numéro du service d’assistance. Ainsi, lorsque les employés appellent pour obtenir de l’aide, cet individu leur demande leurs mots de passe et identifiants, lui permettant d’accéder aux renseignements privés de l’entreprise.

Ou encore, le pirate informatique contacte la personne ciblée sur un réseau social et entame une conversation. Petit à petit, le pirate gagne la confiance de la cible et utilise cette confiance pour avoir accès à des informations sensibles comme un mot de passe ou des coordonnées bancaires.

*Source: https://en.wikipedia.org/wiki/Social\_engineering\_(security)*