O RGANISATIONNEL
T ECHNIQUE
C OMPORTEMENTAL

Les réseaux sociaux et la e-réputation

fiche 16

L'utilisation des réseaux sociaux peut être privée et/ou professionnelle. Il faut néanmoins être bien conscient qu'une utilisation considérée comme privée peut, bien souvent, avoir des répercussions professionnelles.

O Le salarié sur les réseaux sociaux

- Sensibiliser les personnels, en lien avec l'entreprise, grâce à une charte d'utilisation des réseaux sociaux. Leur rappeler les droits et devoirs de tout employé, comme par exemple la loyauté, la discrétion ou le devoir de réserve.
- Prévoir, dans le contrat de travail, une clause spécifique relative à la communication externe.

C

- Ne jamais utiliser le même mot de passe pour accéder à un réseau social et aux ressources informatiques de l'entreprise.
- Prendre conscience qu'une information (texte, photo, etc.) publiée sur internet n'appartient plus à celui qui la met en ligne et peut difficilement être effacée.
- Éviter de communiquer des informations personnelles précises sur les réseaux sociaux (date et lieu de naissance, numéro de téléphone, etc.).
- Etre attentif aux données de géolocalisation ouvertes sur les réseaux sociaux. Elles peuvent apporter des renseignements sur son emploi du temps professionnel : absence, vacances, missions, etc.
- Ne jamais publier de photo, ni y identifier quelqu'un, sans un accord exprès de la personne concernée.
- Veiller à ce que les informations publiées sur les réseaux sociaux ne comportent pas d'information sensible concernant l'entreprise : organigramme précis, systèmes techniques utilisés, mission à l'étranger, contrat en cours de négociation, conflit social frémissant, etc.
- Être vigilant quant aux sollicitations via les réseaux sociaux. Ils sont fréquemment utilisés comme vecteur d'ingérence : virus, usurpation d'identité, ingénierie sociale, etc.
- Toujours se déconnecter du réseau social après l'avoir utilisé, même sur l'ordinateur personnel. S'il n'est pas verrouillé, une utilisation par une tierce personne est possible, avec des conséquences multiples : usurpation d'identité, accès aux données, canular, etc.

O L'entreprise sur les réseaux sociaux

- Identifier correctement le besoin en communication de l'entreprise sur les réseaux sociaux. Une audience faible peut avoir un effet contreproductif.
- Choisir correctement la plateforme de communication. Chacune a ses spécificités en termes de cibles, d'instantanéité, de fréquence d'utilisation, etc.
- Déterminer, après une analyse de risques, qui devra prendre en compte le fait que tous les destinataires ne sont pas forcément bienveillants :

  - quelles informations communiquer ?
  - Qui valide les informations ?
  - Qui les publie ?
  - Quel rythme de publication va être observé ?

- Être très attentif à la cohérence et à l'intégrité des messages de communication externe, eu égard aux réalités de l'établissement.
- Mettre en place une veille rigoureuse sur les noms de la société, de ses dirigeants et des marques afin d'être en capacité de réagir rapidement contre les dénigrements, les « **cybersquats** » ou toute autre action à l'encontre de l'entreprise.
- Privilégier la communication interne. Apprendre une nouvelle sur un réseau social ou par la presse, plutôt que par ses dirigeants peut être déstabilisant pour un employé.
- Désigner un administrateur du compte qui suivra rigoureusement les évolutions techniques du réseau social : sécurité, confidentialité, etc.

T

- Paramétrer les comptes selon les objectifs d'utilisation recherchés (public, semi-public, privé).
- Utiliser un mot de passe robuste afin d'éviter toute utilisation frauduleuse du compte de l'entreprise sur le réseau social. La diffusion de celui-ci sera strictement encadrée.

Premier ministre
Délégation interministérielle à l'intelligence économique

Avril 2014

C

- Signaler tout abus à l'opérateur du réseau social, par l'intermédiaire des pages de contact prévues à cet effet.
- Ne pas hésiter à solliciter la commission nationale de l'informatique et des libertés (CNIL) ou à déposer plainte. L'assistance d'un conseiller juridique doit alors être envisagée.
- Réfléchir, en cas de recours, à l'impact médiatique qui pourra en résulter, souvent démultiplié par la viralité des réseaux.
- Prendre garde à ne pas sur-réagir à chaud en cas de rumeur, de tentative de déstabilisation, de désinformation ou d'intoxication concernant votre entreprise. Faire une analyse rigoureuse des tenants et aboutissants des réactions envisagées avant de les engager.

MOT-CLÉ

Cybersquat :
Acte qui consiste à déposer un nom de domaine en usurpant le nom de l'entreprise ou celui de ses marques (nasa.com était un site pornographique alors que le site officiel est nasa.org, par exemple). Il existe une variante : le "typosquat" qui repose sur une orthographe incorrecte (elyseee.fr pour elysee.fr, par exemple).

POUR ALLER PLUS LOIN

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Guide d'hygiène informatique – http://www.ssi.gouv.fr/IMG/pdf/guide_hygiene_informatique_anssi.pdf
- Recommandations de sécurité relatives aux mots de passe – http://www.ssi.gouv.fr/IMG/pdf/NP_MDP_NoteTech.pdf

RÉFÉRENTS

- **ANSSI, CCI France, CGPME, CNB, HFDS du ministère de tutelle, MEDEF, Odre des avocats de Paris.**