

08/02/2010

www.enisa.europa.eu

En ligne instantanément – les 17 règles d’or pour lutter contre les risques en ligne et pour une meilleure sécurité de la navigation sur les réseaux sociaux mobiles.

L'Agence de << cyber sécurité >> de l'UE - l'ENISA (Agence européenne chargée de la sécurité des réseaux et de l'information) présente aujourd'hui un nouveau rapport sur l'accès des réseaux sociaux par les téléphones portables, '[En ligne instantanément](#)'. Le rapport souligne les risques et les menaces des services mobiles de réseaux sociaux, par exemple: le vol d'identité, la fuite des informations d'entreprise et les risques de réputation des réseaux sociaux mobiles. Le rapport donne également les 17 «règles d'or» pour lutter contre ces menaces.

Les sites de réseaux sociaux en ligne (SRSL) ont connu une tendance de croissance exceptionnelle sur Internet. 211 millions d'utilisateurs (sur 283 millions) en Europe utilisent les SRS; principalement Facebook dans 11 des 17 pays étudiés. La façon moderne de rester en contact au niveau professionnel et personnel se fait par le biais de SRS et autres outils numériques. Par conséquent, les moyens par lesquels les gens se rencontrent, échangent des avis communiquent des informations et des idées, évoluent. Avec la popularité croissante des SRS, la demande d'accès instantané et permanent par téléphone portable a augmenté, comme les réseaux sociaux mobiles (RSM). Plus de 65 millions d'utilisateurs accèdent désormais au réseau social Facebook via leur portable. Les utilisateurs de RSM sont 50% plus actifs que les utilisateurs non-mobiles et sont estimés à 134 millions en Europe d'ici 2012.

De nombreux utilisateurs de RSM utilisent également leur téléphone portable comme périphérique de sauvegarde de leur courrier professionnel, données personnelles, contacts et codes d'accès. En conséquence, la perte d'un téléphone portable peut causer des dommages importants, notamment lorsqu'ils sont utilisés illégitimement pour accéder aux RSM. De nombreux téléphones portables sont vendus en offre complète avec des applications intégrées comme les services de 'plate-forme' par exemple.

Plusieurs histoires venues d'Italie, de France, d'Espagne, de Grèce, du Royaume-Uni témoignent d'une grande méconnaissance des utilisateurs des SRS et des RSM quant aux risques de sécurité, aux problèmes liés à la protection de la vie privée et les menaces liées à l'utilisation frauduleuse des informations mises en ligne sur un service de réseau social et de la protection de la vie privée en ligne. Plusieurs risques/menaces exceptionnels sont identifiés dans ce rapport. [Le rapport de l'ENISA](#) donne une vue d'ensemble de la situation et souligne en particulier l'importance de la sensibilisation des utilisateurs sur l'utilisation des réseaux sociaux en ligne de manière plus sûre sur un téléphone portable pour éviter des dommages et les conséquences imprévisibles. Les risques incluent le vol d'identité, et des dommages importants à la réputation de la personne et de l'entreprise ou de la fuite des informations. Deux exemples d'études de cas :

08/02/2010

www.enisa.europa.eu

- **Le faux profil sur Facebook.** Un professeur de l'Université de Turin a découvert que quelqu'un avait créé un profil pour lui sur Facebook avec des détails insultants, affectant sa réputation.
- **Fuite des informations/réputation de l'entreprise.** Après un incident en 2008, Virgin Atlantic airlines a licencié 13 membres de son personnel qui avait posté des commentaires sur Facebook qui critiquaient la propreté de la flotte de la compagnie et les passagers. De la même manière, le personnel de l'enregistrement de British Airlines à Gatwick avait posté des messages sur Facebook disant par exemple que les voyageurs « sentaient mauvais » et le fonctionnement « chaotique » à Heathrow. Le rapport donne également une vue complète du monde des SRS sous l'objectif de la directive européenne sur la protection des informations (Dir. 95/46/EC). Le directeur exécutif de l'ENISA Udo Helmbrecht commente: *«Ce rapport fournit des conseils pratiques aux utilisateurs sur la manière de renforcer la sécurité en ligne partout et à tout moment lorsqu'ils profitent de ces services de réseaux sociaux.»*

Le document inclut 17 «règles d'or» pratiques. En voici quelques exemples:

- Ne pas oublier de se déconnecter du réseau social après utilisation.
- Ne pas permettre la mise en mémoire du mot de passe par le réseau social (cette fonction s'appelle «Auto-complete»).
- Ne pas mélanger les contacts professionnels avec les contacts privés.
- Faire immédiatement état de la perte/du vol de téléphone portable contenant des contacts, photos ou informations personnelles en mémoire.
- Paramétrer le profil au niveau de confidentialité adéquat.

Pour toute recommandation, téléchargez le rapport complet sur : (

<http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens>)

Source : ENISA – Agence européenne chargé de la sécurité des réseaux et de l'information

Pour toute demande d'interview : Ulf Bergstrom, porte-parole de l'ENISA, press@enisa.europa.eu, Portable : +30-6948-460143, or Isabella Santa, Expert sur la sensibilisation. ENISA, awareness@enisa.europa.eu