1Password

Comment sécuriser **votre personnel hybride**

« Si vous ne veillez pas à ce que vos utilisateurs trouvent facile de faire ce qu'il faut, attendez-vous à ce qu'ils négligent complètement la sécurité. »

La sécurité contre la productivité

Les professionnels de la sécurité ne doivent pas l'oublier : dans l'esprit des employés, la productivité l'emporte souvent sur la sécurité. Quand des pratiques de sécurité sont gênantes, elles sont ignorées.

Ne motivez pas par la peur et n'accablez pas vos utilisateurs. Instaurez une culture favorable à la sécurité en faisant ce qui suit :

- Éliminez les tensions.
- Soyez disponible pour résoudre les problèmes.
- Éduquez et soutenez les utilisateurs.
- Récompensez les choix judicieux et sûrs.

Pourquoi c'est important pour le travail hybride

Shadow IT est une présence constante. Elle constitue désormais une partie intégrante du travail hybride et il convient de la gérer de manière constructive.

Statistiques clés de recherche de 1Password

64 % des employés ont ouvert au moins un compte sans que leur service informatique en soit informé au cours de l'année passée.

33 % d'entre eux ont réutilisé des mots de passe mémorables pour ces comptes.

48,2 % ont utilisé une série de mots de passe semblables.

37 % ont communiqué des identifiants de compte à des collègues.

89 % des personnes qui communiquent des mots de passe sans sécuriser leurs communications utilisent des séries de mots de passe semblables ou réutilisent plusieurs fois le même mot de passe.

Cultiver une culture de la sécurité

Des relations ouvertes : Les employés doivent sentir que les équipes chargées de la sécurité se soucient d'eux.

Une approche centrée sur l'aspect humain : Éduquez vos employés et faites-leur confiance pour qu'ils agissent judicieusement.

L'appréciation : Récompensez et remerciez ceux qui soulèvent des questions de sécurité et ceux qui suivent les meilleures pratiques.

Des outils qui autonomisent : Faites de la voie sécurisée la voie la plus simple à suivre.

Deux victoires faciles pour commencer

1. **Réévaluez vos politiques de sécurité**
   Commencez par les politiques sur l'usage d'appareils personnels, les protocoles de sécurité réseau, les règles de sécurité liées aux voyages. Soyez attentif aux politiques irréalistes qui nuisent à la conformité.
2. **Appliquez le principe du moindre privilège**
   Assurez-vous que les accès sont limités à ce qui est strictement nécessaire. Ce qui est simple est mieux accepté.