









1. Le message, son aspect général :

✉ :-((****eBay Summary Confirmation**** - Message (HTML)

Fichier Edition Affichage Insertion Format Outils Actions ?

 Répondre
  Répondre à tous
  Transférer
 





De : My eBay [aw-confirm@ebay.com]
 À : Packing@aol.com
 Cc :
 Objet : ****eBay Summary Confirmation****

Welcome to eBay!

Shopping on eBay is easy and fun.

[Go to eBay](#)

[http://64.202.162.1/ws/eBayISAPI.dll?SignIn&pUserId=&co_partnerId=2
&siteid=0&pageType=-1&pa1=&i1=-1&UsingSSL=1&bshowgif=0
&favoritenav=&errmsg=8](http://64.202.162.1/ws/eBayISAPI.dll?SignIn&pUserId=&co_partnerId=2&siteid=0&pageType=-1&pa1=&i1=-1&UsingSSL=1&bshowgif=0&favoritenav=&errmsg=8)

???

Dear eBay valued member,

Due to concerns, for the safety and integrity of the eBay account we have issued this warning message.

It has come to our attention that your account information needs to be updated due to inactive members, frauds and spoof reports. If you could please take **5-10 minutes** out of your online experience and renew your records you will not run into any future problems with the online service. However, failure to update your records will result in account suspension. This notification expires on **06/06/2005**.

Once you have updated your account records your eBay account service will not be interrupted and will continue as normal.

Please follow the link below and login to your account and renew your account information

Sincerely, eBay customer department!

[Go to eBay](#)

2. La technique utilisée :

Ce cas de phishing est basé sur une image « ->Go to eBay » associée à :

http://64.202.162.1/ws/eBayISAPI.dll?SignIn&pUserId=&co_partnerId=2&siteid=0&pageType=-1&pa1=&i1=-1&UsingSSL=1&bshowgif=0&favoritenav=&errmsg=8

L'analyse de l'IP utilisée avec Whois aboutit à :

```
OrgName: Go Daddy Software, Inc.
OrgID: GDS-31
Address: 14455 N Hayden Road
Address: Suite 226
City: Scottsdale
StateProv: AZ
PostalCode: 85260
Country: US

NetRange: 64.202.160.0 - 64.202.191.255
CIDR: 64.202.160.0/19
NetName: GO-DADDY-SOFTWARE-INC
NetHandle: NET-64-202-160-0-1
Parent: NET-64-0-0-0-0
NetType: Direct Allocation
NameServer: CNS1.SECURESERVER.NET
NameServer: CNS2.SECURESERVER.NET
```

Le header du message est aussi intéressant pour identifier le serveur de messagerie:

```
Return-Path: <aw-confirm@ebay.com>
...
Received: from [212.118.16.139] (helo=comp)
    by server2.thehostinghut.com with esmtpa (Exim 4.50)
    id 1Dd5wf-0001Xw-5J; Tue, 31 May 2005 07:34:09 -0500
From: "My eBay" <aw-confirm@ebay.com>
Subject: **eBay Summary Confirmation**
To: Packing@aol.com
Content-Type: text/html;iso-8859-1
Reply-To: aw-confirm@ebay.com
Date: Tue, 31 May 2005 15:34:12 +0300
X-Priority: 3
X-Library: Indy 8.0.25
X-AntiAbuse: This header was added to track abuse, please include it with any abuse report
X-AntiAbuse: Primary Hostname - server2.thehostinghut.com
X-AntiAbuse: Original Domain - associatedwinners.com
X-AntiAbuse: Originator/Caller UID/GID - [47 12] / [47 12]
```

L'adresse 212.118.16.139 est associée à un serveur en Jordanie :

```
inetnum: 212.118.16.0 - 212.118.30.255
netname: JO-NETS-981026
descr: National Equipment & Technical Services
country: jo

person: Marwan S Juma
address: National Equipment and Technical Services
address: PO Box 811912
address: Amman 11181 , Jordan
phone: +962-6-619870
fax-no: +962-6-619871
e-mail: admin@nets.com.jo
```

3. Un cas de phishing très reconnaissable

Les observations habituelles permettent de reconnaître la fraude :

- URL ne correspondant pas à une source « racine » eBay.
- Absence de site HTTPS,
- Absence de clé SSL (icône zone sécurisée).

L'étude des autres documents décrivant les tentatives de phishing sur eBay permet de reconnaître immédiatement la « charte graphique » utilisée !

