AIDE-MÉMOIRE

DIFFUSER DE L'INFORMATION SUR LES RÉSEAUX SOCIAUX

Objectif du document

Diffuser de l'information sur les réseaux sociaux de manière sécuritaire.

Les réseaux sociaux tels que Facebook ou Twitter sont de plus en plus utilisés pour communiquer à grande échelle auprès des clients. Cependant, ces plateformes ne sont pas destinées à être utilisées pour échanger de l'information confidentielle, car elles sont susceptibles d'être piratées et l'information échangée peut être rendue publique.

Les réseaux sociaux sont un bon moyen de communication pour une entreprise, afin d'interagir avec des clients connectés, faire passer des messages et développer une vitrine de marque. Cependant, une mauvaise utilisation de ceux-ci peut permettre à une personne mal intentionnée de voler les accès aux réseaux exploités et d'y diffuser du contenu malveillant. De plus, choisir les bons messages à diffuser permet à l'entreprise de se différencier des sites ou pages malveillantes qui tentent de faire de l'hameçonnage auprès de ses clients.

Recommandations

Échanger via les réseaux sociaux uniquement de l'information non confidentielle

- Transmettre de l'information publique : nouvelles, description des produits, etc.;
- Dans le cadre de concours et promotions : seuls le nom, le prénom, les adresses (courriel et postale), l'âge et le numéro de téléphone inscrits au dossier peuvent être demandés;
- Ne pas insérer de lien qui demanderait à un client d'entrer de l'information personnelle ou confidentielle ou de télécharger un fichier.

Faire la liste de vos comptes, tant sur les réseaux sociaux que dans les communautés virtuelles

- Déterminer des critères pour la sélection des sites sur lesquels vous ouvrez un compte d'entreprise;
- Éviter l'enchevêtrement de réseaux sociaux (ex. : se connecter sur Twitter avec son compte Facebook).

Protéger les comptes administrateurs

- Utiliser des mots de passe complexes, d'un minimum de 10 caractères, respectant l'une de ces deux options :
    - Option 1 : mot de passe incluant lettres et/ou chiffres choisis aléatoirement
        - Astuce : utiliser les premières lettres de chaque mot d'une phrase
        - Exemple : la phrase « Mon chien Fido est un caniche blanc de race pure » devient « mcfeucbdrp »
    - Option 2 : mot de passe composé d'au moins 3 mots, excluant les mots à éviter
        - Exemple : tablefeuillemanger
        - Mots à éviter : mots associés à l'environnement immédiat, professionnel ou personnel. Exemples : nom du conjoint, d'un enfant, du chien, marque de votre ordinateur ou de votre souris, pensée du jour affichée sur le babillard, saison, jour de la semaine, mois ou année.
- Utiliser des mots de passe uniques : ne pas attribuer le même mot de passe à plusieurs comptes administrateurs;
- Assurer le caractère confidentiel des mots de passe : le mot de passe d'un compte administrateur ne doit jamais être communiqué ou prêté.

Transmettre de l'information depuis le compte de l'entreprise

- Limiter les accès aux comptes administrateurs uniquement aux personnes autorisées;
- Supprimer immédiatement les accès d'administration à la suite du départ ou du changement de poste d'un employé;
- Surveiller les imposteurs qui se font passer pour des employés ou pour votre entreprise.

Avantages de lancer la vérification de la sécurité de Facebook pour tous les comptes administrateurs

- Se déconnecter de Facebook sur les applications et les navigateurs inactifs;
- Recevoir des alertes lorsqu'une personne essaie de se connecter à votre compte à partir d'un nouvel ordinateur ou téléphone.

En cas de compte piraté

Sécuriser immédiatement tout compte administrateur piraté. Pour cela, se rendre sur l'Aide en ligne de Facebook, section Sécurité, dans la page Comptes piratés.