CPA COMPTABLES PROFESSIONNELS AGRÉÉS CANADA

Protégez votre marque et votre réputation sur les médias sociaux

TENDANCE TECHNOLOGIQUE

Comment votre entreprise utilise-t-elle les médias sociaux?

De nos jours, les clients s'attendent à pouvoir communiquer avec les entreprises par l'entremise des médias sociaux. D'ailleurs, 71 % des gens qui ont une perception positive de leur expérience sur ces plateformes à l'égard d'une marque sont enclins à la recommander à leurs amis et à leur famille[1], mais moins de 64 % des petites entreprises ont un site Web[2]. Dès lors, une petite entreprise peut tirer un bon avantage concurrentiel de la solide réputation que pourrait avoir sa marque sur les médias sociaux, d'autant plus que la valeur des dommages causés par une atteinte à la réputation a doublé depuis l'avènement de ces médias[3]. Sachant cela, il serait utile de voir comment les CPA peuvent aider leurs organisations à tirer profit des médias sociaux sans que leurs marques soient exposées inutilement à des risques.

Importance

> « Il faut 20 ans pour bâtir une réputation, mais seulement cinq minutes pour la compromettre. » [TRADUCTION] — Warren Buffett

Pour connaître le succès, une entreprise doit adapter la gestion de ses relations avec le public et se constituer une vaste clientèle avec qui elle entretient des relations d'affaires directes. Les rapports sur les médias sociaux ne sont pas fondés sur l'argent, mais sur la confiance. Les activités commerciales qui en découlent sont donc le fruit d'établissement de relations de confiance ayant permis à l'entreprise de bien cerner les besoins de ses clients en vue de leur proposer des biens et des services appropriés, et ce, tout en atténuant les risques de mauvais usage. Une stratégie d'utilisation professionnelle des médias sociaux sans plan adéquat pour atténuer les risques pourrait embarrasser publiquement l'entreprise ou lui causer des pertes financières.

1 www.lyfemarketing.com/blog/social-media-marketing-statistics

2 https://clutch.co/website-builders/resources/small-business-websites-2018

3 www.aon.com/getmedia/2882e8b3-2aa0-4726-9efa-005af9176496/Aon-Pentland-Analytics-Reputation-Report-2018-07-18.pdf

Malheureusement, les études récentes démontrent que les atteintes à la sécurité des données sur les médias sociaux représentent 56 % de toutes les atteintes qui se sont produites en 2018[4]. Donc, pour les CPA, une stratégie d'utilisation des médias sociaux peut non seulement servir à des fins de marketing et de conformité, mais aussi permettre d'éviter de désastreuses erreurs pouvant miner la confiance des gens et compromettre la sécurité de données.

Avantages et considérations pour les entreprises

Les médias sociaux font souvent partie intégrante de l'empreinte numérique d'une organisation. Ce sont plus que des outils de marketing, car, lorsqu'utilisés correctement, ils permettent :

- de communiquer rapidement du nouveau contenu à un large public;
- de faire connaître sa marque facilement et à moindre coût;
- d'offrir du soutien à la clientèle de manière interactive;
- de générer de nouvelles occasions d'affaires;
- d'avoir son propre espace sur le Web.

Cependant, même si les médias sociaux peuvent être un moyen efficace pour établir une réputation et des liens de confiance, ils peuvent aussi mettre les organisations à mal encore plus rapidement qu'auparavant en cas de mauvaise gestion. Ces plateformes s'inscrivent donc maintenant dans la stratégie de gestion de toute organisation, quelle qu'en soit la taille. Même une simple politique relative aux médias sociaux peut aider les employés à adapter leur conduite en ligne, à sensibiliser les utilisateurs aux risques d'atteinte à la réputation et à imposer une discipline cohérente sur l'utilisation et la publication de contenu délicat. La confiance, comme mesure et valeur fiduciaire du monde numérique, est insaisissable, difficilement acquise et facilement perdue.

Alors, à quels risques de sécurité la présence des organisations sur les médias sociaux les expose-t-elle? Le tableau qui suit fournit une liste des erreurs à éviter sur ces plateformes afin de vous aider à préserver votre réputation, à établir votre marque et à favoriser la confiance du public.

4 www.itweb.co.za/content/G98YdqLxZZNqX2PD

10 principaux risques liés aux médias sociaux	Stratégies d'atténuation des risques
Usurpation d'identité	• Protégez votre nom en le réservant sur les médias sociaux et en créant des profils officiels, même sur les plateformes que vous n'utilisez pas. • Surveillez l'utilisation de votre nom dans les médias à l'aide de Google Alertes.
Propagation de logiciels malveillants par la publicité (« malvertising »)	• L'utilisation de la publicité à des fins malveillantes est de plus en plus répandue. Évitez les sites à risque et veillez à ce que votre clientèle fasse de même. • Portez attention aux publicités associées à votre nom ou à vos services dans les moteurs de recherche. • Si vous affichez de la publicité d'annonceurs sur votre site Web ou si vous faites de la publicité sur d'autres sites, veillez à ne vous associer qu'à des marques et des plateformes bien connues.
Piratage de profils	• Certaines des organisations les plus importantes et les plus respectées au monde ont déjà subi des vols de profils. Il vous faut donc protéger les comptes servant à gérer votre présence professionnelle sur les médias sociaux. • Vérifiez régulièrement vos droits d'utilisateur et les comptes des profils de votre organisation sur les médias sociaux pour vous assurer qu'aucun nouvel administrateur n'y a été ajouté. • Gardez sous la main une liste de liens, d'adresses courriel et de numéros de téléphone à utiliser en cas de problème, car, si vos profils sont piratés, vous voudrez retirer tout contenu non autorisé le plus rapidement possible.
Infection de sites Web par des modules d'extension vulnérables	• Les blogues et les modèles de WordPress sont populaires parce qu'ils permettent aux entreprises de créer et de publier du nouveau contenu. Toutefois, les produits proposés sont souvent fournis par des développeurs indépendants dont le code peut contenir des failles sur le plan de la sécurité. • Les pages sur les médias sociaux dirigent souvent ceux qui les consultent vers les formulaires et les dernières nouvelles de votre site Web. Effectuez donc régulièrement une analyse de vos modules d'extension WordPress pour repérer les bogues et les infections afin d'éviter d'y exposer vos clients potentiels. • Utilisez des outils comme Cloudflare ou Comodo pour protéger en permanence votre site Web contre des attaques et des infections avant que des utilisateurs de médias sociaux y accèdent.

10 principaux risques liés aux médias sociaux	Stratégies d'atténuation des risques
Attaque en force contre des comptes avec des mots de passe volés	• L'utilisation d'un même mot de passe à plusieurs endroits est une pratique risquée qui compte parmi les faiblesses notables les plus couramment exploitées par les pirates pour prendre le contrôle de comptes sur les médias sociaux et porter atteinte à la sécurité de sites Web. Pour abuser de cette faille, les individus malveillants n'ont qu'à tenter de se connecter sur différents sites Web populaires au moyen de mots de passe volés jusqu'à ce qu'ils réussissent. C'est pourquoi toute organisation ou personne ayant de nombreux mots de passe devrait avoir recours à une solution fiable pour créer aléatoirement des authentifiants uniques, les conserver de manière sécuritaire et les gérer facilement. • Protégez votre marque et votre identité organisationnelle à l'aide de politiques relatives aux médias sociaux qui imposent l'utilisation de mots de passe uniques et préviennent leur transmission à d'autres employés. • Lorsque possible, utilisez la fonction d'authentification à facteurs multiples.
Fil d'actualité contenant des messages malveillants	• Pour une entreprise, sa présence sur les médias sociaux s'accompagne de responsabilités. Suivez de près les messages publics et répondez-y tout en demeurant respectueux des différentes opinions. • Soyez toujours prêt à supprimer les messages contenant des liens malveillants, car ils peuvent nuire à vos clients et à votre réputation. Bloquez et signalez les comptes qui en sont à l'origine. • Ne censurez pas trop rapidement les messages du public et faites-le prudemment, car les gens prennent note de la façon dont vous les gérez et veillez à faire respecter les politiques des plateformes de médias sociaux.
Cybersquattage menant les utilisateurs vers des sites Web malveillants	• Les cybersquatteurs enregistrent souvent des noms de domaine semblables à ceux d'entreprises légitimes afin de tromper les utilisateurs qui les écrivent de façon erronée. Enregistrez quelques noms mal orthographiés de votre site Web parmi les plus courants pour vous assurer qu'ils redirigent les utilisateurs à la bonne page. • Souvenez-vous des dates d'expiration de vos noms de domaines. Les cybersquatteurs possèdent des outils sophistiqués pour en prendre le contrôle dès qu'ils ne sont plus protégés afin d'exiger une rançon. Entre-temps, tout le trafic de votre site Web pourrait être redirigé vers des pages malveillantes. De plus, des courriels confidentiels pourraient être interceptés par des criminels.

10 principaux risques liés aux médias sociaux	Stratégies d'atténuation des risques
	• Lorsque combinée avec le piratage de comptes sur les médias sociaux ou la publication de liens malveillants sur votre fil d'actualité, l'utilisation mal intentionnée de noms de domaine peut également compromettre et mettre à mal vos relations avec vos clients. Assurez-vous de surveiller les liens publiés et d'aviser les utilisateurs lorsqu'ils doivent faire preuve d'une plus grande vigilance.
Piratage de nom de domaine pouvant interrompre vos activités et intercepter vos communications	• Le nom de domaine de votre entreprise peut être votre bien le plus précieux. Vous pouvez vous en servir pour créer une infinité de sous-domaines et d'adresses courriel. Toutefois, si quelqu'un de mal intentionné se l'approprie, vos activités pourraient être perturbées et vos services en ligne, interrompus. • Assurez-vous de conserver vos droits sur votre nom de domaine et lisez toujours attentivement vos avis de renouvellement avant d'envoyer un paiement ou de donner accès aux interfaces de gestion de vos comptes. • Ne vous attendez pas à ce que votre revendeur ou registraire protège votre nom de domaine pour vous. Assurez-vous d'utiliser une authentification à facteurs multiples et de porter attention aux tentatives de connexion non autorisées qui pourraient être des attaques potentielles.
Vol de données pendant qu'elles sont stockées sur des sites Web ou transférées par l'entremise de ceux-ci	• Le chiffrement est le moyen le plus fiable au monde pour préserver la confidentialité et protéger les renseignements personnels. Maintenant que les navigateurs indiquent quels sites Web ne chiffrent pas leurs transmissions à l'aide de certificats SSL ou TLS, assurez-vous d'offrir cette protection de base aux visiteurs de votre site. De plus, gardez l'œil ouvert pour les liens non autorisés qui dirigent les utilisateurs vers des pages dont l'adresse n'a pas le fameux « s » à la fin du « http ». • De nombreuses entreprises utilisent maintenant les médias sociaux pour diffuser des documents, gérer des courriels et de la messagerie instantanée, et même pour accepter des paiements. Assurez-vous de toujours offrir des services assortis de la meilleure protection par chiffrement offerte par des organisations de confiance. • Votre présence sur le Web inclut-elle des services infonuagiques en plus de vos comptes sur les médias sociaux? Puisque l'intégration de ces services est souvent inapparente pour les utilisateurs, veillez à ce que toutes les données confidentielles (comme celles relatives aux dossiers, aux paiements et aux renseignements personnels) soient chiffrées sur les serveurs où elles sont stockées, que ce soit par vous ou par votre fournisseur. N'oubliez pas que c'est votre marque et votre image qui sont en jeu.

10 principaux risques liés aux médias sociaux	Stratégies d'atténuation des risques
Omission d'obtenir le consentement avant d'établir le contact	• De nombreuses entreprises croient souvent à tort que « consentement » signifie simplement « permission » (c'est-à-dire d'avoir la « permission » implicite ou par défaut de gérer des renseignements, à moins d'indication contraire). Les utilisateurs s'attendent non seulement à ce qu'on leur demande explicitement leur permission, mais aussi à pouvoir donner leur *consentement éclairé* : ils veulent savoir ce qu'il adviendra des renseignements qu'ils vous communiqueront. • Le consentement est le droit légal qu'a l'utilisateur de savoir qu'une organisation qui utilise ses renseignements personnels ne les divulguera pas sans son autorisation. Protégez les données de vos clients et prenez les mesures nécessaires pour éviter qu'elles soient publiées en ligne (comme sur les médias sociaux) ou qu'elles soient conservées trop longtemps (et qu'elles fassent ainsi l'objet d'un vol éventuel). • Faites toujours de la sensibilisation auprès des utilisateurs : informez-les des risques auxquels sont exposées leurs données et de la façon dont vous atténuez ces risques mieux que quiconque. De plus, ne cachez ni ne minimisez les risques qu'ils courent, et respectez leur consentement. Le lien de confiance que vous établirez avec eux portera fruit.

Conclusion

Les médias sociaux sont devenus des outils indispensables pour les entreprises qui souhaitent être accessibles, connectées et concurrentielles. Comme une enseigne, ils sont un moyen pertinent et branché de se faire connaître. Ils exposent toutefois les organisations à un plus grand risque d'attaque si elles ne sont pas prêtes à gérer activement et régulièrement leurs publications, à surveiller leur contenu et à appliquer les meilleures pratiques en matière de sécurité. Ajoutez ces activités à votre plan d'affaires relatif aux médias sociaux et profitez des avantages continus que vous offre une saine présence en ligne gérée de manière résiliente, contrôlée et novatrice.

La présente publication s'inscrit dans la **série Tendance technologique**, qui porte sur les grandes tendances du domaine touchant le milieu comptable. Les documents de cette série sont disponibles sur notre site Web.

AVIS DE NON-RESPONSABILITÉ

Le présent document, préparé par Comptables professionnels agréés du Canada (CPA Canada), fournit des indications ne faisant pas autorité. CPA Canada et les auteurs déclinent toute responsabilité ou obligation pouvant découler, directement ou indirectement, de l'utilisation de ce document.

© 2019 Comptables professionnels agréés du Canada

Tous droits réservés. Cette publication est protégée par des droits d'auteur et ne peut être reproduite, stockée dans un système de recherche documentaire ou transmise de quelque manière que ce soit (électroniquement, mécaniquement, par photocopie, enregistrement ou toute autre méthode) sans autorisation écrite préalable.

Pour demander cette autorisation, veuillez écrire à **permissions@cpacanada.ca**.