Facebook : les utilisateurs sont trop bavards

Une enquête publiée par l'éditeur britannique Sophos se penche sur le réseau Facebook qui revendique 26,6 millions de visiteurs par mois, 31 millions de membres, et pas moins de 100.000 nouvelles inscriptions par jour.

En conséquence, Facebook est une cible particulièrement alléchante pour des cybercriminels. Ces derniers sont assurés de trouver quantité de données personnelles comme des emails, des numéros de téléphone, des adresses…

Une fois toutes ses informations collectées, organisées et étudiées, les hackers ont l'embarras du choix. Sophos s'inquiète de cette prolifération de données personnelles, et ce n'est pas la première fois que l'éditeur tire la sonnette d'alarme.

Signalons d'ailleurs qu'en octobre 2006 la « National Cyber Security Alliance » aux USA expliquait : *» le simple fait de donner un numéro de sécurité sociale couplé à une adresse et une date de naissance est suffisant pour un attaquant. En agissant de la sorte, on donne des munitions aux pirates qui peuvent ensuite récupérer des informations financières et accéder à des comptes bancaires. »*

Et le danger ne cesse d'augmenter, puisque d'après Sophos, 41 % des utilisateurs de Facebook sont prêts à révéler des informations personnelles sans contrôler d'où provient la demande.

Les équipes de Sophos ont infiltré le réseau

Les experts de Sophos ont d'abord créé sur Facebook une fiche de personnalité artificielle au nom de ?Freddi Staur' (une anagramme de ?ID Fraudster'), représenté par une petite grenouille en plastique et ne contenant qu'un minimum d'informations sur lui-même.

Ils ont ensuite envoyé des « friend requests » à un échantillon aléatoire de 200 utilisateurs, afin de voir combien répondraient et quelle quantité d'informations ils accepteraient de divulguer. Sur Facebook, ces demandes peuvent être soit acceptées soit refusées par le destinataire, qui peut choisir de donner à l'émetteur un accès total ou partiel à son profil en ligne.

87 personnes sur 200 ont répondu à ?Freddi', qui a eu dans la majorité des cas accès à des photos de famille ou d'amis, à des informations sur leurs goûts, leurs hobbies, leur profession et à d'autres éléments personnels. De nombreux utilisateurs ont également dévoilé le nom de leur compagne ou compagnon, plusieurs y ajoutant leur CV complet. L'un d'entre eux a même indiqué le nom de jeune fille de sa mère, une information souvent demandée par les sites bancaires pour accéder à un compte en ligne.

« Il est inquiétant de constater la facilité avec laquelle Freddi a eu accès à ces informations, que la plupart des gens refuseraient de donner à un inconnu dans la rue ou en réponse à un message de spam. Il en a ainsi appris suffisamment pour créer des messages de phishing ou des programmes malveillants personnalisés, pour deviner des mots de passe, ou même pour usurper leur identité », commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos France et Europe du Sud.

« Il faut savoir que les fonctionnalités mises en place par Facebook pour protéger l'intimité des utilisateurs vont bien au-delà de celles proposées par de nombreux autres sites de réseau social concurrents. Il s'agit donc uniquement d'une question de comportement humain, qui peut réduire à néant tous les efforts de sécurisation et mettre en danger aussi bien les utilisateurs eux-mêmes que leur entreprise. Une attitude prudente et raisonnable demeure indispensable, même lorsque la demande ne provient pas d'un message de spam. »

Facebook poursuivit pour plagiat. L'URL qui met en relation les internautes est attaquée par un tribunal du Massachusetts. La justice américaine, doit déterminer si le fondateur de Facebook.com, Mark Zukerberg, s'est inspiré d'un autre site nommé : ConnectU.Ironie de l'histoire Zukerberg avait participé à la création de cette page communautaire en 2003.Reste qu'entre les deux projets, celui du créateur de Facebook occupe la première place du podium contre seulement une centaine de milliers pour ConnectU.