Restons vigilants.

Une recrudescence d'attaques virales est en cours actuellement par des fraudeurs malhonnêtes et malveillants qui par hameçonnage tente de contacter des personnes en se faisant passer pour des instances officielles telles que banques, assurances ou autres. Par courrier électronique, on vous demande vos accès ou mots de passe pour des raisons diverses telle que vérification d'identité ou réactiver votre compte.

Si vous recevez un tel message même avec une adresse connue ;

Ne répondez jamais ou dans le doute renseignez-vous, c'est probable une arnaque

Par précaution, il est impératif actuellement d'avoir un logiciel anti-virus performant

R. Ansermet

Hameçonnage

L'**hameçonnage**, ***phishing*** ou **filoutage** est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. En effet, le plus souvent, une copie exacte d'un site internet est réalisée dans l'optique de faire croire à la victime qu'elle se trouve sur le site internet officiel où elle pensait se connecter. La victime va ainsi rentrer ses codes personnels qui seront récupérés par celui qui a créé le faux site, il aura ainsi accès aux données personnelles de la victime, et par exemple dans le cadre d'un jeu, pourra dérober tout ce que la victime possède sur le jeu. (On retrouve cela principalement dans les MMORPG, où les objets du jeu peuvent avoir une valeur financière). Elle peut aussi faire par courrier électronique ou autres moyens électroniques.

Sur Internet

Les criminels informatiques utilisent généralement l'hameçonnage pour voler de l'argent. Les cibles les plus courantes sont les services bancaires en ligne, les fournisseur d'accès à internet, les sites de ventes aux enchères tels qu'eBay, et le système de paiementPaypal. Les adeptes de l'hameçonnage envoient habituellement des courriels à un grand nombre de victimes potentielles.

Typiquement, les messages ainsi envoyés semblent émaner d'une société digne de confiance et sont formulés de manière à alarmer le destinataire afin qu'il effectue une action en conséquence. Une approche souvent utilisée est d'indiquer à la victime que son compte a été désactivé à cause d'un problème et que la réactivation ne sera possible qu'en cas d'action de sa part. Le message fournit alors un hyperlien qui dirige l'utilisateur vers une page Web qui ressemble à s'y méprendre au vrai site de la société digne de confiance. Arrivé sur cette page falsifiée, l'utilisateur est invité à saisir des informations confidentielles qui sont alors enregistrées par le criminel.

En 2007, ces criminels informatiques ont changé de technique en utilisant un moyen de piratage appelé attaque de l'homme du milieu pour recueillir les informations confidentielles données par l'internaute sur le site visité.

Afin d'entretenir la confusion, il arrive que l'utilisateur soit ensuite redirigé vers la vraie adresse du site web, sur lequel l'authentification lui est à nouveau demandée.

Exemple

Les attaques par hameçonnage sont le plus souvent dirigées vers les sites sensibles tels que les sites bancaires. Les sites de réseaux sociaux sont aujourd'hui également la cible de ces attaques. Les profils des utilisateurs des réseaux sociaux contiennent de nombreux éléments privés qui permettent aux pirates informatiques de s'insérer dans la vie des personnes ciblées et de réussir à récupérer des informations sensibles