



# INGENIERIE SOCIALE

**Ingénierie sociale:** Approche systémique et psychologique, souvent facilitée par une manœuvre dolosive, par laquelle une personne mal intentionnée recueille, à leur insu, des informations précises sur une entreprise ou un particulier.

*Croire qu'un pirate informatique élabore son attaque par la seule voie logicielle est erroné.*

*En effet, toute faille constitue pour le hacker un moyen d'atteindre son objectif. L'ingénierie sociale, dénommée également "faille humaine", en est une composante essentielle.*

*Récupérer des informations parfois sensibles est tellement facile ! Les réseaux sociaux servent en partie ces informations sur la place publique virtuelle. Il est aussi possible de se les procurer directement et plus simplement en téléphonant à la future victime !*

*Les escrocs, réalisant de tels actes, excellent dans cet art.*

## Explications – Précautions – Réactions

### **Explications :**

L'ingénierie sociale est un " art négatif " réalisé pour parvenir à des objectifs illégitimes, en contournant les différentes sécurités physique et informatique existantes. Il devient alors possible de « découvrir » des informations relevant du domaine du sensible. La finalité en est multiple : pénétrer un système ; détourner, voler ou détruire des informations ; escroquer financièrement une société ou une personne.

Les « prédateurs » font preuve de persuasion en exploitant la naïveté et le stress de leur « proie » ainsi que d'une parfaite maîtrise des techniques de manipulation qui met inévitablement la victime dans un état d'acceptation de la demande.

Les arnaques d'ingénierie sociale se réalisent souvent suivant le modus operandi ci-dessous :

- ➊ Mise en confiance du correspondant. Se faire passer pour un chef hiérarchique en est l'illustration la plus fréquente – technique utilisée dans les Faux Ordres De Virements Internationaux FOVI (fiche N°2).
- ➋ Déstabilisation de l'interlocuteur par une mise en alerte et une demande impérieuse.
- ➌ Rassurer le correspondant et le forcer à limiter sa focalisation sur l'alerte donnée précédemment.

Pour rappel, ces attaques se font par courrier, par courriel et par téléphone.

A titre d'exemple, récemment, un anonyme s'est fait passer pour un dépanneur en télémaintenance de Microsoft auprès d'une société en usant de l'ingénierie sociale. Cela lui a permis de prendre la main sur l'ordinateur de la personne contactée et d'y installer un scareware, faux logiciel de sécurité qui simule des alertes de sécurité. Il a créé ainsi un état d'anxiété chez l'utilisateur pour l'amener à « obéir » aux différentes mesures préconisées par le logiciel.

Enfin, le danger potentiel est également l'utilisation de cet ordinateur pour procéder à des attaques de déni de service ou pour installer rançongiciels et autres programmes malins.

**SI VOUS SOUHAITEZ VISUALISER LA TOTALITÉ DE  
CETTE FICHE DE SENSIBILISATION, CONTACTEZ MOI :  
[jmlathiere@intellie.fr](mailto:jmlathiere@intellie.fr)**