OUCH! Novembre 2021

Magasiner en ligne de façon sécuritaire

Le temps des fêtes approche. Bientôt des millions de personnes chercheront le cadeau parfait, et plusieurs d'entre-nous le ferons en ligne. Malheureusement, les cybercriminels seront également actifs, créant de faux sites web d'achat et d'autres escroqueries d'achat en ligne pour voler vos informations ou votre argent. Découvrez comment trouver de bonnes affaires sans devenir une victime.

Les fausses boutique en ligne

Les criminels créent de fausses boutiques en linge qui imitent l'apparence de sites officiel ou utilisent les noms de magasins ou de marques bien connus. Lorsque vous cherchez pour les meilleurs offres en ligne, vous pouvez vous retrouver sur l'un de ces faux sites. En achetant sur de tels sites, vous pouvez vous retrouver avec des articles contrefaits ou volés, ou vos achats peuvent ne jamais vous être livrés. Suivez ces étapes pour vous protéger:

- Dans la mesure du possible, achetez dans des magasins en ligne que vous connaissez déjà, en qui vous avez confiance et avec lesquels vous avez déjà fait affaire. Ajoutez ces boutiques à vos favoris.
- Méfiez-vous des publicités ou des promotions 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 invraisemblable, c'est probablement une arnaque.
- Soyez vigilant avec les sites web n'ayant pas de moyens pour les contacter, qui ont des formulaires qui ne fonctionnent pas, ou utilisant des adresses de courriel personnel.
- Méfiez-vous si un site Web ressemble à celui que vous avez utilisé dans le passé, mais que le nom de domaine du site Web ou le nom du magasin est différent. Par exemple, vous pouvez être habitué de magasiner chez Amazon, qui a son site web à l'adresse www.amazon.com, mais vous vous retrouvé sur un site frauduleux qui lui ressemble, mais qui a l'adresse www.amazonshoppers.com.
- Entrez le nom de la boutique en ligne ou son adresse web sur un moteur de recherche afin de voir ce que d'autres ont a dire 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 n'arrivez pas à vous souvenir de tous vos mots de passe? Songez à les sauvegarder tous dans un gestionnaire de mots de passe.

Escrocs sur des sites web légitimes

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

© SANS Institute 2021

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

Paiements en ligne pour les achats

Examinez régulièrement vos relevés de carte de crédit pour identifier les frais suspects. Si possible, activez l'option de vous avertir par e-mail, SMS ou application lorsqu'un débit est effectué. Si vous trouvez une activité suspecte, signalez-la immédiatement à votre compagnie de carte de crédit. Utilisez des cartes de crédit au lieu de cartes de débit pour les paiements en ligne. Les cartes de débit prélèvent de l'argent directement sur votre compte bancaire; si une fraude est commise, 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 cryptomonnaie ou qui nécessitent des méthodes de paiement obscures.

Ce n'est pas parce qu'une boutique en ligne a une apparence professionnel qu'elle est légitime. Si le site web vous met mal à l'aise, ne l'utilisez pas. Au lieu de cela, dirigez-vous vers un site bien connu auquel vous pouvez faire confiance ou que vous avez utilisé en toute sécurité dans le passé. Vous ne trouverez peut-être pas cette offre incroyable, mais vous êtes beaucoup plus susceptible d'éviter de vous faire arnaquer.

Rédacteur invité

Mark Orlando est un leader de la sécurité qui a défendu des réseaux au Pentagone, à la Maison Blanche et de nombreux clients du secteur privé. Aujourd'hui, il est PDG et co-fondateur de la société de cybersécurité Bionic, et est instructeur et auteur de cours à l'Institut SANS. [Twitter: @markaorlando]

Ressources

Simplifier les mots de passe: https://www.sans.org/newsletters/ouch/making-passwords-simple/
Attaques d'ingénierie sociale: https://www.sans.org/newsletters/ouch/social-engineering-attacks/
Attaques de messagerie: https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
Vous arnaquer via les réseaux sociaux: https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/

Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka

OUCH! Publié par SANS Security Awareness et distribué sous Creative Commons BY-NC-ND 4.0 license. Vous êtes libre de partager ou de distribuer cette lettre de nouvelles tant que vous ne la vendez pas ou ne la modifiez pas. Équipe d'éditeur: Walter Scrivens, Phil Hoffman, Alan Waggoner, Les Ridout, Princess Young.