



Votre bulletin mensuel sur la sensibilisation à la sécurité



# Le nettoyage de printemps numérique en 7 étapes simples

## Aperçu

Nous entendons souvent parler de "nettoyage de printemps", cette période de l'année où nous faisons le tri dans nos affaires et organisons notre maison et nos vies en vue de l'été à venir. C'est aussi le moment idéal pour faire un bilan annuel de votre vie numérique. Ces sept mesures simples, à faire une fois par an, vous permettront de tirer le meilleur parti de la technologie, en toute sécurité.

**COMPTES** : Passez en revue chacun de vos comptes. L'utilisation d'un mot de passe long et unique pour chaque compte garantit que si l'un d'entre eux est compromis, vos autres comptes sont toujours en sécurité. Vous ne pouvez pas vous souvenir de tous ces mots de passe ? Ne vous inquiétez pas, nous non plus. Nous vous recommandons d'utiliser un gestionnaire de mots de passe pour stocker en toute sécurité tous vos mots de passe et vous rendre la vie beaucoup plus simple et plus sûre. Enfin, activez l'authentification à deux facteurs dès que possible, en particulier pour les comptes de messagerie ou financiers. C'est la mesure la plus importante que vous puissiez prendre pour sécuriser un compte en ligne. Si vous avez des comptes en ligne auxquels vous n'avez pas accédé depuis plus d'un an, il est peut-être temps de les supprimer tout simplement.

**PROGRAMMES** : En maintenant vos appareils et logiciels à jour, vous vous assurez que les dernières fonctions de sécurité sont installées et que les vulnérabilités connues sont corrigées. Le moyen le plus simple d'y parvenir est de vous assurer que la mise à jour automatique est activée sur tous vos ordinateurs, appareils mobiles et même appareils domestiques intelligents. Supprimez tous les programmes ou applications inutilisés sur vos appareils mobiles et ordinateurs. Certaines applications nécessitent de grandes quantités de stockage, peuvent introduire de nouvelles vulnérabilités et peuvent même ralentir vos appareils. Moins vous avez d'applications, plus votre système et vos informations sont sécurisés. De nombreux appareils vous indiquent le temps écoulé depuis que vous avez utilisé une application. Si cela fait plus de quelques mois, il est probable que vous n'en ayez pas besoin !

**FINANCES** : Assurez-vous que vos comptes bancaires et comptes de retraite sont configurés pour vous alerter chaque fois qu'une transaction est effectuée, en particulier pour les achats importants ou les transferts d'argent. Ainsi, vous serez toujours informé lorsqu'une transaction financière est effectuée et vous pourrez repérer immédiatement toute fraude ou activité non autorisée. Plus tôt vous détectez une activité frauduleuse, plus tôt vous pouvez l'arrêter. Selon le pays dans lequel vous vivez, un gel des avoirs peut être l'un des moyens les plus efficaces de protéger votre identité.

**Se débarrasser de ses appareils** : Au fil du temps, vous pouvez vous retrouver à collecter de vieux appareils dont vous n'avez plus besoin - peut-être un vieux smartphone ou un appareil de maison intelligente. Si vous vous débarrassez de l'un de ces appareils, effacez d'abord toutes les informations personnelles qu'il contient. La plupart des appareils disposent d'une fonction d'effacement simple qui permet de purger en toute sécurité toutes les informations personnelles (ou de rétablir les paramètres d'usine) avant de jeter l'appareil.

**SAUVEGARDES** : Quel que soit votre niveau de sécurité, vous aurez probablement besoin à un moment donné de sauvegardes pour récupérer vos informations importantes. Configurez vos appareils pour qu'ils effectuent automatiquement des sauvegardes sur le cloud. La création et la planification de sauvegardes automatiques vous permettent de récupérer vos informations les plus importantes.

**L'ÉDUCATION DES ENFANTS** : Si vous êtes un parent ou un tuteur, c'est le moment de revoir tous les paramètres de contrôle parental que vous avez mis en place pour les enfants. Au fur et à mesure que les enfants grandissent, vous devrez probablement mettre à jour les paramètres de ces contrôles..

**RÉSEAUX SOCIAUX** : Vérifiez les paramètres de confidentialité de vos comptes de réseaux sociaux - ils constituent une mine d'or d'informations personnelles. Passez en revue vos comptes pour vérifier que vous ne partagez pas d'informations sensibles telles que votre date d'anniversaire, votre numéro de téléphone, votre adresse personnelle, vos informations bancaires ou votre géolocalisation dans vos photos personnelles.

En consacrant seulement quelques heures par an à ces mesures, vous contribuerez grandement à votre protection, à celle de vos appareils et de vos informations.

## Rédacteur Invité

Ritu Gill (@OSINTtechniques) est un instructeur SANS en développement et un analyste du renseignement spécialisé dans le renseignement de source ouverte (OSINT). Plus d'informations sur Ritu ici : <https://www.sans.org/profiles/ritu-gill> et ici <https://www.osinttechniques.com>.



## Ressources

**Gestionnaires de mots de passe** : <https://www.sans.org/newsletters/ouch/password-managers/>

**Le pouvoir des mises à jour** : <https://www.sans.org/security-awareness-training/resources/power-updating>

**Se débarrasser de vos appareils mobiles** : <https://www.sans.org/newsletters/ouch/disposing-mobile-devices/>

**Les sauvegardes** : <https://www.sans.org/security-awareness-training/resources/got-backups>

**La sécurité en ligne pour les enfants** :

<https://www.sans.org/newsletters/ouch/online-security-kids/>

**Traduit pour la communauté par : Juliette Busson**

OUCH! Est publié par SANS Security Awareness et est distribué sous la licence [Creative Commons BY-NC-ND 4.0](https://creativecommons.org/licenses/by-nc-nd/4.0/). Vous êtes libre de partager ou de distribuer ce bulletin d'information, à condition de ne pas le vendre ou le modifier. Comité de rédaction : Walter Scrivens, Phil Hoffman, Alan Waggoner, Leslie Ridout, Princess Young.