

L'hameçonnage (ou fishing en anglais)

PCTOULON Maintenance informatique à domicile De Toulon ouest à Bandol (ou plus loin...)	Cyril : 06 09 89 25 98 pctoulon@free.fr http://pctoulon.fr
---	---

Non, je ne vais pas parler de pêche à la truite, mais de pêche d'identité et de compte bancaire, et le poisson c'est vous !

1 / Définition

L'hameçonnage (Phishing, appelé aussi filoutage), est une méthode utilisée par les pirates pour obtenir des renseignements dans le but de voler des informations personnelles à l'internaute

Ces informations peuvent être un mot de passe, carte de crédit,,

2 / Comment ça marche ?

La technique est que le pirate utilise une méthode de communication (courrier électronique par exemple) pour se faire passer par un organisme de confiance (votre banque, votre fournisseur d'accès internet, les impôts...) et de vous voler des informations personnelles

L'exemple type est un courrier électronique qui vient d'un organisme d'abonnement vous annonçant qu'il y a eu un problème sur votre compte, que pour arranger le problème il suffit de se connecter sur votre compte via le lien internet mis dans le courrier électronique

Ce lien internet est en fait un faux site internet ressemblant de très près à celui de l'original, sauf que toute information que vous donnerez (nom d'utilisateur, mot de passe, numéro de carte bancaire...) sera récupérée par le pirate

Il y a des tentatives d'hameçonnage sur les comptes d'abonnement internet, les comptes Paypal et eBay, les comptes bancaires, les impôts, les réseaux sociaux (FaceBook, Twitter)...

Pour résumer : les courriers électroniques envoyés semblent d'être émis par une société digne de confiance et sont conçus de manière à vous inquiéter et de vous pousser à faire une action spécifique qui est de cliquer sur le lien internet pour corriger le problème, ce lien est un clone du vrai site internet que vous avez l'habitude de voir, arriver à cette page trompeuse, vous êtes invités à saisir des informations confidentielles (nom d'utilisateur, mot de passe, carte de crédit...) qui seront enregistrés par le criminel

3 / Un exemple ?

Les images parlent mieux que les textes, donc voyons un exemple d'hameçonnage, sur un compte d'abonnement internet Free

Imaginez que vous êtes abonné chez Free, un jour vous recevez un courrier électronique de Free qui dit ceci :

De : Service Client Free
Sujet : Double prélèvement
Pour : -----@free.fr
Monsieur, madame
<p>Nous sommes désolés de vous informer qu'une défaillance dans notre système est survenue lors des prélèvements mensuels effectués sur le compte de notre clientèle, en effet le 23 juillet 2010 votre compte a été indument débité d'un double prélèvement .</p> <p>Cette faute est essentiellement due à la similitude de vos noms et prénoms avec ceux d'un autre client, en vue du remboursement de cette somme prélevée, et dans les plus brefs délais, nous vous prions de vous connecter sur le lien qui apparaît en dessous de ce message .</p> <p style="text-align: center;"><i>Cliquez ICI</i></p> <p>A partir de la, il ne vous reste plus qu'à compléter les informations de votre formulaire spécial remboursement.</p>

Déjà c'est pas agréable d'apprendre qu'on paye deux fois son abonnement internet, avec le « Cliquez ICI » vous ouvrez une page internet qui ressemble à la page d'accueil de Free

Freebox Interface de gestion

S'abonner

- ▶ Freebox
- ▶ Free 50 heures
- ▶ Accès gratuit

Freebox

- WiFi - Routeur
- Téléphonie
- Télévision
- Plateforme multimédia

Espace Abonnés

- Identifiez-vous

Plus d'infos

- Nos offres
- Le dégroupage

Assistance

- Documentations
- Faq

VOTRE INTERFACE DE GESTION - IDENTIFICATION

Pour gérer les fonctionnalités liées :

- à votre compte "Freebox", vous pouvez vous identifier avec votre numéro de ligne, votre numéro de ligne Freebox ou votre identifiant Freebox.
- à votre compte Free 50 Heures, identifiez-vous avec votre numéro de ligne. Si vous disposez d'un compte "Free 50 Heures" et d'un compte "Freebox" au même numéro, entrez seulement votre numéro de ligne.
- à votre compte email, identifiez-vous avec l'identifiant de ce dernier.



IDENTIFICATION

Identifiant

Mot de passe

PUBLICITE

Freebox

S'abonner

- Freebox
- Free 50 heures
- Accès gratuit

Freebox

- WiFi - Routeur
- Téléphonie
- Télévision
- Plateforme multimédia

Espace Abonnés

- Identifiez-vous
- Plus d'infos
- Nos offres
- Le dégroupage
- Assistance
- Documentations
- Faq

VOTRE INTERFACE DE GESTION - VERIFICATION

Pour gérer les fonctionnalités liées :

- Afin d'activer l'accès et la sécurité de votre compte nous devons mettre à jour vos information.
- Il est fortement recommandé d'enter vos informations postale pour recevoir un suivi de vos factures mensuelles.

VERIFICATION D'IDENTITE

Nom :

Prénom :

Adresse :

Ville :

Code Postale :

Pays : **France**

Telephone :

Ensuite, à cette page ci dessus on vous demande de confirmer votre identité...

Ensuite, comme le montre l'image à droite on vous demande des informations bancaires, pour vous « rembourser » le double prélèvements

Bien entendu, jusqu'ici vous n'êtes pas sur le vrai site internet du fournisseur d'accès, c'est un faux site internet qui recueille toutes les informations bancaire et adresse d'internet...

Et ça existe aussi bien pour les abonnements internet (Free, Orange, SFR...) que les comptes bancaires, et des services liés à l'argent (Paypal, eBay, jeu en ligne comme le PMU ou la Française des Jeux)

INFORMATIONS BANCAIRES

Nom de la banque

Identifiant de la banque CIC/Crédit Mutuel

Saisissez les 11 chiffres de votre numéro de compte

Nom du Porteur de la carte bancaire

Date de naissance


--jour-- --Mois--

Type de carte

Visa

Numero de carte

Date d'expiration 02 2009

CVN 

(Il s'agit des 3 derniers chiffres du numéro inscrit au dos de votre carte).

4 / La parade ?

Comment éviter de se faire avoir ?

La méfiance avant tout, il y a le service téléphonique pour demander confirmation d'un « soucis » rencontré sur votre compte

Il y a aussi des navigateurs internet (Firefox, Internet Explorer) qui connaissent une « liste » de faux site internet et au cas ou vous allez sur un site internet d'hameçonnage car vous avez reçu un courrier électronique, vous avez ce genre de message qui s'affiche à la place de la page internet

Exemple sur Firefox



Ou sur la barre d'adresse du navigateur internet

Exemple sur Internet Explorer



Mais (car il y a un mais), ce genre de protection n'est pas toujours parfait, car la liste des « faux site » internet n'est pas toujours à jour, et si le faux site est très récent, il se peut qu'il ne soit pas répertorié

Donc méfiance...