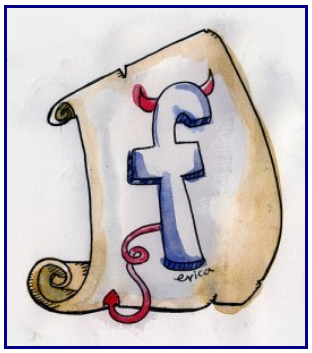
# 10 conseils pour naviguer sur les médias sociaux en toute sécurité



La société **Stonesoft** (spécialisée dans les solutions de sécurité réseau intégrées) propose **10 conseils pour naviguer sur les médias sociaux en toute sécurité :** une série de préoccupations à prendre en compte à mesure que l'utilisation de services de réseaux sociaux se généralisent dans les organisations – conseils qui peuvent être adaptés pour les espaces publics numériques et leurs usagers :

**1. Sensibiliser les employés :** Les personnes ne changeront leur façon de se comporter sur les réseaux sociaux que lorsqu'ils auront été sensibilisés aux risques de sécurité qu'ils présentent. Les entreprises ont donc pour mission d'informer leurs employés quant aux risques engendrés par les réseaux sociaux (même une information qui paraît sans importance risque d'en révéler déjà bien trop sur une société ou la vie privée d'un individu). Diffuser régulièrement des informations concernant les dernières menaces et établir une liste de règles à respecter permettront de sensibiliser encore davantage les utilisateurs. Une personne référente en interne ou en charge des réseaux sociaux peut être utile à cette prise de conscience.

**2. Mettre en place des processus stricts :** Les administrateurs doivent être au courant des dernières menaces repérées sur le web. Il est ainsi conseillé de mettre en places des process stricts en phase avec les flux e travaux (workflows) quotidiens. Les administrateurs doivent être attentifs et s'assurer que les dernières mises à jour de sécurité sont bien téléchargées. Ces mécanismes, qui peuvent sembler quelque peu « simplistes », permettront aux responsables informatiques et internet d'identifier instantanément les attaques réseaux ou même de les éviter pro-activement.

**3. Définir des règles de sécurité solides :** En établissant des règles internes, les administrateurs réseaux peuvent définir des zones et applications réseaux accessibles par certaines personnes à certains moments. Il est ainsi plus facile de superviser l'accès aux données critiques en permanence et l'information ne risque pas de tomber entre de mauvaises mains par des moyens non autorisés. Les entreprises doivent également prendre la conformité en compte. Il est important de mettre les politiques à jour et de les adapter aux différents changements.

**4. Bloquer les sites infectés :** Le risque de se connecter à un site infecté et de télécharger un cheval de Troie existe malgré des formations régulières dispensées aux employés. Les filtres URL permettent aux entreprises de bloquer l'accès aux malwares connus et aux sites de phishing, et autres sites malveillants.

**5. Utiliser des barrières de sécurité (firewalls) à jour :** Les entreprises doivent s'assurer que les technologies de sécurité en place sont toujours à jour. Un firewall moderne permet une analyse complète de toutes les données concernant le trafic. Une inspection approfondie du trafic permet de surveiller tout type de données trafic (navigation web, applications peer-to-peer, données trafic chiffrées dans un tunnel SSL). Lors de l'inspection SSL, le firewall déchiffre le flux de données SSL et le chiffre de nouveau avant de renvoyer les données vers le réseau. C'est un moyen de

protéger les postes de travail, les réseaux internes, les hôtes et les serveurs contre les attaques ayant lieu à l'intérieur des tunnels SSL.

**6. Définir des accès aux applications métiers :** Les utilisateurs mobiles, les partenaires et les distributeurs ont souvent besoin d'accéder au réseau de l'entreprise de l'extérieur. Pour ces groupes d'utilisateurs, il est très difficile de s'intéresser à l'utilisation faite des réseaux sociaux. Il devient essentiel d'octroyer des droits d'accès réseau de façon centralisée, en utilisant par exemple un portail SSL/VPN. Parallèlement, le travail de l'administrateur est facilité par une authentification forte via le SSO au niveau de l'utilisateur. Ainsi, un identifiant unique permet aux utilisateurs d'accéder uniquement aux zones réseau et aux services idoines.

**7. Parer aux vulnérabilités :** Sur tous les réseaux, la gestion des vulnérabilités représente une mission essentielle puisque les attaques exploitant ces dernières, notamment via les réseaux sociaux, se multiplient. Installer un IPS (Système de Prévention des Intrusions) représente un des moyens d'établir une barrière de défense.

**8. Sécuriser l'intranet :** L'intranet de chaque entreprise réunit généralement des informations sensibles. Ces zones doivent être isolées du reste du réseau interne. Pour ce faire, on peut segmenter l'intranet au moyen de pare-feu. Ceci permet à l'entreprise d'isoler des services comme la comptabilité du reste de l'intranet et donc d'éviter que les infections n'atteignent ces zones sensibles du réseau d'entreprise.

**9. Intégrer les appareils mobiles dans les politiques de sécurité :** De nombreux utilisateurs surfent sur les réseaux sociaux via des appareils mobiles (ordinateurs portables, assistants numériques ou smartphones). Ces mêmes outils sont utilisés également pour se connecter au réseau de l'entreprise. Les administrateurs appliquent les politiques de sécurité aux appareils mobiles. Il est possible de le faire, par exemple, via la fonction d'évaluation, capable de vérifier si le dispositif qui se connecte au réseau est conforme aux politiques de l'entreprise et si les logiciels de sécurité nécessaires y sont bien installés. Cette fonctionnalité s'assure également qu'un hôte firewall adapté et mis à jour est bien installé et que le système d'exploitation, le logiciel anti-virus et l'ensemble des correctifs sont correctement mis à jour. Si l'une de ces conditions n'est pas remplie, l'appareil mobile voit son accès au réseau limité voire refusé. Le cas échéant, l'appareil mobile est redirigé vers un site web de confiance où il pourra télécharger les mises à jour requises.

**10. Administrer de façon centralisée :** Une gestion centralisée permet aux responsables informatiques d'administrer et de configurer l'ensemble du réseau et des appareils mobiles via une console unique. Ils ont également accès à des rapports leur permettant de voir qui a accédé à quelles données et quand. Il est plus aisé pour eux de se prémunir efficacement contre les attaques et de garantir une protection plus efficace aux applications vulnérables.

*D'après : Stonesoft : 10 conseils pour surfer sur les medias sociaux en toute sécurité.*

*Crédit illustration : Dessin par Erica sous Licence Creative Commons.*