Les 5 règles pour votre sécurité numérique

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)

Les 5 règles pour votre sécurité numérique

Internet occupe aujourd'hui une place de choix dans notre vie quotidienne. On utilise Internet pour s'informer, pour organiser un voyage, pour payer ses factures, ou tout simplement pour communiquer avec ses amis ou connaissances.

Mais au-delà de toutes les possibilités offertes, Internet nous expose aussi à de nouveaux dangers. D'innombrables logiciels malveillants cherchent constamment de nouveaux moyens de s'immiscer dans nos ordinateurs, smartphones ou tablettes, sur lesquels nous stockons toutes sortes de données personnelles (photos, lettres ou autres documents confidentiels). Une cyber-attaque réussie peut causer de graves préjudices, à vous et à vos dispositifs. Les cyberpirates sont en effet capables de modifier et de supprimer vos données, ou bien de détourner les informations qu'ils contiennent pour faire par exemple leurs courses sur Internet, à votre nom et à vos frais bien sûr.

Voilà pourquoi il convient de protéger vos données et vos dispositifs en suivant «les 5 règles pour votre sécurité numérique»:

Règle 1 **Sauvegarder** les données

Règle 2 **Surveiller** avec l'antivirus et le pare-feu

Règle 3 **Prévenir** avec les mises à jour logicielles

Règle 4 **Protéger** les accès Internet

Règle 5 **Faire attention** et être vigilant

Comme la ceinture de sécurité peut vous sauver la vie !
Un backup vous préserve d'une perte de données !

1

Sauvegarder les données

Quelle importance attribuez-vous à vos données ? Sauvegardez-les régulièrement sur au moins deux supports et vérifiez qu'elles ont bien été copiées.

Principaux conseils à suivre :

- Sauvegardez régulièrement vos données sur un disque dur externe, sur DVD, CD ou bien sur une plateforme de stockage en ligne (cloud).
- Vérifiez que les données ont effectivement été copiées et qu'elles peuvent être restaurées.
- Ne connectez votre disque dur de sauvegarde qu'au moment de son utilisation. De même, vous ne devez pas rester constamment connecté à votre compte de stockage en ligne. Votre connexion doit être limitée au temps nécessaire pour le processus de sauvegarde.

De nos jours, ordinateurs, tablettes et smartphones contiennent une foule de documents, courriels, photos, vidéos, musique et autres données numériques. Or, on ne peut exclure l'éventualité que ces contenus puissent être perdus, partiellement ou dans leur totalité, du fait d'une erreur de manipulation (par ex. suppression accidentelle), d'un défaut technique (par ex. défaut du disque dur), d'un vol ou de la perte de votre dispositif, ou à cause des logiciels malveillants qui circulent sur le Net (virus, vers, chevaux de Troie…).

→ **Sauvegardez vos données en effectuant un back-up de secours avant de subir une perte de données !**

Vous trouverez de plus amples informations, avec des instructions détaillées et des références à des outils logiciels, à l'adresse suivante :

www.ebas.ch/step1

Avec le cockpit, tout est sous contrôle.
Avec l'antivirus et le pare-feu, la circulation des données est surveillée.

2

Surveiller avec l'antivirus et le pare-feu

Quelles « portes » votre dispositif laisse-t-il ouvertes et quels virus viennent s'y présenter ? Dans la pratique aucune, si vous avez activé un pare-feu et installé un programme de protection antivirus.

Principaux conseils à suivre :

- Utilisez un programme antivirus et activez la fonction de mise à jour automatique.
- Vérifiez régulièrement que votre dispositif n'a pas été infecté en procédant à un scan complet du système.
- Activez le pare-feu embarqué de Windows ou mac OS avant de connecter votre dispositif à Internet ou à tout autre réseau.

Sans une protection adéquate, un ordinateur, une tablette ou un smartphone se trouvent livrés sans défense aux dangers de l'Internet et peuvent rapidement être infectés par des logiciels malveillants. L'ensemble des données stockées peut ainsi être consulté, manipulé, voire même effacé par des tiers non autorisés.

→ **Surveillez vos communications Internet avec un programme antivirus et un pare-feu activé !**

Vous trouverez de plus amples informations, avec des instructions détaillées et des références à des outils logiciels, à l'adresse suivante :

www.ebas.ch/step2

Une maintenance régulière pour votre voiture !
Une mise à jour régulière pour tous vos programmes !

3

Prévenir avec les mises à jour logicielles

En ce qui concerne vos logiciels, qui d'autre que leur fabriquant est mieux placé pour assurer leur sécurité ? Veillez à ce que votre système d'exploitation, de même que vos programmes et applications soient régulièrement mis à jour.

Principaux conseils à suivre :

- N'installez que les programmes et applications dont vous avez besoin et veillez à toujours les télécharger depuis la page de l'éditeur ou d'un store officiel.
- Activez la fonction de mise à jour automatique pour le système d'exploitation et l'ensemble de vos programmes et applications.
- Pour accéder à Internet, vous devez veiller à ce que votre navigateur soit parfaitement à jour.

Les programmes obsolètes présentent souvent des failles de sécurité, ce qui facilite la tâche des hackers cherchant à prendre le contrôle de votre dispositif. Les éditeurs de logiciels corrigent ces vulnérabilités et publient des correctifs sous la forme de mises à jour.

Chasse au superflu

N'installez que les programmes et applications dont vous avez vraiment besoin et assurez-vous qu'ils proviennent de sources sûres, c'est-à-dire directement de l'éditeur ou des stores officiels (p. ex. Apple App Store ou Google Play Store).

Maintenez vos dispositifs à jour

Assurez-vous d'avoir toujours la version logicielle la plus récente. Pour commencer, votre système d'exploitation doit être « parfaitement à jour ». Ce principe est valable pour tous les programmes, y compris le navigateur (par ex. Firefox, Chrome) ou Adobe Reader.

→ **Prévenez les attaques en installant les dernières mises à jour disponibles !**

Vous trouverez de plus amples informations, avec des instructions détaillées et des références à des outils logiciels, à l'adresse suivante :

www.ebas.ch/step3

Une clé : pas de vol de voiture.
Un mot de passe : pas de vol de données.

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 (smartphones, tablettes, etc.) contre tout accès non autorisé et verrouillez l'écran lorsque vous n'êtes plus actif.
- Utilisez des mots de passe forts (minimum 10 caractères, dont des chiffres, des majuscules, des minuscules et des caractères spéciaux).
- N'employez pas partout le même mot de passe. Au contraire, il faut en composer un pour chaque compte.
- Activez si possible une méthode d'authentification dite forte, c'est-à-dire à deux facteurs (2FA).

Une utilisation réfléchie des mots de passe

Un mot de passe simple et court n'offre pas une protection suffisante dans la mesure où il pourrait être facilement deviné en cas d'attaque. Évitez donc les noms, prénoms d'enfants ou d'animaux, les mots pouvant figurer dans un dictionnaire d'une langue connue, les combinaisons de touches voisines (ex. : « qsdfg » ou « 45678 »), de même que les dates de naissance. **L'idéal est de créer une combinaison arbitraire d'au moins 10 caractères contenant à la fois des lettres majuscules et minuscules, des chiffres et des caractères spéciaux.** N'utilisez pas partout le même mot de passe. Au contraire, il faut en composer un pour chaque compte et ne jamais les communiquer à qui que ce soit. Mémorisez vos mots de passe ou conservez-les sous forme écrite dans un lieu sûr.

Créer un mot de passe sûr n'est pas si difficile que ça ! Choisissez une phrase facile à mémoriser et élaborez votre mot de passe en prenant la première lettre de chaque mot et en incluant des chiffres et des caractères spéciaux : « Ma fille Tamara fête son anniversaire le 19 janvier ! ». Vous obtenez alors une chaîne de caractères apparemment arbitraire mais facile à mémoriser : **MfTfsal19j!**

Un **gestionnaire de mots de passe** permet d'enregistrer tous vos mots de

5

Faire attention et être vigilant

Croyez-vous vraiment à tout ce que l'on vous raconte ? Exercez votre sens des responsabilités et restez toujours méfiant lorsque vous surfez sur Internet.

Principaux conseils à suivre :

- Soyez toujours prudent lorsque vous surfez sur Internet et réfléchissez bien avant de communiquer vos données personnelles.
- Les instituts financiers, les opérateurs téléphoniques ou autres fournisseurs de service ne vous demanderont jamais (ni par email, ni par téléphone) de leur communiquer votre mot de passe, ni de le modifier.
- Lorsque vous utilisez vos dispositifs mobiles, vous devez appliquer les mêmes mesures de précaution que celles que vous observez normalement sur votre ordinateur fixe à la maison.
- En cas d'incertitude ou si vous craignez d'avoir été victime d'une attaque, n'hésitez pas à demander de l'aide.

passe sous une forme chiffrée, ne vous laissant plus qu'un mot de passe unique à mémoriser.

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.

→ **Protégez vos appareils et l'accès en ligne contre les risques d'effraction !**

Vous trouverez de plus amples informations, avec des instructions détaillées et des références à des outils logiciels, à l'adresse suivante :

www.ebas.ch/step4

Les 4 premières règles vous ont permis de très bien sécuriser vos dispositifs et vos accès en ligne d'un point de vue technique. Or, le comportement des utilisateur·ice·s continue de représenter le principal risque, au point de constituer la cible des attaques. À vous donc d'agir en conséquence en vous armant de bon sens.

Se protéger contre le phishing (hameçonnage) et les attaques d'ingénierie sociale

Dans le cas du phishing, les escrocs tentent de gagner la confiance des utilisateurs par courriel ou par téléphone en se faisant passer par exemple pour leur institut financier, dans le but de les attirer sur un site Web (via un lien hypertexte) ressemblant comme deux gouttes d'eau à celui de leur banque. Si vous tombez dans le piège et que vous communiquez vos identifiants et codes d'accès, vous leur donnez la possibilité de dévaliser votre compte en toute tranquillité.

Des risques accrus pour les dispositifs mobiles

De nombreuses applis accordent sans raison apparente des droits d'accès illimités. Or, les applications ne nécessitent pas toutes d'accéder par exemple à la position géographique, au répertoire des contacts ou au statut du téléphone. Lorsque vous accordez tel ou tel droit d'accès, réfléchissez s'il est vraiment nécessaire au fonctionnement de l'application et désactivez tous les droits superflus.

→ Soyez prudent et faites preuve de vigilance sur Internet !

Vous trouverez de plus amples informations, avec des instructions détaillées et des références à des outils logiciels, à l'adresse suivante :

www.ebas.ch/step5

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

Lucerne University of
Applied Sciences and Arts

HOCHSCHULE
LUZERN

Informatik
FH Zentralschweiz

eBanking en toute sécurité!

«eBanking – en toute sécurité!»

«eBanking – en tout sécurité!» est une plate-forme indépendante de la Haute École Spécialisée de Lucerne – Informatique, créée dans le but de vous aider à gérer la sécurité de vos informations personnelles. Notre site Internet www.ebas.ch informe les internautes intéressés par les questions de sécurité en informatique sur les mesures à mettre en œuvre ainsi que les règles de comportement à adopter pour une utilisation sécurisée des applications d'e-Banking.

- Page d'accueil : **https://www.ebas.ch**
- Page Facebook :
  https://www.facebook.com/ebankingabersicher
- Chaîne YouTube :
  https://www.youtube.com/user/ebankingabersicher
- Section Médias :
  https://www.ebas.ch/mediasection

Haute École Spécialisée de Lucerne – Informatique

La Haute École Spécialisée de Lucerne – Informatique propose sur son campus des filières de licence et de master, des activités de recherche appliquée et développement ainsi que des offres de formation continue en informatique et informatique de gestion.

- Page d'accueil du Département Informatique:
  https://www.hslu.ch/informatik
- Information Security & Privacy:
  https://www.hslu.ch/forschung-information-security

Janvier 2020

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

www.skppsc.ch