Dix règles d'or pour protéger votre identité et autres informations personnelles

Lorsque vous utilisez l'e-mail ou la messagerie instantanée, faites des achats ou exécutez des transactions bancaires en ligne, il vous arrive souvent de communiquer des informations personnelles — p. ex. des adresses, des numéros de téléphone, des numéros de compte, des noms d'utilisateur et des mots de passe. Malheureusement, vous courez le risque qu'une personne mal intentionnée s'empare de ces informations personnelles, pour éventuellement les exploiter en usurpant votre identité, ou utilise votre ordinateur comme rampe de lancement d'autres attaques.

Pour protéger votre identité et vos informations personnelles, suivez ces quelques conseils :

1. **Procurez-vous un logiciel de sécurité fiable et multiniveau.** Cherchez à vous procurer un logiciel de sécurité complet et multiniveau qui vous protège contre les virus, les logiciels espions (spywares), les logiciels publicitaires (adwares), les pirates, le courrier indésirable, les escroqueries par phishing et l'usurpation d'identité. Portez votre choix sur une marque connue et fiable, comme McAfee®.

2. **Placez toujours un pare-feu entre votre ordinateur et Internet.** Un pare-feu offre une couche de sécurité supplémentaire entre votre ordinateur et Internet ; il empêche que des pirates dérobent des informations d'identité, détruisent vos fichiers ou utilisent votre ordinateur pour en attaquer d'autres.

3. **Utilisez un ordinateur sécurisé.** Les pirates peuvent facilement récupérer les données sensibles envoyées via une connexion Internet non sécurisée. Si vous devez transmettre des informations confidentielles ou effectuer une transaction en ligne, utilisez un ordinateur dont vous savez qu'il est sécurisé et souvenez-vous que la sécurité informatique comporte des multiples facettes. Certains ordinateurs bénéficient d'une sécurité minimale alors que d'autres, jouissent d'une protection complète.

4. **Méfiez-vous des escroqueries par phishing.** Les arnaques utilisant la technique du phishing ont recours à des e-mails frauduleux et à des faux sites web à l'apparence légitime pour inciter des utilisateurs trop confiants à révéler des informations de connexion ou de compte privées. Même si votre ordinateur est sécurisé, le risque d'accéder, sans le savoir, à un site web malveillant est bel et bien réel. Les sociétés légitimes ne vous demandent jamais de mettre à jour des informations personnelles par e-mail. Vérifiez toujours les adresses web avant d'envoyer des informations personnelles.

5. **Sécurisez votre réseau sans fil.** Les risques sont accrus si vous accédez à Internet via un réseau Wi-Fi. Dans la mesure où les ondes radio de votre réseau sans fil traversent les murs, un pirate équipé d'une simple antenne pourrait vous attaquer à plusieurs kilomètres de distance pour voler vos informations ou utiliser votre réseau sans fil pour ses propres communications. Pensez à sécuriser explicitement votre connexion Wi-Fi.

6. **N'installez jamais des programmes potentiellement indésirables, tels que des logiciels espions (spywares) ou logiciels publicitaires (adwares).** De nombreux programmes gratuits, téléchargés à partir d'Internet et en apparence inoffensifs, sont conçus à des fins malveillantes et susceptibles d'enregistrer vos frappes, de suivre vos connexions à Internet, de transmettre vos informations confidentielles ou de rediriger votre navigateur vers des sites web factices. Dans certains cas, il suffit parfois de cliquer sur un lien publicitaire d'un site web pour lancer leur installation.

   Les logiciels de sécurité bloquent l'installation de ces programmes. N'installez que les programmes qui vous sont familiers, dont vous connaissez par ailleurs le site web d'origine, et après avoir lu le contrat de licence utilisateur final dans son intégralité.

7. **Ne répondez pas à des e-mails en chaîne.** Même si votre ordinateur est sécurisé, certains e-mails en chaîne envoyés par des amis peuvent vous demander des informations personnelles. Ne téléchargez pas des fichiers envoyés par des proches ou des connaissances à moins d'être certain de la fiabilité de leur contenu.

8. **Surveillez votre historique bancaire et vos extraits de compte, faites preuve de circonspection.** Vérifiez au moins une fois par an votre historique bancaire. C'est la meilleure façon de s'assurer que personne n'utilise vos informations financières personnelles à votre insu. Consultez le site de support Gateway pour découvrir les conseils les plus récents en matière de sécurisation des ordinateurs ou celui de la FTC (Federal Trade Commission) pour connaître les dernières tendances concernant l'usurpation d'identité.

9. **Surveillez l'utilisation d'Internet par vos enfants.** Limitez le temps qu'ils passent en ligne. Installez un logiciel de contrôle parental qui vous permet de surveiller les activités en ligne de vos enfants et de filtrer ou de bloquer leur accès à des sites web indésirables et le partage d'informations personnelles.

10. **Effectuez des sauvegardes régulières des données critiques.** Conservez une copie des fichiers importants sur un support amovible, par exemple des disques ZIP ou des CD-ROM enregistrables (CD-R ou CD-RW). Utilisez des outils de sauvegarde, si vous en possédez, et conservez les disques de sauvegarde dans un endroit sûr afin de pouvoir les récupérer en cas d'urgence.

McAfee
Tour Franklin, La Défense 8
2042 Paris La Défense Cedex
France
+33 1 47 62 56 00
www.mcafee.fr