

# Le phishing

## par Gilles Bouchard (Vidéo Déry Ltée)

Le phishing est une forme d'escroquerie sur Internet qui prend de plus en plus d'ampleur. Il est un sport à la mode chez les escrocs ayant internet pour terrain de jeux. Il s'agit d'aller à la pêche aux informations par mail qui vous invite à vous connecter en ligne par le biais d'un simple lien et de mettre à jour des informations vous concernant dans un formulaire d'une page web factice, copie conforme du site original. Le mail vous invite par exemple à une mise à jour d'un service, une intervention du support technique, ou encore une vérification de sécurité. Ainsi, les pirates réussissent à obtenir vos identifiants et mots de passe ou bien vos données personnelles ou bancaires qu'ils pourront réutiliser à leur propre fin.

### Détecter les URL "cachées"

Les pirates tentent toujours de "masquer" les URL des sites sur lesquels la victime de phishing est redirigée. Voici quelques méthodes :

#### ---- Ecriture hexadécimale de l'URL

Afin de rendre l'URL plus difficilement lisible, les caractères de l'adresse IP sont exprimés en caractères hexadécimaux

*http://%32%30%39%2E%39%38%2E%38%36%2E%32%33%36%38%37%63%69%74%69%6E%64%65%78%2E%68%74%6D*. Après conversion, cette URL devient *http://209.98.86.236:87/cit*, ce qui est bien plus lisible. Une fois l'IP découverte, vous pouvez alors effectuer un reverse DNS. Le but de cette manoeuvre est de trouver à quel nom de domaine est associé l'adresse.

#### ---- Utilisation de login automatique

Il est possible d'intégrer le login et le mot de passe dans une URL pour accéder à une page protégée. Dans ce cas, tout ce qui se trouve entre *http://* et *@* dans l'URL sera alors ignoré. Cela permet ainsi de créer des URL fantaisistes très simplement.

### Important de faire une vérification de l'existence d'un protocole sécurisé

Il est important de vérifier que la page du site vous demandant des informations personnelles est sécurisée. Dans ce cas, l'URL doit commencer par *https://* (pour HyperText Transfer Protocol Secure). Votre navigateur vous informe et affiche un petit cadenas fermé en bas à droite.

### Conseils

- Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet très rare qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone.
- Lorsque vous saisissez des informations sensibles sur Internet, assurez-vous que votre navigateur est en mode sécurisé. Un petit cadenas est affiché dans la barre d'état du navigateur.
- De nombreuses failles de sécurité sont régulièrement corrigées, alors pensez à mettre à jour votre système régulièrement.
- Ne jamais se fier à l'adresse email de l'expéditeur, celle-ci pouvant être très facilement piratée.
- Se méfier des propositions trop alléchantes.
- En cas de doute, ne pas cliquer sur le lien contenu dans l'email suspect.

- Toujours se poser ces deux questions "*Est-ce normal que cet organisme connaissance mon email ?*" et "*Est-ce normal que cet organisme me contacte par email pour cette raison ?*".

## Les outils pour lutter contre le phishing

On distingue deux types d'outils destinés à contrer le phishing.

- La première est basée sur des *blacklists*. Lorsque l'internaute navigue sur un site, le programme consulte alors sa base de données en ligne afin de savoir si le site en question est recensé comme frauduleux.
- La seconde analyse la page puis évalue une « *note* » en fonction de divers critères. Ainsi, plus la « *note* » sera haut, plus le risque que présente le site sera élevé.

Voici quelques-uns de ces outils :

### Barre Netcraft :

La barre anti-phishing de Netcraft regroupe pour sa part ces deux méthodes au sein d'un même outil. Il s'agit sans doute de la solution la plus utilisée mais également la plus efficace pour lutter contre le phishing. Existant pour Internet Explorer et Firefox, cette barre d'outil anti-arnaque vient se greffer au navigateur afin d'offrir différentes informations sur le site consulté. Cette barre reste connectée à la base de données de l'éditeur où est recensé l'ensemble de sites frauduleux connus et permet ainsi d'avertir l'utilisateur si celui-ci se connecte sur l'un d'entre eux.

### ScamWatch :

Cet outil anti-phishing se voit intégré dans le client mail Eudora depuis sa version 6.2. La détection des potentiels sites frauduleux se fait alors en amont, avant même que l'utilisateur n'arrive sur le site incriminé. Dès la réception, l'outil analyse les liens présents dans l'email en vérifiant notamment si les liens utilisent une adresse IP en lieu et place d'un nom de domaine (pratique courante dans les attaques par phishing). La différence entre l'URL affiché et l'URL réelle du lien est également analysée. En cas de problème, l'utilisateur est alors averti de l'existence du lien potentiellement dangereux.

Ainsi, le futur Internet Explorer 7 ou la prochaine version de Netscape intégreront un outil anti-phishing par défaut.