Qu'est-ce que l'ingénierie sociale ?

Pr Chérif DIALLO, CISSP
Professeur Titulaire des Universités
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept. Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

" Excès de confiance conduit à l'excès de déception." Thomas Gatabazi.

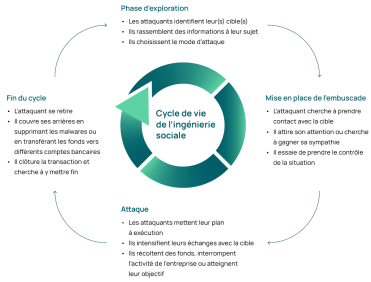
Résumé : Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui la problématique des attaques d'ingénierie sociale. Après une brève définition, ce bulletin présente donc le cycle et les tactiques utilisées dans les attaques par ingénierie sociale, et enfin les stratégies de protection à adopter pour faire face à ces menaces.

Mots clés : Ingénierie sociale, hameçonnage, spam.

---

1. Définition

Les attaques d'ingénierie sociale visent à manipuler les individus pour qu'ils communiquent des informations confidentielles, qu'ils téléchargent des logiciels malveillants, qu'ils se rendent sur des sites Web dangereux, qu'ils envoient de l'argent à des criminels ou qu'ils commettent d'autres erreurs qui compromettent leur sécurité personnelle ou leur organisation.





Dans le domaine de la cybercriminalité, ces escroqueries qui reposent sur le « piratage de l'être humain » ont tendance à amener les utilisateurs sans méfiance à divulguer des données, propager des programmes malveillants ou octroyer un accès à des systèmes contrôlés. Ces attaques peuvent se dérouler en ligne, en personne ou par l'intermédiaire d'autres interactions.

Les escroqueries qui intègrent l'ingénierie sociale exploitent la manière dont l'être humain réfléchit et agit. Les attaques qui reposent sur cette technique sont dès lors particulièrement utiles pour manipuler le comportement d'un utilisateur. Dès que l'attaquant a identifié ce qui motive un utilisateur à agir, il est en mesure de tromper et de manipuler ce dernier de manière efficace.

De plus, les pirates essaient également d'exploiter l'ignorance de l'utilisateur. Étant donné la vitesse à laquelle les technologies évoluent, certains consommateurs ou employés ne sont pas conscients de certaines menaces, comme les téléchargements furtifs. Il se peut également que les utilisateurs n'aient pas vraiment conscience de la valeur de leurs données personnelles comme les numéros de téléphone. Par conséquent, nombreux sont les utilisateurs qui ne savent pas comment obtenir la meilleure protection pour eux-mêmes et leurs données. Voici quelques cas illustratifs d'attaques par ingénierie sociale :

- Hôtel Marriott : Un groupe de pirates a utilisé des tactiques d'ingénierie sociale pour obtenir 20 Go de données personnelles et financières dans un hôtel Marriott. Ils ont trompé un employé de l'hôtel pour accéder à son ordinateur.
- Département américain du travail (DoL) : Le DoL (Department of Labor) a été victime d'une attaque visant à dérober les identifiants de connexion à Office 365. Les attaquants ont usurpé des domaines

ressemblant à ceux du DoL pour envoyer des e-mails de phishing, demandant aux destinataires de soumettre une offre pour un projet gouvernemental, ce qui a conduit à un site de phishing.

- Utilisateurs de Zoom : Une campagne de phishing a touché au moins 50 000 utilisateurs en créant une fausse peur de licenciement, incitant les employés à cliquer sur un lien pour une réunion avec les RH via Zoom. Ce lien dirigeait les employés vers un faux site de connexion Zoom conçu pour voler les mots de passe.
- FACC : Le constructeur aéronautique autrichien FACC a perdu environ 42 millions d'euros à cause d'une escroquerie "Business Email Compromise" (BEC). Les escrocs ont usurpé le compte de messagerie du PDG pour demander un transfert de fonds urgent, que l'employé a effectué.
- Crowdstrike : Ce fournisseur de sécurité a été la cible d'une attaque sophistiquée d'ingénierie sociale. Les escrocs ont exploité la réputation de confiance de Crowdstrike pour envoyer des e-mails de phishing aux employés, prétendant que leur ordinateur était infecté et demandant de les appeler pour résoudre le problème. En appelant, les employés donnaient accès à leurs ordinateurs aux attaquants.

2. Cycle d'une attaque par ingénierie sociale et tactiques utilisées

La majorité des attaques par ingénierie sociale repose sur une communication réelle entre les attaquants et leurs victimes. Au lieu de recourir à des méthodes reposant sur la force brute, l'attaquant préfère convaincre l'utilisateur de compromettre lui-même ses données. Le cycle de l'attaque met un processus fiable à la disposition des criminels pour vous tromper. Voici les étapes qui constituent en général le cycle d'une attaque par ingénierie sociale :

- ***Préparation*** : impliquant la collecte d'informations à votre sujet ou au sujet d'un groupe plus important dont vous êtes membre.
- ***Infiltration*** : grâce à l'établissement d'une relation ou d'une interaction qui a permis de bâtir une certaine confiance.
- ***Exploitation de la victime*** : une fois que l'attaquant a acquis la confiance de celle-ci et identifié ses faiblesses pour passer à l'attaque.
- ***Abandon*** : une fois que l'utilisateur a réalisé l'action souhaitée.

Ces cybermenaces s'appuient sur des tactiques d'ingénierie sociale :

- ***Hameçonnage :*** L'hameçonnage est sans conteste la cybermenace faisant appel à l'ingénierie sociale la plus répandue. Utilisant des courriels, de faux sites Web ou des messages textes trompeurs, les cybercriminels cherchent à dérober des informations personnelles ou organisationnelles sensibles à des victimes généralement peu méfiantes. Et malgré la notoriété de ces techniques d'hameçonnage, 1 employé sur 5 clique toujours sur ces liens suspects.
- ***Harponnage :*** Le harponnage est un cybercrime qui utilise les courriels pour mener des attaques ciblées contre des individus et des entreprises. Les criminels mettent en place des tactiques ingénieuses pour recueillir des données personnelles sur leurs cibles pour ensuite envoyer des courriels qui semblent familiers et dignes de confiance.
- ***Appâtage :*** Ce type d'attaque peut être perpétré en ligne ou dans un lieu physique. Le cybercriminel promet généralement à la victime une récompense en échange d'informations sensibles. Par exemple, brancher une clé USB ou télécharger une pièce jointe en échange d'un accès à vie à des films gratuits. L'ordinateur, et potentiellement le réseau, est ensuite infecté par un logiciel qui peut capturer les données d'accès ou envoyer de faux courriels.
- ***Prétexte :*** Dans ce type d'attaque, l'auteur prend une fausse identité pour inciter ses victimes à communiquer des informations. Cette technique est souvent utilisée contre des organisations disposant d'une grande quantité de données clients, comme les banques, les fournisseurs de cartes de crédit et les sociétés de services publics. Par exemple, le cybercriminel peut savoir que la victime a récemment acheté un article chez Apple. Il lui enverra donc un courriel en prétextant être un représentant du service à la clientèle d'Apple qui a besoin de confirmer ses informations de carte de crédit.
- ***Attaque de point d'eau :*** L'attaque de point d'eau (Water-holing) cible un groupe d'utilisateurs ainsi que les sites Web qu'ils visitent fréquemment. Le cybercriminel explore ces sites Web à la recherche d'une faille de sécurité puis l'infecte avec un maliciel. L'un des membres du groupe ciblé est éventuellement contaminé par le maliciel. Cette technique d'ingénierie sociale est très spécifique et difficile à détecter.
-

3. Solutions : comment se protéger contre les attaques par ingénierie sociale ?

Le fait de savoir reconnaitre les signes d'une attaque par ingénierie sociale fait partie des premières solutions à adopter. Plusieurs questions, dont voici quelques exemples, pourraient aider à reconnaitre facilement les messages suspects :

- Ce message provient-il d'un expéditeur légitime ?
- Ce message provient-il vraiment d'une de mes connaissances ?

- L'offre semble-t-elle trop belle pour être vraie ?
- Cette personne est-elle en mesure de prouver son identité ?

En second lieu, il convient d'adopter diverses stratégies de défense pour faire face à ces menaces. Voici une liste non exhaustive de solutions :

- ***Ne cliquez jamais sur les liens repris dans les e-mails ou les SMS.*** Prenez l'habitude de toujours saisir manuellement l'adresse Internet dans la barre d'adresse, et ce quel que soit l'expéditeur du message. Faites toutefois l'effort de rechercher une version officielle de l'adresse Internet en question. Ne cliquez jamais sur une adresse Internet avant d'avoir confirmé s'il s'agissait d'une adresse officielle ou légitime.
- ***Utilisez l'authentification à plusieurs facteurs.*** La sécurité des comptes en ligne est renforcée si vous ne vous contentez pas du simple mot de passe pour les protéger. L'authentification à plusieurs facteurs introduit des étapes supplémentaires de vérification de l'identité lors de l'ouverture d'une session. Ces « facteurs » peuvent être des données biométriques comme les empreintes digitales ou la reconnaissance faciale ou des codes d'accès temporaires envoyés via SMS.
- ***Évitez de partager vos détails personnels (date/lieu de naissance, plat préféré, etc.).*** Vous pourriez dévoiler sans le savoir la réponse à une de vos questions de sécurité ou une partie de votre mot de passe.
- ***Utilisez un réseau privé virtuel (VPN).*** Un VPN est un service qui permet de se connecter à Internet via un « tunnel » privé et chiffré (crypté). Non seulement la connexion est à l'abri des curieux, mais les données sont anonymisées, si bien qu'il sera impossible de remonter jusqu'à la cible à l'aide de cookies ou d'autres méthodes.
- ***Formation, communication et sensibilisation.*** Il faut tirer avantage d'un modèle flexible de formation en sensibilisation à l'ingénierie sociale qui propose des animations vidéo, de la formation interactive en ligne, des services de sécurité gérés, des modules de microlearning et des simulations d'hameçonnage pour offrir un support en continu.
- ***Le moindre privilège***. Les attaques par ingénierie sociale ciblent généralement les informations d'identification de l'utilisateur, qui peuvent être utilisées dans des attaques ultérieures. Le fait de restreindre l'accès des utilisateurs (au minimum nécessaire par rapport à leurs besoins) limite les dommages qui peuvent être causés par ces informations d'identification.
- ***Séparation des tâches***. La responsabilité des processus critiques, tels que les virements électroniques, doit être répartie entre plusieurs parties. Cela permet de s'assurer qu'aucun employé ne peut être piégé ou contraint par un pirate à effectuer ces actions.
- ***Solutions anti-hameçonnage***. L'hameçonnage est la forme la plus courante d'ingénierie sociale. Les solutions anti-hameçonnage, telles que l'analyse du courrier électronique, permettent d'identifier et de bloquer les courriels malveillants qui parviennent dans les boîtes de réception des utilisateurs.
- ***Sécurité des postes***. L'ingénierie sociale est couramment utilisée pour diffuser des logiciels malveillants dans les systèmes cibles. Les solutions de sécurité des postes peuvent limiter les impacts négatifs d'une attaque d'hameçonnage réussie en identifiant et en remédiant aux infections du logiciel malveillant.

4. En conclusion

" Faites confiance à ce que vous ressentez, pas à ce qu'on vous dit." Sandrine Fillassier.

Bien que les techniques d'ingénierie sociale soient courantes, les exemples présentés soulignent combien il peut être difficile de les repérer. La nature humaine étant ce qu'elle est, il est facile pour un cybercriminel de pousser sa victime vers les actions souhaitées. D'où l'importance de miser sur l'éducation et la sensibilisation à la cybersécurité, notamment l'apprentissage des techniques d'ingénierie sociales, pour mettre en place une véritable culture de la sécurité au sein des entreprises. À long terme, la prise de conscience des cybermenaces permet une modification durable des comportements problématiques en ligne et la réduction de ces risques.

