

G-Data : Dangers sur Internet : se protéger et les combattre

Sécurité

Posté par : JPilo

Publié le : 14/6/2010 0:00:00

G Data Software AG détaille les solutions de protection et les moyens pour prendre part au combat.

Rendre Internet plus sûr est l'affaire de tous. En sécurisant son ordinateur, chacun peut éviter qu'il ne soit contaminé ou utilisé à des fins malveillantes (intégrés dans des réseaux Botnet par exemple). Mais ce premier pas peut aussi être suivi d'un autre : en utilisant les plateformes de signalement et de collectes nationales, chaque utilisateur a la possibilité de combattre la cybercriminalité. Les bonnes pratiques pour se protéger



1. Gardez votre système d'exploitation à jour, ainsi que toutes les applications installées. Ceci réduit le risque d'utilisation de failles de sécurité lors de la navigation sur Internet.

2. Dans Windows, utilisez par défaut un compte utilisateur standard. Comparé à un compte administrateur, l'utilisation d'un compte standard permet de réduire de près de 90 % l'exploitation des failles Windows.

3. Fuyez les cracks, Keygen et autres logiciels piratés disponibles gratuitement sur Internet. Tous ces contenus illégaux renferment souvent des fichiers nuisibles. Sur les réseaux peer to peer, en moyenne 8 programmes diffusés illégalement sur 10 intègrent des codes malveillants.

4. Ne cliquez jamais sur un lien intégré dans un email provenant d'un organisme financier, d'un État ou un site marchand, surtout s'ils vont inviter à communiquer vos coordonnées. En France, PayPal.fr est l'organisme le plus souvent ciblé (près de 70 % des courriels d'hameçonnage).

5. L'argent facile et légal n'existe pas, sur Internet pas plus que dans la vie de tous les

jours. Un « travail » où il suffit de réaliser quelques transferts d'argent pour être rémunéré est un travail douteux. Ne succombez pas aux promesses trop alléchantes.

6. Utiliser un antivirus intégrant un filtre HTTP et garder le programme à jour. Seul un antivirus peut détecter et bloquer des fichiers infectés. N'importe quel site Internet, n'importe quel fichier, même bureautique, peut contenir du code malveillant.

7. Activez un filtre anti-hameçonnage dans le logiciel de messagerie ou dans le navigateur Internet. Ces options permettent de bloquer une grande partie des tentatives d'escroqueries.

Les adresses pour combattre la cybercriminalité

1. Lutte contre les dérives de l'Internet : internet-signalement.gouv.fr

Cette base de collecte est accessible à tout internaute ayant connaissance de contenus ou de comportements illicites sur le Web. Le domaine de compétence de cette base est très étendu : Pédophilie ou corruption de mineur, incitation à la haine raciale ou provocation à la discrimination, menaces ou incitation à la violence, trafic, mise en danger de personnes, incitation à commettre des infractions, injure ou diffamation, escroquerie. Il suffit de quelques clics pour signaler un abus. La requête est ensuite traitée par les services de police compétents.

2. Lutte contre le spam et l'hameçonnage : signal-spam.fr

Cette plate-forme nationale met à disposition des internautes un système de signalement de spam. Deux méthodes de signalement sont possibles. Pour les utilisateurs de messagerie Internet (webmail), le courriel indésirable peut être signalé via un formulaire à partir du site internet : signal-spam.fr. Pour les utilisateurs de clients de messagerie, le signalement peut être réalisé à l'aide d'un plug-in à installer dans Outlook (2003 ou 2007) ou Thunderbird 2.0.

3. Lutte contre le spam et l'arnaque SMS : 33700-spam-sms.fr

Le spam et l'arnaque SMS sont de plus en plus courants. Une plateforme instituée par le gouvernement en partenariat avec la Fédération française des télécoms est disponible pour combattre ces pratiques. Un utilisateur qui reçoit un SMS frauduleux peut transférer ce message au 33700. Après validation de l'alerte (l'utilisateur doit répondre à un SMS de retour pour valider sa transmission) l'abus signalé est étudié. S'il est établi, les opérateurs sont prévenus par la plateforme et peuvent mettre très rapidement fin au service. Dans les cas les plus graves, les informations sont transmises aux services de police.