OUCH! | Novembre 2015

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

La saison où il faut faire preuve de prudence

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, il s'agit également de l'époque préférée de l'année, choisie par les cybercriminels pour commettre des fraudes en ligne ou financières. Dans ce numéro, nous expliquons les dangers des achats en ligne et les façons de vous protéger.

Editeur invité

Jonathan Homer (**@JonathanLHomer**) est un leader reconnu dans le domaine de la sensibilisation à la cybersécurité et est actif à la fois au sein du gouvernement et du secteur privé. Jonathan se spécialise dans l'engagement du public et les principales techniques de formation de pointe.

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:

- 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 les fautes de grammaire et les fautes d'orthographe.
- Soyez très méfiant si un site semble être une réplique exacte d'un site Web bien connu que vous avez utilisé dans le passé, mais que le nom de domaine de site Web ou le nom de la boutique est légèrement différente. Par exemple,

Achats en ligne en toute sécurité

vous allez peut être utiliser le lien https://amazon.com pour aller sur le site d'Amazon pour l'ensemble de vos achats. Soyez cependant très méfiant si vous deviez vous trouver sur un site Web faisant semblant d'être Amazon avec l'URL http://store-amazon.com.

- Tapez le nom ou l'URL de la boutique dans un moteur de recherche et observez ce que les autres ont dit sur le site dans le passé. Recherchez les mots comme "escroquerie", "plus jamais ça" ou "faux". Un manque d'avis est également un mauvais signe car cela indique que le site est récent.

Rappelez-vous que ce n'est pas parce que le site a l'air professionnel que cela signifie pour autant qu'il est légitime. Si quelque chose sur le site vous alerte, prenez le temps d'enquêter. 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.

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

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 est sécurisé. Les cybercriminels vont essayer d'infecter vos appareils afin qu'ils puissent récolter vos comptes bancaires, informations de carte de crédit et mots de passe. Prenez les mesures suivantes en considération pour garder vos dispositifs sécurisés:

- Si vous avez des enfants à la maison, envisagez d'avoir deux appareils, l'un pour vos enfants et l'autre pour les adultes. Les enfants sont curieux et interactifs avec la technologie, par conséquent, ils sont plus susceptibles d'infecter leur propre appareil. En utilisant un ordinateur ou une tablette séparée juste pour les transactions en ligne, tels que les services bancaires en ligne et de shopping, vous réduisez le risque d'infection. Si des dispositifs distincts ne sont pas une option, il est recommandé d'avoir dans ce cas des comptes séparés sur l'ordinateur partagé, et également de vous assurer que vos enfants n'ont pas de droits administrateurs.
- Connectez-vous uniquement aux réseaux sans fil que vous gérez, tels que votre réseau domestique, ou autres réseaux auxquels vous pouvez faire confiance lors de transactions financières. Utiliser les réseaux publics Wi-Fi tels que celui du café du coin peut être bien pour lire les nouvelles en ligne, mais certainement pas pour accéder à votre compte bancaire.
- installez toujours les dernières mises à jour et exécutez le logiciel anti-virus mis à jour. En prenant ces mesures en considération, il sera beaucoup plus difficile pour un cybercriminel d'infecter votre appareil.

Achats en ligne en toute sécurité

Votre carte de crédit

Gardez un œil sur vos relevés de carte de crédit afin d'identifier les charges suspectes. Vous devriez vérifier vos relevés de compte régulièrement, au minimum au moins une fois par mois. Certains fournisseurs de cartes de crédit vous offrent la possibilité de vous avertir par e-mail ou SMS à chaque fois qu'une charge est prélevée sur votre carte ou lorsque des charges dépassent un montant déterminé. Une autre option est d'avoir une carte de crédit seulement pour les achats en ligne, de cette façon si elle est compromise, vous pouvez facilement changer la carte sans impact sur l'une de vos autres activités de paiement. Si vous pensez qu'une fraude a été commise, appelez votre compagnie de carte de crédit tout de suite et expliquez-lui la situation. Voilà aussi pourquoi les cartes de crédit sont mieux pour les achats en ligne que les cartes de débit. Les cartes de débit prennent l'argent directement de votre compte bancaire, et si la fraude a été commise, il peut être beaucoup plus difficile de récupérer votre argent.

Enfin, il y'a une nouvelle technologie qui vous permet de payer sans exposer votre numéro de carte de crédit. Considérez les cartes de crédit qui génèrent un numéro de carte unique pour chaque achat en ligne, ou utilisez les services de paiement bien connus, tels que PayPal, qui ne vous obligent pas à divulguer votre numéro de carte de crédit au vendeur.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients. Pour en savoir plus, veuillez vous référer aux liens suivants : http://www.answer.ch et http://answersecurity.com/

Sources

Cinq étapes pour rester sécurisé :	https://www.securingthehuman.org/ouch/2014#october2014
Sécuriser votre réseau domestique :	https://www.securingthehuman.org/ouch/2014#january2014
Sécuriser votre tablette :	https://www.securingthehuman.org/ouch/2013#december2013
Conseil du jour par du SANS sécurité :	https://www.sans.org/tip_of_the_day.php

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Marilyn Combet