4.

PROTÉGEZ VOS DONNÉES IMPORTANTES

De la même manière que vous prenez soin des objets de valeur chez vous, prenez soin des données que vous stockez en ligne.

Un **nettoyage ciblé** est parfait pour effectuer quelques améliorations rapides. Cherchez des informations précises dans votre messagerie ou tout autre compte et supprimez-les : des numérisations de vos pièces d'identité, vos coordonnées bancaires ou vos informations d'assurance maladie, par exemple. Si vous pensez avoir besoin de ces données et documents par la suite, vous pouvez toujours les télécharger ou les imprimer avant de les supprimer de votre messagerie.

Un **nettoyage en profondeur** sera plus efficace. Il est bon d'en faire un par an. Archivez toutes les données de vos comptes de messagerie ou de médias sociaux, téléchargez-les et supprimez-les de vos comptes pour repartir de zéro.

Conseil : Supprimer ne suffit pas, videz votre corbeille et effacez les fichiers temporaires !

À vous de décider si vous voulez enregistrer vos archives et documents sur un service de cloud ou les conserver sur un disque dur externe ou une clé USB. Employez la méthode qui vous convient le mieux et, quel que soit votre choix, faites en sorte de ne pas perdre vos données et de les protéger avec un mot de passe robuste.

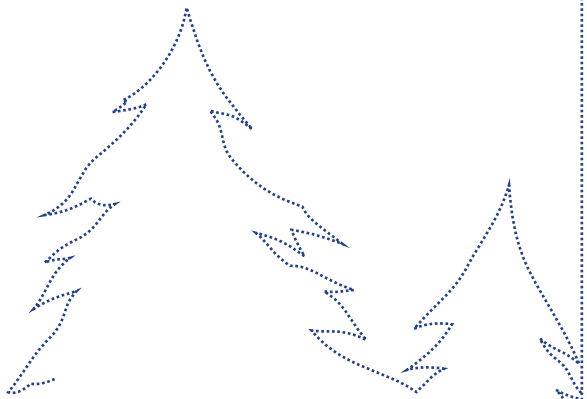
5.

PASSEZ LE MESSAGE

Lorsque vous sécurisez vos comptes, renforcez vos mots de passe et nettoyez vos données, ce sont **tous·tes celles et ceux à qui vous êtes connecté·es qui en bénéficient et gagnent en sécurité.**

Lorsque vous nettoyez vos comptes de messagerie et de médias sociaux, réfléchissez à ce que vous pourriez télécharger et supprimer qui pourrait aider vos proches et collègues : les coordonnées bancaires de votre sœur, le code de la porte de votre bureau, ou encore une numérisation du passeport de votre fils sont des données qui, si elles tombaient entre de mauvaises mains, pourraient vous causer bien des soucis.

Passez le message ! Il suffit de suivre quelques étapes simples pour améliorer votre sécurité en ligne. Faites passer ce Data Detox (détox de données) à vos proches ou vos collègues pour les aider à changer leurs habitudes à leur rythme.



DATA DETOX KIT

CHANGEZ VOS PARAMÈTRES

pour protéger vos données

Si internet ne servait qu'à échanger des photos de chiens en costumes de dinosaures, nous n'aurions pas besoin de mots de passe. Mais sur internet, vous pouvez aussi payer vos factures, renouveler vos ordonnances et vous enregistrer sur les listes électorales. Réfléchissez à toutes les données personnelles et importantes que vous faites transiter par internet et que vous stockez sur vos appareils. **Pourquoi devraient-elles moins bien protégées que vos clés ou votre portefeuille ?**

Il existe un bon moyen d'empêcher les autres d'accéder à vos données importantes : **choisissez des mots de passe difficiles à deviner.** La plupart du temps, aucune compétence technique n'est nécessaire pour accéder à vos comptes. Il suffit de quelques tentatives pour deviner un mot de passe, ou d'utiliser un programme qui le fait automatiquement.

Et lorsqu'une personne a accès à un compte, elle peut essayer d'utiliser le mot de passe de ce dernier pour accéder à d'autres comptes, rassembler des informations sur vous et vos habitudes, prendre le contrôle de vos comptes, voire de votre identité en ligne.

En suivant ce Data Detox (détox de données), vous trouverez des mesures concrètes pour améliorer votre sécurité en ligne.

Allons-y !

Produit par
TACTICAL TECH

Avec le soutien de
Firefox

datadetoxkit.org
#datadetox

1.

VERROUILLEZ LA PORTE DE VOTRE UNIVERS NUMÉRIQUE

La protection de votre téléphone, tablette ou ordinateur, sera toujours meilleure avec n'importe quel type de verrouillage que sans. Et à l'image des différents types de verrous que vous pouvez avoir à vos portes, **certains écrans de verrouillage sont plus robustes que d'autres.**

De tous les verrouillages existants, les mots de passe longs et uniques sont la meilleure protection. Cela signifie que si vous utilisez un mot de passe pour protéger votre appareil, il doit comprendre des lettres, des chiffres et des caractères spéciaux.

Si vous déverrouillez votre téléphone tout simplement en faisant glisser votre doigt sur votre écran, vous pouvez augmenter le niveau de sécurité en passant à un long mot de passe. Si vous utilisez un motif de verrouillage, pourquoi ne pas en choisir un plus long ? Votre code PIN est 1234 ? Vous pourriez lancer des dés sept fois et utiliser les chiffres obtenus en guise de code PIN.

Une petite modification peut avoir un énorme impact sur le contrôle que vous avez sur vos appareils.

2.

RÉGLEMENTER LES ACCÈS

Pour créer des mots de passe de qualité, c'est simple. Il suffit de respecter quelques règles de base. Vos mots de passe doivent être :

Longs : **les mots de passe doivent être composés de 8 caractères au minimum. Pour un mot de passe encore plus sécurisé, employez entre 16 et 20 caractères !**

Uniques : **chaque mot de passe – pour chaque site – doit être différent.**

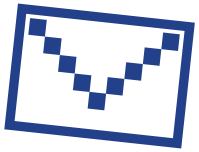
Aléatoires : **vos mots de passe ne doivent pas suivre un schéma logique ou être trop faciles à deviner. Un gestionnaire de mots de passe vous sera donc très pratique.**

Les meilleurs mots de passe sont composés de lettres, de chiffres et de caractères spéciaux. Il n'y a toujours pas de meilleur conseil pour créer un mot de passe robuste et difficile à deviner. Certains systèmes ne vous permettent toutefois pas d'utiliser des caractères spéciaux (comme @#$%-=+), mais une longue combinaison de lettres et de chiffres sera toujours meilleure qu'un mot de passe plus court.

La solution idéale est d'utiliser un **gestionnaire de mots de passe** pour générer et stocker tous vos mots de passe. Il s'agit d'un logiciel — comme 1Password ou KeePassXC, qui sont recommandés par des experts en matière de sécurité — dont la fonction principale est de protéger vos identifiants et autres données sensibles.

3.

AJOUTEZ UN DEUXIÈME VERROU



En instaurant une vérification en deux étapes (2FA) ou une authentification multi-facteurs (MFA), même si quelqu'un trouve votre mot de passe, **il lui manquera probablement les informations d'authentification associées pour accéder à votre compte.**

Consultez les paramètres de sécurité des sites et applications que vous utilisez le plus souvent pour voir si cette fonctionnalité est disponible. Commencez par les plus importants — les applications bancaires, ou les services de messagerie que vous utilisez pour récupérer les informations d'accès à vos autres comptes.

Google:
Connectez-vous à myaccount.google.com → Sécurité → Validation en deux étapes → Commencer

Facebook:
Menu → Paramètres → Sécurité et connexion → Utiliser l'authentification à deux facteurs

Conseil : Au moment d'établir un niveau de vérification supplémentaire, vous devrez sélectionner un autre moyen de confirmer votre identité. Évitez de choisir les SMS (messages textuels envoyés à votre téléphone), au cas où vous perdriez votre téléphone. Un e-mail est généralement plus fiable.