Acheter en ligne en toute sécurité

La saison des vacances approche. Bientôt, des millions de personnes chercheront à acheter les cadeaux parfaits, et beaucoup d'entre nous feront leurs achats en ligne. Malheureusement, les cybercriminels seront également actifs, créant de faux sites d'achat et d'autres arnaques du shopping en ligne pour voler vos informations ou votre argent. Découvrez comment trouver de bonnes affaires sans vous faire piéger.

Faux magasins en ligne

Les criminels créent de fausses boutiques en ligne qui imitent l'apparence de sites réels ou utilisent les noms de magasins ou de marques connus. Lorsque vous recherchez les meilleures offres en ligne, vous pouvez vous retrouver sur l'un de ces faux sites. En achetant sur ces sites, vous risquez de vous retrouver avec des articles contrefaits ou volés, ou de ne jamais être livré. Prenez les mesures suivantes pour vous protéger :

- Dans la mesure du possible, achetez dans des boutiques en ligne que vous connaissez déjà, auxquelles vous faites confiance et avec lesquelles vous avez déjà fait affaire. Mettez ces magasins en ligne dans vos favoris.
- Méfiez-vous des annonces ou des offres promotionnelles sur les moteurs de recherche ou les réseaux sociaux qui sont nettement inférieures à celles que vous voyez dans les magasins en ligne établis. Si une offre semble trop belle pour être vraie, il peut s'agir d'une escroquerie.
- Méfiez-vous des sites web qui ne disposent d'aucun moyen de les contacter, dont les formulaires de contact ne fonctionnent pas ou qui utilisent des adresses électroniques personnelles.
- Méfiez-vous si un site web ressemble à un site que vous avez utilisé par le passé, mais que le nom de domaine du site ou le nom du magasin est différent. Par exemple, vous avez peut-être l'habitude de faire des achats sur Amazon, dont l'adresse du site Web est www.amazon.com, mais vous vous retrouvez sur un faux site qui semble similaire, mais dont l'adresse est www.amazonshoppers.com.
- Tapez le nom de la boutique en ligne ou son adresse web dans un moteur de recherche pour voir ce que d'autres personnes ont dit à son sujet. Recherchez des termes tels que "fraude", "escroquerie", "plus jamais" et "faux".
- Protégez vos comptes en ligne en utilisant un mot de passe unique et fort pour chacun de vos comptes. Vous ne pouvez pas vous souvenir de tous ces mots de passe ? Pensez à utiliser un gestionnaire de mots de passe.

Des escrocs sur des sites web légitimes

Restez sur vos gardes, même lorsque vous faites des achats sur des sites de confiance. Les magasins en ligne proposent souvent des produits vendus par des tiers - différentes personnes ou entreprises - qui peuvent avoir des intentions frauduleuses. Ces destinations en ligne sont comme les marchés du monde réel, où certains vendeurs sont plus dignes de confiance que d'autres.

- Vérifiez la réputation de chaque vendeur avant de passer la commande en lisant leurs avis.
- Méfiez-vous des vendeurs qui sont nouveaux sur la boutique en ligne, qui n'ont pas d'avis ou qui vendent des articles à des prix anormalement bas.
- Examinez la politique du magasin en ligne concernant les achats auprès de ces tiers.
- En cas de doute, achetez les articles vendus directement par la boutique en ligne, et non par les vendeurs tiers qui participent à son marché en ligne.
- Même avec les vendeurs légitimes, assurez-vous de bien comprendre les politiques de garantie et de retour du vendeur avant d'effectuer votre achat.

Paiement en ligne des achats

Examinez régulièrement vos relevés de carte de crédit pour repérer les dépenses suspectes. Si possible, activez l'option permettant de vous avertir par e-mail, texto ou l'application lorsqu'un prélèvement est effectué. Si vous constatez une activité suspecte, signalez-la immédiatement à la société émettrice de votre carte de crédit. Utilisez des cartes de crédit plutôt que des cartes de débit pour les paiements en ligne. Les cartes de débit prélèvent l'argent directement sur votre compte bancaire ; en cas de fraude, vous aurez beaucoup plus de mal à récupérer votre argent. Les services de paiement électronique ou les portefeuilles électroniques tels que PayPal sont également une option plus sûre pour les achats en ligne, car ils ne vous obligent pas à divulguer un numéro de carte de crédit au vendeur. Évitez les sites web qui n'acceptent que les paiements en crypto-monnaies ou qui exigent des méthodes de paiement obscures.

Ce n'est pas parce qu'une boutique en ligne a une apparence professionnelle qu'elle est légitime. Si le site vous met mal à l'aise, ne l'utilisez pas. Allez plutôt sur un site connu auquel vous pouvez faire confiance ou que vous avez utilisé en toute sécurité dans le passé. Vous ne trouverez peut-être pas la bonne affaire, mais vous aurez beaucoup plus de chances d'éviter de vous faire arnaquer.

Rédacteur Invité

Mark Orlando est un leader de la sécurité qui a défendu les réseaux du Pentagone, de la Maison Blanche et de nombreux clients du secteur privé. Aujourd'hui, il est PDG et cofondateur de la société de cybersécurité Bionic, et il est instructeur et auteur à SANS Institute. [Twitter : @markaorlando]

Ressources

Simplifier les mots de passe: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Ingénierie sociale: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Hameçonnage par message:
https://www.sans.org/security-awareness-training/resources/messaging-smishing-attacks
Vous arnaquer grâce aux médias sociaux: https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/

Traduit pour la communauté par: Juliette Busson