Qu'est-ce que le phishing - hameçonnage - scam ? Commen...

Auteur:
Webcreatif Network SA

Cr11 May 2010 8:46 AM

DÃ©finition du filoutage (phishing)

Le filoutage, ou phishing, est une technique utilisÃ©e par des personnes malveillantes dans le but dâ€™obtenir des informations confidentielles sur leurs victimes puis de sâ€™en servir. Pour ce faire les fraudeurs contactent leurs victimes sous diffÃ©rents prÃ©textes en usurpant lâ€™identitÃ© dâ€™un tiers dans lequel la victime pourrait avoir confiance (Votre banque, un site de commerceâ€¦).

Ces arnaques visent aujourdâ€™hui principalement les clients des sites bancaires, mais il nâ€™est pas rare de constater quâ€™elles peuvent aussi sâ€™attaquer aux clients de Webcreatif Network SA ou d'autres organismes.

Sur lâ€™internet on trouve Ã©galement le terme dâ€™hameÃ§onnage, filoutage (Phishing): Vol dâ€™identitÃ©s ou dâ€™informations confidentielles (codes dâ€™accÃ¨s, coordonnÃ©es bancaires) par subterfuge : un systÃ¨me dâ€™authentification est simulÃ© par un utilisateur malveillant, qui essaie alors de convaincre des usagers de lâ€™utiliser et de communiquer des informations confidentielles, comme sâ€™il sâ€™agissait dâ€™un systÃ¨me lÃ©gitime.

Remarque : Les sites sont reproduits, aprÃ¨s avoir Ã©tÃ© aspirÃ©s. Lâ€™utilisateur est souvent invitÃ© Ã visiter le site frauduleux par un courrier Ã©lectronique.

Principe de fonctionnement

GÃ©nÃ©ralement la victime reÃ§oit dans sa messagerie Ã©lectronique un courriel, semblant provenir de sa banque ou dâ€™un organisme de confiance, lui indiquant quâ€™un problÃ¨me est survenu sur son compte.
Le contenu du mail est vraisemblable, il utilise nos logos et invite la victime Ã cliquer sur le lien contenu dans le courrier afin de rÃ©soudre ce soi-disant problÃ¨me. Le lien affichÃ© est dâ€™ailleurs correcte (quand le message est affichÃ© au format HTML).

Le lien internet masquÃ©, contenu dans le mail, conduit en fait Ã un site ressemblant Ã sâ€™y mÃ©prendre au site de lâ€™organisme de confiance. Cette imitation a Ã©tÃ© dÃ©posÃ©e par une personne malintentionnÃ©e sur un autre site internet compromis.
DÃ¨s quâ€™une victime saisit des informations personnelles (identifiants, mots de passe, coordonnÃ©es bancaires), celles-ci sont immÃ©diatement envoyÃ©es Ã la personne malveillante qui sâ€™empressera de les utiliser.

Ces courriers frauduleux ne sont gÃ©nÃ©ralement pas ciblÃ©s mais envoyÃ©s Ã des milliers dâ€™adresses.

Comment sâ€™en protÃ©ger ?

» Nous n'envoyons jamais ce genre de courriel, ni votre banque d'ailleurs : dâ€™une maniÃ¨re gÃ©nÃ©rale, nous ne vous demanderons jamais de venir saisir leurs informations personnelles dans un courrier Ã©lectronique. Pour se connecter Ã notre site, il vaut mieux entrer manuellement lâ€™adresse (URL) dans votre navigateur.
» PrÃ©fÃ©rer saisir des informations personnelles (identifiants, mots de passe, coordonnÃ©es bancairesâ€¦) sur des sites internet sÃ©curisÃ©s : un cadenas apparaÃ®t dans le navigateur et lâ€™adresse du site commence par HTTPS au lieu de HTTP.
» Ne pas cliquer sur les liens contenus dans les courriers Ã©lectroniques : les liens affichÃ©s dans les courriers Ã©lectroniques peuvent en rÃ©alitÃ© diriger les internautes vers des sites frauduleux. En cas de doute, il est prÃ©fÃ©rable de saisir manuellement lâ€™adresse dans le navigateur.
» Ãtre vigilant lorsquâ€™un courriel demande des actions urgentes.
» Utiliser le filtre contre le filoutage du navigateur internet : la plupart des navigateurs (Microsoft Internet Explorer 7, Mozilla Firefox, OpÃ©ra) proposent une fonctionnalitÃ© dâ€™avertissement contre le filoutage. Leurs principes peuvent Ãªtre diffÃ©rents (liste noire, liste blanche, mot clÃ©â€¦) et sans Ãªtre parfaites, ses fonctions aident Ã maintenir la vigilance de lâ€™utilisateur.
» Utiliser un logiciel de filtre anti-pourriel : la plupart du temps ces tentatives dâ€™escroquerie se diffusent par le biais de courriers Ã©lectroniques. MÃªme si les logiciels de filtrage ne sont pas parfaits, ils permettent de rÃ©duire le nombre de ces courriels.
» Ne jamais rÃ©pondre ou transfÃ©rer ces courriels.
» En cas de doute ou de problÃ¨me, prendre contact rapidement avec nous.
» Dâ€™une maniÃ¨re gÃ©nÃ©rale, Ãªtre vigilant et faire preuve de bon sens : ne pas croire que ce qui vient de lâ€™internet est forcÃ©ment vrai.
Vous pouvez, de votre cÃ´tÃ©, signaler un site malveillant, cela seul permet de lutter efficacement contre ce flÃ©au, malheureusement plus prÃ©sent que jamais. Pour cela, il vous faut suivre ces guides:

Sur Internet Explorer 8
Sur Mozilla Firefox

Sources :

http://www.securite-informatique.gouv.fr/gp_article44.html
http://www.securite-informatique.gouv.fr/gp_rubrique33_lettre_H.html