Après la fuite de Facebook, ESET délivre ses conseils pour se protéger sur les réseaux sociaux.

Le 2 Août 2010

Les Pavillons-sous-Bois, le 2 Août 2010, **ESET**, spécialiste de la conception et du développement de logiciels de sécurité, conseille les utilisateurs d'ordinateur sur la meilleure façon de protéger et sécuriser ses données confidentielles et personnelles sur les réseaux sociaux.

Les informations personnelles d'environ 100 millions sur le demi-milliard d'utilisateurs Facebook ont récemment été compromises par une fuite sur le net. Ce n'est pas la première ni la dernière fois que les réseaux sociaux sont ciblés. David Harley, chercheur chez ESET, présente très souvent ses observations sur les cas de SPAM et de fraudes exploités par les applications utilisées sur Facebook. Afin d'aider ses utilisateurs à rester protéger, ESET a dressé une liste des bonnes pratiques à suivre lorsqu'on navigue sur les réseaux sociaux.

Au regard de la politique de sécurité de Facebook, David Harley commente « *il est clair que ce n'est pas la société Facebook qui prendra les mesures nécessaires à la préservation des données confidentielles de ses utilisateurs. La réaction des responsables de Facebook est de dire « Qu'aucune données personnelles n'a été compromise. A proprement parlé, ils ont raison car les données qui ont fuient ne sont pas confidentielles, puisque non protégées par les configurations les plus strictes de protection de données confidentielles disponibles sur Facebook* » ajoute le chercheur basé à Londres.

Harley observe que le bateau a déjà coulé car même si les utilisateurs changent la configuration de leurs informations personnelles et confidentielles maintenant, leurs données sont déjà dans le domaine public et ont sans doute été téléchargées par un millier de personnes.

Ce n'est pas la seule faille de sécurité sur Facebook ce mois-ci, comme la spectaculaires propagation de l'escroquerie à propos de « *La vérité sur Coca Cola* » ou encore la vidéo de « *ce professeur qui a failli tuer ce garçon* ». La plupart des Rogue (Faux antispyware) et des vers présents dans les applications des réseaux sociaux sont utilisés comme outils marketings ou par des cybercriminels à la recherche d'utilisateurs à escroquer. « *Ils continuent d'infester les utilisateurs de Facebook, en spammant leur comptes et en propageant des virus par le biais de liens à travers le réseau social* » ajoute David Harley. Les utilisateurs ne s'en aperçoivent même pas après avoir installé ou utilisé l'application.

Quelques règles d'or pour éviter les désagréments sur les réseaux sociaux

Ajustez votre configuration de données personnelles sur Facebook :

Permettez seulement à vos amis de confiance de voir votre profil en entier, utilisez un profil limité pour les autres. Dans les options de configuration de Facebook, vous pouvez choisir ce que vous voulez partager : Votre page d'actualité, les messages sur le mur, les informations personnelles ou photos. De temps en temps, Facebook change les configurations de confidentialité, veillez à toujours contrôler si vous les autorisez. Si vous découvrez qu'une personne parmi vos contacts n'est pas digne de confiance, retirez-la.

évitez de cliquer sur les liens :

Vous n'ouvririez jamais un lien douteux dans un E-mail, même s'il vous est envoyé par un ami. Vous devez procéder avec la même précaution sur Facebook. Le message peut provenir d'un intrus ou d'un cybercriminel et non de votre ami.

N'acceptez que les amis que vous connaissez :

Les utilisateurs doivent éviter d'accepter des amis qu'ils ne connaissent pas et dans aucun cas ils ne doivent leur permettre de voir leur profil entier. Vous devez toujours garder à l'esprit de maîtriser avec qui vous partagez quoi.

Les données circulent pour toujours :

Ne supposez pas que quand vous effacez une photo ou le compte de votre réseau social, toutes vos données sont effacées pour toujours. Il n'en est rien. Vos photos et informations pourraient être déjà sauvegardées sur un ordinateur. Réfléchissez à deux fois avant de poster une photo ou une information sur internet.

Soyez prudent quand vous installez des applications :

Beaucoup d'applications de tiers pourraient être le fruit des cybercriminels et entrer dans la catégorie non désirée de Spam. Vous ne voulez, sans doute, pas partager vos informations privés avec ces entités.

Réfléchissez avant de cliquer :

Avant de cliquer sur le bouton « *clique ici* », réfléchissez. Vos amis peuvent être atteints du ver *clickjacking*. En cliquant sur ce bouton, l'image apparait sur votre page d'accueil incitant vos amis à cliquer à leur tour, ainsi vous spammez tous vos amis. Si vous voulez retirer ce ver, vous devez retirer le message infecté de votre page d'actualité et de votre mur et examinez vos configurations d'application pour vous assurer qu'elles ne sont pas douteuses.

A propos d'ESET

La société ESET est spécialisée dans la conception et le développement de logiciels de sécurité offrant une protection globale contre les menaces évolutives qui sévissent dans les environnements informatiques. Pionnier en matière de détection proactive des menaces, ESET est aujourd'hui le leader dans ce domaine. ESET a développé un vaste réseau mondial de partenariats, y compris avec des entreprises telles que Canon, Dell et Microsoft. ESET possède des bureaux à Bratislava (Slovaquie), Bristol (Royaume-Unis), Buenos Aires (Argentine), San Diego (USA), Prague (République Tchèque), et est représenté dans plus de 110 pays. Pour plus d'informations, veuillez visiter les sites Internet :www.eset-nod32.fr ou www.athena-gs.com