G-Data : RemÃ¨de contre Les mauvaises habitudes de l'achat en ligne
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 9/12/2010 13:30:00

Ã lâ occasion des fÃªtes de fin dâannÃ©e, les Internautes vont multiplier les achats en ligne. La pratique est-elle sÃ»re ? Absolument ! Ã condition de mettre fin Ã quelques **mauvaises habitudes recensÃ©es par G Data Software**.

Les mauvaises pratiques qui pourraient gÃ¢cher NoÃ«l

1. Utiliser un systÃ¨me d'exploitation et un navigateur Internet obsolÃ¨tes.

Le risque : Les failles de sÃ©curitÃ© connues par les cybercriminels et non corrigÃ©es par lâutilisateur du systÃ¨me sont des portes dâentrÃ©e pour de potentiels dangers. Des logiciels malveillants peuvent Ãªtre insÃ©rÃ©s dans le systÃ¨me et peuvent rÃ©cupÃ©rer les donnÃ©es bancaires saisies lors de lâachat en ligne

La solution : vÃ©rifier sur Windows Update la disponibilitÃ© de mises Ã jour critiques et les installer. Mettre Ã jour son navigateur internet via le menu Â« Ã propos Â» ou par mise Ã jour automatique.

2. Cliquer sur des offres allÃ©chantes contenues dans des e-mails dâexpÃ©diteurs inconnus.

Le risque : une offre trop belle pour Ãªtre vraie est, par essence, trop belle pour Ãªtre vraie. Ã lâapproche de NoÃ«l, les cybercriminels multiplient les emails dâhameÃ§onnage dans le but de voler les donnÃ©es bancaires des internautes. CrÃ©er de faux sites de commerce en ligne est une des stratÃ©gies employÃ©es.

La solution : ne pas cliquer sur des liens contenus dans des emails. Activer les filtres anti hameÃ§onnage des navigateurs Internet ou dâune solution de sÃ©curitÃ©.

3. Acheter en ligne Ã partir dâ□□un ordinateur public ou en utilisant une connexion wifi non sÃ©curisÃ©e.

Le risque : les ordinateurs des cybercafÃ©s ne sont pas toujours suffisamment protÃ©gÃ©s. Lors de lâ□□achat en ligne, lâ□□internaute saisie des donnÃ©es personnelles et bancaires qui peuvent Ãªtre rÃ©cupÃ©rÃ©es par un cybercriminel. Le risque est identique lors dâ□□une connexion Ã un rÃ©seau wifi public non protÃ©gÃ© : les donnÃ©es transmises peuvent Ãªtre interceptÃ©es par un utilisateur mal intentionnÃ©.

La solution : en situation de mobilitÃ©, il est prÃ©fÃ©rable dâ□□effectuer des opÃ©rations bancaires en utilisant une connexion Internet via clÃ© 3G.

4. Saisir ses donnÃ©es de carte bancaire sans vÃ©rifier les dispositifs de sÃ©curitÃ© mis en place par le navigateur Internet.

Le risque : Des donnÃ©es confidentielles saisies dans un formulaire non sÃ©curisÃ© (protocole HTTP) peuvent facilement Ãªtre rÃ©cupÃ©rÃ©es par un logiciel malveillant installÃ© sur un ordinateur infectÃ©. Lâ□□utilisation dâ□□un protocole non sÃ©curisÃ© sur un site marchand doit aussi alerter sur lâ□□authenticitÃ© de ce site.

La solution : vÃ©rifier lors de lâ□□achat que tous les dispositifs de sÃ©curitÃ© sont prÃ©sents : le cadenas et l'abrÃ©viation Â« HTTPS Â» devant l'adresse du site Internet.

5. Ne pas utiliser de solution antivirus Ã jour.

Le risque : Un logiciel malveillant dans un ordinateur se dÃ©tecte rarement au premier coup dâ□□Å□il. Souvent trÃ¨s discrets, certains scrutent les moindres faits et gestes de lâ□□utilisateur et enregistrent toutes les informations intÃ©ressantes. Sans antivirus Ã jour, dÃ©tecter et bloquer ces indÃ©sirables est impossible.

La solution : Pourquoi ne pas profiter de cette pÃ©riode de NoÃ«l pour Ã©quiper son ordinateur dâ□□une solution de sÃ©curitÃ©â□¦