

# Alerte aux malwares par Facebook

Une nouvelle [campagne](#) de messages non-sollicités sévissent sur Facebook. Une méthode éculée mais qui fonctionne en général très bien.

Cette fois, il s'agit d'un contact qui souhaiterait devenir votre nouvel ami. L'internaute reçoit alors un message lui demandant de **confirmer cette toute nouvelle amitié naissante**. Dès lors, le message joue sur sa **ressemblance frappante avec une véritable page**

**Facebook**. De plus l'adresse affichée ressemble de près à celle du site.

Les pirates s'attaquent décidément régulièrement au site. On connaissait les spams incluant un **fichier zip** (compressé) censés contenir une photographie. Une fois ouvert, le fichier ne comprenait alors qu'un simple **virus**... Il y eut aussi le temps des applications vérolées de Facebook, bref tout un bestiaire rien que pour ce site.

Dès lors, afin de maintenir leur niveau d'attaques réussies, les pirates ont décidé de changer leur fusil d'épaule. Ils sont donc passés des fichiers joints aux simples **faux-liens** afin d'induire les internautes en erreur. « *Une pratique plus difficile à détecter par les Antivirus car tous n'ont pas la **capacité de scanner et détecter les liens contenus dans les e-mails*** » constate Websense.

Selon les laboratoires de l'éditeur, qui affirment traiter **350 millions de courriels par semaine**, cette méthode est en très nette augmentation chez les spammeurs. De même, les sites de [réseaux sociaux](#) sont, disent-ils, des [cibles parfaites](#) pour ce type d'attaques. Vu leur popularité, les sites de Web 2.0 permettent alors de mener des offensives très larges.

L'éditeur de sécurité recommande aux internautes la plus grande **prudence** et de se doter d'une gamme de sécurité mise à jour.