Sécurité : les 7 péchés capitaux de l'été - selon Norman

L'été, entre deux longueurs de piscine, il est facile d'oublier les risques de la sécurité informatique. Or, les virus et autres codes malfaisants ne prennent pas de congés… Alors, quelles préventions?

L'éditeur Norman a répertorié « 7 péchés » à ne pas commettre:

1. Relâcher les mises à jour de protection

Avant de partir, il faut revérifier que l'on a distribué les versions les plus récentes des logiciels antivirus, antispam et antispywares, et que ces programmes continueront à être mis à jour pendant la période des congés.

2. Retarder les correctifs du système d'exploitation

Lorsque l'on se connecte à Internet, il faut accorder un moment à la mise à jour et à la recherche des correctifs du système d'exploitation. Les exploitations sans délai des vulnérabilités (zero day) deviennent incroyablement communes, et les éditeurs, dont Microsoft, proposent des correctifs d'urgence lorsqu'ils estiment qu'une telle exploitation est critique.

3. Négliger le paramétrage des pare-feu

Vérifiez que les pare-feu personnels sont aussi sécurisés que possible, et que seules quelques connexions sont autorisées. Rappel: si l'on ouvre les connexions menant au système et si la sécurité n'est pas assez stricte ou non mise à jour, quelqu'un peut accéder au système et l'employer frauduleusement afin de piller des informations de toutes sortes.

4. Ouvrir de nouvelles connexions Internet sans précautions

Rappeler que si l'on se connecte à un réseau WiFi ouvert, la passerelle Internet à laquelle se connecte le WiFi peut intégrer une application « proxy » qui stockera l'intégralité du trafic Internet ainsi que les mots de passe employés. Il faut donc être très prudent lors de la soumission d'informations avec des connexions de ce type. Le meilleur moyen d'éviter ce problème est d'employer des transmissions sécurisées (SSL/https)

5. Utiliser des éléments partagés d'un réseau

Lors des connexions à Internet par câble, modem ou WiFi, vérifier que l'on a ouvert aucun partage. Chaque élément partagé est accessible aux autres personnes travaillant sur le même réseau. Cette possibilité est généralement désactivée par les fournisseurs d'accès lors d'une connexion directe (par exemple, par modem ou ADSL).

Cependant, ne pas oublier que le cas d'une connexion par câble ou WiFi est particulier : les routeurs/commutateurs intermédiaires ne sont pas contrôlés par le fournisseur d'accès et peuvent être configurés (intentionnellement), ce qui autorise l'accès aux dossiers partagés et permet leur consultation ou l'ajout d'éléments.

6. Activer en permanence sa connexion Bluetooth

La plupart des ordinateurs portables récents disposent de capacités Bluetooth. Mieux vaut rappeler que cette connexion sans fil peut devenir un hôte réseau qui permettra aux personnes de son voisinage d'examiner son système à son insu. Donc, mieux vaut conseiller de désactiver Bluetooth.

7. Vérifier ses comptes bancaires dans des cybercafés

Si l'on prévoit d'utiliser un ordinateur dans un cybercafé, prudence surtout si l'on veut vérifier l'état de son compte bancaire. L'identité de connexion et le mot de passe sont capturés et, si l'on effectue un transfert de foncs, le numéro de transaction peut également être enregistré.

A qui veut contrôler son compte en banque depuis un cybercafé, il faut recommander de créer un nouveau document de texte comportant toutes les lettres de l'alphabet en majuscules et en minuscules. Ensuite, copier et coller les caractères nécessaires au mot de passe avec la seule souris. Ainsi, les détecteurs de frappe auront plus de difficultés à repérer le numéro de compte ainsi que le mot de passe. Et lorsque l'on a terminé, procéder à l'effacement sécurisé des fichiers Internet et du document de texte.

Et bon congés!