SÃ©curitÃ© : Conseils pour bien faire vos achats de NoÃ«l en sÃ©curitÃ©
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 24/11/2010 14:00:00

NoÃ«l approche Ã grands pas et plus de 2 internautes sur 3 ont lâ□□intention de faire leurs achats sur le Web dâ□□aprÃ¨s la rÃ©cente Ã©tude de la Fevad et de MÃ©diamÃ©trie. Câ□□est donc le bon moment de rappeler **quelques conseils importants pour acheter en ligne sans danger** et Ã©viter que votre ordinateur soit infectÃ© et / ou que vos informations bancaires ne soient volÃ©es.

1. Les emails non sollicitÃ©s : Les spammers et les escrocs aiment cette pÃ©riode de fin dâ□□annÃ©e car ils savent quâ□□un grand nombre de personnes surfent sur le Web Ã la recherche de bonnes affaires, prÃªts Ã dÃ©penser de lâ□□argent. Alors quâ□□il est trÃ¨s tentant de cliquer sur le lien dâ□□un email annonÃ§ant : â□□Bonne Affaire sur les iPadsâ□¦ 50% de rÃ©duction!â□□ Soyez prudent! En cliquant sur ce lien, vous pourriez Ãªtre dirigÃ© vers un Site Internet qui tÃ©lÃ©charge des logiciels malveillants (ou malwares) sur votre ordinateur. Ce logiciel malveillant peut Ãªtre ensuite utilisÃ© comme enregistreur de frappe de votre ordinateur ou pour tÃ©lÃ©charger dâ□□autres malwares, tels que les faux logiciels dâ□□antivirus, ou tout simplement transformer votre ordinateur en gÃ©nÃ©rateur de spams.

Que faire : Si lâ□□affaire semble trop belle pour Ãªtre vraie, il est probable quâ□□il sâ□□agisse dâ□□un site Internet malveillant. Et si vous Ãªtes toujours tentÃ© de cliquer sur ce lien, placez votre curseur sur le lien (sans cliquer dessus) et vÃ©rifiez lâ□□URL qui apparait. Si lâ□□URL est diffÃ©rente de celle oÃ¹ vous souhaitez Ãªtre dirigÃ©, ne cliquez pas.

2. Les rÃ©sultats malfaisants des moteurs de recherche : Les attaques dâ□□optimisation des moteurs de recherche (appelÃ© SEO) se produisent gÃ©nÃ©ralement lors dâ□□Ã©vÃ©nements majeurs, tels que le Super Bowl, la Coupe du Monde, le World Series et la pÃ©riode de NoÃ«l. Les attaques apparaissent lorsque les cybercriminels crÃ©ent des algorithmes de classement des moteurs de recherche afin de positionner leurs sites Internet malicieux en haut des listes de recherche par mot-clÃ©. Ils peuvent utiliser des termes de recherche tels que â□□Bonnes Affaires de NoÃ«l,â□□ ou â□□Promotions de Fin dâ□□AnnÃ©e.â□□ Lorsquâ□□un utilisateur clique sur le lien malicieux, il peut Ãªtre dirigÃ© vers un site Internet qui pourrait immÃ©diatement compromettre son ordinateur.

Que faire : Comme le prÃ©cÃ©dent conseil, avant de cliquer sur un lien, placez votre curseur dessus pour vous assurer quâ□□il ne vous redirigera pas vers un site diffÃ©rent que celui annoncÃ©. Regardez le rÃ©sumÃ© du rÃ©sultat de recherche avant de cliquer. Souvent les SEO

attaquÃ©s ont un contenu qui nâ□□est pas appropriÃ© Ã vos mots de recherche. Par exemple, il peut y avoir beaucoup de mots-clÃ©s collÃ©s les uns aux autres mais pas placÃ©s dans une phrase correctement formÃ©e.

3. Des marchands en ligne inconnus : Si vous dÃ©couvrez une boutique en ligne qui offre des promotions incroyables sur des produits stars de NoÃ«l, renseignez-vous quâ□□il sâ□□agisse dâ□□un magasin lÃ©gitime et non dâ□□une fausse faÃ§ade qui disparaitra prochainement avec les informations de votre carte de crÃ©dit. Et mÃªme si elle est lÃ©gitime, vous devez vous assurer que son site nâ□□a pas Ã©tÃ©, sans le savoir, exploitÃ© par une injection SQL ou dâ□□autres attaques de type serveur. Les sites Internet exploitÃ©s ne vous dirigent pas toujours vers un site malveillant, mais souvent hameÃ§onneront ou essayeront dâ□□installer furtivement dâ□□autres formes de malwares sur votre ordinateur, tels que des Chevaux de Troie (appelÃ© Trojans), des bots, des enregistreurs de frappe (appelÃ© keylogger) et des outils de dissimulation dâ□□activitÃ© (appelÃ© rootkits), qui sont conÃ§us pour porter atteinte aux ordinateurs et voler les informations personnelles.

Que faire : Etre sÃ»r que votre antivirus soit mis Ã jour, ainsi que la prÃ©vention dâ□□intrusions afin de se prÃ©munir contre les abus qui sont souvent hÃ©bergÃ©s sur des sites exploitÃ©s. Les logiciels malveillants infecteront votre ordinateur de faÃ§on transparente via une attaque conduite par des failles du logiciel de sÃ©curitÃ©. Si vous Ãªtes touchÃ© par une telle attaque sans avoir de mesures prÃ©ventives appropriÃ©es, vous ne saurez probablement pas que vous Ãªtes infectÃ©.

4. MÃ©fiez-vous des mails de vos amis comportant des liens non sollicitÃ©s : Les liens malveillants ne sont pas toujours des spams. Ils peuvent provenir de votre meilleur ami dont lâ□□ordinateur a Ã©tÃ© sans le savoir exploitÃ©. La machine infectÃ©e peut avoir un botnet qui a Ã©tÃ© programmÃ© pour parcourir le carnet dâ□□adresses et envoyer des liens malveillants Ã chacun de vos contacts. Le message peut dire, â□□Salut, va voir ce site !â□□ ou â□□Cet endroit propose -50% sur les produits de NoÃ«l!â□□ En cliquant sur le lien vous pourriez Ãªtre dirigÃ© vers un site Internet malveillant qui installe des malwares sur votre systÃ¨me ou hameÃ§onne les informations dâ□□identification personnelles de votre carte de crÃ©dit.

Que faire : Faites appel Ã votre bon sens. Est ce que votre ami vous informe habituellement des ventes et promotions ? Si tel nâ□□en est pas le cas, une simple rÃ©ponse (de prÃ©fÃ©rence en utilisant un moyen de communication diffÃ©rent) en demandant, â□□As-tu eu lâ□□intention de mâ□□envoyer cet email?â□□. Quand la rÃ©ponse est â□□non,â□□ vous pouvez supprimer en toute sÃ©curitÃ© lâ□□email et informer votre ami quâ□□il devrait scanner le systÃ¨me de son ordinateur, car il pourrait Ãªtre infectÃ©.

5. MÃ©fiez-vous des points dâ□□accÃ¨s (hotspot) Wi-Fi non sÃ©curisÃ©s : Pour les acheteurs qui aiment surfer sur Internet lors dâ□□achats en magasins afin de comparer plus rapidement les prix, attention de ne pas vous connecter Ã un point dâ□□accÃ¨s inconnu non sÃ©curisÃ©. Un point dâ□□accÃ¨s non sÃ©curisÃ© permet aux cybercriminels de capturer toutes les donnÃ©es qui circulent de et Ã partir du hotspot afin dâ□□intercepter les logins et mots de passe, emails, les documents en piÃ¨ce jointe et autres informations personnelles et confidentielles.

Que faire : Si vous avez lâ□□envie de surfer sur le Net alors que vous Ãªtes en ville, allez dans des endroits familiers qui offrent des connexions sÃ©curisÃ©es par cÃ¢bles ou en Wi-Fi. Rappelez vous que les attaques de phishing peuvent survenir sur diffÃ©rents types de plateformes, que vous soyez sur votre ordinateur portable ou smartphone ; alors assurez vous de prendre toutes les prÃ©cautions nÃ©cessaires dÃ©crites ci-dessus.