Zeitschrift: Générations
Herausgeber: Générations, société coopérative, sans but lucratif
Band: - (2019)
Heft: 109

Rubrik: Argent : les risques de l'e-banking

Les risques de l'e-banking

« Quels sont les risques de traiter ses affaires bancaires par internet, sur son ordinateur ou sur son smartphone ? »

ÉRIC, ORBE (VD)

FABIEN MOOSER,
Sous-directeur Sécurité de l'information BCV

Quel que soit le canal utilisé, le risque zéro n'existe pas. Toutefois, en matière bancaire, le système de traitement des données par internet, plus communément appelé «e-banking», a été équipé d'un certain nombre de dispositifs de sécurité pour éviter le vol et l'utilisation frauduleuse d'informations. L'utilisateur doit également s'équiper des mesures de protection recommandées et faire preuve de bon sens en utilisant son ordinateur face aux demandes qui peuvent lui être formulées.

LES RISQUES LIÉS À L'UTILISATION D'INTERNET

LES VIRUS ET AUTRES LOGICIELS MALVEILLANTS

Conçus pour se reproduire et infecter votre ordinateur, les virus et autres logiciels malveillants peuvent avoir une action néfaste ou détruire toutes les données de votre ordinateur. Ils peuvent aussi permettre à une personne malveillante de prendre le contrôle de votre ordinateur (cas particulier du cheval de Troie).

Afin de réduire le risque d'infection, il est recommandé d'installer un antivirus qui les détectent et les éliminent en grande partie. Les versions gratuites à télécharger remplissent bien leur rôle.

LE PHISHING (OU HAMEÇONNAGE)

C'est la technique de la pêche aux mots de passe : le client reçoit un courriel semblant, par exemple, 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. Pour s'en protéger, ne répondez jamais à ce genre de courriels 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. La banque ne prend d'ailleurs jamais contact avec ses clients par e-mail ou par téléphone pour demander des informations en lien avec les mots de passe ou les numéros de compte.

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, en plus, un facteur d'authentification qui se matérialise par SMS, smartID (votre smartphone devient une clé unique et personnalisée qui autorise votre connexion sur ordinateur en scannant un code QR) ou calculette. Lorsque vous faites des paiements avec un nouveau bénéficiaire, le système vous demandera, en outre, de valider une fois de plus qu'il s'agit du bon bénéficiaire.

LE DÉTOURNEMENT DE SESSION

Lorsque vous vous êtes correctement authentifié dans votre système d'e-banking, votre ordinateur est reconnu par le système au moyen de certaines informations techniques. Le détournement de session consiste à essayer de les intercepter pour se connecter à son tour au système d'e-banking, afin d'effectuer des opérations à votre nom. Ce genre d'attaques peut provoquer des situations inhabituelles sur l'ordinateur : messages d'erreur, temps d'attente étrangement long, 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 et, si votre application a un comportement inhabituel, n'hésitez pas à prendre contact avec votre banque.

ARNAQUES ET ESCROQUERIES

Les escroqueries sont variées, mais présentent un dénominateur commun: le criminel cherche à gagner la confiance de sa cible, afin de lui soutirer

Illustration: Helen Tilbury

un maximum d'argent. Les aînés sont plus souvent victimes d'arnaques de type «faux neveu», «faux héritage» ou «gain à la loterie». Généralement, la victime doit payer à l'avance un «impôt anticipé» ou des «frais de dossier». Dernièrement sont apparues des variantes plus sophistiquées, sous forme de chantage émotionnel: l'escroc prétend détenir des informations sensibles ou des photos compromettantes et exige de l'argent pour ne pas les divulguer. Il s'agit alors de garder la tête froide et d'évaluer la plausibilité des dires avant toute action.

LES SMARTPHONES ET LA SÉCURITÉ

Facilité, rapidité et gratuité ont été les clés du succès des transactions via l'ordinateur. Les smartphones et les tablettes y ajoutent la mobilité grâce au paiement mobile ou au porte-monnaie électronique (stockage d'argent sans lien avec un compte bancaire). Mais la mobilité implique la connexion aux réseaux wifi publics qui n'offrent guère de garanties en matière de sécurité. Mieux vaut donc les éviter, dans la mesure du possible.

Un autre fléau, le vol. D'autant plus ennuyeux si le portable est équipé pour le paiement mobile, 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 notamment l'identification par empreintes digitales ou la reconnaissance faciale.

BON À SAVOIR

1. **Antivirus et pare-feu sont des outils incontournables pour protéger votre ordinateur.**
2. **Au moindre doute, mieux vaut interrompre une transaction et prendre contact avec sa banque.**
3. **Pour vous connecter à votre e-banking, privilégiez un réseau que vous connaissez. Evitez les accès gratuits dans les lieux publics.**
4. **Pour vous connecter à votre e-banking, privilégiez l'utilisation d'un appareil que vous connaissez. Evitez les ordinateurs publics, comme dans les hôtels.**
5. **Retrouvez les «Recommandations de sécurité relatives à l'utilisation d'internet» sur www.bcv.ch**