INFORSUD TECHNOLOGIES
Solutions et impulsions pour l'avenir

INGÉNIERIE SOCIALE
Une mécanique bien rodée !

INGÉNIERIE SOCIALE

Dans le contexte de la sécurité de l'information, l'ingénierie sociale regroupe un ensemble de techniques de manipulation à des fins d'escroquerie.

L'objectif est d'inciter les collaborateurs d'une organisation à communiquer des données confidentielles, en se faisant passer pour un tiers de confiance ; services publics, Ameli.fr, Crit'Air, banque, opérateur téléphonique, fournisseurs, etc.

Cette méthode peut se faire par email, SMS, téléphone, voire dans le cadre d'un échange par visioconférence ou une demande de mise à jour suspecte.

ÉTAPE 1
LA RECHERCHE DE LA CIBLE

ÉTAPE 2
LE PRÉTEXTE

ÉTAPE 3
L'EXTRACTION DE DONNÉES CONFIDENTIELLES

ÉTAPE 4
LA CLÔTURE

EXEMPLES COURANTS DE MANIPULATION

	Fraude au faux fournisseur	Fraude au président/PDG
Cible	Service administratif ou technique par email ou par téléphone	
Identité usurpée	Se fait passer pour un fournisseur de confiance, connu et habituel	Se fait passer pour le dirigeant de l'entreprise
Technique d'identification	L'attaquant a déjà collecté plusieurs informations de sources publiques : réseaux sociaux, site web, revue de presse … Usurpation d'identité	
Mode opératoire	• Demande d'effectuer le paiement des prochaines factures sur un nouveau RIB. • Demande de cliquer sur un lien malveillant pour réaliser une opération de maintenance.	Demande de réaliser un virement bancaire urgent et confidentiel
Moyen de pression	• Caractère urgent du paiement de la facture. • Crainte du collaborateur d'avoir des soucis techniques.	Relations hiérarchiques, intimidation

INFORSUD TECHNOLOGIES
Solutions et impulsions pour l'avenir

INGÉNIERIE SOCIALE
Les bons réflexes à adopter !

Ne vous fiez pas systématiquement au nom indiqué, vérifiez l'identité de l'interlocuteur.

À réception d'un email ou d'un SMS et avant de cliquer, soyez toujours vigilant.e aux liens et pièces jointes.

En cas de redirection vers un site, vérifiez la présence du S dans le https// et chaque lettre de l'URL.

Être particulièrement vigilant.e sur les périodes de congés, veille de week-ends ou fêtes.

Ne cédez jamais à la pression d'un interlocuteur pour la transmission d'informations confidentielles.

En cas de doute, lors d'un paiement, suivez la procédure de contre-appel et de vérification du RIB auprès de la banque.

Obtenez la validation de votre hiérarchie dans tous les cas.

EN CAS DE DOUTE, S'ABSTENIR !

NE RESTEZ PAS SEUL.E - PAS DE HONTE À AVOIR

Dès le moindre doute, informez votre responsable hiérarchique et/ou votre service informatique.