

27. Phishing, le nouveau fléau sur Internet.

De nos jours les internautes s'exposent à un nombre infini de dangers, parmi lesquels on compte le phishing.

C'est quoi le "phishing"?

Le phishing, appelé encore "*hameçonnage par courrier électronique*" désigne une forme d'escroquerie en ligne qui a pour but d'obtenir par Internet et par des moyens détournés, en trompant la vigilance des utilisateurs, des informations personnelles et confidentielles telles que des informations relatives aux comptes bancaires et aux codes de cartes bancaires.

http://www.cases.public.lu/publications/dossiers/phishing/phishing_2/

Comment cela fonctionne-t-il ?

Les internautes sont avertis par courrier électronique falsifié que leur compte bancaire et/ou leur compte chez **eBay** (voir figure ci-dessous) ne fonctionne plus correctement dû à une panne du système informatique. Un autre truc consiste à faire croire que les coordonnées de facturation sur eBay sont périmées et qu'on doit saisir à nouveau les données endéans les 24 heures, autrement le compte sera éliminé (comme montré dans la figure ci-dessous)! Le courrier électronique contient toujours un lien sur lequel on demande de cliquer pour arriver au site d'administration qui, à première vue, est tout à fait semblable au site web original et qui en plus fait croire qu'il s'agit d'une connexion sécurisée en indiquant le début du lien avec **https://**.

Von: [Crystal Harden](#)
Datum: 12/13/05 01:32:38
An: leone@pt.lu
Betreff: [Norton AntiSpam] eBay Account Notice - Suspicious Activity

Dear eBay @ User,

Dear valued eBay member, It has come to our attention that your eBay Billing Information records are out of date. That requires you to update the Billing Information.

However, failure to do so will result in account termination. Please update your records in maximum 24 hours. Once you have updated your account records, your eBay session will not be interrupted and will continue as normal.

Please click the secure link below to update your billing records.

<https://ebay.com/awc/gi/eBayISAPI.dll/%ebay.verify/support>

Thank you,
 eBay Accounts Management

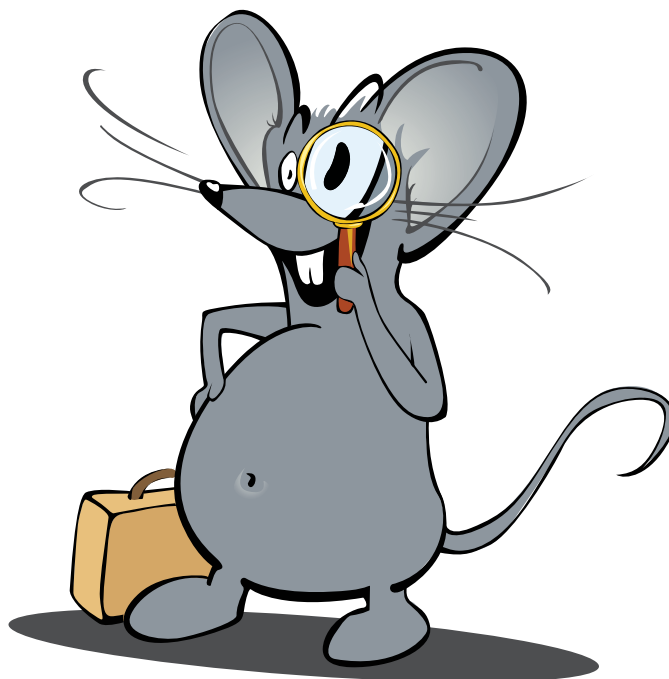
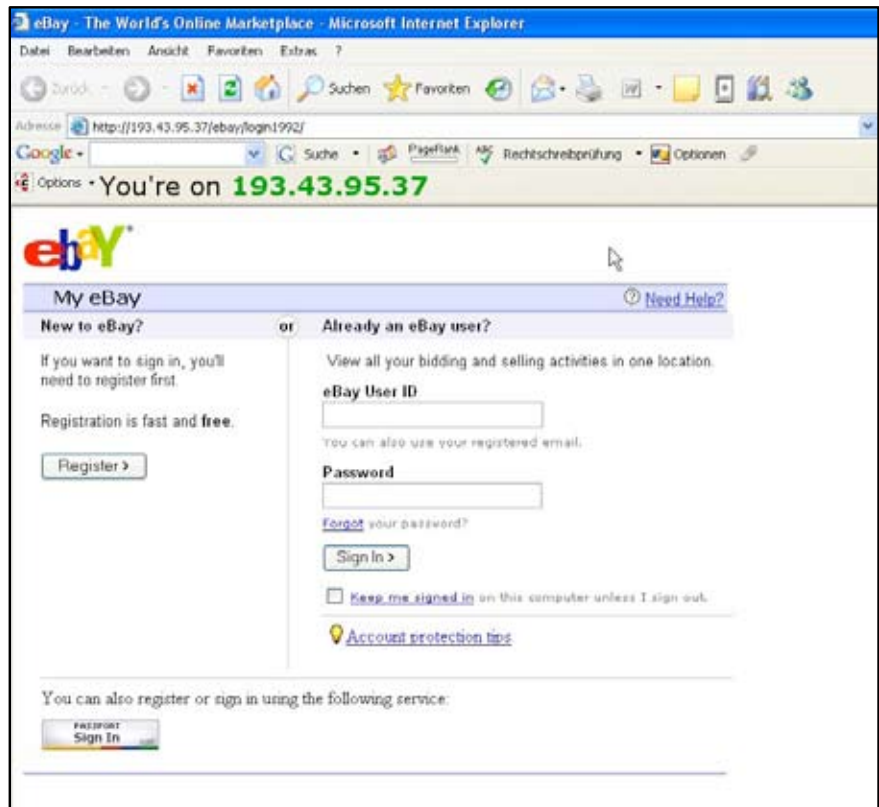
 Thank you for using eBay!

 Do not reply to this email.

Copyright © 1995-2004 eBay Inc. All Rights Reserved.



Ce que vous ne voyez pas (si vous n'avez pas installé de **barre antiphishing**) c'est que (l'adresse IP) **l'URL est différente!** Si maintenant on saisit les données dans les champs de texte (**User ID et Password**), le criminel informatique les intercepte et réagit instantanément. Dans le cas de eBay il aura les coordonnées d'accès et il pourra faire autant d'achats que possible qui seront facturés aux utilisateurs ainsi attaqués! Le site truqué n'est en principe opérationnel que pendant 24 heures et hébergé la plupart du temps sur des serveurs en Russie et Ukraine (dans notre exemple c'est l'Ukraine), ce qui rend très difficile et/ou presque impossible de le retracer et de prouver son existence.



Comment se protéger contre le phishing?

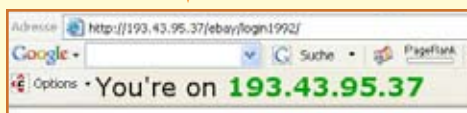
D'abord une bonne portion de vigilance (méfiance) est de rigueur; c.-à-d.: aucun établissement, qu'il soit bancaire et/ou gouvernemental, ni commercial n'enverra par courrier électronique une telle demande pour renouveler des données confidentielles! Ces actions, pour garder la confidentialité et la protection de la vie privée, se font d'office par courrier normal!

Néanmoins il existe des utilitaires, même gratuits (freeware/gratuciels), qui s'intègrent dans le navigateur (browser) et qui nous indiquent l'adresse URL et/ou l'adresse IP du site web visité; dans notre exemple il s'agit de Spoofstick qui peut être téléchargé à l'adresse suivante: <http://www.spoofstick.com>. On appelle cet utilitaire antiphishing tool bar. Ce "BHO" (Browser Helper Objects), en français "utilitaire d'aide pour le navigateur", s'intègre automatiquement comme nouvelle barre d'outils dans le navigateur et vous indique l'adresse URL exacte du site web.



Dans notre capture d'écran ci-dessus vous pouvez vous rendre compte que l'adresse URL marquée dans le champ d'adresse ne correspond pas du tout avec l'adresse qui a été affichée dans le courriel.

Please click the secure link below to update your billing records.
<https://ebay.com/awcgi/eBayISAPI.dll?%ebay.verify/support>



Veuillez noter que la nouvelle version d'Internet Explorer, IE7, a intégré une barre antiphishing.

Si cela vous arrive, comme dans notre exemple, vous devez devenir méfiant (vigilant) et fermer tout de suite votre navigateur! Si jamais on vous adressait un courrier pareil, ne jamais l'ouvrir et l'effacer de suite, et vider aussi la corbeille!

Le plus intelligent est encore d'utiliser le "webmail" pour vérifier votre courrier électronique, car vous travaillerez sur le serveur de votre F.A.I. (I.S.P.) et pas sur votre ordinateur. Sur le serveur de votre compte web mail vous pouvez tout de suite sélectionner les courriers non sollicités et non désirés et les effacer de suite sans qu'ils ne viennent à votre ordinateur.

C'est quoi le webmail?

En quelques mots, le webmail n'est rien d'autre qu'un compte chez votre F.A.I. (I.S.P.) que vous utilisez de toute façon, car votre courrier électronique est envoyé de ce compte vers votre ordinateur. Lors de votre demande auprès de votre F.A.I. pour recevoir une adresse électronique, celui-ci vous a fourni votre adresse et votre mot de passe, que vous avez probablement choisis vous-même et qui sont nécessaires pour consulter votre courrier.

Le webmail n'est rien d'autre qu'une boîte postale virtuelle.

Dans le monde réel, c'est les P&T qui sont notre fournisseur de lettres et dans le monde virtuel c'est notre F.A.I.

Pour visiter les P&T (monde réel) nous devons connaître leur adresse (ville, rue et numéro) et pour exécuter le webmail (monde virtuel) nous devons savoir l'adresse URL (ex.: <http://www.pt.lu>) et aussi l'emplacement des guichets et locaux (le lien du web mail) <http://webmail.pt.lu>. Quand nous avons une boîte postale auprès des P&T nous recevons le numéro de la boîte postale et une clé pour l'ouvrir.

Dans le monde virtuel (webmail) notre numéro de boîte postale est notre adresse électronique et la clé pour l'ouvrir est notre mot de passe. Avec ces deux données nous pouvons accéder à notre boîte postale électronique de n'importe où au monde!



www.cte.lu

www.myschool.lu

www.mysecureit.lu

www.etwinning.lu



MINISTÈRE DE L'ÉDUCATION NATIONALE
ET DE LA FORMATION PROFESSIONNELLE
Centre de technologie de l'éducation



Copyright © 2005, www.mySchool.lu

Tous droits réservés. Ce document est la propriété de mySchool! (CTE) et peut être reproduit pourvu qu'aucune modification ne soit effectuée et que cette notice soit préservée. Les informations véhiculées par la présente fiche le sont dans l'espoir qu'elles seront utiles. La responsabilité des auteurs ne pourra être engagée à aucun moment.