SANS SECURITY AWARENESS
Pélissier & Partners
Explorateurs de connaissances

OUCH! | Novembre 2017

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

OUCH!

Dans ce numéro...

- Faux magasins en ligne
- Votre ordinateur / Appareil mobile
- Votre carte de crédit

Achats en ligne en toute sécurité

Vue d'ensemble

La saison des vacances approche et bientôt des millions de personnes du monde entier seront à la recherche du cadeau parfait. Beaucoup d'entre nous choisissent de faire des achats en ligne à la recherche d'une bonne affaire et dans le but d'éviter les longues files d'attente et des foules impatientes. Malheureusement, c'est aussi la période de l'année où de nombreux cybercriminels créent de faux sites commerciaux pour escroquer et voler les autres. Nous expliquons ci-dessous les risques liés au shopping en ligne et les façons d'obtenir une offre exceptionnelle en toute sécurité.

Editeur invité

Lenny Zeltser conçoit des produits de sécurité chez Minerva Labs et enseigne la lutte contre les logiciels malveillants à l'Institut SANS. Lenny est actif sur Twitter en tant que **@lennyzeltser** et écrit un blog de sécurité sur **zeltser.com**.

Faux magasins en ligne

Alors que la plupart des magasins en ligne sont légitimes, certains ne le sont pas : il s'agit en fait de faux sites implémentés par des cybercriminels. En effet, ces derniers créent des faux sites web en copiant le look ou en utilisant le nom de magasins bien connus. Ils utilisent ensuite ces sites pour attaquer des personnes qui sont à la recherche de la meilleure affaire possible. Lorsque vous effectuez une recherche en ligne dans le but de cibler les prix les plus bas, vous êtes susceptible d'être dirigé vers l'un de ces faux sites Web. Lors de votre sélection d'un site Web pour acheter un produit, vous devez vous méfier des sites qui affichent des prix considérablement moins chers que partout ailleurs ou encore des sites Web qui offrent des produits qui sont vendus dans tout le pays. La raison pour laquelle leurs produits sont si peu chers ou disponibles c'est parce que ce que vous allez recevoir n'est sans doute pas légitime, il s'agira probablement d'une contrefaçon ou d'un objet volé, ou encore, dans certains cas, vous ne recevrez même jamais rien. Protégez-vous en procédant comme suit :

- Dans la mesure du possible, achetez sur des sites Web que vous connaissez déjà, auxquels vous faites confiance et sur lesquels vous avez déjà fait affaire.
- Vérifiez que le site Web a une adresse postale légitime et un numéro de téléphone relatif aux ventes ou des questions relatives à l'assistance. Si le site semble suspect, appelez pour être certain de parler à une personne.
- Recherchez les signes précurseurs évidents comme des offres trop alléchantes pour être vraies. De même avec les fautes de grammaire et les fautes d'orthographe trop énormes.
- Soyez très méfiant si un site Web semble être une réplique exacte d'un site Web bien connu que vous avez utilisé dans le

Achats en ligne en toute sécurité

passé, mais le nom de domaine du site Web ou le nom de la boutique en ligne est légèrement différent. Par exemple, vous pouvez être habitué à acheter en ligne sur Amazon, dont le site Web est https://www.amazon.com. Mais soyez très méfiant si vous vous trouvez sur des sites Web prétendant être Amazon comme http://store-amazoncom.com.

- Saisissez le nom ou l'URL du magasin dans un moteur de recherche et voyez ce que les autres personnes ont dit à propos du site Web par le passé. Recherchez des termes tels que « fraude », « escroquerie », « plus jamais » ou « faux ». Un manque de commentaires peut également signifier que le site Web est très récent et pourrait ne pas être fiable.
- Avant d'acheter des articles, assurez-vous que votre connexion au site Web est cryptée. La plupart des navigateurs affichent des connexions chiffrées avec un verrou et/ou les lettres HTTPS en vert juste avant le nom du site.

Protégez-vous en ligne en faisant des achats uniquement sur des sites de confiance ayant une réputation établie.

Rappelez-vous que ce n'est pas parce que le site a l'air professionnel que cela signifie pour autant qu'il soit légitime. Si vous n'êtes pas à l'aise avec le site, ne l'utilisez pas. Au lieu de cela, trouvez un site bien connu, auquel vous pouvez faire confiance ou que vous avez déjà utilisé en toute sécurité dans le passé. Vous ne trouverez sans doute pas un deal aussi attrayant, mais vous serez davantage sûr de vous retrouver avec un produit légal et éviterez que vos données personnelles et financières ne soient volées.

Votre ordinateur / Appareil mobile

En plus de faire du shopping sur des sites Web légitimes, vous voulez vous assurer que votre ordinateur ou appareil mobile soit sécurisé. Les cybercriminels tenteront d'infecter vos appareils afin qu'ils puissent récolter vos comptes bancaires, vos informations de carte de crédit et vos mots de passe. Suivez les étapes suivantes pour sécuriser vos appareils :

- Si vous avez des enfants dans votre maison, envisagez d'avoir deux appareils, un pour vos enfants et un pour les adultes. Les enfants sont curieux et interactifs avec la technologie, ils sont donc plus susceptibles d'infecter leur propre appareil. En utilisant un ordinateur ou une tablette séparé(e) uniquement pour les transactions en ligne, telles que les opérations bancaires en ligne et les achats, vous réduisez les risques d'infection.
- Installez toujours les dernières mises à jour et exécutez un logiciel anti-virus à jour. Cela sera plus difficile pour un cybercriminel d'infecter votre appareil.

Achats en ligne en toute sécurité

Votre carte de crédit

Passez régulièrement en revue vos relevés de carte de crédit pour identifier les frais suspects, surtout après avoir utilisé vos cartes pour faire de nombreux achats en ligne ou après avoir utilisé un nouveau site en ligne. Certains fournisseurs de cartes de crédit vous donnent la possibilité de vous avertir par e-mail ou par SMS chaque fois que des frais sont facturés à votre carte ou lorsque les frais dépassent un montant fixe. Une autre option est d'avoir une carte de crédit uniquement pour les achats en ligne, de cette façon si elle est compromise, vous pouvez facilement changer la carte sans impact sur vos autres activités de paiement. Si vous pensez qu'une fraude a été commise, appelez immédiatement votre compagnie de carte de crédit. C'est aussi la raison pour laquelle il est préférable d'utiliser les cartes de crédit pour tous les achats en ligne. Evitez d'utiliser des cartes de débit lorsque c'est possible. Les cartes de débit prennent l'argent directement de votre compte bancaire, si la fraude a été commise, il peut être beaucoup plus difficile de récupérer votre argent. Enfin, considérez les cartes de crédit qui génèrent un numéro de carte unique pour chaque achat en ligne, vos cartes-cadeaux ou utilisez des services de paiement réputés tels que PayPal, qui n'exigent pas que vous divulguiez votre numéro de carte de crédit au vendeur.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Sources

Ingénierie sociale :	https://securingthehuman.sans.org/ouch/2017#january2017
Quatre étapes pour rester sécurisé :	https://securingthehuman.sans.org/ouch/2016#october2016
Sécuriser votre réseau domestique :	https://securingthehuman.sans.org/ouch/2016#february2016
Conseil du jour du SANS Security :	https://www.sans.org/tip_of_the_day.php

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley
Traduit par : Marilyn Combet