

Planifier le départ d'employés

Que ce soit en raison d'un transfert, d'une retraite ou d'un licenciement, le départ d'un employé peut laisser la porte ouverte aux fraudes et aux pirates informatiques. Toute entreprise devrait planifier le départ d'employés.

Après le départ d'un employé, des pirates informatiques, voire d'anciens employés, pourraient exploiter les comptes inutilisés et les mots de passe pour accéder à vos données d'entreprise, vos données financières ou vos informations personnelles. Ils pourraient aussi utiliser les mots de passe pour publier des messages frauduleux sur votre site Web ou vos comptes de médias sociaux, ce qui pourrait nuire à la réputation de votre entreprise.

La plupart de ces menaces peuvent être évitées avec de la planification. Vous préparez à l'inattendu fait partie des bonnes pratiques.

Le plus important est de faire le suivi de tous les documents auxquels l'employé a accès, en ligne et sur les réseaux internes. Chaque mot de passe attribué ou permission donnée devrait être documenté pour que l'accès puisse être changé sans préavis.

Liste des choses à faire quand un employé quitte votre entreprise :

- Changez tous les mots de passe utilisés par l'employé.
- Supprimez les permissions donnant accès aux réseaux internes et externes.
- Révoquez l'accès aux comptes et le statut d'administrateur de la page des médias sociaux de l'entreprise.
- Cherchez à savoir si l'employé connaissait les mots de passe de collègues. Si oui, changez-les.

Si un employé est mis à pied ou congédié, assurez-vous qu'il soit escorté en permanence lorsqu'il quitte le lieu de travail. Empêchez-le d'avoir accès à des ordinateurs de travail et récupérez tous les items appartenant à l'entreprise, tels que les ordinateurs portables, les clés et les badges d'accès.