Sécurité et mots de passe

Comment protéger vos comptes en ligne contre les accès non autorisés

Votre Police et la Prévention Suisse de la Criminalité (PSC) – un organe intercantonal de coordination spécialisé de la Conférence des directrices et directeurs des départements cantonaux de justice et de police (CCDJP), en collaboration avec la Haute école spécialisée de Lucerne et « eBanking – en toute sécurité ! »

De la même manière que vous fermez la porte de votre maison ou de votre appartement lorsque vous sortez, vous devez tout mettre en œuvre pour empêcher des intrus d'accéder à vos appareils et vos comptes en ligne.

Ce que vous devez savoir :

- Protégez votre ordinateur et vos dispositifs mobiles (smartphones, tablettes, etc.) contre les accès non autorisés et **verrouillez l'écran** lorsque vous n'êtes plus actif sur votre appareil.
- Utilisez des **mots de passe forts** (minimum 12 caractères, dont des chiffres, des lettres majuscules et minuscules, ainsi que des caractères spéciaux).
- N'employez pas le même mot de passe partout. Au contraire, choisissez un **mot de passe différent** pour chacun de vos comptes.
- À chaque fois que cela est possible, activez la **méthode d'authentification à deux facteurs.**

L'accès à mon compte en ligne a-t-il été piraté ?

Pour savoir si vous avez été victime d'un vol de mot de passe sur l'un de vos comptes en ligne, rendez-vous sur **www.ebas.ch/haveibeenpwned**. Ce site est relié à la base de données de la célèbre plateforme **haveibeenpwned.com** et vous présente les résultats en langue française. Ainsi, vous découvrez si vos identifiants de connexion ont été utilisés ou s'ils ont été publiés dans le cadre d'une fuite de données. Attention : saisissez uniquement vos noms d'utilisateur ou votre adresse email et jamais le mot de passe correspondant !

www.ebas.ch/fr/have-i-been-pwned

haveibeenpwned.com

Comment protéger vos dispositifs contre les abus

Protégez l'accès de tous vos dispositifs. N'oubliez pas que le risque de perte ou de vol est bien plus élevé pour les notebooks, tablettes et smartphones que pour les ordinateurs fixes.

Assurez-vous par conséquent, et en particulier pour vos dispositifs mobiles, que le verrouillage automatique de l'écran est activé (par code d'accès, mot de passe, empreinte digitale ou reconnaissance faciale).

Il convient par ailleurs de chiffrer les données de votre appareil mobile, et en particulier les supports de stockage auxiliaires, tels que les disques durs externes ou les clés USB, afin d'empêcher toute tentative d'accès à vos données et à vos applications par des systèmes étrangers.

iPhone/iPad

- Verrouillage d'écran jusqu'à l'iPhone 9 : sous **Réglages/ Touch ID** et code, vous avez la possibilité de protéger votre appareil avec un code d'accès, un mot de passe ou une empreinte digitale.
- Verrouillage d'écran à partir de l'iPhone 10 : sous **Réglages/ Face ID et code,** vous pouvez configurer la reconnaissance faciale.
- Sur l'iPhone et l'iPad, les données sont automatiquement chiffrées.

Android

- Selon les appareils, vous avez la possibilité de paramétrer le verrouillage d'écran sous **Paramètres/Sécurité et confidentialité.**
- Le chiffrement des données peut être activé sous **Paramètres/Sécurité et confidentialité/Autres paramètres/Chiffrement et identifiants.** Idem pour vos éventuels supports de stockage.

Comment créer des mots de passe forts

Les mots de passe restent aujourd'hui encore la forme la plus courante et la plus utilisée pour protéger l'accès à des données électroniques sensibles et privées. À condition d'appliquer quelques règles simples.

Six règles à respecter pour créer un mot de passe fort

1 Au minimum 12 caractères.
2 Des chiffres, des lettres majuscules et minuscules, ainsi que des caractères spéciaux.
3 Pas de combinaisons de chiffres en séquence ni de lettres voisines sur le clavier, telles que « asdfgh » ou « 45678 ».
4 Aucun mot figurant dans un dictionnaire, quelle que soit la langue.
5 Un mot de passe différent pour chaque compte.
6 Ne jamais stocker son mot de passe sous une forme non chiffrée.

Voici comment créer un mot de passe fort en toute simplicité :

- Choisissez une phrase facile à mémoriser et élaborez votre mot de passe en prenant la première lettre de chaque mot, et en incluant la ponctuation et les chiffres : « **M**a **f**ille **T**amara **M**orel **f**ête **s**on **a**nniversaire **l**e **19 j**anvier **!** »
- Vous obtenez alors une chaîne de caractères apparemment arbitraire mais facile à mémoriser : « **MfTMfsal19j!** »

Gestionnaire de mots de passe

Un gestionnaire de mots de passe permet d'enregistrer tous vos mots de passe sous une forme chiffrée, ne vous laissant plus qu'un mot de passe unique à mémoriser. Pour en savoir plus :

www.ebas.ch/step4

Visionner la vidéo sur les gestionnaires de mots de passe :

www.youtube.com/watch?v=Jc1uCh-AWGk

La méthode d'authentification à deux facteurs

En plus de la protection offerte par un mot de passe fort, la méthode d'authentification à deux facteurs permet de renforcer la sécurité de vos comptes en ligne. Ainsi, pour vous connecter à un compte, vous devrez saisir, en plus du premier élément de sécurité (généralement un mot de passe), un deuxième élément de sécurité indépendant. Il peut s'agir par exemple d'un code numérique envoyé sur votre téléphone mobile ou généré directement par ce dernier.

Aujourd'hui, la méthode d'authentification à deux facteurs n'est plus l'apanage des instituts financiers dans la mesure où elle est proposée par de plus en plus de services en ligne (p. ex. Google, Facebook). Activez l'authentification 2FA pour une sécurité renforcée. Vous trouverez une description des différentes méthodes utilisées par les instituts financiers sur

www.ebas.ch/fr/les-conseils-a-suivre-pour-ouvrir-une-session-de-banking

Visionner la vidéo sur l'authentification à deux facteurs :

www.youtube.com/watch?v=4O6kkjweCDg

Les passkeys

Basés sur des paires de clés cryptographiques et la technologie biométrique, les passkeys ont pour ambition de remplacer les mots de passe. Ce nouveau système offre aux utilisateurs une méthode simple et sécurisée pour accéder à leurs comptes en ligne. Ce mécanisme fait appel à une paire de clés : une clé publique et une clé privée. La clé privée est stockée sur l'appareil de l'utilisateur et validée à chaque utilisation via un capteur biométrique (empreinte digitale ou reconnaissance faciale par exemple) ou un code PIN. Même en cas de vol de votre appareil, personne ne pourra accéder à vos passkeys sans vos données biométriques ou votre code PIN. Pour en savoir plus sur le fonctionnement et la génération d'un passkey, consultez notre article sur

www.ebas.ch/passkeys

Janvier 2025

Prévention Suisse de la Criminalité
Maison des Cantons
Speichergasse 6
3001 Berne

www.skppsc.ch

Ce dépliant a été réalisé en collaboration avec la **Haute école spécialisée de Lucerne** et **«eBanking – en toute sécurité!»**

www.ebas.ch | www.ebankingentoutesecurite.ch

HSLU Hochschule Luzern

eBanking en toute sécurité!