Violations de données sur les réseaux sociaux - portrait de 2020

Devolutions

IL Y AURA EU DE NOMBREUSES VIOLATIONS DE DONNÉES DE HAUT NIVEAU SUR LES RÉSEAUX SOCIAUX EN 2020

Il reste encore quelques semaines à l'année, mais on peut déjà dire qu'il y aura eu de nombreuses violations de données de haut niveau sur les réseaux sociaux en 2020. En voici quelques exemples :

- En février, Twitter a suspendu un vaste réseau de faux comptes utilisés pour associer les numéros de téléphone aux utilisateurs.

- En juin, la firme marketing Preen.Me, spécialisés en réseaux sociaux, a révélé que les données personnelles d'environ 100 000 influenceurs avaient été divulguées. La même violation a également mené à la publication des données de plus de 250 000 utilisateurs de médias sociaux sur un forum de piratage sur le deep web.
- En juillet, Twitterverse a sombré dans le chaos lorsque les comptes de certaines des personnalités les plus connues au monde, telles que Barack Obama, Jeff Bezos, Elon Musk et Bill Gates, ont été compromis. Les pirates informatiques ont ciblé un petit nombre d'employés de Twitter avec des attaques d'hameçonnage afin de générer du trafic vers des fraudes Bitcoin.
- En août, des chercheurs de Comparitech ont révélé que les données de près de 235 millions de profils Instagram, TikTok et YouTube étaient exposées et non protégées par des mots de passe ou autre type d'authentification.
- En août, YouTube a supprimé 2 millions de chaînes et 51 millions de vidéos en raison de fraudes.

Les dangers cachés des réseaux sociaux

Ce qui rend les réseaux sociaux si populaires les rend aussi **très risqués** : les gens croient qu'ils communiquent avec des personnes qu'ils connaissent (ou s'ils ne les connaissent pas personnellement, ils leur font confiance) et **ils baissent leur garde**.

Comme mentionné dans un article du New York Times : « L'erreur humaine qui pousse les gens à cliquer sur un lien qui leur est envoyé dans un courriel est exponentiellement plus importante sur les sites de médias sociaux, parce que les gens se considèrent entre amis. »

Conseils pour rester en sécurité

Certains d'entre vous trouveront ces conseils « évidents », mais les évidences ne sont pas tout le temps si « évidentes » justement. Plusieurs de vos collègues professionnels non techniques ne sont pas aussi conscients des cybermenaces que vous. Voici ce qu'il faut garder en tête et expliquer à vos collègues, clients, membres de votre famille et à tous ceux qui souhaitent rester en sécurité :

- **Ne cliquez jamais sur des messages ou des liens suspects**, même s'ils semblent provenir d'une personne que vous connaissez.
- **Ne publiez jamais d'informations personnelles sur les réseaux sociaux**. Les pirates informatiques exploitent régulièrement ces informations afin de créer des profils de victimes potentielles, ainsi que

des indices pour obtenir des réponses aux contrôles de sécurité (par exemple, la ville où vous êtes né, le nom de votre premier animal de compagnie, le nom de votre école secondaire, etc.).

- **Utilisez toujours des mots de passe (ou phrases secrètes) uniques et forts pour chacun de vos comptes de médias sociaux**. On estime en effet que 81 % des violations de données sont le résultat de mots de passe faibles.
- **Utilisez des 2FA/MFA** (authentification à deux facteurs/authentification à facteurs multiples) pour tous vos comptes.
- **Utilisez un gestionnaire de mots de passe fiable.**
- **Ne partagez jamais vos mots de passe avec des collègues, des amis ou des membres de votre famille**. Oui, cela peut être pratique, mais ce n'est pas sécuritaire!
- **Essayez de ne pas vous connecter à des réseaux sociaux lorsque vous utilisez un réseau Wi-Fi public**. Si c'est impossible, utilisez un VPN réputé pour chiffrer vos données et masquer votre identité.

Formation en cybersécurité

Nous vous recommandons également de fournir à vos employés une **formation en cybersécurité**, qui comprend (mais sans s'y limiter) une utilisation sécuritaire des médias sociaux. Comme la formation en personne est un défi de nos jours, nous suggérons d'utiliser une **plateforme de formation en ligne** à la cybersécurité.

L'un des principaux avantages d'un portail en ligne est que les superviseurs et les gestionnaires peuvent suivre les progrès de chaque employé et cibler rapidement les thématiques qui nécessitent une formation supplémentaire. En savoir plus ici.

Partagez vos conseils

Que faites-vous pour rester en sécurité lorsque vous vous immergez dans le magnifique monde des médias sociaux? Partagez vos conseils pour que nous puissions tous ensemble réduire le risque d'être la prochaine victime d'un piratage.