

# Phishing, Slamming et Pharming

janvier 2006

## > Edito

Faux sites et détournement de données confidentielles sont malheureusement à la mode chez les pirates informatiques. En échangeant des données en réseau, vous les exposez à de graves dangers, et la sécurité en informatique, cheval de bataille du CRI74, devient alors primordiale.

Mais si ces dangers sont potentiellement graves, les solutions pour les minimiser sont souvent simples. Les connaître est la première étape indispensable.

Après les virus, les spams ou les spywares, ce CRI Pratique dénonce le phishing, le slamming et le pharming. Les deux premiers termes relèvent d'ingénierie sociale, le dernier est un acte de piratage direct.

## Ingénierie sociale : ne vous laissez pas abuser !

L'ingénierie sociale désigne l'acte d'abuser de la confiance, de la crédulité ou de l'ignorance d'une personne pour lui soutirer des informations. Le phishing et le slamming relèvent de cette catégorie. (*Attention : l'ingénierie sociale revêt diverses formes : courriers électronique et papier, téléphone, etc.*)

### > Le phishing

Le phishing, ou *hameçonnage*, consiste à se faire passer pour une autorité digne de confiance afin d'obtenir des informations confidentielles (comme les mots de passe, codes bancaires...).

*Dans le jargon des pirates informatiques la lettre f est souvent remplacée par les lettres ph. Le mot anglais fishing (pêcher) est donc devenu phishing.*

### Les méthodes les plus fréquentes pour leurrer l'utilisateur

#### - La fausse URL

Vous recevez un e-mail rédigé, semble-t-il, par votre banque, qui contient un lien vers votre compte, et qui vous invite à confirmer votre mot de passe ou votre code de carte bancaire. Le prétexte le plus souvent invoqué concerne la réactivation de votre compte suite à un problème technique.

En cliquant sur le lien, vous êtes en fait redirigé à votre insu vers un autre site web, à l'aspect identique à celui de votre banque (même logo, même présentation, etc.). Vous rentrez donc les informations demandées en toute confiance, informations qui sont récupérées et détournées par le pirate.

#### - Le Cross Site Scripting

La méthode diffère légèrement : le pirate vous contacte par le biais d'un e-mail, se faisant encore passer pour une autorité légitime et vous invitant à vous connecter à son site web. Ici, l'URL est particulière : elle est très longue, et utilise de nombreux signes tels que le %.

Exemple : `http://www.exemple-une-banque.com/index.php?%72%65%64%69%72%65%63%74%3D%68%74%74%`

Cette URL renvoie en fait à celle-ci :

`http://www.exemple-une-banque.com/index.php?redirect=http://www.site-pirate.com/`

Le pirate utilise ici une faille de sécurité présente sur le site web de l'organisme et, grâce à cette faille, vous redirige vers son faux site.

**Astuce :** le logiciel de messagerie Thunderbird a intégré un outil anti-phishing très pratique qui vous alerte en cas d'e-mail douteux et relevant de cette catégorie.

### Que faire ?

- Méfiez-vous systématiquement des **e-mails** qui vous demandent de vous connecter à un site pour confirmer votre commande ou votre code d'accès. En cas de doute, prenez contact avec l'institution sensée vous avoir envoyé le message, de préférence par téléphone.

- Soyez attentif à l'**adresse du site web** sur lequel vous êtes redirigé : dans le cas du phishing, le pirate est obligé de modifier légèrement l'adresse du faux site. Attention, ces modifications sont toujours très discrètes ! (*exemple : `www.credit-mutuei.fr` au lieu de `www.credit-mutuel.fr`*).

- Soyez attentif à l'**aspect du site web** sur lequel vous avez été redirigé : vous pensez être sur le site de votre banque, et pourtant il ne semble pas normal. Le procédé d'identification et/ou l'information fournie ne correspond pas à ce dont vous avez l'habitude, ou il vous est demandé plus d'informations que nécessaire : les faux sites demandent des informations ou des vérifications supplémentaires, ce qui est anormal.

### L'icône cadenas et le préfixe https

S'ils sont sensés attester de la fiabilité du site web, ils peuvent cependant être présents sur des faux sites. Quelques explications pour y voir plus clair :

- Normalement, l'**icône représentant un cadenas** apparaît en bas de la page lorsqu'un site web légitime demande des informations confidentielles. Il signifie que la session est cryptée en SSL (pour Secure Socket Layer).

- Le **préfixe https** est une variante du protocole de communication http utilisé pour Internet. Le **s** (signifiant secure) permet à l'internaute de vérifier l'identité du site auquel il accède grâce à un certificat d'authentification. Il est généralement utilisé pour les transactions financières en ligne : commerce électronique, banque en ligne, courtage en ligne, etc. Il est également utilisé pour chiffrer la communication, et donc protéger les échanges.

*Exemple : lorsque vous vous connectez au Webmail du CRI74 pour relever votre messagerie, le préfixe s signifie que vous pouvez entrer votre mot de passe et relever vos e-mails en relative confiance (attention cependant, car votre connexion a pu être interceptée !).*

### Le certificat d'authentification

Des autorités compétentes et reconnues sont chargées de signer les certificats utilisés dans les sites web en https. Mais cette certification est payante et non obligatoire.

Les sites web proposant des transactions financières en ligne le font cepen-

# Phishing, Slamming et Pharming

janvier 2006

dant, de manière systématique. Le CRI74 ne l'a pas encore fait.

Lorsque votre navigateur affiche la page d'accueil de WebMail, en https, il va vérifier automatiquement si le certificat est signé. S'il ne trouve pas la signature, il affichera cet avertissement ; *a contrario*, s'il la trouve, il n'affichera aucun avertissement. *Attention : les navigateurs ne connaissent pas toutes les autorités de certification !*

Dans le cas du WebMail du CRI74, l'existence ou non d'un certificat signé a une importance moindre (vous n'effectuez pas de transactions financières par son biais). Dans le cas d'une banque par exemple, le certificat signé existe obligatoirement.

### Que faut-il en déduire ?

Lorsque vous êtes dirigé vers le site web d'une banque, et que cet avertissement s'affiche, méfiez-vous ! En effet, le vrai site de votre banque a obligatoirement une signature certifiée, et un tel message ne doit jamais s'afficher (sauf si votre navigateur ne connaît pas l'autorité de certification...).

*Les attaques par phishing se sont répandues, mais les utilisateurs sont de mieux en mieux avertis. Les banques, premières victimes, ont largement contribué à la diffusion d'avertissements. Mais les pirates ne manquent pas d'imagination et ont mis en place d'autres méthodes pour tromper l'internaute : service de chat, messagerie instantanée ou différée, tous les moyens sont bons pour récupérer des informations cruciales.*

### > Le slamming

Le slamming, technique totalement différente, trouve sa place dans ce CRI Pratique car il relève également d'arnaques "ingénierie sociale". Ici, le but consiste à inciter les propriétaires de sites web à **leur confier la gestion de leurs noms de domaine**. Il s'agit parfois de prestataires mal intentionnés, qui alertent les titulaires d'un nom de domaine de la prochaine expiration de leurs droits, et se proposent de la renouveler à des tarifs bien supérieurs à ceux du marché.

En France, l'AFNIC a immédiatement réagi en contactant les prestataires qui se livraient à de telles pratiques, et les tentatives relevées de slamming sur les noms de domaine en .fr restent donc isolées : la mise en place d'une escroquerie à grande échelle est de toute façon plus difficile à mettre en place en France puisque la base de données de l'Afnic n'est pas publique. Mais elle reste possible.

### De l'abus de confiance au piratage

Parallèlement au phishing, de véritables techniques de piratage ont fait leur apparition : leurs objectifs restent les mêmes (détourner des données confidentielles) mais les méthodes diffèrent.

### > Le pharming

Cette forme d'attaque est toujours associée au piratage du serveur DNS de la banque ou du fournisseur d'accès Internet.

*Un serveur DNS permet de faire la concordance entre l'adresse IP d'un site Internet et son nom. C'est l'équivalent d'un annuaire.*

Là encore, les méthodes de pharming sont nombreuses, mais la plus fréquente concerne la **pollution de cache DNS** : le pirate va exploiter une faille du serveur DNS pour modifier la correspondance adresse IP / nom de domaine. Lorsque l'internaute tapera l'adresse du site Internet de sa banque, il sera renvoyé vers le site du pirate.

Attention : il est ici impossible de voir la différence entre le vrai et le faux site en étudiant attentivement l'URL ! En effet, absolument rien ne les distingue, et tout se fait de manière transparente pour l'internaute. Heureusement, la demande de validation du certificat pourra vous alerter.

### La documentation "+" du CRI74

> **Tout sur les virus** : CRI Pratique n°2

[http://www.thematic74.fr/rubrique.php3?id\\_rubrique=43](http://www.thematic74.fr/rubrique.php3?id_rubrique=43)

> **Tout sur les spams** : CRI Pratique n°4

[http://www.thematic74.fr/rubrique.php3?id\\_rubrique=45](http://www.thematic74.fr/rubrique.php3?id_rubrique=45)

> **Qu'est-ce qu'une URL ?** : CRI Pratique n°11 - article Terminologie

[http://www.thematic74.fr/article.php3?id\\_article=72](http://www.thematic74.fr/article.php3?id_article=72)

> **Tout sur les noms de domaine** : CRI Pratique n°11

[http://www.thematic74.fr/rubrique.php3?id\\_rubrique=52](http://www.thematic74.fr/rubrique.php3?id_rubrique=52)

> **Liens utiles** :

- <http://www.hsc.fr/ressources/presentations/rs05-phishing/index.html>
- <http://www.hsc.fr/ressources/presentations/csm05-phishing/index.html>
- <http://www.hsc.fr/ressources/presentations/jip05-xss/index.html>
- <http://www.lephare.be/forums/viewtopic.php?id=107>
- <http://www.hoaxbuster.com/hoaxliste/hoax.php?idArticle=22498>
- <http://www.antiphishing.fr/>
- <http://www.antiphishing.or>
- <http://www.zdnet.fr/actualites/internet/0,39020774,39166512,00.htm>

### > Conclusion

Les principaux organismes visés sont les services bancaires en ligne et les sites de vente aux enchères en ligne. En 2004, un rapport du cabinet Gartner a révélé que les pertes dues aux méfaits tels que le phishing étaient évaluées à 2,4 milliards de dollars pour les 12 mois précédents.

Il est relativement simple de se prémunir contre l'ingénierie sociale : vigilance et prudence sont les armes les plus efficaces.

Et, en cas de doute, n'hésitez pas à contacter le CRI74, notamment pour le slamming : si vous avez confié la gestion de votre nom de domaine au CRI74, nous sommes votre seul contact. Si un organisme prétend que vos droits arrivent à expiration, ne faites rien sans nous consulter avant.

Pour les actes de piratage de pharming, il est plus difficile de s'en prémunir, et même des informaticiens aguerris se sont laissés prendre.