

1. Le message, son aspect général :

De nombreuses versions de phishing visant eBay ont été reportées :



*****Urgent Safeharbor Department Notice*****

eBay Fraud Mediation Request

Date: Tue, 7 Jun 2005

You have received this email because you or someone had used your account to make fake bids at eBay. For security purposes, we are required to open an investigation into this matter.

THE FRAUD ALERT ID CODE CONTAINED IN THIS MESSAGE WILL BE ATTACHED IN OUR FRAUD MEDIATION REQUEST FORM, IN ORDER TO VERIFY YOUR EBAY ACCOUNT REGISTRATION INFORMATION.

Fraud Alert ID CODE: 00937614

(Please save this Fraud Alert ID Code for your reference.)

To help speed up this process, please access the following form to complete the verification of your eBay account registration information:

http://scgi.ebay.com/verify_id=-ebay &fraud alert id code=00937614

Please Note:

If we do not receive the appropriate eBay account verification within 48 hours, then we will assume this eBay account is fraudulent and will be suspended. The purpose of this verification is to ensure that your eBay account has not been fraudulently used and to combat the fraud from our community.

We appreciate your support and understanding, as we work together to keep eBay a safe place to trade.

Thank you for your patience in this matter.

Regards, Safeharbor Department (Trust and Safety Department)

eBay Inc.

2. La technique utilisée :

Ce cas de phishing est basé un lien à cliquer.

On peut lire dans le code associé :

```
<p><strong><font size="2" face="Arial, Helvetica, sans-serif">
```

```
<a href="http://61.30.150.11/ebay/">
```

```
http://scgi.ebay.com/verify_id=-ebay &fraud alert id code=00937614
```

```
</a></font></strong></p>
```

Le site ouvert par le lien est : <http://61.30.150.11/ebay/>

L'utilitaire « nslookup » permet de repérer l'émetteur :

```
C:\Documents and Settings\Administrator>nslookup
Default Server: name.nordnet.fr
Address: 194.206.126.253

> 61-30-150-11.static.tfn.net.tw
Server: name.nordnet.fr
Address: 194.206.126.253

Non-authoritative answer:
Name: 61-30-150-11.static.tfn.net.tw
Address: 61.30.150.11

>
```

L'analyse de l'IP utilisée avec Whois aboutit à un site hébergé à Taiwan :

```
inetnum: 61.30.0.0 - 61.30.255.255
netname: TFN-NET
descr: Taiwan Fixed Network CO.,LTD.
descr: 7Fl., No. 498, Ruei-Guang Rd., Nei-Hu
descr: Taipei Taiwan 114.
country: TW
admin-c: TT164-AP
tech-c: SH376-AP
mnt-by: MAINT-TW-TWNIC
changed: cwkuo@twmic.net.tw 20020425
status: ALLOCATED PORTABLE
source: APNIC

inetnum: 61.30.150.8 - 61.30.150.15
netname: CHH-NET
descr: TFN
descr: 7Fl., No. 498, Ruei-Guang Rd., Nei-Hu
descr: Taipei Taiwan
country: TW
admin-c: CWT20-TW
tech-c: CWT20-TW
mnt-by: MAINT-TW-TWNIC
remarks: This information has been partially mirrored by APNIC from
remarks: TWNIC. To obtain more specific information, please use the
remarks: TWNIC whois server at whois.twmic.net.
changed: ting_tseng@twfn.com.tw 20030404
status: ASSIGNED NON-PORTABLE
source: TWNIC
```

3. Un cas de phishing « graphique » mais très reconnaissable :

Les observations habituelles permettent de reconnaître la fraude :

- URL ne correspondant pas à la source,
- Demande des identifiants de la carte à débiter dès la première page,
- Absence de clé SSL (icône zone sécurisée) pour un site HTTPS affiché.

eBay.com: Account: Verify Information - Microsoft Internet Explorer

Address <http://61.30.150.11/ebay/>

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

Browse Search Sell My eBay Community Powered By IBM

Enter Your Ebay Information

E-mail

Ebay User ID

Ebay Password

Ebay Account: Verify Information

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

- Credit or debit card If you don't have these available,
- Checkbook (checking account) please use [ID Verify](#) instead (\$5 fee).

First, verify that your information below is correct.

First name Last name

Street

City

State Zip code Country

Primary telephone () - ext.:

Ebay Account: Provide Credit Card Identification

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

MasterCard VISA AMERICAN EXPRESS DISCOVER

4. Actions engagées :

- La publication de ce document,
- Ce cas a été reporté au niveau « .org »