Devolutions

L’importance d’utiliser un gestionnaire de mots de passe

CERTAINES PME UTILISENT UN GESTIONNAIRE DE MOTS DE PASSE ET D’AUTRES NON

Devolutions a récemment interrogé des décideurs dans des PME du monde entier à propos des pratiques et tendances en matière de cybersécurité. Les réponses à chaque question sont présentées dans ce rapport et mises en évidence dans cette infographie.

Ce qui est intéressant dans ce sondage, entre autres, c’est de voir que **certaines PME utilisent un gestionnaire de mots de passe et d’autres non**. C’est donc une bonne et une mauvaise nouvelle à la fois.

La mauvaise nouvelle :

- **47 % des PME autorisent toujours les utilisateurs finaux à réutiliser les mots de passe sur leurs comptes personnels et professionnels**, même s'il s'agit d'un risque majeur pour la sécurité.
- 29 % des PME dépendent de la « mémoire humaine » pour stocker les mots de passe. C'est pourtant la pire pratique en gestion de mots de passe, parce qu'un utilisateur doit garder en mémoire en moyenne 191 mots de passe. Ça l'oblige à saisir des informations d'identification en moyenne 154 fois par mois. C'est juste trop pour la mémoire humaine.
- 15 % des PME n'utilisent AUCUN outil pour protéger ou gérer les mots de passe.

La bonne nouvelle :

- **81 % des PME stockent leurs identifiants dans un gestionnaire de mots de passe pour protéger leurs données personnelles.**
- **88 % des PME offrent une formation en cybersécurité à leurs utilisateurs finaux.** Même si ça devrait être 100 %, c'est un signe que les choses s'en vont dans la bonne direction!
- **76 % des PME estiment que les gestionnaires de mots de passe sont les meilleures solutions pour valider et surveiller les bonnes pratiques en matière de mots de passe.**

La solution

Il y a trois choses que toutes les PME devraient faire pour protéger leurs données, leurs clients et leur réputation : utiliser un gestionnaire de mots de passe, appliquer les bonnes pratiques et éduquer les utilisateurs finaux.

1. Utiliser un gestionnaire de mots de passe

La première chose (et la plus évidente) est d'utiliser un gestionnaire de mots de passe. Dans le meilleur des mondes, il faut une version pour les besoins de l'entreprise et une autre version (personnelle) pour que chaque utilisateur final puisse stocker ses informations d'identification non professionnelles et d'autres informations sensibles. Des recherches ont montré que 81 % des violations de données sont causées par des mots de passe

compromis, faibles et réutilisés, tandis que 29 % de toutes les violations (quel que soit le type d'attaque) impliquent l'utilisation d'informations d'identification volées.

Chez Devolutions, on offre **Password Hub Business pour les entreprises** et **Password Hub Personal** pour les utilisateurs finaux:

- Password Hub Business est un gestionnaire de mots de passe sécurisé et basé sur le nuage conçu pour les équipes. Il permet aux organisations de sécuriser et de gérer facilement et en toute sécurité les mots de passe et autres informations sensibles des utilisateurs via une interface Web conviviale et accessible à partir de n'importe quel navigateur. Cliquez ici pour en savoir plus.
- Password Hub Personal est notre gestionnaire de mots de passe sécuritaire, facile à utiliser et gratuit pour les utilisateurs individuels qui souhaitent stocker des mots de passe personnels dans un coffre sécurisé. Les utilisateurs peuvent facilement créer et accéder à leur propre Password Hub Personal à partir de leur compte Devolutions. Cliquez ici pour en savoir plus.

2. Mettre en place des politiques strictes de gestion des mots de passe

Voici quelques-unes des **bonnes pratiques de gestion des mots de passe que les PME devraient appliquer dès maintenant :**

- Utiliser l'authentification à facteurs multiples
- Utiliser des phrases secrètes complexes
- Changer les mots de passe s'ils sont compromis
- Comparer les mots de passe à une liste connue de mots de passe faibles et compromis
- Appliquer le principe d'accès « juste à temps » pour les comptes privilégiés
- Implanter une politique d'historique des mots de passe
- Éliminer la réutilisation des mots de passe

3. Éduquer les utilisateurs finaux

Un **moyen efficace et abordable d'aider les utilisateurs finaux** à faire partie de la solution – au lieu

de contribuer involontairement au problème – consiste à utiliser une **plateforme de formation sur la cybersécurité**.

Il s'agit d'un portail qui offre aux utilisateurs finaux une **formation pratique** en matière de détection et d'atténuation des menaces. Les utilisateurs apprennent **à leur rythme** avec des simulations réalistes et dynamiques.

Les menaces peuvent inclure les rançongiciels, l'hameçonnage, les attaques DDoS, etc. Le programme de formation peut être personnalisé pour couvrir des sujets spécifiques comme l'ingénierie sociale, la sécurité concernant les courriels, la sécurité des appareils mobiles, la navigation Web sécuritaire, la sécurité et les réseaux sociaux, la protection des informations de santé, etc.

De plus, les superviseurs et les gestionnaires peuvent suivre les progrès de chaque utilisateur final et fournir un encadrement ou des ressources supplémentaires au besoin.

Lisez le rapport

Téléchargez le rapport sur le portrait de la cybersécurité dans les PME en 2020-2021 et **consultez l'infographie** qui met en évidence nos principales conclusions.