4 – Protéger les accès Internet

Vous avez l'habitude de fermer la porte derrière vous lorsque vous quittez votre maison ou votre appartement ? Faites de même avec vos dispositifs et accès en ligne et protégez-les contre les risques d'effraction.

Principaux conseils à suivre :

- Protégez votre ordinateur et vos dispositifs mobiles (smartphones, tablettes, etc.) contre tout accès non autorisé et verrouillez l'écran lorsque vous n'êtes plus actif sur l'appareil.
- Utilisez des mots de passe forts (minimum 12 caractères, dont des chiffres, des majuscules, des minuscules et des caractères spéciaux).
- N'employez pas partout le même mot de passe. Au contraire, il convient d'en trouver un différent pour chaque compte.
- Activez si possible une méthode d'authentification dite forte, c'est-à-dire à deux facteurs (2FA).

4 – Protéger les accès Internet

5 règles pour votre sécurité numérique

Un voleur *ne vole pas* votre voiture s'il en a la clé.
Un hacker *ne vole pas* vos données s'il possède votre **mot de passe**.

eBanking en toute sécurité! www.ebas.ch

Sécurisez vos dispositifs contre les accès non autorisés

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

Assurez-vous donc, et en particulier pour vos dispositifs mobiles, que le verrouillage automatique de l'écran est activé (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 comme les disques durs externes ou les clés USB, afin d'empêcher quiconque d'accéder à vos données et à vos applications par l'intermédiaire de systèmes étrangers.

iPhone/iPad

Verrouillage d'écran jusqu'à l'iPhone 9 : dans **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.

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

Verrouillage d'écran jusqu'à 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 l'appareil, vous pouvez 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** (le cas échéant pour vos supports de stockage également).

Un mot de passe sécurisé

Les mots de passe restent aujourd'hui encore la forme la plus courante et la plus utilisée de protéger l'accès à des données électroniques sensibles et privées. A ce sujet, quelques règles simples suffisent pour éviter les problèmes.

Les 6 règles pour créer un mot de passe fort...

- minimum 12 caractères
- des chiffres, des lettres majuscules et minuscules ainsi que des caractères spéciaux
- pas de combinaisons en séquences ni de lettres voisines sur le clavier comme « asdfgh » ou « 45678 »
- pas de mots appartenant à aucune langue connue; le mot de passe ne doit avoir aucune signification et ne figurer dans aucun dictionnaire
- utilisez un mot de passe différent partout
- ne stockez pas votre mot de passe s'il n'est pas sécurisé par cryptage

Choisir un mot de passe sûr n'a rien de compliqué. Voici quelques conseils simples pour choisir un mot de passe sûr et facile à retenir :

- 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**eier **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.

Windows

Pour les dispositifs sous Windows, nous vous conseillons les gestionnaires de mots de passe suivants, certains étant disponibles gratuitement :

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

- KeePass (https://www.keepass.info)
- Password Safe (https://www.passwordsafe.de)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

macOS

Pour les dispositifs sous Mac, nous vous conseillons les gestionnaires de mots de passe suivants, certains étant disponibles gratuitement :

- KeePassXC (https://keepassxc.org)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

Smartphone und Tablet

Pour les dispositifs sous Smartphones et tablettes, nous vous conseillons les gestionnaires de mots de passe suivants, certains étant disponibles gratuitement :

- KeePass (https://www.keepass.info)
- Password Safe (https://www.passwordsafe.de)
- SecureSafe (https://www.securesafe.com)
- eWallet (https://www.iliumsoft.com)

https://www.ebas.ch/wp-content/uploads/2023/04/SKP_NCSC_Passwortmanager_fr.mp4

Vous trouverez de plus amples informations ainsi qu'un comparatif détaillé des gestionnaires de mots de passe courants dans la fiche « Fact Sheet Password Manager » (https://docs.datenschutz.ch/u/d/publikationen/factsheets-engl/fact-sheet_password_managers.pdf) du préposé à la protection des données du canton de Zurich.

La méthode d'authentification à deux facteurs (2FA)

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.

https://www.ebas.ch/wp-content/uploads/2023/04/SKP_NCSC_2FA_fr.mp4

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 ici (https://www.ebas.ch/category/23) une description des dif-

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique

férentes méthodes utilisées par les instituts financiers.

Votre compte en ligne a été piraté ?

Contrôlez si le mot de passe d'un de vos comptes en ligne a été piraté :

Have I been Pwned (https://www.ebas.ch/fr/have-i-been-pwned/)

Vous pourrez savoir si vos identifiants de connexion ont été compromis ou publiés dans le cadre d'une fuite de données. La page consulte la base de données de la plateforme https://haveibeenpwned.com (https://haveibeenpwned.com) et présente les résultats en français. Veillez à ne saisir que vos noms d'utilisateur ou votre adresse mail et jamais le mot de passe correspondant !

Protégez vos données et tous vos dispositifs en suivant les « 5 règles pour votre sécurité numérique » :

Règle n°1 – Sauvegarder (https://www.ebas.ch/fr/1-sauvegarder-les-donnees/)

Règle n°2 – Surveiller (https://www.ebas.ch/fr/2-surveiller-avec-lantivirus-et-le-pare-feu/)

Règle n°3 – Prévenir (https://www.ebas.ch/fr/3-prevenir-avec-les-mises-a-jour-logicielles/)

Règle n°4 – Protéger

Règle n°5 – Faire attention (https://www.ebas.ch/fr/5-faire-attention-et-etre-vigilant/)

Copyright © 2024 – Tous droits réservés. Haute Ecole Spécialisée de Lucerne – Informatique