Guides de sécurité pour les petites entreprises

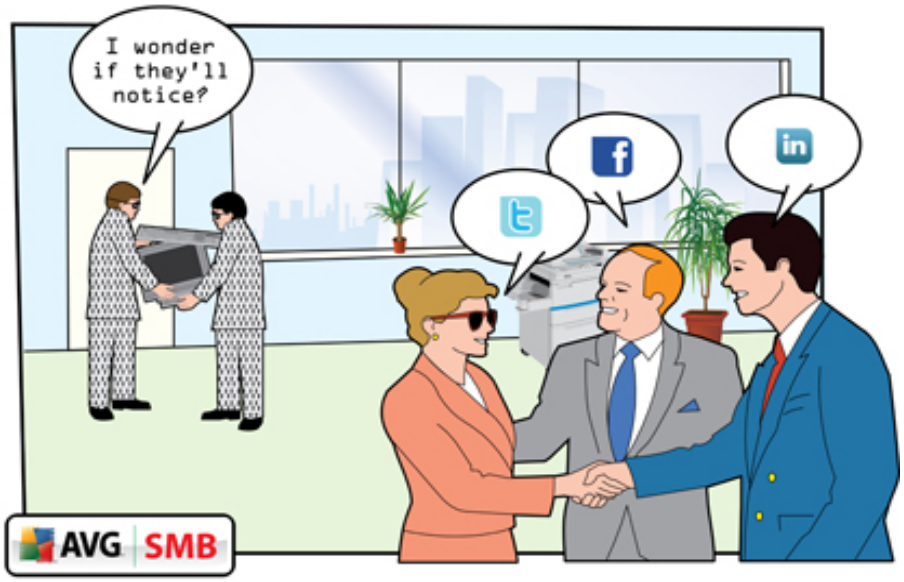
Réponse aux questions concernant la sécurité de votre petite entreprise : **réseaux sociaux, données sensibles, transactions bancaires professionnelles**

AVG AU TRAVAIL

Réponse aux questions concernant la sécurité de votre petite entreprise : réseaux sociaux, données sensibles, transactions bancaires professionnelles

Question : Si les réseaux sociaux constituent un tel risque, ne devrions-nous pas simplement bloquer leur accès ?

Lorsque les sites de réseaux sociaux tels que MySpace et Facebook sont apparus, certaines entreprises les ont considérés comme une distraction et les ont interdits dans le cadre professionnel. Toutefois, depuis l'arrivée de nouveaux formats de réseaux sociaux, comme Twitter, les entreprises ont commencé à prendre en compte ce potentiel de collaboration. Les réseaux sociaux ont évolué : autrefois réservés aux communications personnelles, ils sont devenus un support de communication de masse. De nombreuses entreprises considèrent désormais les sites tels que Twitter comme des canaux de publicité précieux.



Compte tenu de ces nouvelles utilisations légitimes par les entreprises, une stratégie interdisant entièrement ces sites semble contre-productive. Même si ces outils peuvent servir à des fins professionnelles, pour des raisons de sécurité, les entreprises devraient toujours surveiller la manière dont les employés les utilisent. Les experts de la sécurité comme Herbert Thompson, professeur au département Science informatique de l'Université de Columbia, ont lancé un avertissement à propos des dangers liés à la divulgation des informations personnelles sur les réseaux sociaux. Les gens peuvent publier des informations personnelles, telles que le nom de jeune fille de leur mère, qui sont souvent utilisées par les sites sécurisés comme des indices permettant de retrouver les mots de passe.

« Les utilisateurs publient tout et n'importe quoi : ils balancent sur ces réseaux des informations de toutes sortes. On a assisté à une croissance de la technologie du partage d'informations, mais la formation à ce sujet n'a pas suivi », explique-t-il.

Par conséquent, même si une interdiction stricte des sites de réseaux sociaux n'est sans doute pas la réponse, les entreprises devraient envisager de mettre en place et de faire respecter des réglementations concernant leur utilisation, notamment par rapport à leurs activités. Une étude récente organisée par l'école professionnelle IESE en Espagne, E. Philip Saunders, le College of Business at the Rochester Institute of Technology aux États-Unis et la Henley Business School au Royaume-Uni, a révélé que six entreprises sur sept ne possèdent pas une stratégie formelle concernant l'utilisation des réseaux sociaux dans le cadre professionnel. « En ne tenant pas compte de l'utilisation et de l'influence croissantes des réseaux sociaux et des outils Web 2.0, les entreprises s'exposent à des risques d'utilisation frauduleuse, pouvant aboutir à la divulgation d'informations sensibles ou à une mauvaise représentation de la société », explique Evgeny Kaganer, Ph.D., chercheur principal et professeur assistant à l'IESE Business School.

Selon Roger Thompson, responsable de la recherche chez AVG, outre le développement de stratégies perfectionnées régissant l'utilisation des réseaux sociaux, les responsables peuvent fournir à leur personnel quelques directives simples en vue de minimiser les risques.

« Le caractère convivial de ces réseaux les rend dangereux. Vous acceptez volontiers de dire à vos amis où vous vivez ou quelle est la date de votre anniversaire, ou encore le nom de jeune fille de votre mère. Mais si les pirates parviennent à infiltrer le compte de votre ami, ils découvriront également ces informations », explique Thompson.

Thompson préconise certaines règles très simples, mais qui peuvent être efficaces, comme la création de mots de passe distincts pour chaque site, différents de ceux qui permettent de se connecter aux systèmes de l'entreprise. « Si vous souhaitez assurer votre sécurité sur ces sites, il faut utiliser un ID d'utilisateur et un mot de passe uniques pour chacun d'eux, ou au moins un mot de passe unique », dit-il.

Il est utile de faire preuve de prudence à propos des interlocuteurs du personnel et des applications qu'installent les employés. « Votre mère vous a toujours recommandé de ne pas parler à des étrangers. Le même conseil est valable pour les réseaux sociaux : si vous ne savez pas qui est votre interlocuteur, ne lui parlez pas », ajoute-t-il. « Enfin, soyez prudent quant aux applications que vous acceptez d'installer. Un million de personnes développent des applications pour ces sites et mon petit doigt me dit qu'elles ne sont pas toutes bienveillantes ».

Pour plus d'informations à propos de la sécurisation des réseaux sociaux, voir (Les directives et les interdits des réseaux sociaux, Roger Thompson) (http://www.youtube.com/watch?v=poHqIXvxmfg)

Question : Quelle est ma responsabilité en cas de perte de données sensibles ?

La réponse à la question concernant les conséquences juridiques auxquelles les entreprises peuvent être exposées en cas de brèche ou de perte de données dépend d'un certain nombre de facteurs tels que la nature des données en question et l'endroit où l'incident s'est produit. De toute évidence, toute perte de données pourrait entraîner un impact en termes de publicité négative si elle était divulguée en externe, mais lorsqu'il s'agit de poursuites judiciaires précises, les règles les plus strictes s'appliquent à la perte de données résultant d'un tiers.

Aux États-Unis par exemple, la Californie est devenue en 2003 le premier état à adopter une loi exigeant que les entreprises informent leurs clients en cas de perte de données. Depuis lors, 44 autres états ont voté des lois allant dans le même sens. Une loi fédérale, appelée H.R. 2221, la loi Data Accountability and Trust Act (DATA), est également à l'étude, mais n'a pas encore été adoptée. La loi DATA obligerait les entreprises, quel que soit l'état dans lequel elles sont installées, à révéler un tel incident à toute personne « étant un citoyen ou un résident des États-Unis dont les informations personnelles ont été acquises par une personne non autorisée à la suite d'une telle brèche de sécurité » et l'entreprise en question devrait également en aviser la Federal Trade Commission (Commission Fédérale du Commerce). Même si la forme exacte qu'aura cette législation demeure incertaine, les entreprises qui choisissent de crypter leurs données seront considérées de manière plus favorable et ne seront pas tenues d'aviser tous les intéressés s'il peut être prouvé que les données sont protégées ou illisibles.

Le Royaume-Uni envisage également de resserrer sa réglementation en termes de protection des données sensibles. Le Bureau du Commissaire de l'Information est chargé de la protection des données au Royaume-Uni et ses pouvoirs ont progressivement augmenté à la suite d'une série de brèches de sécurité dans des organismes gouvernementaux. Depuis avril 2010, cet organisme est en mesure d'infliger aux entreprises des amendes pouvant atteindre 571 000 € si elles ne protègent pas correctement les données de leurs clients.

La perte de données est également un problème pour les petites entreprises qui ne disposent souvent pas de ressources affectées à la sécurité informatique. Selon une enquête réalisée en 2009 par la US National Cyber Security Alliance, 86 pour cent des petites entreprises interrogées ne disposaient pas d'un employé exclusivement chargé de la gestion de la sécurité informatique et 28 pour cent d'entre elles seulement ont reconnu avoir mis en place une stratégie formelle de sécurité informatique. Cette enquête a également révélé que 66 pour cent des entreprises permettent l'utilisation hors site de PDA et d'ordinateurs contenant des informations sensibles.
(http://www.staysafeonline.org/resource-document/2009-smb-security-study)

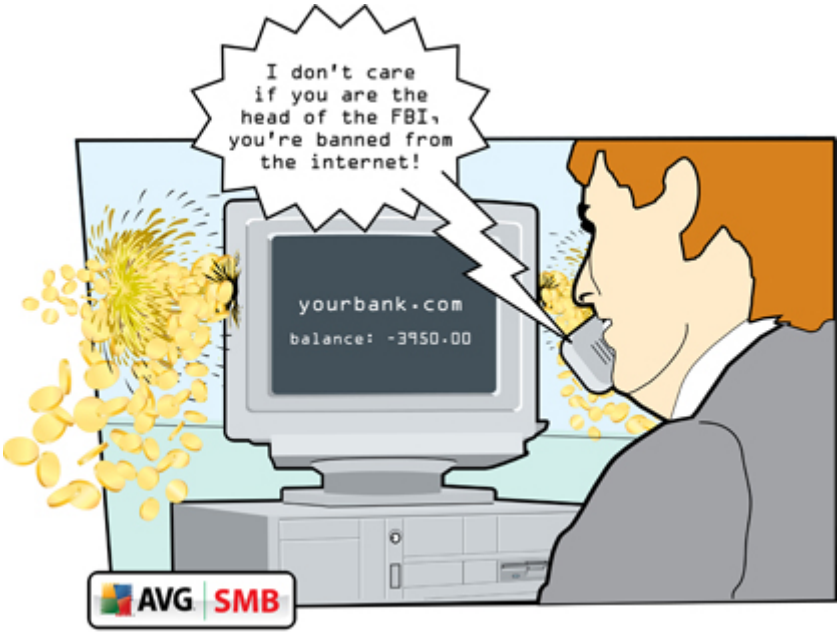
Question : Les transactions bancaires en ligne sont-elles sécurisées ?

Même si les entreprises, comme les particuliers, sont attirées par la souplesse des transactions bancaires en ligne, il est à noter que cet excellent outil présente des risques de sécurité inhérents. N'oublions pas que le Directeur du FBI, Robert Mueller, a récemment annoncé que son épouse lui avait interdit d'utiliser Internet après qu'il a failli être victime d'un programme de hameçonnage.

L'épouse de Mueller a sans doute des raisons d'être inquiète. Les chiffres enregistrés au Royaume-Uni en 2008 font apparaître que la fraude en ligne avait augmenté de 132 pour cent par rapport à 2007. Selon le groupe de banques britanniques APACS, la fraude sur Internet à elle seule représentait un montant d'environ 52,5 millions de livres.

Pour les entreprises, les menaces posées par les transactions bancaires en ligne pourraient être plus aiguës compte tenu des risques associés aux « menaces internes ». Les experts de la sécurité informatique affirment depuis longtemps que le personnel d'une entreprise représente une menace plus importante pour la sécurité que les cybercriminels externes. Cela n'est peut-être plus tout à fait exact depuis l'arrivée des groupes criminels organisés au milieu des années 1990 et compte tenu du perfectionnement croissant des cybercriminels, mais les transactions bancaires en ligne fournissent sans aucun doute un nouveau canal pour permettre aux pirates, internes ou externes, de voler de l'argent ou des informations confidentielles.

Une étude réalisée récemment par AVG au Royaume-Uni a démontré que le nombre de transactions financières réalisées sur Internet est en hausse, puisque 85 pour cent des personnes utilisent désormais Internet pour faire des achats et plus de deux tiers des habitants choisissent également ce support pour leurs transactions bancaires. Cette étude a en outre révélé que les craintes à propos des vols sur Internet sont également en hausse. En effet, 43 pour cent des personnes interrogées ont déclaré se sentir plus vulnérables à la cybercriminalité qu'aux cambriolages, agressions ou vols.



Malgré ces préoccupations, l'enquête d'AVG a également fait apparaître qu'environ 30 pour cent des personnes interrogées pensaient ne pas prendre les mesures nécessaires pour se protéger. Les banques pourraient également en faire plus. Par exemple, l'utilisation de menus déroulants dans le cadre du processus de connexion pourrait contribuer à déstabiliser les logiciels pirates. Les criminels utilisent ces logiciels pour enregistrer les frappes sur le clavier. Or, les menus déroulants ne peuvent pas faire l'objet de ce type de piratage, car ils sont activés par la souris de l'utilisateur. D'autres approches possibles comprennent l'envoi de périphériques externes aux clients, lesquels génèrent des codes personnels uniques chaque fois que l'utilisateur accède à son compte.

La plupart des utilisateurs ont une certaine connaissance des risques associés aux transactions bancaires en ligne et des outils qui peuvent être utilisés pour les combattre. Cette prise de conscience doit se développer des deux côtés et surtout, ces éléments ne doivent pas être ignorés.

Pour plus d'informations à propos de la sécurisation des transactions en ligne, voir **Comment puis-je me protéger contre les vols sur Internet ?** (http://www.avg.com/fr-fr/77954).

En lire plus sur : AVG Blogs | Small Business
http://small-business.blog.avg.com/2010/02/your-small-business-security-questions-answered-social-networks-sensitive-data-business-banking.html#ixzz0lBnmXlHX

AVG SMB group :
bit.ly/AVGSMB

Devenez fan d'AVG :
facebook.com/avgfree

Lisez nos blogs :
blogs.avg.com

Suivez-nous sur :
twitter.com/
officialAVGnews

Devenez un affilié AVG :
avg.com/gb-en/
affiliate

Regardez notre chaîne :
youtube.com/user/
officialAVG

AVG Technologies France
1, Place de la Chapelle
64600 Anglet
France
www.avg.fr

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
République Tchèque
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
États-Unis
www.avg.com/us-en/
homepage

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Royaume-Uni
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Allemagne
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosie, Chypre
www.avg.com

AVG AU TRAVAIL