Recommandations de sécurité relatives à l'utilisation d'internet

Les banques et leurs clients sont de plus en plus la cible de tentatives malveillantes de la part de cybercriminels, nous souhaitons vous faire part de mesures de précautions utiles à suivre sur internet.

1. Quand vous réalisez des transactions bancaires

En cas d'utilisation de logiciels de paiements hors ligne :

- Utiliser ce type de logiciel uniquement sur un ordinateur dédié, qui n'est en aucun cas utilisé pour naviguer sur internet et/ou recevoir des e-mails.
- Respecter les recommandations de sécurité proposées par les éditeurs de ce type de logiciels.
- Annoncer immédiatement les éventuels paiements suspects à votre banque afin que des mesures appropriées puissent être prises.

Lors de vos paiements sur internet :

- Garder tous vos codes d'accès secrets.
- Des intermédiaires de paiement vous demandent parfois de leur livrer vos codes d'accès lorsque vous procédez à des achats ou à des réservations sur le web. Toutefois, la banque estime que ce procédé contrevient aux règles élémentaires liées à la confidentialité de vos codes d'accès.

2. En tout temps

Utiliser des mots de passe complexes :

- choisir des mots de passe d'une longueur minimale de huit caractères;
- éviter les noms ou prénoms connus;
- opter pour un mélange de lettres, de chiffres et de caractères;
- changer régulièrement les mots de passe et éviter de réutiliser les anciens;
- garder les mots de passe secrets, ne les partager avec personne et ne pas les écrire;
- ne pas utiliser le même mot de passe pour accéder à plusieurs services.

Mettre régulièrement à jour vos logiciels afin de diminuer le risque qu'une personne malveillante puisse exploiter des failles de sécurité connues et accéder à vos données ou prendre le contrôle de votre ordinateur:

- s'assurer que le système d'exploitation, les applications utilisées et le navigateur sont à jour lors de la navigation sur internet;
- penser à activer les mises à jour automatiques.

Installer et utiliser un logiciel antivirus et un pare-feu afin de prévenir les infections de votre ordinateur par des virus informatiques et d'empêcher des connexions malveillantes:

- s'assurer que le logiciel antivirus est mis à jour et procéder régulièrement à des analyses (scans);
- activer le logiciel pare-feu de l'ordinateur, si ce dernier en propose un. Sinon, des pare-feux sont disponibles sous forme de logiciels additionnels qui peuvent être téléchargés gratuitement depuis des sites internet.

Veiller à toujours installer des applications mobiles depuis des sites de téléchargement officiels comme AppStore, Google Play, etc.

Adopter le bon comportement en naviguant sur internet afin de détecter les tentatives de piratage:

- se méfier des courriers électroniques dont l'expéditeur n'est pas connu. Ne pas cliquer sur les liens et ne pas ouvrir les fichiers contenus dans ces courriers;
- ne pas répondre aux spams (courriers électroniques publicitaires non sollicités), car une réponse indique à l'expéditeur que l'adresse électronique existe et entraîne l'envoi d'autres spams non désirés;
- être attentif en ouvrant des pièces jointes à des messages provenant de connaissances, car celles-ci peuvent s'être fait pirater leur boîte électronique;
- protéger la vie privée; il ne faut ni tout dire ni tout montrer sur Internet. Ces données restent accessibles d'une manière ou d'une autre;
- lors d'achats en ligne, n'entrer son numéro de carte de crédit que sur des pages sécurisées (adresse commençant par «https://») et s'assurer du sérieux du fournisseur, en se renseignant, par exemple, via une recherche Google avant toute transaction;
- lorsque la navigation sur internet est terminée, fermer l'ensemble des sessions en se déconnectant via les fonctions prévues à cet effet;
- éteindre l'ordinateur lorsqu'il n'est pas utilisé.

Faire preuve de bon sens et d'esprit critique afin de détecter les tentatives d'arnaques:

- ne pas donner suite lorsque l'on gagne à un jeu auquel on n'a pas joué;
- se méfier des héritages venant d'un parent éloigné, récemment décédé à l'étranger, mais inconnu (arnaque de type «faux héritage»). Le mode opératoire consiste à demander le versement préalable d'une certaine somme afin de régler, notamment, les frais de succession;
- ne jamais payer par avance de prétendus impôts ou frais administratifs lors d'une vente sur internet afin de permettre à l'acheteur de libérer l'ensemble des fonds et ainsi de les envoyer;
- ne jamais divulguer ses codes d'accès, même si la personne de contact prétend être employée par la banque ou si l'e-mail reçu semble provenir de la CEN.

3. Des sites internet pour en savoir plus

- **La centrale d'enregistrement et d'analyse pour la sûreté de l'information MELANI** (http://www.melani.admin.ch/)
  Cette plateforme s'adresse aux particuliers ainsi qu'aux petites et moyennes entreprises en Suisse (PME). Elle détaille les risques liés à l'utilisation d'internet et expose des mesures de prévention spécifiques.
- **e-banking en toute sécurité** (https://www.ebas.ch/fr/)
  Cette plateforme propose plusieurs mesures destinées à améliorer la sécurité des utilisateurs d'internet et des systèmes d'e-banking. Elle donne des marches à suivre simples et des liens vers des outils, tels que des logiciels antivirus et des pare-feux.