

Le phishing ou l'exploitation de la faille humaine

Article sécurité - Septembre 2009

Dernière mise à jour : 01/09/2009

Auteur : Salima Cosadia

28 Août 2009 - Le phishing est une forme d'escroquerie informatique qui utilise la confiance, l'ignorance ou la crédulité de ses victimes pour perpétrer des usurpations d'identité. Des moyens de lutte informatique existent. Cependant, devant ce type d'attaque, il n'y a rien qui puisse remplacer notre bon sens et notre vigilance.



Le phishing ou l'exploitation de la faille humaine

Le phishing ou la « pêche aux mots de passe »

Le phishing ou hameçonnage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité.

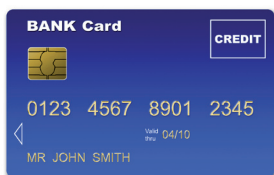
Elle consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, etc.) afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc.

Le hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou tout autre moyen électronique.¹

La manipulation par la communication : le social engineering

C'est une forme d'attaque informatique reposant sur l'ingénierie sociale ou 'social engineering', forme d'escroquerie utilisée en informatique pour obtenir un bien ou une information.

L'escroc abuse ainsi de la confiance, l'ignorance ou la crédulité de personnes possédant ce qu'il tente d'obtenir, et utilise ses connaissances, son charisme, l'imposture ou le culot.



Une attaque type

Vous recevez un email aux couleurs d'une société commerciale, comme une banque par exemple. On peut citer les cas de phishing faisant référence à la Société Générale ou encore BNP Paribas.

Imaginez un email plagiant une grande banque réunionnaise. Cet email vous demande de vous connecter sur votre compte en ligne pour confirmer votre mot de passe ou mettre à jour vos données personnelles sur un site qui imite parfaitement celui de votre banque, en général sous la forme de fausses pages de maintenance technique avec une adresse de site qui semble correcte.

Votre identifiant, votre mot de passe, votre numéro de carte bancaire, etc., vous sont demandés. Vous êtes ensuite informé que tout s'est bien passé, que le problème est réglé et vous êtes même remercié(e) sur la dernière page. En bref, pour vous, tout va bien.

Mais l'escroc a désormais tout loisir d'accéder à vos comptes sur lesquels il est désormais en mesure d'effectuer en toute « légitimité » toutes les opérations que vous êtes autorisé(e) à réaliser quand vous êtes connecté(e).

Les autres types d'attaque « phishing »

Outre les faux emails, les attaques « phishing » prennent la forme de phishing par téléphone fixe ou mobile, par fax, par VoIP (Vishing), ainsi que la circulation depuis 2005 d'une fausse barre du moteur de recherche Google propagée par messagerie instantanée qui vise à récupérer les numéros de cartes bancaires.

Comment lutter contre les attaques « phishing » ?

La lutte contre les attaques « phishing » passe par des messages de prévention tels que la recommandation de ne jamais divulguer ses coordonnées bancaires, ses mots de passe à quiconque, même au responsable du département informatique de sa structure. Les banques préviennent également leurs clients de ne répondre à aucun email leur demandant de se connecter à leur espace sécurisé.

D'autre part, certaines techniques utilisent des failles de sécurité dans les navigateurs Internet, par conséquent, les mises à jour de sécurité doivent être effectuées régulièrement. Il est également recommandé de taper soi-même directement dans la barre d'adresse l'URL d'un site Web.

Autant de petits moyens qui permettent de se préserver de l'usurpation d'identité et qui complètent le bon sens et la vigilance dont peut faire preuve l'être humain.

Sources :

¹ <http://fr.wikipedia.org/wiki/Hame%C3%A7onnage>

<https://informations.lcl.fr/securite/risques/phishing.html#art4>

Salima Cosadia

Pour BinarySEC

BinarySEC FRANCE S.A.S

4, rue Franck Camille Cadet
97427 Etang-Salé

Tél. : +262 (0) 262 45 83 07

Fax. : +262 (0) 262 45 83 20