OUCH! | Novembre 2014

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...



# Ingénierie sociale

## Vue d'ensemble

Une fausse idée commune que les gens ont sur les cyberattaquants est que ces derniers utilisent uniquement des outils de piratage et des technologies de pointe pour s'infiltrer dans les ordinateurs, les comptes et les appareils mobiles des gens. Ce n'est tout simplement pas vrai. Les cyberattaquants ont appris que de simplement vous parler et vous induire en erreur s'avérait être l'un des moyens les plus faciles pour voler vos informations ou pirater votre ordinateur. Dans ce numéro, nous allons apprendre comment ces types d'attaques humaines, appelées attaques d'ingénierie sociale, fonctionnent et ce que vous pouvez faire pour vous protéger.

### Editeur invité

Alissa Torres est une instructrice certifiée SANS, spécialisée dans l'informatique judiciaire de pointe et dans la réponse aux incidents. Son expérience dans l'industrie comprend des mandats comme la gestion d'événements et aussi de travailler sur une équipe de sécurité interne en tant qu'enquêtrice en médecine légale numérique. Alissa peut être trouvée sur Twitter en tant que **@sibertor**.

## Ingénierie sociale

L'ingénierie sociale est un type d'attaque psychologique où un attaquant vous trompe en vous faisant faire quelque chose qu'il veut que vous fassiez. L'ingénierie sociale existe depuis des milliers d'années. L'idée d'escroquer ou d'arnaquer quelqu'un n'est pas nouvelle. Cependant, les cyberattaquants ont appris que l'utilisation de cette technique sur Internet est très efficace et peut être utilisée pour cibler des millions de personnes. La façon la plus simple de comprendre comment fonctionne l'ingénierie sociale consiste à jeter un œil à un exemple commun en situation réelle.

Vous recevez un appel téléphonique de quelqu'un qui prétend provenir d'une entreprise d'assistance informatique ou peut être du support technique Microsoft. Il vous explique que votre ordinateur se comporte étrangement, par exemple, navigue au hasard sur Internet, et il dit qu'il croit qu'il est infecté. Il vous affirme qu'il a été chargé d'enquêter sur la question et à vous aider à sécuriser votre ordinateur. Il utilise ensuite une variété de termes techniques et vous guide à travers des étapes semant la confusion pour vous convaincre que votre ordinateur est infecté.

Par exemple, il peut vous demander de trouver des fichiers spécifiques sur votre ordinateur et vous expliquer comment les trouver. Lorsque vous trouvez ces fichiers, l'appelant vous assure que ces fichiers sont un signe que votre ordinateur est infecté, alors qu'en réalité, ces fichiers ne sont rien de plus que des fichiers systèmes communs que l'on trouve sur chaque ordinateur. Une fois qu'il vous a trompé en vous faisant croire que votre ordinateur est infecté, il va vous forcer à aller sur un site Web et à acheter leur logiciel de sécurité ou vous demander de lui donner un accès à distance à votre ordinateur

# Ingénierie sociale

afin qu'il puisse y remédier. Cependant, le logiciel qu'il vend est en fait un programme malveillant. Si vous achetez et installez le logiciel, non seulement, le cyberattaquant vous aura trompé en infectant votre ordinateur, mais vous l'aurez en plus payé pour le faire. Si vous lui donnez accès à distance à votre ordinateur pour le réparer, il va, en réalité, prendre la relève pour l'infecter.

Gardez bien à l'esprit que les attaques d'ingénierie sociale de ce genre ne se limitent pas seulement aux appels téléphoniques; elles peuvent arriver avec presque n'importe quelle technologie, y compris les attaques de type phishing par e-mail, la messagerie texte, la messagerie Facebook, les messages Twitter ou les chats en ligne. L'essentiel est de savoir ce qu'il faut rechercher.

*Apprendre à prévenir, détecter et arrêter les attaques d'ingénierie sociale est l'une des étapes les plus efficaces que vous pouvez prendre en considération pour vous protéger.*

## Détection / Arrêt des attaques d'ingénierie sociale

La façon la plus simple de se défendre contre les attaques d'ingénierie sociale est de faire appel à votre bon sens. Si quelque chose vous semble suspect ou que vous ne sentez pas bien, il peut s'agir d'une attaque. Certains indicateurs communs d'une attaque d'ingénierie sociale comprennent:

- Quelqu'un crée un grand sentiment d'urgence. Si vous vous sentez sous pression pour prendre une décision très rapide, méfiez-vous.
- Quelqu'un demandant des informations auxquelles il ne devrait pas avoir accès ou devrait déjà les connaître.
- Quelque chose de trop beau pour être vrai. Un exemple courant est que vous êtes averti que vous avez gagné à la loterie bien que vous n'y avez jamais joué.

## Prévention de futures attaques d'ingénierie sociale

Heureusement, il y'a des précautions que vous pouvez prendre afin de vous aider à la prévention de futures attaques d'ingénierie sociale.

- **Ne jamais partager les mots de passe**: Aucune organisation ne vous contactera en vous demandant votre mot de passe. Si quelqu'un vous demande votre mot de passe, il s'agit probablement d'une attaque.

- **Ne pas trop partager**: Plus un attaquant en sait sur vous, plus il est facile pour lui de de vous induire en erreur en vous faisant faire ce qu'il veut. Même le partage de petits détails sur vous-même au fil du temps peuvent être

## Ingénierie sociale

assemblés pour créer une image complète de vous. Moins vous partagez publiquement, y compris sur les sites de médias sociaux, des critiques de produits ou des forums publics et des listes de diffusion, moins vous aurez de risques d'être attaqué.

- **Vérifiez les contacts**: Parfois, vous pouvez être appelé par votre banque, une société de cartes de crédit, fournisseur de services mobiles ou d'autres organisations pour des raisons légitimes. Si vous avez un doute quant à savoir si une demande d'informations est légitime, demander à la personne son nom et son numéro d'extension de poste téléphonique. Ensuite, trouver le numéro de téléphone de l'entreprise à partir d'une source de confiance, tels que le nombre sur le dos de votre carte de crédit, le numéro sur votre relevé de compte bancaire, ou peut-être le nombre sur le site Web de l'entreprise (assurez-vous de taper vous-même l'URL dans votre navigateur). De cette façon, lorsque vous appelez l'organisation, vous savez que vous leur parler vraiment à eux. Bien que cela semble être une corvée, protéger ainsi votre identité et vos informations personnelles vaut bien la peine d'effectuer cette étape supplémentaire.

## Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients.
Pour en savoir plus, veuillez vous référer aux liens suivants :
http://www.answersolutions.ch et http://answersecurity.com/

## Ressources

| | |
|---|---|
| Attaques par phishing: | http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201302_fr.pdf |
| Les réseaux sociaux en toute sécurité: | http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201303_fr.pdf |
| Conseils de sécurité: | http://www.onguardonline.gov/ |



Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet