SÉCURITÉ INFORMATIQUE

Recommandations de sécurité relatives à l'utilisation d'internet

BCV

Recommandations de sécurité relatives à l'utilisation d'internet

Mettre en place des mesures techniques

- Utiliser des mots de passe différents et sophistiqués.
- Mettre régulièrement à jour les logiciels.
- Installer et utiliser un logiciel antivirus et un pare-feu.
- Faire régulièrement des sauvegardes des données importantes.
- Veiller à toujours installer des applications mobiles depuis des sites de téléchargement officiels.

Adopter un comportement prudent

- Prendre le temps d'analyser chaque message électronique reçu.
- Faire preuve de vigilance en naviguant sur internet.

Faire preuve de bon sens

- Faire preuve de bon sens et d'esprit critique.

Chacun peut renforcer sa sécurité numérique en appliquant trois principes simples: mettre en place des mesures techniques, adopter un comportement prudent et faire preuve de bon sens.

Mettre en place des mesures techniques

Utiliser des mots de passe différents et sophistiqués afin de diminuer les risques d'accès malveillants à son ordinateur, ses messageries électroniques, ses comptes de réseaux sociaux et ses comptes bancaires.

- Éviter les noms ou prénoms connus ainsi que les mots du dictionnaire.
- Choisir des mots de passe d'au moins huit caractères (lettres, chiffres et caractères spéciaux).
- Changer régulièrement les mots de passe et éviter de réutiliser les anciens.
- Utiliser des mots de passe différents pour chaque service ou compte.
- Ne partager les mots de passe avec personne. Aucune société sérieuse ne demande un mot de passe par téléphone ou par courrier électronique.
- Utiliser un logiciel de gestion sécurisée des mots de passe pour les stocker.
- Privilégier un mode d'authentification à deux facteurs (par exemple un SMS de confirmation), lorsqu'il est disponible.

Mettre régulièrement à jour les logiciels afin de diminuer le risque qu'une personne malveillante exploite des failles de sécurité connues pour accéder aux données personnelles ou prendre le contrôle de l'ordinateur.

- S'assurer que le système d'exploitation, les applications utilisées et le navigateur sont à jour.
- Penser à activer les mises à jour automatiques.

Installer et utiliser un logiciel antivirus et un pare-feu afin de prévenir les infections de son ordinateur et les connexions malveillantes.

- Mettre à jour le logiciel antivirus 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 peuvent être téléchargés gratuitement depuis des sites internet.

Faire régulièrement des sauvegardes des données importantes afin d'éviter de les perdre définitivement en cas de problème.

- Copier les données sur un disque dur externe pour les sauvegarder et vérifier qu'elles soient lisibles.
- Débrancher ensuite le disque dur externe (ceci évite que les données qui y sont copiées ne soient supprimées en cas d'infection de son ordinateur par un virus informatique).
- Ne pas rebrancher le disque dur externe sur un ordinateur infecté.

Veiller à toujours installer des applications mobiles depuis des sites de téléchargement officiels, comme AppStore, Google Play, etc. afin d'éviter tout risque d'infection de son smartphone par un virus informatique.

- Ne pas chercher à débrider son smartphone via les processus *root* (pour Android) ou *jailbreak* (pour iOS).

Adopter un comportement prudent

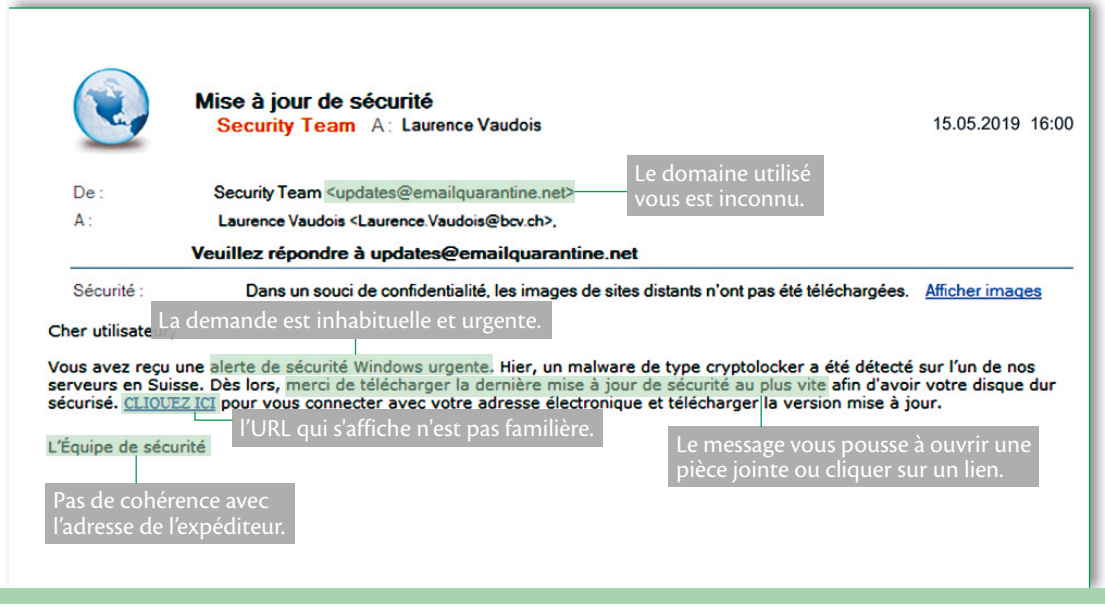
Prendre le temps d'analyser chaque message électronique reçu. Les personnes malintentionnées utilisent très souvent les messages électroniques pour infecter l'ordinateur.

- Se méfier des messages dont l'expéditeur n'est pas connu. Penser à vérifier la cohérence entre l'expéditeur et la signature.
- Déterminer si les formules de politesse utilisées dans le message sont appropriées.
  Exemple: est-ce normal qu'un ami vous vouvoie ou qu'un contact professionnel vous tutoie?
- Observer si la langue utilisée est la même que d'habitude.
  Exemple: est-ce normal qu'un ami avec lequel vous conversez habituellement en français vous écrive en anglais?
- Vérifier la plausibilité du courrier électronique et être particulièrement attentif dès que la notion d'urgence ou de discrétion absolue est présente.
  Exemple: est-ce normal qu'un proche vous demande de réaliser un transfert d'argent très urgent à l'étranger?
- Ne pas cliquer machinalement sur les liens ou les fichiers contenus dans le courrier électronique, surtout s'ils ont les extensions .pif, .com, .bat, .exe, .vbs, .lnk.
- Ne pas répondre aux spams (courrier électronique publicitaire non sollicité), car cela indique à l'expéditeur que l'adresse électronique existe et entraîne l'envoi d'autres spams.
- Être attentif en ouvrant des pièces jointes liées à des messages provenant de connaissances, car celles-ci peuvent s'être fait pirater leur boîte électronique.
- Utiliser des adresses différentes selon le niveau d'importance.
  Exemple: une adresse pour les affaires privées, une pour le commerce en ligne et une autre pour tout le reste.

Faire preuve de vigilance en naviguant sur internet afin de détecter les tentatives de piratage.

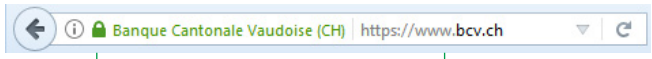
- Protéger la vie privée: il ne faut ni tout dire ni tout montrer sur internet. Dès que des données sont sur internet, on en perd le contrôle.
- Éviter les réseaux wi-fi publics pour effectuer des achats en ligne ou des opérations bancaires.
- Lors d'achats en ligne, s'assurer du sérieux du fournisseur avant toute transaction en se renseignant, par exemple, via une recherche Google. N'entrer son numéro de carte de crédit que sur des pages sécurisées, c'est-à-dire dont l'adresse commence par «https://» accompagné d'un cadenas.
- Lorsque la navigation sur internet est terminée, fermer l'ensemble des sessions en se déconnectant via les fonctions prévues à cet effet et supprimer l'historique de navigation.
- Verrouiller l'ordinateur dès que l'on s'absente et l'éteindre lorsqu'il n'est pas utilisé.

Exemple d'e-mail frauduleux



Comment s'authentifier en toute sécurité sur l'e-banking avec un code SMS?

1

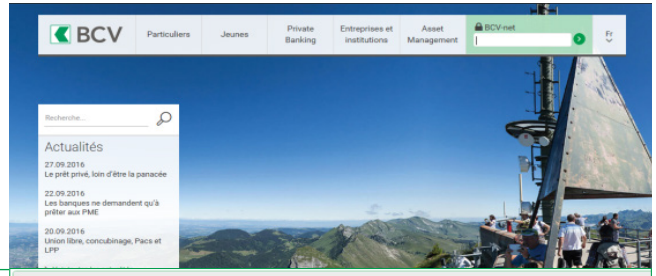


Votre navigateur vous confirme-t-il que la connexion est sécurisée?

Êtes-vous bien sur www.bcv.ch?

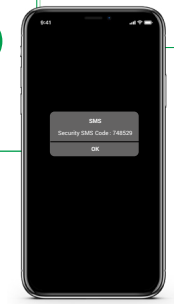
2

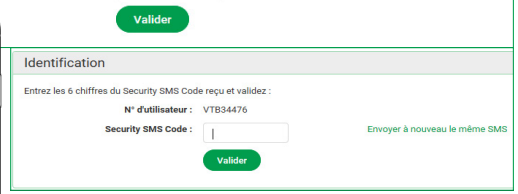
Est-ce que les écrans qui apparaissent ressemblent à ceux que vous avez l'habitude de voir? La BCV ne changera pas la structure de son site sans que vous en soyez averti.



3

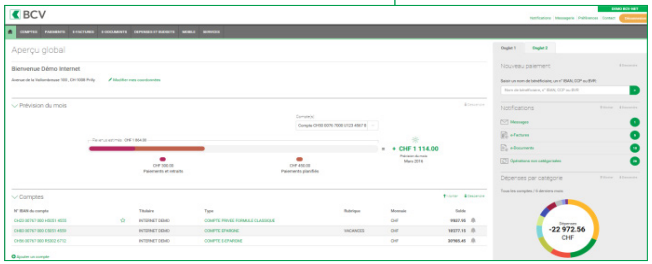
Vous devez recevoir un SMS de login et en aucun cas un SMS de confirmation de paiement (qui contient un IBAN et un montant).





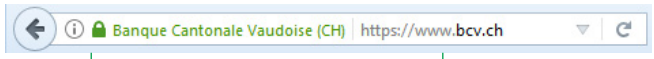
Une fois sur l'e-banking: est-ce que le processus global d'authentification vous semble normal ou y a-t-il eu des comportements étranges durant l'authentification (lenteur extrême, messages inhabituels ou demandes d'informations supplémentaires)?

4



Comment s'authentifier en toute sécurité sur l'e-banking avec SmartID?

1



Votre navigateur vous confirme-t-il que la connexion est sécurisée?

Êtes-vous bien sur www.bcv.ch?

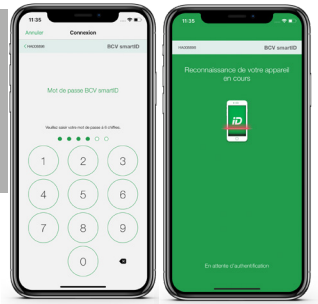
2

Est-ce que les écrans qui apparaissent ressemblent à ceux que vous avez l'habitude de voir? La BCV ne changera pas la structure de son site sans que vous en soyez averti.

3

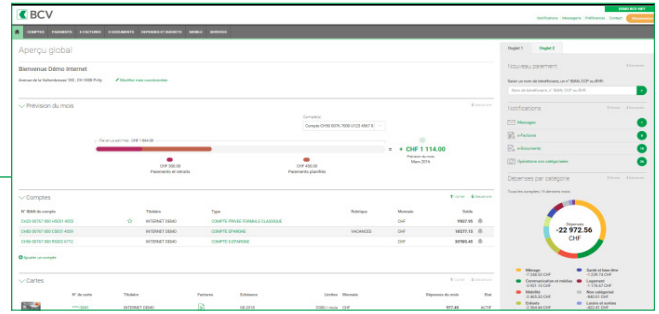
Prenez garde de bien être sur l'écran de login et non sur l'écran d'autorisation de paiement! **Faites très attention!**

Est-ce que le processus d'authentification ressemble à ce que vous avez l'habitude de voir?



Une fois sur l'e-banking: est-ce que le processus global d'authentification vous semble normal ou y a-t-il eu des comportements étranges durant l'authentification (lenteur, messages inhabituels ou demandes d'informations supplémentaires)?

5



Faire preuve de bon sens

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 »). N'effectuer aucun versement préalable destiné à régler, notamment, de prétendus frais de succession.
- Ne jamais payer par avance de prétendus impôts ou frais administratifs lors d'une vente sur internet, soi-disant pour permettre à l'acheteur de libérer l'ensemble des fonds et ainsi les envoyer.
- Être particulièrement attentif aux contacts non sollicités de personnes inconnues.
- Se méfier des clés USB et disques durs externes lorsque leur provenance n'est pas connue, car ils peuvent contenir un virus informatique.
- Ne pas désactiver les options de sécurité présentes par défaut sur son ordinateur ou smartphone (mot de passe de déverrouillage de son smartphone, verrouillage automatique de son ordinateur, etc.).
- Ne jamais divulguer ses codes d'accès à BCV-net, même si la personne de contact prétend être employée par la BCV ou si l'e-mail reçu semble provenir de la BCV.
- Ne jamais donner accès à votre session BCV-net à une personne tiers que se soit physiquement sur votre ordinateur ou téléphone ou à distance. (ex: support informatique connecté sur votre ordinateur à distance)

Exemples de cas réels d'attaque

On vous demande votre numéro de téléphone dans le formulaire d'authentification. Est-ce légitime? Non! D'abord, la BCV ne vous demandera pas ce genre d'information par ce biais. De plus, elle dispose déjà de votre numéro de téléphone. Finalement, elle vous avertit au préalable s'il y a un changement dans le processus d'authentification.

En cas de doute, ne continuez pas le processus d'authentification et prenez contact avec la Banque.

De manière générale, ne donnez pas d'informations surtout si celles-ci ne semblent pas nécessaires.

Vous avez fourni votre nom d'utilisateur et votre mot de passe. Tout à coup, une fenêtre inhabituelle s'affiche, vous demandant de patienter.. Tout changement de processus non annoncé par la BCV devrait vous alerter.

Dans ce cas, ne continuez pas le processus d'authentification et prenez contact avec la Banque.

Des sites internet pour en savoir plus

La Centrale National pour la Cybersécurité NCSC
Cette plateforme détaille les risques liés à l'utilisation d'internet et expose des mesures de prévention spécifiques, aussi bien pour les particuliers que pour les PME en Suisse (https://www.ncsc.admin.ch/).

e-banking en toute sécurité
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 (www.ebas.ch/fr).

Banque Cantonale Vaudoise
Case postale 300
1001 Lausanne
www.bcv.ch

42-562/23.11