

Les 8 conseils du Laboratoire de Panda Security pour un été en toute sécurité

Paris, le 17 juillet 2009

Passer l'été à se changer les idées, c'est ce que tout le monde souhaite. Mais n'oubliez pas, les cybercriminels ne prennent pas de vacances. Souvent, l'été, les ordinateurs sont utilisés pour des activités plus orientées vers les loisirs. L'utilisation de services tels que les chats, les jeux en ligne ou les achats en ligne augmentent car les utilisateurs ont plus de temps libre que d'habitude. Les enfants ont également tendance à passer plus de temps devant leur ordinateur pendant les vacances.

Les cybercriminels vont alors essayer de profiter de toutes ces victimes potentielles.

Voici une série de recommandations pour vous aider à protéger votre ordinateur cet été.

- **Faites plus attention à vos e-mails**, c'est un canal fréquemment utilisé pour la diffusion de menaces, telles que les attaques de phishing ou autres escroqueries contenues dans les spams. Typiquement à cette période de l'année, des vagues de spams émergent pour vous offrir des vacances à moindre coût. Ces messages demandent furtivement aux utilisateurs de révéler des données confidentielles ou les incitent à télécharger des informations, qui sont en réalité des fichiers infectés. Par conséquent, il est préférable d'ignorer tous les e-mails dont vous ne connaissez pas l'expéditeur.

- **Installez rapidement les derniers patchs de sécurité pour vos installations.** Les cybercriminels lancent fréquemment des attaques qui exploitent les failles dans la sécurité des programmes couramment utilisés. Les développeurs créent constamment des patchs de protection capables de résoudre les problèmes détectés. Si votre application ne vous avertit pas de la disponibilité de ces mises à jour, vous devez aller occasionnellement sur la page officielle du produit pour vérifier si de nouveaux patchs ont besoin d'être installés. Le mieux est de mettre à jour les applications de votre ordinateur juste avant de partir et au retour de vos vacances.

- **Ne téléchargez pas de programmes sur des sites Internet douteux, ils pourraient être infectés.** La période estivale voit une augmentation du nombre de téléchargements. Il est important d'accorder une attention particulière à ce que vous téléchargez sur Internet. Plus précisément, vous devriez scanner tous les téléchargements avant de les lancer, d'autant que les logiciels malveillants sont souvent déguisés dans des fichiers comme les films, les séries, etc. pour tromper les utilisateurs.

- **Faites attention aux informations que vous entrez dans vos réseaux sociaux. Assurez-vous que vous ne publiez pas des détails comme le jour de votre départ en vacances, surtout si votre adresse est disponible sur ces mêmes réseaux sociaux.**

- **Eteignez votre routeur.** Cela vous protégera des autres utilisateurs connectés à votre réseau, qui ont peut-être de mauvaises intentions pendant votre absence. Par exemple, quelqu'un pourrait se connecter à votre réseau et télécharger un code malveillant qui pourrait rester sur le réseau jusqu'à ce que vous allumiez votre ordinateur ce qui par conséquent l'infecterait.

- **Prenez des précautions si vous utilisez des ordinateurs publics.** Pendant les vacances, beaucoup d'internautes vont dans des cybercafés pour lire leurs e-mails, chatter avec des amis, rester en contact avec leur réseau social, etc. Si c'est votre cas, vous devez prendre des précautions. Premièrement désactivez toutes les options de sauvegarde de mot de passe quand vous vous connectez à vos comptes à partir d'un ordinateur public. Cela évitera au prochain utilisateur de l'ordinateur d'accéder à vos comptes. Assurez-vous également que l'ordinateur que vous utilisez ne soit pas infecté. Au premier signe suspect (pop-ups, mauvais fonctionnement...), arrêtez son utilisation. Enfin, **n'utilisez jamais d'ordinateur public pour vos opérations bancaires.**

- **Utilisez des programmes de contrôle parental.** Pendant les vacances d'été, les enfants vont sans doute utiliser l'ordinateur plus que d'habitude, et peut-être même un autre ordinateur. C'est pourquoi il est si important de leur enseigner comment naviguer sur Internet sans danger. C'est une bonne idée de fixer des créneaux horaires pour l'accès à Internet, de garder un oeil sur eux pendant qu'ils naviguent et de bloquer l'accès à certaines pages ou contenus qui leur seraient inappropriés. Ceci dit les parents ne seront pas toujours derrière eux pour vérifier comment ils utilisent le Web, il est donc conseillé d'installer un programme de contrôle parental, un outil qui vous aidera à définir quelles pages Web vos enfants peuvent ou ne peuvent pas aller voir.

- **Assurez-vous que votre ordinateur ait une solution installée de mise à jour et d'activation d'antivirus. Il y a des programmes antivirus disponibles gratuitement sur le Web, tel que Panda Cloud Antivirus, que vous pouvez télécharger sur www.cloudantivirus.com.**

À propos de Panda Security

Panda Security est un développeur international de premier plan de solutions de sécurité, avec des millions de clients dans le monde et des produits localisés en une vingtaine de langues. La mission de Panda est de garder les systèmes d'informations de nos clients à l'abri des menaces informatiques, en leur apportant la meilleure protection possible et en consommant le moins de ressources.

Chaque jour, des milliers de nouveaux codes malveillants sont créés. Pour faire face à cette menace, **Panda Security** a développé un modèle de sécurité innovant et unique sur le marché qui analyse et classe automatiquement des milliers de malwares chaque jour. Ce modèle, **l'Intelligence Collective Antimalware**, permet aux solutions de sécurité Panda d'apporter une protection contre davantage de menaces que les solutions concurrentes.