

F-Secure : Attention aux arnaques aux dons !

S  curit  

Post   par : JPilo

Publi  e le : 20/1/2010 15:00:00

Peu de temps apr  s la catastrophe qui a frapp   Ha  ti, les cybercriminels s  en donnent   c  ur joie. Les chercheurs de **F-Secure ont d  tect   plusieurs types d  arnaqes** allant du r  f  rencement de sites frauduleux sur les moteurs de recherche (attaques SEO) aux scams classiques sollicitant des dons par emails ou via les r  seaux sociaux.

Attaques de type SEO

Ce type d  attaques s  appuient sur des termes que l  internaute va indiquer dans un moteur de recherche. Certaines recherches et liens sponsoris  s li  s au tremblement de terre    Ha  ti dirigent l  internaute vers un site qui installe alors un programme malveillant dans le syst  me    l  insu de l  utilisateur.



Arnaques par Scam

Le scam est une arnaque qui consiste en l  envoi massif d  emails ayant pour objectif de tromper des internautes. Le plus connu est celui du riche h  ritier demandant de l'aide pour pouvoir transf  rer sa fortune en France en   change d  une r  tribution.

Dans le cadre de l  arnaque li  e au s  isme d  Ha  ti, les cybercriminels cherchent    se faire passer pour des associations souhaitant recueillir des dons en faveur des victimes. Pour cela, ils vous feront soit parvenir des num  ros de t  l  phones frauduleux (via une alerte Twitter ou un SMS par exemple), soit vous enverrons des emails accompagn  s d  un formulaire visant    r  cup  rer des donn  es personnelles et bancaires.

Les r  gles d  or :

   **Ne jamais r  pondre en direct aux sollicitations re   ues par emails** et surtout ne pas cliquer sur les liens contenus dans ces messages ou contacter les num  ros de t  l  phones indiqu  s.

   **Toujours proc  der    une v  rification de l'existence** r  elle des associations et

organisations humanitaires dont on aurait entendu parler et auxquelles on souhaite faire un don. Privilégier les organismes reconnus et éviter les intermédiaires.

Ne jamais transmettre ses coordonnées bancaires par email ou par téléphone à une personne vous ayant contacté spontanément

Bien entendu, ces règles s'appliquent également aux divers réseaux sociaux par lesquels il est possible de transmettre le même type d'informations erronées, soit par les messageries/groupes qui y sont présents, soit au travers des « statuts » qui autorisent la mise en ligne de liens ou numéro de téléphones frauduleux.

Les activités criminelles comme celles-ci se multiplient systématiquement à l'annonce de faits d'actualité majeurs (désastres, catastrophes, événements sportifs, etc.). F-Secure encourage donc les personnes qui souhaitent venir en aide aux victimes d'Haïti, à faire particulièrement attention que cela soit dans le cas d'une démarche spontanée ou après avoir été sollicité.