Article #2 – L'ingénierie sociale

L'**ingénierie sociale** est une forme de cyberattaque qui exploite la manipulation psychologique pour inciter les individus à divulguer des informations sensibles, partager des identifiants, accorder l'accès à des terminaux personnels ou compromettre la sécurité numérique d'une quelconque manière.

L'ingénierie sociale est une technique qui exploite l'erreur humaine et les sentiments des individus dans le but d'obtenir des informations confidentielles, un accès ou des biens de valeur.

Elle est parfois appelée « piratage humain » (*human hacking* en anglais) car elle vise à manipuler les individus pour qu'ils commettent des erreurs qui compromettent leur sécurité personnelle ou celle de leur organisation.

Voici quelques-uns des **dangers** associés à l'ingénierie sociale :

1. **Hameçonnage** : L'hameçonnage, également appelé *phishing* en anglais, utilise des courriels, des SMS, des réseaux sociaux ou d'autres formes de communication personnelle pour inciter les utilisateurs à cliquer sur des liens malveillants, télécharger des fichiers infectés ou divulguer des informations personnelles telles que des mots de passe ou des numéros de compte. Les attaques de phishing modernes sont sophistiquées et peuvent se faire passer pour des commerçants, des fournisseurs de services ou des administrations publiques.
2. ***Whaling*** : Cette attaque d'hameçonnage cible spécifiquement des individus de haut niveau, tels que des dirigeants d'entreprise ou des personnalités publiques. Les cybercriminels se font passer pour des personnes de confiance pour accéder à des informations sensibles.
3. ***Baiting*** : L'attaque par appât consiste à attirer les utilisateurs en leur proposant des incitations, comme des fichiers musicaux ou des logiciels gratuits, qui contiennent en réalité des *malwares*. Une fois téléchargés, ces fichiers compromettent la sécurité de l'utilisateur.
4. **Vol par diversion** : Les cybercriminels détournent l'attention des victimes en créant une situation d'urgence ou en suscitant des émotions fortes. Pendant ce temps, ils accèdent aux informations personnelles ou aux terminaux.
5. **Faux-semblant** : Les attaquants inventent des scénarios crédibles pour obtenir des informations personnelles. Par exemple, ils peuvent se faire passer pour des employés d'une entreprise et demander des détails confidentiels, car il y a une urgence de sécurité sur votre compte.
6. **Arnaque sentimentale** : Les cybercriminels exploitent les émotions et les relations personnelles pour accéder aux informations d'une personne. Cela peut inclure des tentatives de séduction en ligne ou des rencontres dans la vie réelle.
7. **Talonnage**: Les attaquants profitent de la gentillesse des individus en les suivant dans des zones sécurisées, comme des bureaux, pour accéder aux informations ou aux terminaux.

Les **signes d'une attaque par ingénierie sociale** peuvent varier, mais voici quelques indicateurs courants à surveiller :

1. **Demandes urgentes ou inhabituelles** : Soyez vigilant si vous recevez des demandes urgentes, spécialement si elles proviennent d'une source inattendue. Les attaquants utilisent souvent des scénarios d'urgence pour inciter les gens à agir rapidement.

2. **Insistance sur la confidentialité** : Si quelqu'un vous demande de garder secret un échange d'informations, cela peut être un signe d'ingénierie sociale. Les attaquants veulent éviter que vous consultiez d'autres personnes pour vérifier la légitimité de la demande.
3. **Utilisation de noms familiers** : Les cybercriminels peuvent se faire passer pour des collègues, des amis ou des membres de la famille. Soyez prudent si quelqu'un utilise votre nom ou celui d'une personne que vous connaissez.
4. **Demandes d'informations personnelles** : Méfiez-vous des demandes de mots de passe, de numéros de carte de crédit, de codes PIN ou d'autres informations sensibles. Les attaquants essaient souvent d'obtenir ces données par le biais de l'ingénierie sociale.
5. **Menaces ou intimidation** : Certains attaquants peuvent menacer de révéler des informations embarrassantes ou compromettantes si vous ne coopérez pas. Ne cédez pas à la pression.
6. **Réseaux sociaux et reconnaissance** : Les cybercriminels collectent des informations sur vous à partir de vos profils de réseaux sociaux, de vos publications en ligne et d'autres sources. Soyez conscient de ce que vous partagez publiquement.
7. **Offres trop belles pour être vraies** : Si quelque chose semble trop avantageux, soyez sceptique. Les escrocs utilisent souvent des offres alléchantes pour attirer leurs victimes.
8. **Demandes de téléchargement de fichiers ou de clic sur des liens** : Si vous recevez des courriels ou des messages inattendus avec des liens ou des pièces jointes, soyez prudent. Ils pourraient contenir des *malwares*.

En résumé, soyez conscient, posez des questions et ne partagez pas d'informations sensibles sans vérification appropriée. L'ingénierie sociale peut être subtile, mais en restant vigilant, vous pouvez réduire les risques.

Rappelez-vous, vous ne devriez pas vivre d'émotions fortes dans vos fonctions de travail courantes. Si une demande vous brusque, il s'agit peut-être d'une tentative d'hameçonnage!

Pour toute question ou obtenir de l'information additionnelle en matière de cybersécurité, veuillez communiquer avec nous, par courriel à : investia@solulan.com.