Panoptinet

Gardez un oeil sur votre réseau

Ensemble contre le phishing

admin · Friday, January 14th, 2011

Le Phishing – ou hameçonnage – est une menace qui pèse de plus en plus sur les internautes. Pour lutter contre cette pratique, Microsoft, Paypal et le Cert-Lexsi innovent et proposent un outil participatif : Phishing Initiative.

Microsoft, Paypal et le Cert-Lexsi viennent d'inaugurer un nouveau site internet, Phishing Initiative, qui invite les internautes à rapporter leurs dernières expériences d'hameçonnage, et notamment à renseigner l'adresse des sites impliqués. Après vérification, la base de données Phishing Initiative est enrichie de ces connaissances, qui sont ensuite transmises aux principaux navigateurs web : Internet Explorer, Firefox, Safari, Chrome. Ainsi, les internautes pourront être avertis s'ils visitent par mégarde un site frauduleux.

Alors, pour le bien de tous, n'hésitez pas à participer !

Source : 01.net

L'analyse de Panoptinet

Qu'est-ce que le phishing ?

Aussi appelé hameçonnage, le phishing est une activité frauduleuse consistant à tromper un internaute pour l'amener sur un site Internet ressemblant en tout point à un site officiel : banque, institution sociale, fournisseur d'accès Internet, etc. L'objectif est de convaincre l'internaute de donner ses coordonnées bancaires.

Pourquoi le phishing devient une activité réellement inquiétante ?

Cette pratique existe depuis quelques années, mais seuls les internautes les plus crédules ou les moins attentifs se faisaient berner : les sites de phishing censés copier des sites officiels étaient mal reproduits, de nombreuses fautes d'orthographes n'étaient pas corrigées, et le discours n'était pas toujours soigné. Or nous assistons aujourd'hui à une nette amélioration de ces défauts, au détriment des internautes qui se font avoir.

Comment est-on amené vers un site de phishing ?

Généralement, la victime reçoit un mail qui reprend l'identité d'une institution "digne de confiance" : logo, texte, références, etc. Souvent même, l'adresse d'expédition du message prête à confusion (ex : hautdebit@freetelecom.fr). La plupart du temps, le mail s'adresse directement à son lecteur, en lui faisant part d'un problème administratif à régler rapidement, ou d'un beau cadeau qu'il est censé gagner. Le message termine immanquablement par un lien sur lequel nous sommes invités à cliquer, et qui envoie vers un site factice, reprenant tous les codes graphiques du site copié.

Voici pour exemple deux cas typiques d'hameçonnage :

Nous avons etudie vos droits.

Il apparait apres culcul que pour Caisse d'Allocations Familiales pour la periode du 01.06.2009 au 30.09.2009, vous n'avez rien recu alors que vous avez droit a 325,54 euro.

Cliquez ici

Comment peut-on déceler la tentative frauduleuse ?

Sans devenir paranoïaque, il faut sans cesse rester vigilant sur Internet, un monde où les apparences sont particulièrement trompeuses. Concrètement voici les réflexes à adopter :

1. Un mail qui demande à renseigner des informations administratives ou bancaires est nécessairement suspect. Jamais votre banque par exemple ne vous demandera une telle chose par Internet.
2. Analyser l'adresse de l'expéditeur : souvent bien imitées, elles sont aussi parfois alambiquées. Si vous avez un doute, ne tenez pas compte du message envoyé.
3. Faire attention aux tournures de phrase et à l'orthographe : même si les messages de phishing semblent de plus en plus authentiques, on trouve encore quelques mails fort mal écrits. Si tel est le cas, ne tenez pas compte du message envoyé.
4. Survolez de la souris le lien qui conclut le message, et regardez en bas de votre écran à gauche vers quelle adresse (URL) il pointe : très souvent, l'adresse web de destination est très longue et ne ressemble pas du tout à celle de l'organisme auquel vous êtes censés croire.
5. Enfin, si aucune de ces étapes ne vous a mis la puce à l'oreille, ne donnez jamais aucune information personnelle ou bancaire sur un site dont l'adresse (URL) ne commence pas par **https**://www… Le "S" de https signifie "sécurisé". Tous les sites bancaires et commerciaux dignes de ce nom ont un espace en https pour les règlements en ligne.

This entry was posted on Friday, January 14th, 2011 at 5:28 pm and is filed under Actualités décryptées par Panoptinet
You can follow any responses to this entry through the Comments (RSS) feed. You can leave a response, or trackback from your own site.