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 cyberattaque 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 **Protéger** avec un programme antivirus

Règle 3 **Surveiller** à l'aide du pare-feu

Règle 4 **Prévenir** avec les mises à jour logicielles

Règle 5 **Prendre garde** et faire preuve de vigilance

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

1

Sauvegarder les données

Quelle valeur 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 un nuage de stockage en ligne.
- Vérifiez que les données ont effectivement été copiées et qu'elles peuvent être restaurées.
- Afin de protéger au mieux les données sauvegardées contre l'attaque d'un malware, le disque dur de sauvegarde ne doit être connecté qu'au moment de son utilisation. De même, il convient de se connecter à son nuage de stockage uniquement pendant le processus de sauvegarde et de se déconnecter lorsque celui-ci est terminé.

De nos jours, ordinateurs, tablettes et smartphones contiennent une foule de données sous la forme de documents de texte, courriels, photos, vidéos, musique et autres. Or, on ne peut exclure l'éventualité que ces données puissent être détruites, 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) ou à cause de la vermine qui circule 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 !**

www.ebas.ch/step1

Le pare-brise vous protège !
L'antivirus vous débarrasse de la vermine numérique !

2

Protéger avec un programme antivirus

Quels virus arrivent sur votre ordinateur, tablette ou smartphone ? Pratiquement aucun, si vous avez installé un programme de protection antivirus.

Principaux conseils à suivre

- Utilisez un programme antivirus parfaitement à jour
- Configurez le programme de protection antivirus pour qu'il procède automatiquement à sa mise à jour. De cette manière, il sera correctement armé pour se défendre contre les dernières menaces présentes sur le Net.
- Vérifiez régulièrement que votre ordinateur ou que votre dispositif mobile n'a pas été infecté. Pour cela, faites analyser l'ensemble du système par le programme antivirus en procédant à une analyse complète du système.

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, ces fameux malwares qui peuvent se présenter sous la forme de virus, vers ou chevaux de Troie. L'ensemble des données stockées peut ainsi être consulté, manipulé, voire même effacé par des tiers non-autorisés.

→ **Protégez vos dispositifs au moyen d'un programme antivirus !**

www.ebas.ch/step2

Avec un garage, votre voiture est à l'abri des voleurs !
Avec un pare-feu, vos données le sont aussi!

3

Surveiller à l'aide du pare-feu

Avez-vous bien fermé les «portes» de votre ordinateur ou de vos dispositifs mobiles ? Un pare-feu activé permet de sécuriser leur fermeture tout en surveillant le trafic Internet de votre appareil.

Principaux conseils à suivre

- Le pare-feu embarqué de votre système d'exploitation doit absolument être activé avant de connecter votre dispositif à Internet ou à tout autre réseau.
- Certains programmes en ligne, comme par exemple les jeux en ligne, exigent l'ouverture de certaines «portes d'accès» (ports). Dans ce cas, veillez à ce que seuls les ports nécessaires soient ouverts mais ne désactivez pas complètement votre pare-feu.

Lorsque les internautes naviguent sur Internet depuis leur ordinateur, tablette ou smartphone, des «portes d'accès» invisibles (ports) s'ouvrent sur les différents dispositifs qui se trouvent ainsi exposés aux attaques des cybercriminels. Une fois installé, le pare-feu réduit autant que possible l'ouverture de ces portes et surveille le trafic de données entre les dispositifs et la toile. Le pare-feu tire la sonnette d'alarme dès qu'il détecte un trafic «suspect».

→ **Surveillez vos communications Internet à l'aide d'un pare-feu !**

www.ebas.ch/step3

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

4

Prévenir avec les mises à jour logicielles

Qui d'autre mieux que le fabriquant de vos programmes peut agir pour assurer leur sécurité ? Effectuez la maintenance de vos programmes et applications en vous procurant régulièrement les dernières mises à jour. Vous ferez ainsi le choix de la sécurité.

Principaux conseils à suivre

- Activez la fonction Mises à jour automatiques pour tous les programmes et applications installés (en particulier pour le système d'exploitation, le programme antivirus, le pare-feu, le navigateur et ses plugins, ainsi que pour les programmes de visualisation de fichiers).
- Programmes, applications et leurs mises à jour respectives doivent toujours être téléchargées depuis le site officiel du fabricant et non sur les sites de fournisseurs tiers.
- Pour accéder à Internet, votre navigateur doit être parfaitement à jour.

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

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

www.ebas.ch/step4

Sagesse au volant !
Bon sens sur Internet!

5

Prendre garde et faire preuve de vigilance

Comment se comporter de manière responsable ? Ne croyez pas tout ce que l'on raconte sur la toile et observez une méfiance de bon aloi lorsque vous naviguez sur Internet. Par ailleurs, protégez votre ordinateur et vos dispositifs mobiles avec un mot de passe sécurisé.

L'utilisateur représente très souvent le premier facteur de risque. À vous donc de faire preuve de bon sens ! Exemple : dans les cas d'une attaque de phishing par courriel ou par téléphone, des escrocs peuvent se faire passer pour votre institut financier et essayer de vous attirer sur un site contrefait qui ressemble presque parfaitement à celui de votre banque. Si vous tombez dans le panneau et que vous communiquez vos codes d'accès, les malfaiteurs pourront dévaliser votre compte en toute tranquillité. **N'oubliez jamais qu'un institut bancaire sérieux ne vous demandera jamais vos données d'accès à son service de banque en ligne.** Faites donc preuve du juste degré de méfiance !

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 (que ce soit par email ou 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 domestique.

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 par un attaquant. 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 convient d'en trouver un différent pour chaque compte et de ne jamais communiquer vos sésames à qui que ce soit. Mémorisez vos mots de passe ou conservez-les sous forme écrite dans un lieu sûr.

- Choisissez des mots de passe de 10 caractères au moins. Ils doivent être composés d'une combinaison arbitraire de chiffres, de lettres majuscules et minuscules, et de caractères spéciaux.
- Ne communiquez à personne vos mots de passe et conservez-les toujours en lieu sûr, sous forme chiffrée si possible.
- N'enregistrez pas les mots de passe que vous utilisez pour accéder à des sites protégés dans votre navigateur. Les navigateurs n'assurent généralement pas un niveau de sécurité suffisant pour la gestion de ces mots de passe.

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 : « **M**a **f**ille **T**amara **f**ête **s**on **a**nniversaire **l**e **19** **j**anvier **!** ». Vous obtenez alors une chaîne de caractères apparemment arbitraire mais facile à mémoriser : « **MfTfsal19j!** »

→ Soyez prudent et faites preuve de vigilance sur Internet !

www.ebas.ch/step5

Ce fascicule 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.ebankingentoutesecurite.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.ebankingentoutesecurite.ch
  https://www.ebas.ch
- 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

SKPPSC

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

www.skppsc.ch