Zeitschrift: Générations plus : bien vivre son âge
Herausgeber: Générations
Band: - (2014)
Heft: 58

Rubrik: Votre argent

IdeaGU

Ma banque sur internet, c'est risqué?

«Quels sont les dangers de faire mes paiements et autres opérations avec mon ordinateur?»

Marie-France, Neuchâtel

Fabrice Welsch
Directeur Prévoyance & conseils financiers BCV

Quel que soit le canal, le risque zéro n'existe pas. Toutefois, en matière bancaire, le traitement des données par internet, plus communément appelé e-banking, s'est équipé d'un certain nombre de sécurités pour éviter le vol et l'utilisation frauduleuse d'informations. Mais cela ne dispense pas l'utilisateur de faire preuve de prudence et de vigilance, en adoptant un regard critique sur les demandes qui peuvent lui être envoyées et, aussi, d'équiper son ordinateur des protections usuelles contre les actions malfaisantes telles que décrites ci-dessous.

Les virus

Conçus pour se reproduire et infecter votre ordinateur, les virus peuvent avoir une action néfaste ou détruire toutes les données de votre ordinateur. Pour s'en protéger, il y a les antivirus* qui les détectent et les éliminent en grande partie, sans toutefois pouvoir jamais atteindre 100% d'efficacité à tout moment.

Le phishing (ou hameçonnage)

C'est la technique de la pêche aux mots de passe: le client reçoit un courriel semblant provenir de sa banque (adresse, logo, signature, etc.) qui l'informe qu'il doit cliquer sur le lien proposé afin de confirmer certaines informations personnelles. Il est redirigé sur un faux site ressemblant à s'y méprendre à celui de sa banque. Il lui est demandé d'entrer ses données personnelles et confidentielles, comme le numéro d'utilisateur, le mot de passe ou un code d'accès. Cela peut aussi se faire par téléphone!

Ne répondez jamais à ce type de courriels ou de téléphone et ne cliquez pas sur les liens proposés. Passez toujours par le site de votre banque pour vous connecter. Ne communiquez à personne votre mot de passe ou vos codes d'accès, car la banque n'a

pas à les connaître. Lorsque vous vous connectez au site de votre banque, il y a généralement plusieurs contrôles de sécurité pour vous protéger au mieux. A la BCV, par exemple, il y a un numéro d'utilisateur, un mot de passe et un numéro aléatoire transmis par SMS au moment de la demande de connexion. Lorsque vous effectuez des paiements que vous n'avez pas l'habitude de faire ou lorsque le destinataire est nouveau, le système vous demandera, en outre, de valider une fois de plus le paiement.

Le détournement de session

Le détournement de session consiste à intercepter certaines informations techniques au moment de votre connexion sur le site d'e-banking. Lorsque vous vous êtes correctement identifié dans votre système d'e-banking, votre ordinateur est reconnu par le système au moyen de certaines informations techniques. Le détournement de session va les intercepter et les utiliser pour se connecter à son tour au système d'e-banking, afin d'effectuer des opérations à votre nom. Ce type d'attaques peut provoquer des situations inhabituelles sur l'ordinateur: messages d'erreur, dérangements lors de la session ou ouverture d'une fenêtre vide à la fermeture de la session.

Pour s'en protéger, il faut éviter de vous connecter sur votre site bancaire depuis un lieu public ou un réseau sans fil que vous ne connaissez pas; il est recommandé d'utiliser un logiciel antivirus* et d'installer un pare-feu** pour empêcher des tiers de se connecter à votre ordinateur.

En sus, pour garantir la confidentialité des données, celles qui sont échangées pendant la session d'e-banking sont cryptées, le système est bloqué en cas de mot de passe erroné saisi un certain nombre de fois et il est déconnecté en cas de non-utilisation pendant un certain laps de temps.

***Antivirus:** logiciel conçu pour identifier, neutraliser et éliminer des programmes malveillants pouvant, par exemple, modifier ou supprimer des fichiers sur l'ordinateur contaminé.
****Pare-feu:** outil informatique conçu pour éviter le piratage informatique en filtrant les flux de données selon le niveau de confiance accordé.

Les 5 règles de base pour protéger son ordinateur

1. Sauvegarder régulièrement ses données et les conserver dans un lieu sûr, déconnecté du réseau internet.
2. Utiliser un logiciel antispam pour filtrer les courriels indésirables.
3. Installer un antivirus et un pare-feu.
4. Ne pas accéder à internet depuis le compte administrateur de son ordinateur, mais depuis un simple compte utilisateur qui, en cas d'exécution de virus, ne permet pas l'accès aux droits de l'administrateur et donc à tout le système.
5. Ne pas cliquer sur n'importe quel lien, notamment sur les liens reçus dans votre messagerie.

Les smartphones face au défi sécuritaire

D'ici à cinq ans, plus de la moitié des paiements à distance devrait s'effectuer via les tablettes et, surtout, les téléphones portables multifonctions ou smartphones, qui permettent de surfer sur internet. Comme pour l'ordinateur, ces derniers doivent relever un défi de taille, celui de la sécurité des transactions.

Facilité, rapidité et gratuité ont été les clés du succès des transactions via l'ordinateur. Les smartphones y ajoutent la mobilité grâce au m-paiement (paiement mobile) ou au porte-monnaie électronique (stockage d'argent sans lien avec un compte bancaire), promis à un bel avenir. Le téléphone portable est le tout-en-un qui permet de payer, en quelque sorte, «quand je veux et où je veux». Il profite également de l'évolution du comportement des clients, notamment des plus jeunes, amateurs de nouvelles technologies.«Le talon d'Achille des smartphones, comme des ordinateurs, est le système d'exploitation, mais d'autres dangers découlent de leurs principaux atouts», rappelle toutefois Bogdan Iancu, responsable Online et Mobile Banking à la BCV. «La mobilité implique en effet la connexion aux réseaux wi-fi publics qui n'offrent guère de garanties en matière de sécurité. On peut se protéger en se dotant d'antivirus et en téléchargeant les logiciels cryptés, aux demandes d'identification accrues, fournis par les partenaires financiers.»

Un autre fléau, le vol. D'autant plus ennuyeux si le portable est équipé pour le m-paiement et peut donc être utilisé comme un porte-monnaie ou une carte de crédit. Dans ce cas de figure, les pistes s'orientent vers la protection de l'appareil. Parmi les parades figurent l'identification par empreintes digitales ou des puces qui cryptent les communications et les données stockées dans l'appareil.Les spécialistes s'accordent toutefois à dire qu'aucune de ces mesures n'est la panacée. Ils rappellent que rien ne vaut la vigilance et qu'il importe de suivre les conseils de prévention recommandés par les établissements financiers.