SANS SECURITY AWARENESS

Votre bulletin mensuel sur la sensibilisation à la sécurité

Achats en ligne en toute sécurité

Aperçu

Les fêtes de fin d'année arrivent à grands pas et des millions de personnes vont commencer à chercher le cadeau idéal. La plupart d'entre nous vont chercher les offres en ligne, évitant ainsi la foule. Malheureusement, les cybercriminels aussi vont s'activer, créant de faux sites internet et utlisant des tactiques d'escroquerie. Dans ce bulletin, nous allons voir comment acheter en ligne sans risque et sans devenir une victime.

Fausses boutiques en ligne

Les cybercriminels créent de fausses boutiques en ligne en utilisant des noms de marques ou magasins connus et en recréant leurs sites à l'identique. Quand vous cherchez les meilleurs offres en ligne, vous pouvez vous retrouver sur ces sites. En achetant chez eux, vous pouvez vous retrouver avec des produits volés ou contrefaits, ou encore ne jamais recevoir votre commande. Utilisez ces étapes pour ne pas vous retrouver sur ces faux sites :

Quand c'est possible, achetez sur des sites que vous savez sûrs et sur lesquels vous avez déjà acheté. Ajoutez dans vos favoris les sites que vous avez déjà visité et que vous savez sûrs.

Méfiez-vous des prix bien plus bas que ceux proposés en grands magasins en ligne. Si l'offre est trop belle pour être vraie, elle est sûrement fausse.

Soyez sur vos gardes si un site ressemble à un que vous avez utilisé précédemment, mais porte un nom ou utilise un domaine légèrement différent. Par exemple, vous avez l'habitude d'acheter sur Amazon, passant par l'adresse www.amazon.com, mais finissez par tomber sur un faux site avec une adresse similaire, où la lettre « o » est remplaçée par le chiffre « 0 ».

Tapez le nom ou l'adresse du site dans un moteur de recherche pour voir ce que d'autres en ont pensés. Soyez attentifs aux termes comme « fraude », « scam », « plus jamais » ou « faux ».

Utilisez un mot de passe unique pour chacun de vos comptes. Vous ne pouvez pas vous souvenir de tous ces mots de passe ? Songez à utiliser un gestionnaire de mots de passe.

Escros sur sites légitimes

Soyez sur vos gardes même lorsque vous utilisez des sites de confiance. Les grands sites en ligne proposent souvent des produits vendus par des particuliers ou des entreprises externes qui ont des intentions frauduleuses. Ces sites sont un peu comme de vrais marchés, où certains vendeurs sont plus fiables que d'autres. Vérifiez les recommandations pour chaque vendeur avant de passer commande. Méfiez-vous des nouveaux vendeurs ou de ceux qui vendent à des prix défiant toute concurrence. Relisez la politique du magasin en ligne par rapport à l'achat auprès de tiers. En cas de doutes, achetez des articles vendus directement par la boutique en ligne et non par les vendeurs tiers.

Paiements en ligne

Examinez régulièrement vos relevés bancaires pour identifier les opérations suspectes. Si possible, activez les notifications par e-mail ou sms chaque fois qu'une transition bancaire est effectuée. Si vous trouvez une opération suspecte, appelez immédiatement votre banque et reportez-la. Evitez d'utiliser votre carte bancaire quand c'est possible. Les cartes bancaires permettent une transaction directe de votre compte : si une fraude a été commise, vous aurez beaucoup plus de difficulté à récupérer votre argent. Une autre solution consiste à utiliser des services connus tel que Paypal pour vos achats en ligne, vous permettant ainsi de ne pas partager vos coordonnées bancaires avec le vendeur. Enfin, songez à utiliser une carte cadeau pour ces achats.

Le fait qu'un site soit bien conçu et paraisse professionnel ne fait pas de lui un site légitime. Si vous n'êtes pas à l'aise avec un site, ne l'utilisez pas. Utilisez plutôt un site connu et fiable que vous avez déjà utilisé avant. Vous n'allez peut-être pas trouver cette superbe offre, mais vous aurez plus de chance de vous retrouver avec un produit légitime et éviter de vous faire arnaquer.

Rédacteur Invité

Lenny Zeltser *est le Responsable de la Sécurité des Systèmes d'Information d'Axonius, ainsi que formateur et auteur au SANS Institute. Vous pouvez le suivre sur Twitter(@lennyzeltser) et lire son blog sur* zeltser.com.

Ressources

Ingénierie sociale :	http://www.sans.org/u/X7k
Escroquerie via les médias sociaux :	http://www.sans.org/u/X7p
Les mots de passe simplifié :	http://www.sans.org/u/Xu9