SwissBanking

Septembre 2009

Secure e-Banking

1 e-banking en toute sécurité

L'e-banking est un moyen de communication établi et économique entre la clientèle privée ou commerciale et sa banque. Il offre des avantages aux deux parties. D'une part, le client ne doit plus se rendre à la banque pour effectuer un virement ou interroger le solde de son compte. Ces services de base sont en permanence à sa disposition en ligne, indépendamment des horaires d'ouverture de la banque. D'autre part, la banque dispose d'un instrument de communication lui permettant de s'adresser au client à tout moment. Ainsi, l'e-banking contribue à améliorer la qualité de la relation d'affaires.

Internet ne présente toutefois pas que des avantages; en effet, divers risques en matière de sécurité sont également liés à l'utilisation de l'e-banking. Citons par exemple la lecture non autorisée, la modification ou la suppression de données lors des transmissions, ainsi que l'obtention frauduleuse de données par des personnes non-autorisées, au moyen de faux prétextes.

Ce document s'adresse aux clients e-banking et a pour objectif de souligner les risques en matière de sécurité et d'indiquer les mesures à prendre afin de lutter contre les menaces et dangers les plus courants sur Internet.

L'utilisation de l'e-banking en toute sécurité est garantie dès lors que les clients connaissent suffisamment bien les menaces qui existent afin de lutter conjointement avec leur banque contre la criminalité croissante sur Internet.

Afin de se protéger des risques lors de l'utilisation de l'e-banking, il est recommandé à chaque utilisateur d'adopter un comportement fondamentalement prudent et de contrôler régulièrement ses mouvements de compte. Si le client soupçonne qu'il a été victime de criminels sur Internet, il lui est conseillé de faire bloquer l'accès en ligne à son compte bancaire, et de signaler immédiatement à sa banque les transactions dont il n'a pas connaissance.

2 Dangers et menaces sur Internet

Les dangers et les menaces sur Internet font l'objet de changements continuels et souvent très rapides. Parmi les menaces les plus fréquentes sur Internet, on peut mentionner: virus, vers, chevaux de Troie, hameçonnage (*phishing*), infection par «*drive-by download*» et *pharming*. Vous trouverez ci-après davantage d'explications au sujet de ces termes ainsi que des indications sur la manière de faire face à ces menaces.

2.1 Virus

Les virus ont des caractéristiques similaires aux virus responsables de maladies; ils peuvent se répandre par eux-mêmes et ont le potentiel de causer des dégâts considérables. Un virus inoffensif peut modifier les contenus de fichiers et au pire des cas, conduire à l'effacement complet du disque dur. Les virus accèdent au disque dur de l'ordinateur par le biais des documents attachés aux e-mails ou via des fichiers infectés téléchargés à partir d'Internet. Une fois activés, ils peuvent se propager très rapidement par e-mail ou par Internet.

2.2 Vers

Les vers génèrent des dommages similaires. Il s'agit toutefois de programmes autonomes, c'est-à-dire qu'ils n'ont pas besoin de programme hôte pour se reproduire. Ils utilisent plutôt les lacunes de sécurité ou des erreurs de configuration des systèmes d'exploitation ou des applications (e-mail, Internet), pour se propager de manière autonome d'ordinateur à ordinateur.

2.3 Chevaux de Troie

Les chevaux de Troie sont des programmes - souvent téléchargés depuis Internet - qui, de manière larvée, exécutent des actions préjudiciables sur un ordinateur, sans que l'utilisateur ne s'en rende compte. L'objectif de la plupart des chevaux de Troie est d'espionner les données sensibles (p. ex. les mots de passe) et de les envoyer ensuite au propriétaire dudit cheval de Troie, voire de détourner directement les transactions. Un cheval de Troie permet à son propriétaire d'accéder de manière non autorisée à un ordinateur inconnu et d'en prendre

ainsi le contrôle à distance. Les chevaux de Troie se présentent en règle générale à l'utilisateur comme des applications ou des fichiers utiles.

2.4 Hameçonnage (*phishing*)

Le mot *phishing* (hameçonnage) se compose des mots anglais *password* (mot de passe) et *fishing* (pêche). Via l'hameçonnage, des fraudeurs demandent aux utilisateurs d'actualiser ou de ressaisir leurs données d'accès confidentielles pour l'e-banking sur le site Internet de leur établissement bancaire. Cette pratique peut être réalisée à l'aide d'e-mails ou de sites Internet manipulés; elle a pour but de pirater les données confidentielles des utilisateurs telles que données d'accès pour l'e-banking ou la situation du compte.

2.5 Infection par «drive-by download»

Une infection par «*drive-by download*» correspond à l'infection d'un ordinateur par un logiciel malveillant (*malware*), lors de la simple visite d'un site Web. Les sites concernés contiennent dans bien des cas des offres sérieuses, mais ont été contaminés pour la diffusion de logiciels malveillants. Les criminels infiltrent en effet des codes dommageables sur le site Web et il suffit d'une navigation sur le site en question pour infecter un ordinateur.

2.6 Pharming

Le *pharming* est une technique de piratage informatique visant à rediriger l'utilisateur sur un site Web falsifié lors de la connexion à Internet. L'utilisateur saisit une adresse Internet correcte dans son navigateur (*browser*), mais il est toutefois redirigé vers un site Web falsifié.

3 Mesures de protection e-banking

Il est recommandé à l'utilisateur d'ouvrir uniquement les e-mails de personnes ou d'entreprises qu'il connaît, et de n'ouvrir aucun document annexé si l'expéditeur lui est inconnu. En cas de doute, il est préférable de s'adresser à celui-ci. L'installation d'un logiciel antivirus et d'un pare-feu (*firewall*) personnel est également indispensable. Il est par ailleurs essentiel d'actualiser régulièrement le logiciel, soit en téléchargeant et en installant les mises à jour (*updates*) disponibles sur le site Web du fournisseur, soit en utilisant une fonction de mise à jour automatique en ligne.

Par ailleurs, il est conseillé d'installer un système d'exploitation actuel ainsi qu'une version récente du navigateur, y compris des *plugins* correspondants. Les applications doivent également faire l'objet d'une mise à jour régulière pour éviter que des failles dans la sécurité ne permettent à des criminels d'accéder à l'ordinateur.

3.1 Pas d'e-banking à partir d'une adresse Internet autre que celle de sa banque!

Un utilisateur ne doit entrer ses données d'accès e-banking que lorsqu'il est sûr de se trouver sur le site Internet autorisé et protégé de sa banque et d'utiliser une connexion sécurisée. Celle-ci se reconnaît au s (= *secure*, c.-à-d. sûr) ajouté à http dans l'URL de la connexion et indique qu'un certificat de sécurité est utilisé pour le site Web en question (p. ex. https://www.sba.ch). L'authenticité de ce certificat de sécurité peut être vérifiée de la manière suivante: il suffit d'un double-clic sur le symbole de cadenas fermé qui se trouve sur la ligne de statut tout en bas de la fenêtre de navigation. La fenêtre qui s'ouvre alors devrait mentionner le nom de la banque. De plus, la plupart des banques utilisent des certificats *SSL Extended Validation*. Ceux-ci se reconnaissent au fait qu'une partie de la barre d'adresse URL comportant le nom de la banque s'affiche en vert. Si l'on clique sur cette barre, une fenêtre affichant le nom du l'établissement bancaire propriétaire du certificat et celui de l'autorité de certification s'ouvre. Si tel est le cas, on peut partir du principe qu'il s'agit d'un site Internet fiable. Malheureusement, tous les navigateurs n'offrent pas encore la norme *SSL Extended Validation*.

Lors d'achats en ligne, les données d'accès personnelles ne devraient être saisies ni sur les sites de boutiques, ni sur ceux de services de virement en ligne. Il ne faut jamais saisir ses données d'accès confidentielles sur un autre site Internet que celui de sa banque ni les donner à un tiers. En communiquant ses données d'accès e-banking à d'autres entreprises, un client enfreint les devoirs de diligence du contrat e-banking conclu avec son établissement bancaire.

3.2 Protéger les données sensibles

Il convient de protéger ses données d'accès e-banking de tout accès non autorisé et de toute subtilisation. Il ne faut donc pas enregistrer de données sensibles (mots de passe, données d'accès e-banking, numéros de carte de crédit, etc.) sur son ordinateur. En effet, dans le cas d'un ordinateur qui n'est pas utilisé par le seul client, comme c'est le cas sur le lieu de travail par exemple, des tiers pourraient avoir accès à ces données.

Certains logiciels d'espionnage qui se sont installés sur votre ordinateur peuvent surveiller ces données et les envoyer p. ex. à un tiers par e-mail. Si l'utilisateur dispose d'un équipement supplémentaire permettant d'accroître la sécurité, comme un lecteur de carte à puce avec un clavier de saisie du NIP, il convient d'entrer les données confidentielles uniquement lorsque cela est demandé par l'appareil. Surtout, il ne faut jamais enregistrer son mot de passe sur son ordinateur.

La banque ne contactera jamais un client – que ce soit par e-mail ou par téléphone – en lui demandant ses données d'accès confidentielles. Il ne faut jamais répondre à des e-mails de ce type et ne jamais suivre les instructions données, même en cas de menace de conséquences négatives comme la fermeture d'un compte. Il faut par contre informer sa banque si un tel cas de figure se produit.

A l'inverse, si le client contacte sa banque, il se peut que celle-ci lui demande ses données d'accès confidentielles dans le cadre du phone banking, et ce, à des fins d'identification. Le client doit toujours s'assurer qu'il a composé le bon numéro et que la requête correspond à la procédure communiquée avant de répondre à de telles demandes.

Il convient toujours de saisir ses données d'accès confidentielles sur le véritable site Internet de sa banque. Il est également prudent de vérifier que la page d'accueil e-banking qui s'affiche est bien la page habituelle. En effet, un client habitué à voir cette page remarquera immédiatement un changement, même minime, apporté au logo de sa banque p. ex. ou encore à la disposition des titres.

3.3 Choisir un mot de passe sûr

Il faut veiller à utiliser un mot de passe adéquat et sûr pour l'e-banking. Celui-ci doit comporter au moins huit caractères et se composer à la fois de lettres majuscules et minuscules ainsi que de chiffres. Il ne faut jamais entrer son nom, sa date d'anniversaire ou ceux de personnes proches. Une autre règle consiste à changer régulièrement de mot de passe, surtout lorsqu'il est possible qu'un tiers ait espionné ces données. Sur Internet et sur le site Internet de nombreuses banques, on trouve des exemples de mots de passe adaptés et sûrs.

4 Précautions d'ordre général

Il convient d'accéder à l'e-banking uniquement à partir d'un ordinateur personnel. Dans le cas contraire, p. ex. celui d'un ordinateur d'un café Internet, on ne peut jamais savoir à quel point l'accès est protégé par des logiciels de sécurité et quels programmes sont exécutés sur celui-ci. Les claviers aussi peuvent être modifiés. La sécurité ne peut en tout cas pas être garantie et l'e-banking est par conséquent déconseillé sur ces ordinateurs.

Lorsqu'un utilisateur procède à une opération e-banking, il doit veiller à ce que les autres fenêtres de navigation (y compris les onglets) soient fermées et qu'aucune messagerie ne soit ouverte.

Une session e-banking doit toujours être fermée par la fonction prévue à cet effet intitulée «Quitter», «Logout» ou «Fermer». Il faut ensuite supprimer les fichiers Internet temporaires de votre navigateur ainsi que les cookies (une marche à suivre est en principe disponible sur le site Internet des banques).

Liens complémentaires:

- www.swissbanking.org > Dossier: Informations à l'attention de la clientèle bancaire
  http://www.swissbanking.org/home/dossier-bankkunden.htm

- Centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI
  http://www.melani.admin.ch/themen/00103/index.html?lang=fr

- Office fédéral de la sécurité des technologies de l'information (*Bundesamt für Sicherheit in der Informationstechnik*)
  http://www.bsi-fuer-buerger.de/

Cette brochure est également disponible en français, en anglais et en italien et peut être commandée auprès de l'Association suisse des banquiers à l'adresse http://www.swissbanking.org/fr/home/shop.htm.

Il est également possible de télécharger cette brochure au format PDF à l'adresse www.swissbanking.org/fr/home/dossier-bankkunden.htm.

Association suisse des banquiers
Aeschenplatz 7
Case postale 4182
CH-4002 Bâle
T +41 61 295 93 93
F +41 61 272 53 82
office@sba.ch
www.swissbanking.org