

Twitter de plus en plus victime du phishing

Avoir un compte [Twitter](#) et recevoir un message de type « *This you ??* » ou bien « *LOL is this you ?* » est devenu presque courant. Il s'agit en fait de rien de plus qu'un spam ou message non-sollicité visant le site de micro-blogging.

Le site Zataz.com explique que ces faux *tweets* pointent vers un site ressemblant à la page d'accueil de Twitter. Si l'internaute mord à l'hameçon et entre son login et mot de passe, il semble être redirigé vers son propre compte Twitter. Cependant, il vient juste d'être victime d'un pirate qui lui a **subtilisé ses données personnelles**. Une méthode traditionnelle qui aurait déjà fait quelques dégâts.

Certains éditeurs comme F-Secure estiment « *s'attendre très prochainement à voir de nouvelles **attaques de phishing contre Facebook*** ». Les réseaux sociaux confirment leur statut de terrains propices aux piratage.

Un large champ malveillant existe donc puisque, outre le phishing *via* l'envoi de spam, Twitter est aussi le **repère de faux-amis (faux comptes)** censés gonfler votre réputation en ligne suivi mais aussi affaiblissant la sécurité du compte. De même, les **trending topics**

(sujets chauds) s'avèrent parfois plutôt étranges dans le sens où certains redirigent vers des sites de téléchargement illégal voire des sites franchement douteux.

Twitter incite donc les internautes qui reçoivent des messages de *phishing* à changer régulièrement leur [mot de passe](#). Histoire de pouvoir gazouiller en toute sécurité.