N°3

La Lettre du Chiffre

Octobre 2011

Éditorial

Dans cette édition, nous entrons dans le vif du sujet avec le phishing.

N'hésitez pas à me contacter pour toute question.

Daniel Ayache – Responsable Sécurité des Systèmes d'Information.

Le Phishing : à la pêche au gogo.

Le Phishing est une technique d'usurpation très en vogue chez les pirates : elle consiste à envoyer des mails piégés en se faisant passer pour des organismes ou entreprises officielles. Voici comment les reconnaître et comment réagir.

Ils contiennent :
* un message d'accroche indiquant la plupart du temps que le compte de l'utilisateur a été piraté et qu'une mise à jour des données personnelles est indispensable (nom, prénom, identifiant utilisateur, mot de passe et souvent, numéro de carte bancaire, code etc),
* un lien internet vers le site de mise à jour de ces données – supposé appartenir à l'organisme ou la société en question. C'est à ce moment que la tromperie est effective : le site ressemble totalement au site d'origine mais les données saisies iront directement dans la poche des pirates. Une variante 'low cost' consiste à demander ces informations par retour de mail.

Ceci est un exemple que j'ai reçu il y a quelques jours :

De : LA BANQUE POSTALE [info@labanquepostale.fr]
À : AYACHE Daniel
Cc :
Objet : MESSAGE DE SECURITE... URGENT

LA BANQUE POSTALE

Bonjour ,

Votre Carte Bancaire a été suspendue , car notre sytème de sécurité a détecté plusieurs échecs de tentatives de changement de votre code de sécurité .

Pour lever cette suspension, **CLIQUEZ-ICI** et suivez la procedure indiquée pour mettre a jour vos informations personnelles et nous permettre de vérifier et de valider votre carte Ã nouveau.

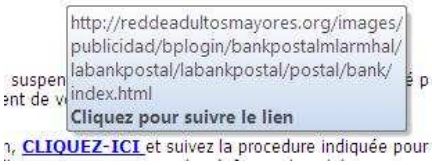
Note: Si ce n'est pas fait dans les 48 heures, nous serons contraint de suspendre votre carte.

Nous vous remercions de votre coopération.

Le Service Client.

Voici les indices qui éveilleront la suspicion de l'utilisateur averti :
* je n'ai pas de compte à la banque postale ! Ceci étant, je reçois également du phishing pour ma vraie banque ou mon fournisseur d'accès internet.
* la plupart du temps, le texte contient des fautes d'orthographe (oublis d'accents, fautes d'accord, formulations lourdes…). C'est le cas ici mais c'est souvent beaucoup plus flagrant : « *En raison de plusieurs frauduleuse tentative sur la carte bancaire de vous, nous vous demandont de confirmé vos données personnels* » - là, l'internaute francophone standard doit normalement commencer à se douter de quelque chose…

* enfin, et c'est systématique, le lien conduit vers un site pirate. Pour le détecter, passez la souris sur le lien du message (sans cliquer !), vous verrez en sur-impression comme ci-dessous – ou dans la barre d'état selon l'outil de messagerie – l'adresse réelle du site qui, dans le cas présent, n'a rien à voir avec le site officiel.



Il arrive cependant que le site pirate ait un nom très proche du site réel (par exemple, « labanquepostale.service.cn »), ce qui ajoute à la confusion.

Imaginez maintenant que des pirates veuillent nous attaquer et nous envoient un message au look Thales nous demandant de ressaisir notre mot de passe LDAP pour corriger un prétendu problème technique…

Exercice pratique.

Avec ce que nous venons de voir, le message suivant vous paraît-il authentique ?

De : ASSISTANCE INTERNET [mailto:service.login.verif@gmail.com]
Envoyé : vendredi 2 septembre 2011 11:05
À : service.login.verif@gmail.com
Objet : ALERTE!!!

assistance internet

Cher(e) Membre,

En raison de la congestion de tous les utilisateurs de compte mail et l'enlèvement de tous les comptes inutilisés de internet nous seront obligés de fermé votre compte vous devrez confirmer votre e-mail en remplissant vos informations de connexion ci-dessous au cas où le formulaire n'est pas totalement rempli votre compte pourra être suspendue dans les 24 heures pour des raisons de sécurité.

Complétez, ci-dessous, les données vous concernant puis validez Vos données

Nom .....
Prénom .....
Login .....
Adresse mail .....
Mot de passe .....
Occupation :.....

Quoi qu'il en soit, si, en définitive, vous êtes persuadé que vous avez reçu un message authentique, ne cliquez jamais sur le lien et ne répondez pas au mail mais discutez-en avec votre RSSI préféré qui saura compléter votre analyse de la situation.