Communiqué de presse du 5 mai 2021

Vos mots de passe sont-ils sûrs?

La journée mondiale du mot de passe ainsi qu'une semaine nationale d'action visent à améliorer la sécurité dans l'espace numérique

Le 6 mai 2021, les mots de passe seront à l'honneur en Suisse – et pas seulement à cause de la journée mondiale du mot de passe. Ce thème sera encore abordé sous toutes ses facettes, ce jour-là, dans le cadre de la semaine nationale d'action sur la «sécurité du cyberespace». Les personnes intéressées découvriront de précieux conseils et astuces à l'adresse www.S-U-P-E-R.ch. Outre la gestion des mots de passe, ce site évoque en détail les thèmes de la sauvegarde des données, des mises à jour de sécurité, de la protection contre les virus et du comportement adéquat sur Internet. La semaine d'action est organisée du 3 au 7 mai 2021 et constitue un projet commun des autorités ainsi que des milieux scientifiques et économiques.

Depuis quelques années, le nombre de services accessibles moyennant inscription a explosé dans le cyberespace. Les ordinateurs, les tablettes, les smartphones, l'e-banking, les comptes de messagerie, les boutiques en ligne et quantité d'autres services exigent un mot de passe. «Pour se simplifier la tâche, les internautes choisissent souvent des mots de passe simples, qu'ils réutilisent pour plusieurs comptes. Les cybercriminels se frottent les mains», explique Fabian Ilg, directeur suppléant de la Prévention Suisse de la Criminalité (PSC). La journée mondiale du mot de passe, lancée en 2013 par Intel Corporation, s'attaque à ce problème et appelle chacun de nous à gérer de manière plus responsable ses mots de passe. En effet, les cybercriminels ont tôt fait de deviner ou de découvrir par tâtonnement les mots de passe trop simples.

Semaine nationale d'action sur la sécurité numérique

Dans le sillage de la journée mondiale du mot de passe, la Prévention Suisse de la Criminalité (PSC) organise une semaine d'action avec le concours du Centre national pour la cybersécurité (NCSC), de la plateforme «eBanking – en toute sécurité!» de la Haute école de Lucerne (HSLU), de la plateforme pour la sécurité sur Internet iBarry de la Swiss Internet Security Alliance (SISA), ainsi que des corps de police cantonaux et municipaux. Une campagne de sensibilisation sera menée du 3 au 7 mai 2021, avec son propre site: www.S-U-P-E-R.ch. Outre les mots de passe, elle abordera les thèmes de la sauvegarde des données, des mises à jour de sécurité, de la protection contre les virus, du comportement adéquat sur Internet, et livrera quantité de trucs et astuces simples et efficaces.

6 règles pour créer des mots de passe sûrs, et une astuce

Les mots de passe restent à ce jour le moyen d'authentification le plus répandu dans l'environnement électronique. Ils permettent à chacun de contrôler l'accès à ses données sensibles ou privées. Quelques règles vous aideront à mieux vous protéger. Respectez-les pour tous vos mots de passe:

- le mot passe aura une longueur minimale de 12 signes;
- il s'agira d'une combinaison de chiffres, de majuscules, de minuscules et de caractères spéciaux;
- toute succession de touches, comme «asdfgh» ou «45678», est à bannir;
- n'utilisez pas des mots d'une langue connue: le mot de passe ne doit pas avoir de sens;
- veillez à ne pas employer partout le même mot de passe;
- ne conservez jamais en clair un mot de passe.

Les mots de passe créés selon ces règles sont plus compliqués à retenir. Il existe toutefois une astuce pour générer des mots aisés à mémoriser:

- Composez une phrase qui vous parle, et créez votre mot de passe à l'aide de la première lettre de chaque mot et des chiffres employés:
  Ma **f**ille **T**amara **M**artin **a** **s**a **f**ête **l**e **19** **j**anvier!
- Vous obtiendrez ainsi un mot de passe conforme aux six règles énoncées et dont vous vous souviendrez aisément: **MfTMasfl19j!**
- Utilisez un gestionnaire de mots de passe. Vous n'aurez ensuite qu'à mémoriser le mot de passe donnant accès à tous les autres. Et vous aurez au passage la vue d'ensemble de tous vos comptes en ligne.

Outre un mot de passe sûr, l'authentification à deux facteurs assure une protection accrue de vos comptes.

La prévention reste le meilleur moyen d'agir

Les cybercriminels piratent les mots de passe pour toutes sortes de motifs: ils peuvent utiliser incognito l'équipement de tiers à des fins criminelles, piller des données privées aussi sensibles que le code d'accès à vos comptes bancaires, ou vous interdire l'accès à vos propres données. «Les enquêtes cybercriminelles sont d'une grande complexité, pour un bilan souvent maigre. La prévention est d'autant plus importante», explique Fabian Ilg, spécialiste en cybercriminalité à la PSC, avant d'exprimer un regret: «rares sont les personnes qui dénoncent les cyberattaques à la police, alors même que le préjudice personnel et financier causé peut être considérable.»

C'est là qu'intervient la semaine nationale d'action, en montrant que les internautes peuvent améliorer leur sécurité personnelle avec des moyens très simples et à peu de frais – en veillant à choisir des mots de passe robustes et à actualiser régulièrement leurs logiciels, en faisant très attention et en restant méfiants dans le cyberespace.

Pour en savoir plus

www.S-U-P-E-R.ch

Matériel graphique

Le matériel graphique est disponible ici. Il ne peut pas être modifié et ne peut être utilisé que dans le cadre d'un compte rendu de la campagne.

Partenaires organisationnels

Prévention Suisse de la Criminalité
«eBanking – en toute sécurité!» – plateforme indépendante de la Haute école de Lucerne
Centre national pour la cybersécurité NCSC
iBarry – Plateforme pour la sécurité sur Internet

Contact pour les questions générales des médias

Fabian Ilg, directeur suppléant
Prévention Suisse de la Criminalité PSC
Maison des cantons
Speichergasse 6
3001 Berne
fi@skppsc.ch
Tél.: +41 31 511 00 08

Interview mise à disposition

Cette interview ne peut être citée que dans le cadre d'un compte rendu de la semaine d'action. La personne doit être préalablement contactée pour toute utilisation de ses propos dans un contexte différent ou sous une forme modifiée.

«Pas besoin de toujours changer de mot de passe.»

Oliver Hirschi, professeur et responsable de la plateforme «eBanking – en toute sécurité!» à la Haute école de Lucerne
oliver.hirschi@hslu.ch / +41 41 757 68 58

À quoi reconnaît-on un bon mot de passe?
Il s'agit d'empêcher autant que possible un pirate de deviner votre mot de passe ou de le trouver en tâtonnant. Par conséquent, plus le mot de passe est long et complexe, et moins il risque d'être découvert.

Comment faire?
Il convient tout d'abord de choisir un mot de passe fort. Nous avons résumé les principales règles à suivre sur le site www.S-U-P-E-R.ch. Ensuite, un mot de passe différent sera utilisé par identifiant (login). Moyennant cette précaution, il est inutile de changer à tout moment de mot de passe, comme on le prétend souvent. Il est encore possible de faire appel à un gestionnaire de mots de passe, dont quelques-uns sont décrits sur le site précité.

Quels sont les risques inhérents aux mots de passe faibles?
La situation peut devenir gênante si, par exemple, des pirates s'emparent du mot de passe de services comprenant des moyens de paiement – de telles informations risquent d'être interceptées et utilisées à mauvais escient. En cas d'intrusion dans vos appareils, des escrocs pourront dérober vos données ou installer des maliciels.