Votre bulletin mensuel sur la sensibilisation à la sécurité

# Les meilleurs conseils de cybersécurité pour les vacances

## Aperçu

Comme la saison des vacances approche, des millions de personnes vont voyager. Si vous faites partie de ces gens là, voici quelques conseils pour vous aider à garder le contact avec internet en toute sécurité.

- **Appareils mobiles** : Amenez le moins d'appareils possible. Moins vous emportez d'appareils, moins vous avez de chance de les perdre ou de vous les faire voler. En effet, saviez-vous que vous avez beaucoup plus de chance de perdre un appareil que de vous le faire voler ? Quand vous quittez une chambre d'hôtel, un restaurant, un taxi, un train ou un avion, vérifiez que vous n'avez pas laissé d'appareils derrière vous. Assurez-vous que les amis ou la famille avec qui vous voyagez vérifient aussi derrière eux, comme un enfant qui aurait laissé un appareil sur un siège ou au restaurant.

  En ce qui concerne les appareils que vous choisissez d'emmener, assurez-vous qu'ils soient à jour pour qu'ils fonctionnent avec le dernier système d'exploitation et des applications mises à jour. Maintenez le verrouillage automatique de l'écran activé. Si possible, assurez-vous d'avoir un moyen de localiser vos appareils à distance s'ils sont perdus. Vous avez également l'option d'effacer les données de vos appareils à distance. De cette manière, si un de vos appareils est volé ou perdu, vous pouvez le localiser et/ou effacer toutes vos données et connexions à vos comptes à distance. Enfin, faites une sauvegarde de tous les appareils que vous emmenez avec vous pour pouvoir récupérer vos données si vous perdez ou si vous vous faites voler votre appareil.

- **Réseau WI-Fi :** Lorsque vous voyagez, vous aurez peut être besoin de vous connecter à un réseau Wi-Fi public. Gardez à l'esprit que vous n'avez souvent aucune idée de qui a configuré le réseau Wi-Fi, qui s'en occupe et comment, et qui d'autre est connecté dessus. Au lieu de vous connecter à un réseau Wi-Fi public, quand c'est possible, utilisez le partage de connexion de votre téléphone. De cette manière, vous savez que vous avez une connexion sûre. Si cela n'est pas possible et vous devez vous connecter à un réseau Wi-Fi public (à l'aéroport, à l'hôtel ou dans un café par exemple), utilisez un Réseau Privé Virtuel, plus souvent appelé VPN (Virtual Private Network). C'est un logiciel que vous installez sur votre ordinateur ou sur vos appareils mobiles qui vous aide à protéger et à anonymer votre connexion Wi-Fi. Certaines solutions VPN incluent des réglages qui activent automatiquement le VPN lors des connexions à des réseaux Wi-Fi non fiables.

- **Ordinateurs publics** : Évitez d'utiliser des ordinateurs publics, tels que ceux mis à disposition dans les hôtels ou les cafés, pour vous connecter à vos comptes ou accéder à des données sensibles. Vous ne savez pas qui a utilisé cet ordinateur avant vous. L'ordinateur peut comporter un virus ou être infecté volontairement par un logiciel malveillant tel qu'un enregistreur de frappe. N'utilisez que des appareils que vous pouvez contrôler et qui sont sûrs.

- **Réseaux sociaux** : Nous adorons partager avec les autres nos voyages et nos aventures à travers les réseaux sociaux, mais nous ne savons pas toujours quels amis sont en ligne. Évitez de trop partager lorsque vous êtes en vacances et attendez de rentrer chez vous pour partager sur vos vacances. De plus, ne partagez pas de photos de cartes d'embarquement, permis de conduire ou passeports car cela peut conduire à une usurpation d'identité.

- **Travail** : Si vous travaillez pendant vos vacances (nous espérons que ce n'est pas le cas !), renseignez-vous à l'avance sur les règles en matière de télé-travail, y compris les appareils et données que vous avez le droit d'emmener avec vous et comment vous connecter à distance aux systèmes de travail en toute sécurité.

Les vacances devraient être un moment pour se relaxer, explorer et s'amuser. Ces quelques étapes simples vous permettront de le faire en toute sécurité.

## Rédacteur Invité

Princess Young est analyste principale chez Southwest Airlines et dirige l'éducation et les formations en matière de cybersécurité pour 60 000 employés dans tout le pays. Princesse aime s'engager auprès des employés afin qu'ils se sentent compétents pour partager la responsabilité de la cybersécurité, quel que soit leur rôle ou leur titre.

## Ressources

**Sécuriser vos appareils mobiles :** https://www.sans.org/security-awareness-training/ouch-newsletter/2018/securing-your-mobile-devices
**Attaques personnalisées :** https://www.sans.org/security-awareness-training/resources/power-updating
**Réseau Privé Virtuel :** https://www.sans.org/newsletters/ouch/Virtual-Private-Networks/
**Attaques personnalisées :** https://www.sans.org/security-awareness-training/resources/got-backups

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