Social engineering - Solutions

Facile

Exercice 1
« Le social engineering n'a lieu que sur Internet ». Cette affirmation est-elle correcte ?

a) Oui.
b) Non.

Solution :
Non. Le « social engineering » se produit aussi bien dans le monde analogue, réel, c'est-à-dire dans la rencontre directe avec des personnes, que dans le monde numérique, lorsque l'on communique en ligne (par exemple, par e-mail).

Exercice 2
Quelle méthode de « social engineering » est particulièrement répandue et se fait le plus souvent par e-mail ?

Solution :
Phishing / Hameçonnage

Moyen

Exercice 3
Quelle est la différence entre « phishing », « smishing » et « vishing » ?

Solution :
Avec les e-mails dits de « phishing », les « social engineers » tentent d'obtenir des mots de passe ou de diffuser des virus / logiciels malveillants (programmes nuisibles). L'hameçonnage se fait le plus souvent par e-mail, mais peut aussi se faire par SMS ou par appel téléphonique. Pour les SMS, on parle de « smishing », pour les appels de « vishing ».

Exercice 4
Que faut-il entendre par « fraude au PDG » ?

Solution :
La fraude au PDF ou la fraude au CEO est une escroquerie. Les employés d'une entreprise sont contactés, par exemple, par e-mail et l'expéditeur se fait passer pour le CEO (Chief Executive

Officer) et demande à « ses » employés de lui rendre un service ou de régler une affaire urgente. La tentative de manipulation s'attend à ce que les employés réagissent, ce qu'ils ne devraient en aucun cas faire.

Exercice 5
Cite trois mesures qui te permettront de te protéger efficacement contre le social engineering !

Solution :
Les mesures de protection les plus efficaces contre le « social engineering » sont :

- Examine de manière critique toutes les prises de contact et tous les messages (e-mail, appels, SMS) !
- Ne communique jamais tes données d'accès et veille à ce que personne ne t'observe lorsque tu tapes un mot de passe !
- Ne clique jamais sur des liens dans des e-mails ou des SMS qui te paraissent suspects ! N'ouvre pas les pièces jointes !
- Si tu es invité à effectuer un paiement par e-mail ou SMS, vérifie soigneusement la demande avec le destinataire et contacte-le au numéro de téléphone officiel !
- Veille à ce que tes appareils et tes logiciels soient toujours à jour !
- Choisis des mots de passe sûrs !
- Fais des copies de sécurité / des sauvegardes de tes fichiers importants !
- Ne visite que des sites web fiables !
- Fais attention à ces lignes d'objet d'e-mails et à d'autres similaires : « Vérification du mot de passe requise immédiatement », « Problème avec votre compte bancaire », « Dernier rappel : veuillez répondre immédiatement », « Votre commande sur Amazon.com ».

Difficile

Exercice 6
Quels sont les éléments qui composent un mot de passe sécurisé ?

Solution :
Observe les critères suivants lorsque tu choisis un mot de passe. Ainsi, il sera délicat pour les pirates d'accéder à tes données.

- Long (au moins 8 caractères, Il vaut mieux 12 ou plus).
- Varié (majuscules et minuscules, chiffres et caractères spéciaux).
- Aléatoire (pas de termes généraux, Il vaut mieux des chaînes de caractères qui n'ont pas de sens).
- Unique (Utilise un mot de passe différent pour chaque login !).

Exercice 7
Comment savoir, entre autres, si un site web est sûr ?

Solution :

- Vérifie si un site web est sécurisé par un certificat de sécurité SSL. S'il y a un petit cadenas dans la barre d'adresse et que l'adresse commence par « https:// » (au lieu de « http:// »), il s'agit plutôt d'un site sécurisé.
- Tu peux utiliser des extensions de navigateur telles que *Web of Trust*, qui t'indiquent le niveau de sécurité d'un site web. Toutefois, l'extension de navigateur peut voir ton comportement d'utilisation dans son intégralité.