Passer les fÃªtes sans Ãªtre piratÃ©
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 6/12/2017 14:30:00

Les ventes dans le commerce de dÃ©tail et sur les sites de e-commerce Ã lâ□□occasion du Black Friday ont atteint des sommets cette annÃ©e. Mais alors que les commerÃ§ants sâ□□attendent Ã des chiffres dâ□□affaires record et que les consommateurs recherchent avidement les meilleures affaires, les cyber criminels se prÃ©parent Ã une intense saison de piratage.

Saviez-vous par exemple quâ□□aux Etats Unis les attaques de phishing (hameÃ§onnage) augmentent de 336% autour de la fÃªte de Thanksgiving ?. Donc nâ□□attendez pas que des pirates rÃ©cupÃ¨rent votre numÃ©ro de carte de crÃ©dit pour agir, et protÃ©gez-vous avant de commencer vos achats avec les conseils qui suivent.

Mettez Ã jour votre logiciel de sÃ©curitÃ©. Avant de commencer vos achats, prenez le temps de renforcer la sÃ©curitÃ© de votre ordinateur.

Il doit Ãªtre Ã©quipÃ© dâ□□un logiciel firewall et antivirus, et assurez-vous que toutes les mises Ã jour disponibles ont Ã©tÃ© installÃ©es.

Evitez les fausses applications dâ□□enseignes de distribution. De plus en plus de pirates crÃ©ent de fausses applications mobiles et les hÃ©bergent sur lâ□□Apple Store et Google Play.

Ces applications peuvent voler vos donnÃ©es personnelles et vos numÃ©ros de carte de crÃ©dit, ou installer un logiciel espion sur votre smartphone.

Avant de tÃ©lÃ©charger toute application mobile vÃ©rifiez les apprÃ©ciations des utilisateurs.

MÃ©fiez-vous des emails frauduleux et des liens dâ□□hameÃ§onnage. Les pirates envoient des quantitÃ©s massives dâ□□emails avec de fausses publicitÃ©s, et lorsquâ□□ils cliquent sur les liens URL qui y figurent, les victimes se retrouvent sur des sites frauduleux.

Evitez des offres qui sont trop belles pour Ãªtre vraies. Ne cliquez sur aucune des Â« super affaires Â» que vous trouvez sur les rÃ©seaux sociaux.

Tout comme les emails frauduleux, les plupart des offres commerciales qui sont trop belles pour Ãªtre vraies le sont effectivement. Les pirates utilisent souvent Twitter et Facebook pour propager des liens malicieux. En fait, 30 millions de tweets malicieux sont envoyÃ©s chaque jour.

Restez sur des sites familiers. Lorsque vous recherchez les meilleures affaires sur le net, Ã©vitez de vous arrÃªter sur des sites qui ne vous sont pas familiers.

Certains criminels crÃ©ent de faux sites web qui paraissent lÃ©gitimes avec des adresses URL trÃ¨s proches de celles des sites officiels. Si vous entrez vos informations de carte de crÃ©dit sur un de ces sites, elles pourront facilement Ãªtre volÃ©es.

Cherchez le cadenas vert. Si vous trouvez une bonne affaire sur un site non familier, cherchez le cadenas vert Ã gauche de lâ□□adresse URL sur votre navigateur, et faites quelques recherches sur le site avant dâ□□acheter quoique ce soit. Pour plus de sÃ©curitÃ©, privilÃ©giez les processus dâ□□authentification en deux Ã©tapes de type 3D Secure.

Utilisez un porte-monnaie Ã©lectronique. Si le site propose cette option, utilisez toujours des porte-monnaie Ã©lectroniques tels que PayPal et Apple Pay pour Ã©viter que des sites malicieux ne rÃ©cupÃ¨rent vos informations de carte de crÃ©dit.

Si cette option nâ□□est pas disponible, utilisez une carte de crÃ©dit plutÃ´t quâ□□une carte Ã dÃ©bit immÃ©diat et vÃ©rifiez votre relevÃ© bancaire pour repÃ©rer toute fraude.

Â

Pascal Le Digol, Country Manager France de WatchGuard