

1. Le message, son aspect général :



We regret to inform you that your eBay account could be suspended if you don't re-update your account information. To resolve this problems please [click here](#) and re-enter your account information. If your problems could not be resolved your account will be suspended for a period of 24 hours, after this period your account will be terminated.

For the User Agreement, Section 9, we may immediately issue a warning, temporarily suspend, indefinitely suspend or terminate your membership and refuse to provide our services to you if we believe that your actions may cause financial loss or legal liability for you, our users or us. We may also take these actions if we are unable to verify or authenticate any information you provide to us.

Due to the suspension of this account, please be advised you are prohibited from using eBay in any way. This includes the registering of a new account. Please note that this suspension does not relieve you of your agreed-upon obligation to pay any fees you may owe to eBay.

Regards,
Safeharbor Department eBay, Inc
The eBay team. This is an automatic message.
Please do not reply.

[Announcements](#) | [Register](#) | [Shop eBay-o-rama](#) | [Security Center](#) | [Policies](#) | [PayPal](#)
[Feedback Forum](#) | [About eBay](#) | [Jobs](#) | [Affiliates Program](#) | [Developers](#) | [eBay Downloads](#) | [eBay Gift Certificates](#)
[My eBay](#) | [Site Map](#)
[Browse](#) | [Sell](#) | [Services](#) | [Search](#) | [Help](#) | [Community](#)

Copyright © 1995-2005 eBay Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this Web site constitutes acceptance of the eBay [User Agreement](#) and [Privacy Policy](#).



2. La technique utilisée :

Ce cas de phishing est basé sur un lien « [click here](#) » très reconnaissable dans une réalisation assez graphique. Le dossier complet est accessible via l'URL :

http://www.antiphishing.org/phishing_archive/03-07-05_Ebay/03-07-05_Ebay.html

L'objectif est de tenter d'obtenir les informations de comptes bancaires des cibles.

L'adresse (temporaire) du site du « phisher » est : 218.154.123.224

3. Un cas de phishing visible :

Le travail graphique est suffisant pour abuser un grand nombre de cibles distraites. On est assez loin des techniques de « MANGLED » utilisées par les spammeurs qui écrivent V*I *A*G*R*A pour traverser les systèmes AntiSpam de première génération :

- mais, l'URL cachée derrière le « [click here](#) » n'est clairement pas un domaine ebay !!!
- <http://218.154.123.224/signin.ebay.com/ws/eBayISAPI.dll?SignIn&favoritenav> (le début seulement)

eBay - New & used electronics, cars, apparel, collectibles, sporting goods & more at low prices - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Print Mail

Address http://218.154.123.224/signin.ebay.com/ws/eBayISAPI.dll?SignIn&favoritenav=&sid=&ruproduct=&pp=&co_partnerId=28ru=&i1=&ruparas=&page

home | pay | register | sign in | services | site map

Buy Sell My eBay Community Help

Notice the URL

4. Suivi des liens proposés

La page de « login » est typique car il est curieux de demander des informations bancaires confidentielles ceci avant toute authentification :

home | pay | register | sign in | services | site map Start new search

Buy Sell My eBay Community Help

The World's Online Marketplace®

Buying new items, brand names, and collectibles on eBay is simple. Here's how it works...

1- Update eBay login information

E-mail

eBay User ID

eBay Password

Paypal Password

2- Verify personal information

Please have the following ready as you'll need both to buy or sell on eBay.com:

3- Provide Credit/Debit Card identification

Credit card/Debit card number Credit Card: MasterCard, Visa, American Express, Discover. Debit Card: MasterCard, Visa

Expiration date Month: -- Year: --

Card type --Card Type--

Credit/Debit card PIN Bank Verification needs this information. Make sure you type correct pin.

CW2 3 digits for Visa, MasterCard, Discover | 4 digits for American Express

VISA MasterCard AMERICAN EXPRESS DISCOVER

5. Action d'une passerelle sécurité

Nous avons reçu cet email par deux voies :

- une fois, en pièce jointe, via le réseau « reportphishing@antiphishing.fr »,
- et, en direct à travers notre passerelle sécurisée.

Ce qui permet de tester le cas de phishing mais aussi le fonctionnement de la passerelle :

Madame, Monsieur,

Nous venons d'arrêter le message de aw-confirm@ebay.com qui vous était destiné, car l'anti-virus installé sur nos serveurs de messagerie a détecté la présence d'un virus (**Trojan-Spy.HTML.Bayfraud.eg**).

Votre ordinateur n'a donc pas été contaminé par le virus contenu dans ce message.

NOTA : certains virus utilisent de fausses identités pour se propager, aw-confirm@ebay.com n'est donc pas nécessairement l'expéditeur du message que nous avons stoppé.

Sincères salutations,

La passerelle sécurité de la société Associated Winners.

Dear Sir, Madame,

We have just stopped a message which was intended to you (sender : aw-confirm@ebay.com) because our antivirus installed on our mail servers detected the presence of a virus : Trojan-Spy.HTML.Bayfraud.eg .

So your computer is not contaminated by the virus contained in the message.

ATTENTION : viruses are able to propagate themselves via spoofed identities, aw-confirm@ebay.com may not necessarily be the person whose computer was infected !

...

6. Les actions engagées :

- La publication de ce document,
- Ce cas étant une variante d'un phishing bien documenté, il est inutile de le centraliser au niveau .org