
# Internet

*Le hameçonnage, nouvelle menace sur le Web*

## Usurpation d'identité

*Contraction de password et fishing, soit «pêche aux mots de passe, le phishing est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique 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 ou autres.*

*Thomas Vauthier*
*th.vauthier@bluewin.ch*

La technique du phishing est une technique d'«ingénierie sociale» c'est-à-dire consistant à exploiter non pas une faille informatique mais la «faille humaine» en dupant les internautes par le biais d'un courrier électronique semblant provenir d'une entreprise de confiance, typiquement des services bancaires en ligne, et les sites de ventes aux enchères tels que eBay.
Le mail envoyé par ces pirates usurpe l'identité d'une entreprise (banque, site de commerce électronique, etc.) et invite l'internaute à se connecter en ligne par le biais d'un lien hypertexte et de mettre à jour des informations les concernant dans un formulaire d'une page Web factice, copie conforme du site original, en prétextant par exemple une mise à jour du service, une intervention du support technique, etc.

### Les leurres

Typiquement, les messages envoyés semblent émaner d'une société digne de confiance et sont formulés de manière à ne pas alarmer le destinataire afin qu'il effectue une action en conséquence. Une approche souvent utilisée est d'indiquer à la victime que son compte a été désactivé à cause d'un problème et que la réactivation ne sera possible qu'en cas d'action de sa part. Le message fournit alors un hyperlien qui dirige l'utilisateur vers une page Web qui ressemble à s'y méprendre au vrai site de la société. Arrivé sur cette page trompeuse, l'utilisateur est invité à saisir des informations confidentielles qui sont alors enregistrées par le criminel.

Les fraudes concernant les banques en ligne visent à obtenir l'identifiant et le mot de passe du titulaire d'un compte. Il est alors possible au fraudeur de se connecter sur le site Web de la banque et d'effectuer des virements de fonds vers son propre compte. Pour parer à ce type de fraude, la plupart des sites bancaires en ligne n'autorisent plus l'internaute à saisir lui-même le compte destinataire du virement.
Grâce à ces données les pirates sont capables de transférer directement l'argent sur un autre compte ou bien d'obtenir ultérieurement les données nécessaires en utilisant intelligemment les données personnelles ainsi collectées.

### Parades

La vérification de l'adresse Web dans la barre d'adresse du navigateur Web peut ne pas être suffisante pour détecter la supercherie, car certains navigateurs n'empêchent pas l'adresse affichée à cet endroit d'être contrefaite. Il est toutefois possible d'utiliser la boîte de dialogue «propriétés de la page» fournie par le navigateur pour découvrir la véritable adresse de la fausse page.

Exemple:

```
<p>
Follow the link to make sure you
are on a secure eBay webpage.<br>
<A
HREF="http://phish.co.kr/signin/">
https://signin.ebay.com/ws/eBayISA
PI.dll?SignIn</A>
<p>
Thank you for using eBay!<br>
```

Derrière le lien https://signin.ebay.com/... se cache en vérité l'URL de l'escroc http://phish.co.kr/...!
Une personne contactée au sujet d'un compte devant être «vérifié» doit chercher à contacter directement la société concernée ou se rendre sur le site Web en tapant manuellement l'adresse dans son navigateur. Il faut savoir que les banques n'utilisent jamais le courriel pour corriger un problème de sécurité avec l'un de leurs clients.
Les navigateurs récents possèdent un système permettant d'avertir l'utilisateur du danger et de lui demander s'il veut vraiment naviguer sur de telles adresses douteuses. Les filtres antipourriels aident aussi à protéger l'utilisateur des criminels informatiques en réduisant le nombre de courriels que les utilisateurs reçoivent et qui peuvent être de l'hameçonnage.

### Comment se protéger du phishing?

Lorsque vous recevez un message provenant a priori d'un établissement bancaire ou d'un site de commerce électronique il est nécessaire de vous poser les questions suivantes:
– Ai-je communiqué à cet établissement mon adresse de messagerie?
– Le courrier reçu possède-t-il des éléments personnalisés permettant d'identifier sa véracité (numéro de client, nom de l'agence, etc.)?

Par ailleurs il est conseillé de suivre les conseils suivants:
– Ne cliquez pas directement sur le lien contenu dans le mail, mais ouvrez votre navigateur et saisissez vous-même l'URL d'accès au service.
– Méfiez-vous des formulaires demandant des informations bancaires. Il est en effet rare (voire impossible) qu'une banque vous demande des renseignements aussi importants par un simple courrier électronique. Dans le doute contactez directement votre agence par téléphone!
– Assurez-vous, lorsque vous saisissez des informations sensibles, que le navigateur est en mode sécurisé, c'est-à-dire que l'adresse dans la barre du navigateur commence par https et qu'un petit cadenas est affiché dans la barre d'état au bas de votre navigateur, et que le domaine du site dans l'adresse correspond bien à celui annoncé (gare à l'orthographe du domaine)!

Infos supplémentaires: www.antiphishing.org/

*A suivre …*