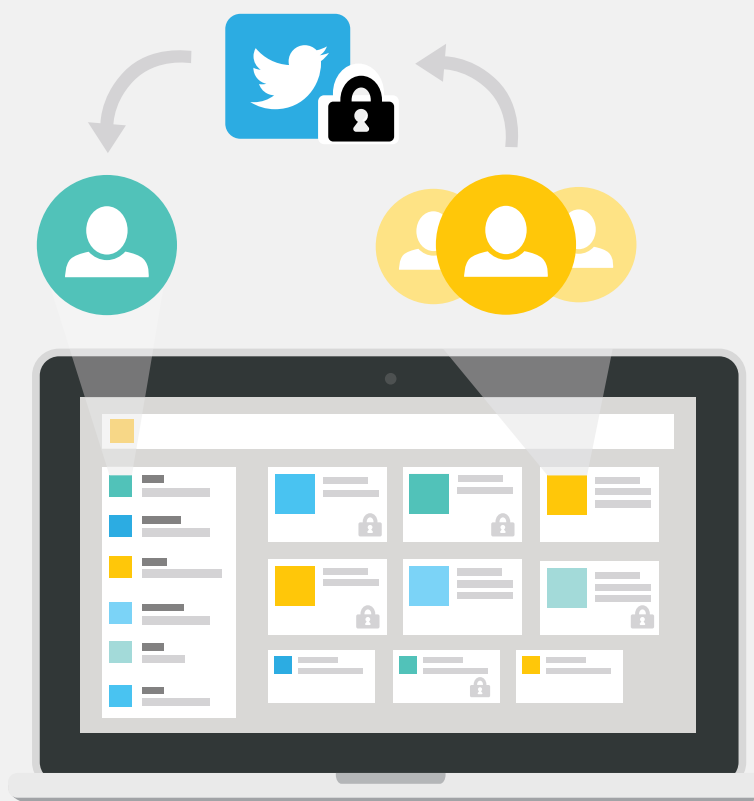


GUIDE

Comment protéger votre marque sur les médias sociaux ?

Les stratégies à adopter pour éviter les 6 plus grandes catastrophes que subissent les marques sur les médias sociaux



Comment protéger votre marque sur les médias sociaux ?

Les stratégies à adopter pour éviter les 6 plus grandes catastrophes que subissent les marques sur les médias sociaux

Table des matières

1. Introduction.....	3
2. Pourquoi protéger votre marque sur les médias sociaux ?.....	4
3. Six risques et menaces fréquents liés aux médias sociaux	5
4. Les stratégies à adopter pour protéger votre marque sur les médias sociaux.....	7
5. Comment gérer une crise liée sur médias sociaux	10
6. Anticipez : investissez pour protéger votre marque sur les médias sociaux.....	12



Introduction

Si les médias sociaux offrent d'incroyables opportunités, ils ne sont pourtant pas sans risques. Les marques endossent désormais la responsabilité qui va de pair avec leur présence permanente sur les médias sociaux.

Mais cela ne signifie pas pour autant qu'il faille redouter ou refuser d'être présent sur les médias sociaux. En fait, ne pas se montrer réactif peut nuire davantage à votre marque : l'entreprise Lockheed Martin en a récemment fait les frais après que le [tweet du Président Donald Trump](#) a entraîné la chute de son action de 4 milliards de dollars.

En adoptant les stratégies appropriées, votre marque peut se montrer active sur les médias sociaux sans être victime de tels événements destructeurs. C'est pourquoi [81 % des dirigeants d'entreprise](#) font désormais de la protection de leur marque en ligne l'une de leurs priorités.

Pour vous aider à vous orienter dans le monde de la protection des marques en ligne, ce guide donne un aperçu de tout ce que vous devez savoir :

- Pourquoi la sécurité sur les médias sociaux est importante pour les marques ?
- Six risques et menaces fréquents liés aux médias sociaux, et comment les gérer
- Que faire en cas de crise sur les médias sociaux ?
- Comment anticiper et minimiser les risques ?

Pourquoi protéger votre marque sur les médias sociaux ?

Toutes les marques doivent être présentes sur les médias sociaux, mais il n'a jamais été aussi important d'opter pour une approche sécurisée.

Les menaces qui pèsent sur la sécurité des médias sociaux ne cessent de se multiplier d'année en année. Les arnaques sur les médias sociaux [ont augmenté de 150 %](#) sur Twitter, Facebook et LinkedIn en 2016. De plus, [le rapport sur les cybermenaces publié par Proofpoint pour le premier trimestre 2017](#) montre que les attaques ont tendance à devenir de plus en plus diversifiées et sophistiquées.

Cette augmentation des menaces relatives aux médias sociaux est en parfaite corrélation avec le temps que nous passons en ligne. Comme le révèle le [rapport de 2016 sur la cybersécurité publié par Norton](#), le besoin d'être connecté en permanence expose des millions de personnes aux cyberattaques chaque année, et cela coûte des milliards de dollars. En 2016, [689 millions de personnes ont été confrontées à un cybercrime](#), ce qui correspond à une augmentation de 10 % par rapport à 2015.

Et tandis que les cyberattaques et les pirates informatiques font fréquemment les gros titres, les risques les plus importants proviennent souvent [d'une négligence et d'erreurs humaines au sein des entreprises](#). Les attaques sont en effet souvent dues à un manque de formation sur les menaces digitales et les protocoles à suivre.

C'est pourquoi il est primordial de savoir identifier les risques et mettre en place un programme de protection de la marque sur les médias sociaux. Comme le suggère le [guide sur le programme de sécurité et la gestion des risques publié par Gartner en 2016](#), « avec l'émergence de l'Internet des objets, la sécurité et la gestion des risques deviennent prioritaires. »

Les risques liés à l'absence de sécurité sur les médias sociaux

- **Une perte de confiance envers la marque :** toute faille de sécurité peut avoir un impact négatif sur votre marque. Lors d'une [enquête menée par FireEye Inc.](#), 36 % des répondants ont déclaré que l'image qu'ils se faisaient d'une marque avait été ternie à la suite d'un incident de sécurité, et un tiers d'entre eux ont affirmé avoir perçu la marque de manière négative après l'incident.
- **Des répercussions négatives sur le chiffre d'affaires :** le coût de tout problème de sécurité ou faux-pas sur les médias sociaux peut s'avérer astronomique. [Des milliards de dollars](#) sont dépensés chaque année pour gérer les failles informatiques et la communication en cas de crise.
- **Un retour sur investissement en baisse :** les événements qui causent des dommages à votre marque sur les médias sociaux amoindrissent la rentabilité de tous vos investissements. Au lieu d'augmenter vos profits, vous devez dépenser pour limiter les dégâts.

Le plus gros risque, c'est de ne rien faire du tout

Comme le souligne [Joanna Belbey](#), experte en conformité, ne rien faire constitue le plus gros facteur de risque.

Si vous n'avez mis en œuvre aucune procédure, aucun outil ni aucun programme de formation pour protéger et sécuriser votre marque sur les médias sociaux, vous serez beaucoup plus vulnérable aux menaces et aux risques sur les médias sociaux. Lorsque vous connaissez et gérez les menaces courantes, vous pouvez utiliser vos comptes de médias sociaux en toute sécurité.

Six risques et menaces fréquents liés aux médias sociaux

Tandis qu'il existe des centaines de menaces en ligne susceptibles d'affecter votre entreprise, les risques sur les médias sociaux se répartissent en six catégories principales, que vous devez connaître.

1. Négligence de votre compte

Si votre entreprise possède des comptes sur les médias sociaux, mais que vous ne les suivez pas activement ou que vous ne répondez pas aux conversations, on parle alors de négligence de compte. Votre marque se trouve ainsi exposée aux plaintes des clients et à leurs questions relatives aux produits qui restent sans réponse, ainsi qu'aux spams, ce qui [peut s'avérer extrêmement préjudiciable pour votre marque](#).

Que vous soyez actif sur les médias sociaux ou non, les consommateurs se rapprocheront forcément de votre marque. Lorsque des clients posent des questions sur les médias sociaux, ils attendent une [réponse dans les heures qui suivent](#)—et [82 % des clients](#) affirment que recevoir une réponse rapidement est essentiel pour que l'expérience avec une marque soit positive.

2. Erreur humaine

Lorsque les processus de sécurité échouent, nous pourrions être tentés de blâmer les systèmes et réseaux défectueux, mais les responsables sont généralement humains.

Lorsqu'un employé met accidentellement en ligne la mauvaise image lors de la publication d'un message sur les médias sociaux, partage des informations sur le mauvais compte ou partage sans le savoir des données sensibles, il s'agit d'une erreur humaine.

D'après un [rapport de Forbes Insights](#), l'erreur humaine constitue la menace dont les répercussions économiques sont les plus importantes. Ce type d'erreur est à l'origine [d'un tiers des problèmes informatiques](#), et est la principale cause de ces perturbations. Si vous n'avez pas mis en place les outils et les procédures nécessaires pour rattraper ces erreurs, une seule erreur peut avoir des conséquences désastreuses sur votre marque.

Par exemple, une [erreur de copier-coller sur le compte Twitter de US Airways](#) est considérée comme l'une des

plus grandes erreurs de communication de marque de tous les temps. En réponse à une plainte d'un client, la société a accidentellement collé un lien pornographique dans son tweet. Un bon système d'approbation aurait permis d'éviter cet incident.

3. Non-conformité

On parle de non-conformité lorsque les règles instituées par votre entreprise ou un organisme de réglementation ne sont pas respectées. D'après un [rapport de Proofpoint](#), plus de 12 organismes de réglementation (dont FINRA, FTC, FDA et SEC) ont établi des règles qui définissent ce que les entreprises peuvent faire sur les médias sociaux.

Un livre blanc publié par Proofpoint, [et intitulé](#) The State of Social Media Infrastructure, explique que « les organismes de réglementation considèrent les médias sociaux comme un canal de communication public assujéti aux réglementations existantes de divulgation des bénéfices, de vérité publicitaire et de confidentialité des données. Ces exigences visent à éviter que les consommateurs soient induits en erreur ou victimes de fraudes. »

Votre équipe a besoin de comprendre ces politiques et leurs enjeux sur votre activité digitale. Sans [processus d'approbation pour protéger vos interactions sur les médias sociaux](#) et repérer toute violation des règles en vigueur, vous vous exposez à de lourdes amendes et risquez d'être confronté à de longues enquêtes.

[Découvrez comment Spectrum Health demeure conforme aux réglementations dans le domaine malgré ses 23 000 employés.](#)

4. Le phishing

Les cybercriminels utilisent le phishing pour voler des informations confidentielles, comme les coordonnées bancaires. Il existe des centaines de stratagèmes d'hameçonnage sur les médias sociaux, et le [nombre de cas de phishing a augmenté de 150 % l'an dernier](#).

Une arnaque courante en la matière consiste en la création d'un [faux compte de service client sur les médias sociaux](#), qui vise à amener les clients à cliquer sur un lien frauduleux et à saisir leurs informations bancaires. Lorsqu'une personne envoie un tweet à votre marque, par exemple, le compte de l'imposteur va intercepter ce message et répondre avec un lien demandant à cet utilisateur de saisir ses renseignements personnels.

5. Piratage de comptes

Un compte est piraté quand un cybercriminel s'empare de votre compte de média social et l'utilise pour envoyer des messages insultants, inappropriés ou sans aucun rapport avec votre marque.

Lorsque le compte d'une marque est piraté, c'est un véritable cauchemar pour votre équipe de communication, car les clients peuvent répondre rapidement et sévèrement. D'après un [rapport de ZeroFOX](#), le [piratage qui a touché en 2016 les comptes sociaux de Laremy Tunsil, un joueur de la NFL](#), a causé des dommages évalués à environ 21 millions de dollars.

Le piratage de comptes n'est pas un phénomène rare. En effet, de grandes marques se font pirater leurs comptes chaque jour : c'est ce que [McDonald's](#) a découvert lorsqu'un pirate informatique a utilisé son compte Twitter pour publier des messages portant sur la politique américaine.

Le compte Twitter du [ministère de la culture en France](#) a été pris pour cible dans la nuit du 18 au 19 juillet 2017. Le compte officiel a été détourné durant environ quatre heures, par un « pirate » qui a affirmé sur le réseau social être le fils d'une personne ayant la charge de ce compte. Le ministère a présenté ses excuses dès le lendemain matin pour les « tweets indésirables » publiés la veille au soir. Une usurpation de compte peut être évitée grâce aux connexions sécurisées et au système d'approbation et aux niveaux d'autorisations personnalisables offerts par la plateforme Hootsuite.

6. Les malwares

Un malware (abréviation de « logiciel malveillant ») est conçu pour accéder à vos systèmes et données informatiques grâce à un code logiciel malveillant. Son intrusion peut conduire à une perte temporaire ou permanente des données confidentielles de votre marque.

Le terme « ransomware » fait référence à un logiciel malveillant qui se verrouille ou crypte les données de votre ordinateur et en bloque l'utilisation jusqu'à ce que vous payiez une rançon exigée par le criminel. Ce genre d'attaque devient également [de plus en plus fréquente](#) : selon un [rapport du ministère de la Justice des États-Unis](#), plus 4 000 attaques par ransomware ont été recensées chaque jour en 2016. Cela représente une augmentation de 300 % depuis 2015.

Les stratégies à adopter pour protéger votre marque sur les médias sociaux

En comprenant les risques auxquels votre entreprise s'expose sur les médias sociaux, vous pouvez mieux préparer votre équipe à mettre en œuvre des stratégies de manière sûre et sécurisée.

Les six stratégies suivantes vous aideront à réduire le risque d'erreur humaine et vous permettront d'identifier et d'écarter les problèmes avant qu'ils ne s'enveniment.

1. Identifier et supprimer les comptes de médias sociaux négligés

Si vous ne savez pas quels comptes sociaux sont associés à votre marque, ou comment ils sont perçus, vous risquez fortement de subir des incidents dommageables pour votre marque.

En identifiant et en fermant les comptes qui n'ajoutent aucune valeur à votre entreprise, vous assurerez une communication cohérente et conforme à l'image de votre marque sur toutes vos canaux digitaux. Prenons l'exemple de [Delaware North](#), une société d'hôtellerie de plusieurs milliards de dollars, qui a décidé d'unifier sa présence sur les médias sociaux en identifiant les 40 comptes qui lui étaient associés. En établissant un simple inventaire, la société a pu supprimer les comptes inactifs ou sans intérêt, et investir davantage dans les comptes les plus utiles.

2. Mettre à jour votre politique relative aux mots de passe

Établir une politique en matière de mots de passe est un aspect important, mais souvent négligé dans le cadre de la protection d'une marque. Si vous utilisez systématiquement des mots de passe forts, il sera alors plus difficile de pirater les comptes de votre société et d'emprunter l'identité de votre marque.

Toute personne utilisant les comptes de médias sociaux de votre entreprise doit appliquer cette stratégie, qui doit au minimum tenir compte des exigences de base suivantes :

- **Mots de passe complexes** : vos mots de passe doivent comprendre entre 8 et 20 caractères, et comporter des majuscules, des minuscules et des caractères spéciaux.
- **Authentification en deux étapes** : un système d'authentification en deux étapes ajoute un deuxième niveau d'authentification lorsque vous vous connectez. Par exemple, après vous être connecté avec votre mot de passe, vous devrez saisir un code envoyé sur votre téléphone mobile. Cela ajoute une sécurité supplémentaire à votre processus de connexion.
- **Système d'authentification unique** : le système d'authentification unique (ou SSO) réduit le nombre de mots de passe utilisés en vous permettant de vous connecter à plusieurs systèmes à l'aide des mêmes identifiants. Par exemple, vous pouvez vous connecter à Hootsuite avec les mêmes noms d'utilisateur et mot de passe que vous utilisez pour accéder à votre messagerie professionnelle : vous aurez donc moins d'identifiants à gérer et à sécuriser.

Les mots de passe doivent être mis à jour régulièrement et gérés par un seul administrateur ou groupe au sein de votre entreprise. Vous devez limiter l'accès aux mots de passe de manière stricte pour qu'ils restent confidentiels.

3. Créer une politique relative à l'utilisation des médias sociaux

Pour minimiser les atteintes à la sécurité et assurer un comportement cohérent au sein de votre entreprise, vous devez créer une [politique en matière de médias sociaux](#).

Cette politique vous permettra d'établir un ensemble de processus et de protocoles dédiés aux canaux sociaux de votre marque. Plus important encore, en procédant ainsi, tous vos employés deviennent responsables de la protection de votre marque contre les comportements malveillants.

La politique de médias sociaux varie d'une entreprise à l'autre. Définissez-en une qui protégera vraiment l'intégrité de votre marque, sa réputation et ses valeurs.

Voici quelques points de départ pour établir une politique efficace :

- Directives et bonnes pratiques de la marque
- Rôles et responsabilités des médias sociaux
- Exemples de comportements appropriés (ou inappropriés)
- Conséquences d'une mauvaise utilisation des médias sociaux
- Processus et protocoles de sécurité
- Lois et réglementations applicables

Actualisez régulièrement votre politique afin de l'adapter à tout changement d'habitude au sein de votre entreprise vis-à-vis des médias sociaux. Proposer votre nouvelle politique sous forme de « document vivant » porte souvent mieux ses fruits. C'est le choix qu'a fait [l'université de Cambridge](#), ce qui a permis aux employés de se sentir plus à l'aise avec le contenu de l'université.

4. Former vos employés

La nouvelle tendance dite [AVEC \(« Apportez votre équipement personnel de communication » ou BYOD en anglais\)](#) augmente de manière significative les risques de problèmes de sécurité. C'est pourquoi tous les employés devraient suivre une formation basique de sensibilisation sur les médias sociaux, qu'ils utilisent les comptes de votre entreprise ou non.

Si vous ne formez pas vos employés et ne les sensibilisez pas sur le sujet, il vous sera difficile de mettre correctement en place vos politiques d'entreprise.

La formation de vos employés doit inclure :

- L'apprentissage des bonnes pratiques et d'une utilisation appropriée des réseaux sociaux
- Une présentation de la politique relative aux médias sociaux de votre entreprise
- Une liste des risques courants liés à l'utilisation des médias sociaux
- Comment faire respecter les directives de l'entreprise et atténuer les risques

Découvrez comment former efficacement [vos employés aux médias sociaux grâce aux cours de la Hootsuite Academy](#).

Pour en savoir plus, consultez notre [guide de création d'une politique relative aux médias sociaux](#).

5. Mettre en place une hiérarchie d'approbation pour les médias sociaux

Tous les comptes de médias sociaux appartenant à la marque de votre entreprise doivent être protégés par un système d'approbation précis afin que rien ne soit publié sans avoir été dûment approuvé. Cela réduit considérablement le risque d'erreur humaine.

Si vous utilisez Hootsuite, vous pouvez configurer [un système de double approbation, avec des autorisations et des rôles définis pour chacun de vos employés](#). Ce faisant, vous décidez qui a un accès illimité au contenu, qui peut publier du contenu, qui peut soumettre le brouillon d'un contenu pour approbation et qui dispose d'un accès limité (en lecture seule). Si vous utilisez des applications ou intégrations tierces comme [Brandwatch](#), vous pouvez également configurer les systèmes pour signaler des contenus potentiellement sensibles et les empêcher automatiquement d'être publiés.

6. Utiliser le social listening

Le social listening est une technique que vous pouvez utiliser pour « écouter » les conversations non filtrées qui circulent sur les médias sociaux et concernent votre entreprise. C'est un excellent moyen de découvrir de nouvelles opportunités, mais aussi un aspect important de la protection de votre marque sur les médias sociaux.

Le social listening vous permet d'apporter des réponses aux plaintes, aux opinions négatives sur votre marque ou aux spams avant que la situation ne devienne incontrôlable.

À l'aide de votre logiciel de gestion des médias sociaux, configurez des [flux ou des alertes](#) afin d'écouter les conversations en utilisant les paramètres suivants :

- **Le nom de l'entreprise (en tenant compte des fautes d'orthographe courantes) :** commencez par rechercher les mentions directes de votre marque et les clients qui tentent de vous contacter directement. C'est une première étape qui vous permettra de vous faire une idée de l'opinion générale sur

votre marque et de résoudre immédiatement les éventuels problèmes. N'oubliez pas d'inclure dans votre recherche les variantes possibles du nom de votre marque (par exemple, pour Coca-Cola, on cherchera notamment Coca Cola, Coca, Cola etc.) ainsi que le nom de votre marque comportant les fautes d'orthographe courantes.

- **Mots-clés et hashtags correspondant à votre secteur d'activité :** rechercher les termes et hashtags spécifiques à votre secteur vous permet de vous impliquer dans des conversations ou autre se déroulant dans un espace plus large que celui de votre entreprise. Par exemple, s'il y a un débat en ligne autour d'un rappel de produit d'un concurrent, les consommateurs peuvent se demander si votre produit présente des problèmes similaires, ou bien se demander s'ils ne vont pas essayer un autre produit. En suivant les conversations en dehors du cercle direct de votre marque, vous pouvez gérer ces problèmes, apporter des précisions et instaurer un climat de confiance avec votre communauté.
- **Mots-clés et hashtags de campagnes :** suivre les mots-clés liés à votre campagne est important pour comprendre comment les consommateurs s'impliquent dans celle-ci. Par exemple, [la campagne Real Beauty Bottles de Dove](#) a rapidement connu un effet « boule de neige » : les commentaires négatifs se sont multipliés sur les réseaux sociaux. De nombreux tweets répondant à la publicité de Dove (qui avait été diffusée dans des articles) n'ont obtenu aucune réponse de la part de Dove. Sans surveiller activement les mots-clés et hashtags de vos campagnes, vous risquez de laisser la conversation vous échapper et ternir la réputation de votre marque.
- **Opinion :** utiliser [les outils d'analyse d'opinion sur les médias sociaux](#) vous permet de surveiller l'opinion des consommateurs du monde entier sur votre marque en plusieurs langues. Vous pouvez obtenir des avis en temps réel sur la façon dont votre contenu est perçu, et ajuster ainsi le message que vous souhaitez communiquer en conséquence.

Pour en savoir plus sur [l'écoute des médias sociaux](#), lisez notre guide complet.

Comment gérer une crise liée sur médias sociaux

Qu'il s'agisse d'un tweet mal venu sur votre marque, d'un message de colère publié par un client mécontent, ou d'une vidéo soudainement virale montrant une bourde commise par votre entreprise dans ses relations publiques, tout événement négatif peut rapidement devenir incontrôlable sur les médias sociaux. Pour vous préparer et savoir gérer la situation de manière appropriée, il vous faut établir un programme de gestion de crise.

Ce programme de gestion de crise vous aidera à minimiser les risques en définissant clairement les rôles, les responsabilités, les protocoles et la communication ; tout ce que vous n'aurez pas le temps d'organiser en cas de situation d'urgence.

Votre programme de gestion de crise lié aux médias sociaux doit couvrir quatre points essentiels :

1. Protocole de suivi des médias sociaux

Surveiller les mentions négatives relatives à votre marque vous donnera au moins l'occasion de résoudre un problème émergent avant qu'il ne dégénère publiquement en crise. Votre protocole doit inclure les éléments à contrôler, l'identité de la personne chargée de surveiller l'activité et les instructions indiquant comment traiter les problèmes courants ou prévisibles.

2. Rôles et responsabilités

Pour pouvoir réagir rapidement en cas de crise, il vous faudra une liste des principaux décideurs, et préciser le rôle et les responsabilités de chacun. Ces personnes doivent être autorisées à gérer la communication externe au nom de votre marque. Par exemple, vous pouvez nommer un responsable principal chargé de gérer l'approbation de tous les messages en relation avec les médias sur les réseaux sociaux, ainsi qu'un responsable suppléant qui remplacera le premier s'il n'est pas disponible.

3. Scénarios et exemples possibles

Pour que vos employés apprennent à gérer une crise, ajoutez des exemples de crises susceptibles de se produire sur les médias sociaux dans votre programme de gestion de crise, ainsi que des informations sur la façon de les gérer.

Grâce à des sessions de formation et des exercices de simulation basés sur des scénarios possibles, vous aiderez vos employés à comprendre les risques qu'encourt votre marque et à réagir de manière adéquate. Vous pourrez également vous faire une idée plus réaliste du temps nécessaire à la gestion d'une crise. De plus, cela constitue une excellente occasion d'identifier les éventuelles lacunes ou faiblesses de votre programme.

4. Messages pré-approuvés

Les responsables de votre équipe en charge des médias sociaux doivent travailler avec votre équipe de relations publiques afin d'élaborer des messages pré-approuvés que vous pouvez utiliser dans chaque scénario pré-défini.

Votre équipe chargée des médias sociaux doit pouvoir accéder et utiliser facilement les documents comportant vos messages pré-approuvés. Ces documents doivent mentionner clairement l'approbation des responsables concernés.

Tout programme de gestion de crise doit vous permettre :

- **D'agir rapidement.** Agir rapidement et efficacement peut faire toute la différence lorsqu'il faut gérer une crise sur les médias sociaux. Un expert en la matière, [Duncan Gallagher, explique que](#) 28 % des crises deviennent internationales en une heure, mais qu'il faut 21 heures en moyenne pour que l'entreprise prépare son message de réponse. C'est un aspect que la plupart des marques peuvent améliorer de manière significative.
- **De faire preuve de transparence.** Montrez-vous ouvert et honnête avec vos clients lorsqu'ils discutent d'un problème sur les médias sociaux. Lorsque c'est possible, continuez la discussion hors-ligne pour résoudre le problème du client. Si la situation a atteint un point où cela n'est plus possible, il vous faudra répondre publiquement aux questions avec autant de précisions qu'il vous est légalement possible de fournir.
- **De communiquer en interne.** Pendant une crise publique, vos employés ont besoin d'être informés régulièrement sur ce qu'il se passe et doivent savoir comment répondre aux questions qu'ils reçoivent des consommateurs. En communiquant en interne, vous pouvez réduire considérablement le risque que vos employés soient mal informés et diffusent des informations erronées.

- **D'instaurer un climat de confiance.** Toute situation de crise est une opportunité d'instaurer un climat de confiance au sein de votre communauté. Par exemple, lorsque [le comté de Morris a été touché par l'ouragan Sandy](#), la ville s'est servie de ses comptes de médias sociaux pour alerter les citoyens et diffuser des informations utiles et fiables, ce qui a permis de sauver des vies et d'éviter de nouvelles catastrophes.

Évaluez et modifiez votre programme après une crise

Une fois la crise passée, vous devrez organiser une séance de débriefing avec les membres de l'équipe concernée pour voir ce qui s'est bien passé et ce que vous pouvez améliorer. Cela vous aidera à identifier les sections de votre programme de gestion de crise qui devront être modifiées.

Pour en savoir encore plus sur la gestion de crise

- [Guide sur la gestion de crise sur les médias sociaux](#)
- [Cours de la Hootsuite Academy sur la préparation aux crises](#)

Anticipez : investissez pour protéger votre marque sur les médias sociaux

Chaque année, les entreprises dépensent des [milliards de dollars](#) pour gérer des problèmes de sécurité en ligne. Sans les outils et procédures adaptés, vous augmentez nettement le risque d'incidents qui pourraient coûter très cher à votre marque et avoir des répercussions négatives sur votre activité à terme.

En faisant de la protection de vos comptes de médias sociaux une priorité, vous pourrez mettre fin aux comportements nuisibles, minimiser les coûts de gestion des incidents affectant votre marque et empêcher qu'un problème ne se transforme en catastrophe.

Investissez pour assurer un avenir sécurisé à votre entreprise

Protéger votre marque doit se faire à l'échelle de toute l'entreprise. [Hootsuite Enterprise](#) vous permet d'impliquer votre public sur tous vos réseaux sociaux tout en vous protégeant des pirates informatiques, en minimisant le risque d'erreur humaine et en restant conforme aux réglementations.

Nous travaillons en collaboration avec des [partenaires](#) grâce auxquels votre entreprise sera toujours en sécurité sur les médias sociaux.

À propos de Hootsuite Enterprise

Accélérez votre transformation sociale avec Hootsuite



Sécurisée et évolutive, la solution Hootsuite Enterprise permet aux organisations, privées ou publiques :

- de mettre en œuvre et piloter efficacement leur stratégie sur les médias sociaux
- de la déployer à tous les niveaux de l'organisation (équipes, marques, régions ou pays)
- tout en contrôlant la sécurité des comptes, la cohérence des messages et les retours générés.

Indépendante, Hootsuite Enterprise s'intègre avec un écosystème ouvert de réseaux et de technologies tierces—compatibles avec vos outils métiers et vos processus existants.

Développer les relations clients et influenceurs, générer des opportunités commerciales, renforcer votre Marque Employeur, recueillir et analyser les données en temps réel... Hootsuite Enterprise vous permet de tirer pleinement parti des médias sociaux.

Depuis sa création, Hootsuite n'a eu de cesse d'innover pour aider les entreprises à accélérer leur transformation digitale. Elle est aujourd'hui la plateforme de Social Media la plus utilisée dans le monde.

Demandez une démo personnalisée:
enterprise.hootsuite.com

Plus de 800 entreprises du Fortune 1000 et la majorité des sociétés du CAC 40 font aujourd'hui confiance à Hootsuite



THALES



BNP PARIBAS

