KEEPER® | Communiqé de presse

C'est la saison ! Comment éviter les cybermenaces liées aux jouets électroniques ?

Partageons les fêtes, et non nos informations personnelles ! Keeper Security vous propose les bonnes pratiques pour protéger votre vie privée et rester en sécurité pendant les fêtes de fin d'année.

CHICAGO, 21 décembre 2023 – Les fêtes de fin d'année s'accompagnent de la joie d'offrir des cadeaux, et il y a une magie particulière de présenter les dernières technologies à ceux que l'on aime. Qu'il s'agisse de gadgets innovants qui stimulent la créativité ou d'appareils interactifs qui rassemblent les familles, les jouets technologiques peuvent ajouter une couche supplémentaire d'excitation et d'émerveillement aux festivités. Keeper Security, le principal fournisseur de logiciels de cybersécurité Zero Truste et Zero Knowledge protégeant les mots de passe et les passkeys, souhaite sensibiliser à l'importance de la protection des données personnelles et de la vie privée à l'occasion des festivités de fin d'année.

Au milieu de la joie des réunions de famille et de l'excitation que suscitent les nouveaux gadgets technologiques, il est essentiel d'adopter les bonnes pratiques pour protéger sa vie privée, sa sécurité et la sécurité numérique de sa famille. Les fêtes de fin d'année sont une période où les cybercriminels sont particulièrement actifs, profitant de l'agitation pour exploiter les personnes qui ont baissé leur garde.

"Alors que nous nous réjouissons d'offrir des cadeaux pendant les fêtes de fin d'année, il est essentiel de reconnaître les risques inhérents aux gadgets technologiques. De la collecte de données aux vulnérabilités, ces appareils peuvent constituer une menace existentielle sérieuse pour la vie privée et la sécurité des enfants et des familles", a déclaré Darren Guccione, CEO et cofondateur de Keeper Security. "Tout le monde devrait prendre des mesures concrètes pour sécuriser son réseau domestique et ses gadgets technologiques afin de s'assurer que la magie des fêtes de fin d'année ne compromette pas la sécurité en ligne."

Dans le cadre de son engagement envers la sécurité des utilisateurs, Keeper conseille vivement aux consommateurs de prendre les précautions suivantes, qu'ils installent un nouveau jouet ou qu'ils ouvrent leur maison à leurs proches :

- **Protéger vos nouveaux appareils :** La plupart des appareils IoT sont livrés avec des mots de passe prédéfinis en usine qui doivent être modifiés immédiatement. Créez un mot de passe fort et unique pour le compte associé à chaque appareil en utilisant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Un gestionnaire de mots de passe permet de générer des mots de passe complexes et de les stocker en toute sécurité dans un coffre-fort chiffré, ce qui simplifie le processus.
- **Sécurisez votre réseau WiFI** : Assurez-vous que votre réseau WiFi est protégé par un mot de passe fort, changez le nom du réseau pour qu'il ne soit pas celui par défaut,

activez le chiffrement de votre routeur que vous pouvez activer dans les paramètres, et mettez régulièrement à jour le logiciel de votre routeur pour installer les nouveaux correctifs de sécurité. Si vous devez partager le mot de passe WiFi, utilisez un outil de partage chiffré tel que One-Time Share de Keeper et changez votre mot de passe après le départ de vos invités.

- **Vérifiez les paramètres de confidentialité** : Lorsque vous vérifiez les paramètres de confidentialité des nouveaux jouets, assurez-vous que la collecte de données est limitée et conforme à la réglementation, et vérifiez les autorisations afin d'éviter tout accès inutile à des fonctions telles que les caméras ou les microphones. Activez les options de suppression des données lorsqu'elles sont disponibles.
- **Mettez à jour les firmwares et les logiciels** : Assurez-vous que vos jouets intelligents utilisent les dernières mises à jour du firmware et du logiciel. Les fabricants publient régulièrement des mises à jour pour corriger les failles de sécurité qui pourraient être exploitées par des cybercriminels. Allez dans les paramètres pour mettre à jour manuellement ou activer les mises à jour automatiques.
- **Utilisez le contrôle parental** : En activant et en personnalisant le contrôle parental, vous pouvez gérer l'accès à des contenus adaptés à l'âge de l'enfant, limiter les interactions en ligne et atténuer les risques potentiels associés à des acteurs malveillants qui cherchent à intimider ou à exploiter votre enfant.
- **Activez l'authentification multi-facteurs** : La mise en œuvre de l'authentification multi-facteurs est une mesure proactive qui garantit que seuls les utilisateurs autorisés peuvent contrôler et interagir avec un jouet ou un appareil, minimisant ainsi le risque d'accès non autorisé ou d'altération par des acteurs malveillants.
- **Communiquez avec vos enfants** : Une étude menée par Keeper a révélé que 30 % des parents n'ont jamais parlé de cybersécurité à leurs enfants. Ouvrez le dialogue avec votre famille sur la nécessité de pratiquer une bonne cyberhygiène, de n'utiliser que des contenus adaptés à l'âge de l'enfant et de limiter le temps passé devant l'écran.

Pour atténuer les risques en matière de protection de la vie privée et de sécurité associés aux nouveaux cadeaux technologiques, il est essentiel que les consommateurs soient conscients des méthodes de traitement des données de chaque jouet technologique, qu'ils mettent à jour les paramètres de leur appareil pour améliorer la sécurité et qu'ils se tiennent informés des vulnérabilités potentielles. En restant vigilants et informés, nous pouvons faire en sorte que l'esprit des fêtes se prolonge par une expérience numérique sûre et respectueuse de la vie privée pour nous-mêmes et nos proches.

###

A propos de Keeper Security:
Keeper Security transforme la cybersécurité pour les personnes et les organisations du monde entier. Les solutions de Keeper, abordables et faciles à utiliser, sont construites sur la base d'une sécurité Zero Trust et Zero Knowledge pour protéger chaque utilisateur sur chaque appareil. La solution de gestion des accès privilégiés de nouvelle génération Keeper se déploie

en quelques minutes et s'intègre de manière transparente à n'importe quelle stack technologique pour prévenir les violations, réduire les coûts du service d'assistance et garantir la conformité.Des millions de personnes et des milliers d'organisations font confiance à Keeper, le leader en matière de gestion de mots de passe et de passkeys, de gestion des secrets, d'accès privilégié, d'accès à distance sécurisé et de messagerie chiffrée.

Pour en savoir plus, visitez le site KeeperSecurity.com
Suivre Keeper: Facebook Instagram LinkedIn X YouTube

Contact Presse :

Christelle Klein :
06 63 97 01 67
cklein@hl-com.com