

# Social network : une cible de choix pour les fraudeurs

Selon le spécialiste américain des technologies d'information [Equifax](#), (finance, santé, crédit...), les adeptes des réseaux sociaux s'exposent eux-mêmes ouvertement à des risques de fraude d'identité en publiant un trop grand nombre d'informations personnelles sur leurs pages de profil.

Avec un taux record d'adhésion aux services comme [MySpace](#), [Bebo](#), [Facebook](#), [Friends Reunited](#), de plus en plus d'informations personnelles sont aujourd'hui à la disposition des fraudeurs et des voleurs d'identité.

*"Les fraudeurs tirent avantage de l'engouement suscité par les réseaux sociaux, et les gens ne réalisent pas l'importance des informations qu'ils publient sur Internet et qui sont ainsi accessibles à n'importe qui", fait observer Neil Munroe, directeur des affaires externes chez Equifax.*

*"De plus en plus de consommateurs adhèrent à ces sites et augmentent ainsi les probabilités de divulguer leurs date de naissance, adresse, adresse e-mail, emploi et statut marital", remarque le représentant d'Equifax. "Nous ne voulons pas que les utilisateurs cessent d'utiliser ces sites, nous leur recommandons simplement de limiter les informations disponibles afin de se prémunir contre le vol d'identité."*

Mark Sunner, analyste sécurité chez [MessageLabs](#), a annoncé l'émergence d'une nouvelle conception de communauté sur Internet. *" De nombreux consommateurs ont simplement fait leur première incursion dans ce nouveau développement passionnant du Web 2.0", commente l'expert. "Ils considèrent cet environnement comme un divertissement. Ils sont loins d'imaginer que ses espaces sont déjà envahis par des spécialistes en vol d'identité, en spam et en phishing."*

Equifax a formulé cinq recommandations à suivre pour éviter de devenir la cible des criminels sur les sites de réseaux communautaires :

- Ne pas fournir d'éléments de vérification courants tels que la date de naissance ou le nom de jeune fille de la mère
- Utiliser des paramètres de confidentialité sur les profils pour que seuls les amis proches puissent accéder à ces informations
- Ne pas publier les dates de congé ou d'autres informations qui pourraient vous exposer à des risques d'infractions
- Ne pas publier d'informations qui pourraient ruiner vos nouvelles opportunités de carrière, car les employeurs potentiels utilisent souvent les sites de "réseau social".
- Se méfier de tout le monde. Les photos et les profils exposés sont souvent trompeurs.

Traduction d'un article de [Vnunet.com](#) en date du 23 juillet 2007