Workforce Security and Risk Training

OUCH!

La lettre d'information mensuelle sur la sensibilisation à la sécurité pour vous

C'est le moment d'être sceptique - Achetez en ligne de manière sécurisée

Une offre des fêtes trop belle pour être vraie

Maya était ravie de trouver une paire d'écouteurs d'une très bonne marque à 70% de réduction. Le site paraissait professionnel, la promotion des fêtes semblait se finir bientôt, et elle a même reçu un email de confirmation, quelques minutes après avoir passé sa commande. Mais les jours sont passés, et son colis n'est pas arrivé. Ses emails et appels sont restés sans réponse, et peu de temps après, sa carte de crédit a été utilisée pour des frais non autorisés. Ce qui semblait être une bonne affaire était devenu une leçon de taille. Maya avait été victime d'une arnaque en ligne conçue pour escroquer les acheteurs des fêtes.

Malheureusement, l'histoire de Maya n'est pas unique. Les achats en ligne continuent à se répandre de plus en plus, surtout pendant les fêtes, et les cyber-criminels voient l'opportunité de piéger leurs victimes sur des faux sites, des promotions contrefaites et des escroqueries. La bonne nouvelle ? Vous pouvez acheter en ligne de manière sûre et repérant les signaux d'alarme et en suivant quelques conseils simples.

Les faux sites en ligne

Les cyber-criminels créent des faux sites qui semblent légitimes ou utilisent le nom de marques très connues. Lorsque vous recherchez les meilleures offres en ligne, vous risquez de vous retrouver sur l'un de ces sites frauduleux. Les criminels en font souvent la promotion sur les réseaux sociaux en proposant des articles à des prix très bas. En achetant sur ces sites, vous pouvez vous faire voler vos informations de carte bleue, recevoir des articles de contrefaçon ou volés, ou ne rien recevoir du tout. Protégez-vous en suivant ces étapes :

- **Achetez sur des sites sûrs**. Achetez sur des sites que vous connaissez déjà et sur lesquels vous avez déjà fait des achats. Ajoutez-les en favoris dans votre navigateur. Vous ne trouverez peut-être pas cette offre incroyable, mais vous risquez beaucoup moins de vous faire arnaquer.
- **Méfiez-vous des promotions importantes**. Si une publicité ou une promotion est nettement inférieure à celles que vous voyez dans les boutiques en ligne établies, il s'agit probablement d'une arnaque.
- **Vérifiez les coordonnées**. Évitez les sites qui ne fournissent aucune coordonnée, dont les formulaires de contact ne fonctionnent pas ou qui utilisent des adresses email personnelles. L'absence d'adresse physique, de numéro de téléphone, de coordonnées du service client et de politique de retour claire sont également souvent des indices permettant de repérer les sites suspects.

- **Examinez l'adresse internet**. Méfiez-vous si un site ressemble exactement à celui que vous utilisiez avant, mais le nom de domaine est différent. Par exemple, vous avez peut-être l'habitude de faire vos achats sur Amazon, dont l'adresse web est www.amazon.com, mais vous vous retrouvez sur un faux site web qui lui ressemble, mais dont l'adresse internet est www.aamazon.deals.
- **Cherchez des avis**. Tapez le nom ou l'URL du magasin dans un moteur de recherche pour voir ce que d'autres utilisateurs en disent. Cherchez les termes "fraude", "arnaque", "à fuir" et "faux".
- **Méfiez-vous des méthodes de paiement**. Les sites qui n'acceptent que les virements bancaires, les cartes-cadeaux ou les cryptomonnaies sont souvent utilisés par des escrocs.
- **Sécurisez vos comptes**. Protégez vos comptes en ligne en utilisant un mot de passe fort et unique. Si vous en rappeler est difficile, envisagez l'utilisation d'un gestionnaire de mot de passe. Activez les fonctionnalités de sécurité supplémentaires telles que l'authentification multifactorielle (MFA) et les clés d'accès partout où elles sont disponibles.

Les escrocs sur des sites d'achats légitimes

Certaines boutiques en ligne proposent des produits vendus par des particuliers ou des petites entreprises, et des escrocs peuvent se cacher parmi eux. Vérifiez la réputation de chaque vendeur avant de passer commande, en lisant les avis laissés par les autres clients. Méfiez-vous des nouveaux vendeurs, de ceux qui n'ont pas d'avis, ou de ceux qui vendent des produits à des prix anormalement bas.

Les paiements en ligne pour les achats

Une autre façon de vous protéger consiste à vérifier régulièrement vos relevés de carte de crédit afin d'identifier les transactions suspectes. Si possible, activez la fonction de notification par email, SMS ou application afin d'être averti, à chaque fois qu'un paiement est effectué avec votre carte. Si vous constatez une activité suspecte, signalez-la immédiatement à votre banque. Utilisez des cartes de crédit plutôt que des cartes de débit pour les paiements en ligne. Les cartes de débit prélèvent directement l'argent sur votre compte bancaire ; en cas de fraude, il vous sera beaucoup plus difficile de récupérer votre argent. Les services de paiement électronique ou les portefeuilles électroniques tels que PayPal constituent également une option plus sûre pour les achats en ligne, car ils ne vous obligent pas à divulguer votre numéro de carte de crédit au vendeur.

Rédacteur invité

Tricia McMahon, présidente de la filiale de Women in Cybersecurity (WiCyS) à San Diego et trésorière de WiCyS Education and Training, s'engage à respecter la mission principale de WiCyS, qui consiste à recruter, retenir et promouvoir les femmes dans le domaine de la cybersécurité. Elle est titulaire d'une maîtrise en cybersécurité et se passionne pour l'apprentissage et le développement professionnel. linkedin.com/in/triciaamcmahon

Ressources

Comment les cybercriminels volent vos mots de passe : https://www.sans.org/newsletters/ouch/unveiling-shadows-how-cyber-criminals-steal-your-passwords/
Comment les cybercriminels exploitent vos émotions : https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions/
Le pouvoir des gestionnaires de mots de passe : https://www.sans.org/newsletters/ouch/power-password-managers/
Le pouvoir des phrases de passe : https://www.sans.org/newsletters/ouch/power-passphrase/

Traduit pour la communauté par : Juliette Busson

Vous pouvez découvrir plus de Ouch! Sur le lien suivant : https://www.sans.org/newsletters/ouch