Phishing, le nouveau fléau sur internet.

Internet → Sécurité

De nos jours les internautes s'exposent à un nombre infini de dangers, tel que 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 à travers 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
- aux codes de cartes bancaires

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

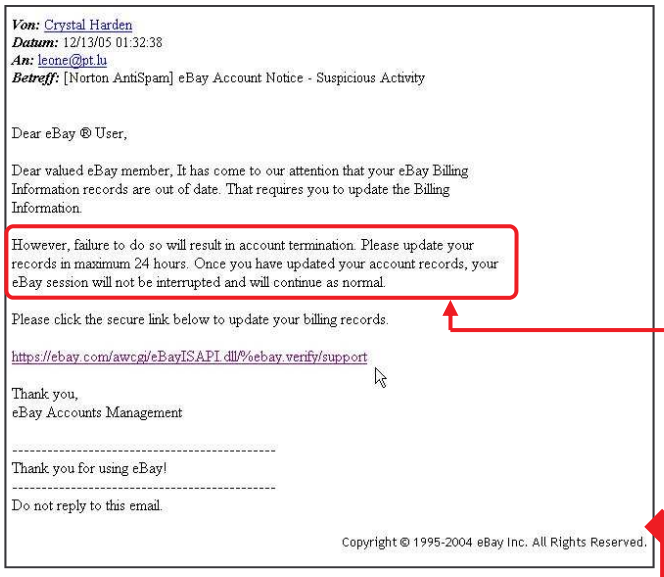
www.spoofstick.com

http://toolbar.netcraft.com/

www.internetmonitor.lu

www.cases.lu

www.mysecureit.lu



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Dear valued eBay member, It has come to our attention that your eBay Billing Information records are out of date.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

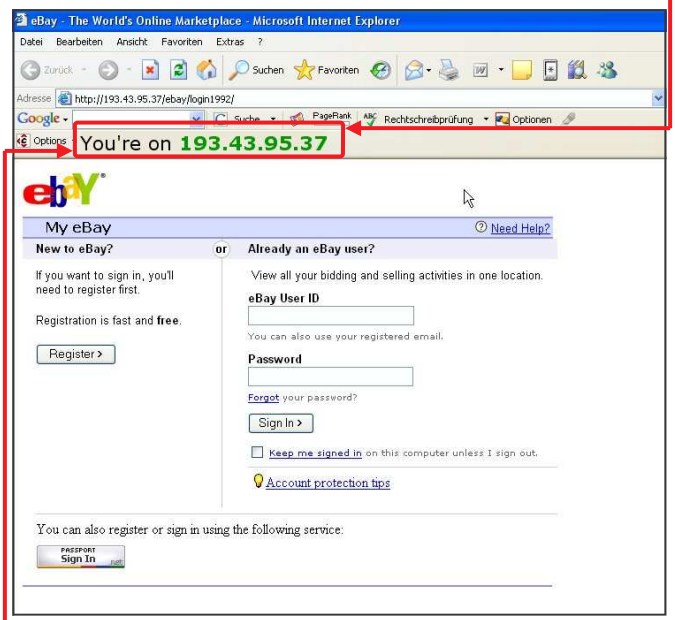
https://ebay.com/awcgi/eBayISAPI.dll/%ebay.verify/support

Thank you,
eBay Accounts Management

Thank you for using eBay!

Do not reply to this email.

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



Comment est-ce que cela fonctionnel ?

Les internautes sont avertis par courrier électronique falsifié que leur compte bancaire et/ou leur compte chez **eBay** (voir figure ci-contre) ne fonctionne plus correctement dû à une panne du système informatique. Un autre truc consiste à vous faire croire que vos coordonnées de facturation sur **eBay** sont périmées et que vous devez saisir à nouveau vos données endéans les 24 heures, autrement votre compte sera supprimé (comme montré dans la figure ci-contre)! Le courrier électronique contient toujours un lien sur lequel on vous demande de cliquer pour arriver au site d'administration qui à première vue est tout à fait semblable au site web original. 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 vous saisissez vos 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 vos coordonnées d'accès et il pourra faire autant d'achats que possible qui vous seront facturés; **bonjour les dégâts!** 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 nous protéger contre le phishing ?

D'abord une bonne portion de **vigilance** (méfiance) est de rigueur. **Aucun établissement, qu'il soit bancaire et/ou gouvernemental, ni commercial ne vous enverra par courrier électronique une telle demande pour renouveler vos données confidentielles!** Ces actions, pour garder la confidentialité et la protection de votre vie privée, **se font d'office par courrier normal!**

Néanmoins il existe des utilitaires, même gratuits (freeware/gratuiciels), qui s'intègrent dans notre 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.** Une fois téléchargé le logiciel il suffit de l'installer et il s'intègre automatiquement comme nouvelle barre d'outils dans le navigateur.

Gust MEES / Formateur pédagogique TIC http://www.internetmonitor.lu **Partenaire officiel de CASES** http://www.cases.lu

SÉCURITÉ

VEUILLEZ DÉCOUPER ICI