Le guide de Websense pour acheter en ligne sans se faire pirater !
Internet
PostÃ© par : JulieM
PubliÃ©e le : 10/12/2009 15:00:00

A lâ□□attention des nombreux consommateurs utilisant les rÃ©seaux de leur entreprise pour accÃ©der Ã Internet en prÃ©paration de NoÃ«l, **Websense a publiÃ© un guide pour Ã©viter les arnaques en cette pÃ©riode de fÃªte**.

Les termes Â« NoÃ«l Â» et Â« Achats Â» vont de pair ; lâ□□annÃ©e derniÃ¨re, les consommateurs britanniques ont dÃ©pensÃ© plus de 4,67 milliards de livres sterling sur le Web pour le seul mois de dÃ©cembre, dont 102 millions pour le seul jour de NoÃ«l.*

Cette annÃ©e, la population, lassÃ©e par la crise, est Ã la recherche de bonnes affaires et devrait une nouvelle fois choisir dâ□□Ã©viter la foule en faisant ses achats en ligne. eBay prÃ©voit que 85 % des consommateurs maintiendront ou augmenteront leurs achats en ligne ce NoÃ«l et des Ã©tudes indiquent que 93 % des clients prÃ©voient dâ□□acheter un cadeau en ligne.*

La derniÃ¨re statistique, notamment, prÃ©sente un intÃ©rÃªt pour les cybercriminels. Elle rÃ©vÃ¨le en effet le nombre potentiel des occasions dâ□□attaque pour eux.

*sources: Interactive Media in Retail Group and eBay.

Les astuces Ã connaÃ®tre pour Ã©viter les mauvaises surprises lors des achats de NoÃ«l

1. Lâ□□arnaque de la Â« bonne affaire Â»Â en ligne

Lâ□□attaque se dÃ©roule ainsi : Lâ□□un des principaux attraits des achats en ligne est quâ□□ils se prÃ©sentent souvent comme une bonne affaire Ã rÃ©aliser. En cherchant une bonne affaire, on peut Ãªtre attirÃ© par les prix bas et oublier de vÃ©rifier qui est le vendeur. Les cybercriminels en sont parfaitement conscients et crÃ©ent de fausses boutiques en ligne pour collecter des informations bancaires, quâ□□ils utilisent ensuite pour leur propre profit. Les produits sont souvent offerts Ã des prix bien plus bas que dans les magasins, cependant aucun colis ne vous sera envoyÃ©. Mais votre carte de crÃ©dit, elle, pourrait bien Ãªtre dÃ©bitÃ©e et vos informations bancaires vendues sur le marchÃ© noir.

Aussi allÃ©chantes que peuvent paraÃ®tre certaines offres, le vieil adage se rÃ©vÃ¨le souvent juste : si cela semble trop beau pour Ãªtre vrai... câ□□est probablement le cas.

Exemple de faux site web commerÃ§ant

Lâ□□astuce: Si vous effectuez des achats sur un site inhabituel, assurez-vous qu'un numÃ©ro de tÃ©lÃ©phone fixe et une adresse postale sont prÃ©cisÃ©s, afin que vous puissiez contacter le revendeur en cas de problÃ¨me. VÃ©rifiez que la connexion de paiement est sÃ©curisÃ©e en recherchant le symbole de cadenas et en vous assurant que l'adresse dans la barre d'adresse

commence par Â« https Â» (le Â« s Â» signifiant sÃ©curisÃ©). Ne fournissez vos informations de carte bancaire quâ□□en cas de connexion sÃ©curisÃ©e. Ne le faites jamais par courrier Ã©lectronique. Souvenez-vous Ã©galement que les lois de l'Union EuropÃ©enne (UE) vous protÃ¨gent contre une utilisation frauduleuse de ces informations dans des transactions au sein de lâ□□UE : les cartes de crÃ©dit vous apportent une protection supplÃ©mentaire.

2. Le camouflage par dÃ©guisement

Lâ□□attaque se dÃ©roule ainsi : Au moment de NoÃ«l, nous envoyons Ã nos amis et collÃ¨gues des cartes Ã©lectroniques ou des liens vers des vidÃ©os amusantes. Malheureusement, sans le savoir, celles-ci peuvent parfois contenir des Ã©lÃ©ments malveillants. Et lâ□□e-mail peut cacher une arnaque au phishing. DissimulÃ©es entre les images joyeuses du PÃ¨re NoÃ«l, des URL malveillantes peuvent contenir des liens vers des malwares ou du code. Cette technique Ã©volue constamment visant Ã augmenter le taux de rÃ©ussite. Elle permet de donner vie Ã de nouvelles attaques de plus en plus sophistiquÃ©es en termes dâ□□imagerie et dâ□□appÃ¢ts utilisÃ©s.

Exemple de fausse carte Ã©lectronique de NoÃ«l

Lâ□□astuce: Nous aimons tous visiter des sites Web de vidÃ©os populaires pour dÃ©couvrir la derniÃ¨re blague ou le dernier clip. Ces sites au contenu crÃ©Ã© par les utilisateurs font lâ□□objet, de par leur nature mÃªme, dâ□□une mise Ã jour constante qui rend difficile la protection classique pour la sÃ©curitÃ© des visiteurs. Lâ□□installation dâ□□un logiciel dâ□□analyse en temps rÃ©el permet dâ□□attÃ©nuer ce risque, mais il faut toujours traiter avec une saine dÃ©fiance tout contenu vidÃ©o.

Si vous recevez une carte Ã©lectronique dâ□□un soi-disant ami, collÃ¨gue ou parent, vÃ©rifiez soigneusement l'adresse e-mail de l'expÃ©diteur et que le message vous est bien destinÃ©. Les personnes qui vous connaissent, nâ□□oublient pas votre nom ! Vous pouvez Ã©ventuellement vÃ©rifier auprÃ¨s de l'expÃ©diteur s'il vous a vraiment envoyÃ© l'e-mail en question. Si cet e-mail vous redirige vers une URL, vÃ©rifiez l'adresse pour dÃ©terminer oÃ¹ mÃ¨ne le lien AVANT de cliquer dessus. Est-ce que l'adresse paraÃ®t diffÃ©rente du site dont elle prÃ©tend provenir ? En cas de doute sur lâ□□origine du message, il est conseillÃ© de le supprimer immÃ©diatement.

3. Le tÃ©lÃ©chargement cachÃ© (drive-by)

Lâ□□attaque se dÃ©roule ainsi : C'est un des types d'attaque les plus dangereux, Ã©tant donnÃ© qu'aucune interaction de l'utilisateur n'est nÃ©cessaire pour que cette infection ait lieu. Il suffit de naviguer sur un site ayant trait Ã NoÃ«l, Ã©videmment infectÃ©, pour permettre lâ□□exÃ©cution dâ□□un code exploitant les vulnÃ©rabilitÃ©s dâ□□un logiciel installÃ© sur lâ□□ordinateur de lâ□□utilisateur. Ainsi, Ã son insu, lâ□□utilisateur tÃ©lÃ©charge des applications malveillantes alors quâ□□il regarde la dÃ©monstration des Â« finger skates Â» ou quâ□□il est en train de se divertir en participant aux jeux organisÃ©s sur les sites de NoÃ«l.

Lâ□□astuce: La plupart des arnaques classiques exploitent les faiblesses (vulnÃ©rabilitÃ©s dÃ©jÃ identifiÃ©es) des logiciels, des navigateurs ou des plug-in tiers. Il est essentiel pour lâ□□utilisateur de tÃ©lÃ©charger les correctifs et les mises Ã jour, sans quoi il sâ□□expose lui-mÃªme Ã des attaques de cybercriminels capables de prendre contrÃ´le de sa machine et de voler des donnÃ©es. Pour se protÃ©ger contre ces types dâ□□attaques, vous devez tÃ©lÃ©charger les derniers correctifs et mises Ã jour disponibles.

4. Les cadeaux empoisonnÃ©s de lâ□□antivirus

Lâ□□attaque se dÃ©roule ainsi : Lâ□□ingÃ©nierie sociale dÃ©signe lâ□□art dâ□□abuser une personne pour quâ□□elle effectue une action. Le faux antivirus est un exemple de technique dâ□□ingÃ©nierie sociale que les laboratoires de sÃ©curitÃ© de Websense constatent souvent. Lorsque lâ□□on navigue sur le Web, il arrive de voir apparaÃ®tre une fenÃªtre pop-up expliquant que lâ□□ordinateur risque dâ□□Ãªtre infectÃ©, et offrant une analyse antivirus gratuite. Ne vous faites pas berner, il n'y aura aucune analyse. En revanche, le programme prÃ©tendra avoir trouvÃ© un virus sur votre machine. En rÃ©alitÃ©, vous n'Ãªtes pas vraiment infectÃ© mais le procÃ©dÃ© vise Ã vous encourager Ã tÃ©lÃ©charger ou Ã payer pour un faux logiciel antivirus, qui n'est en fait rien d'autre qu'un logiciel malveillant. Ainsi, les hackers sont en possession de vos informations bancaires et sont en mesure de prendre le contrÃ´le de votre ordinateur.

Lâ□□astuce: Les rÃ©sultats des moteurs de recherche sont souvent Â« empoisonnÃ©s Â», et vous dirige vers des logiciels malveillants dÃ©guisÃ©s en logiciels antivirus. Lorsque vous recherchez des termes populaires ayant trait Ã NoÃ«l, l'empoisonnement du rÃ©fÃ©rencement pousse des URL infectÃ©es en tÃªte des rÃ©sultats de recherche, afin d'augmenter la probabilitÃ© que vous visitiez le site Web d'un faux antivirus. Soyez vigilants lorsque vous tÃ©lÃ©chargez un logiciel ou visitez un site Web. La rÃ©flexion est la meilleure protection dont vous disposez contre cette attaque. Si vous rÃ©alisez Ãªtre Ã©ventuellement tombÃ© dans une arnaque, contactez les autoritÃ©s compÃ©tentes.

5. Le puzzle de NoÃ«l

Lâ□□attaque se dÃ©roule ainsi : La technique, appelÃ©e fragmentation de script, consiste Ã scinder le code malveillant en petits blocs avec pour objectif de terrasser les moteurs dâ□□analyse. Du code anodin est intÃ©grÃ© dans une page Web. Lorsquâ□□une personne visite la page Web, la routine JavaScript demande lentement du code additionnel dâ□□autres serveurs Web par petites tranches. Une fois reÃ§us, les octets sont stockÃ©s jusquâ□□au transfert de tout le code, ce qui dÃ©clenche l'exploit.

Ce processus peut Ãªtre comparÃ© Ã lâ□□envoi dâ□□une bombe en piÃ¨ces dÃ©tachÃ©es. Ce nâ□□est quâ□□une fois toutes les piÃ¨ces ont Ã©tÃ© reÃ§ues et assemblÃ©es que le danger prend forme entiÃ¨rement. Lorsquâ□□on le rÃ©alise, le pirate se trouve dÃ©jÃ dans la place et peut alors aller dÃ©sactiver lâ□□antivirus et prendre le contrÃ´le de la machine.

Lâ□□astuce: Lâ□□attaque, qui concerne tous les principaux navigateurs, ne repose pas sur une vulnÃ©rabilitÃ© de ceux-ci, mais exploite simplement leur mode de fonctionnement. DÃ©sactiver les scripts JavaScript permet dâ□□empÃªcher lâ□□attaque, mais il ne sâ□□agit pas dâ□□une solution rÃ©aliste pour la plupart des internautes car elle priverait des fonctionnalitÃ©s de la quasi-totalitÃ© des sites Web les plus frÃ©quentÃ©s qui exigent lâ□□utilisation de JavaScript.

Les Laboratoires de sÃ©curitÃ© de Websense utilisent le rÃ©seau Websense ThreatSeekerâ□¢ pour dÃ©tecter, classifier et contrÃ´ler les menaces Internet globales et les anticiper. Chaque heure, le rÃ©seau Threatseeker scanne plus de 40 millions de sites Web et 10 millions dâ□□emails pour dÃ©tecter le contenu et le code malicieux. En utilisant plus de 50 millions de systÃ¨mes collectant les donnÃ©es en temps rÃ©el, le rÃ©seau Websense ThreatSeeker passe en revue plus dâ□□un milliard de contenus quotidiennement, Ã la recherche de nouvelles menaces. Les Laboratoires de SÃ©curitÃ© de **Websense livrent des alertes et partagent sur leur blog**.