

1. Le message, son aspect général :

La technique utilisée est un lien associé à une image à cliquer :



Ce message nous a été transmis sous le format html obtenu depuis un « webmail ». C'est pour cette raison que l'image proposée par le fraudeur n'est pas visible ici... mais le lien est resté actif !

Le code associé est reconnaissable :

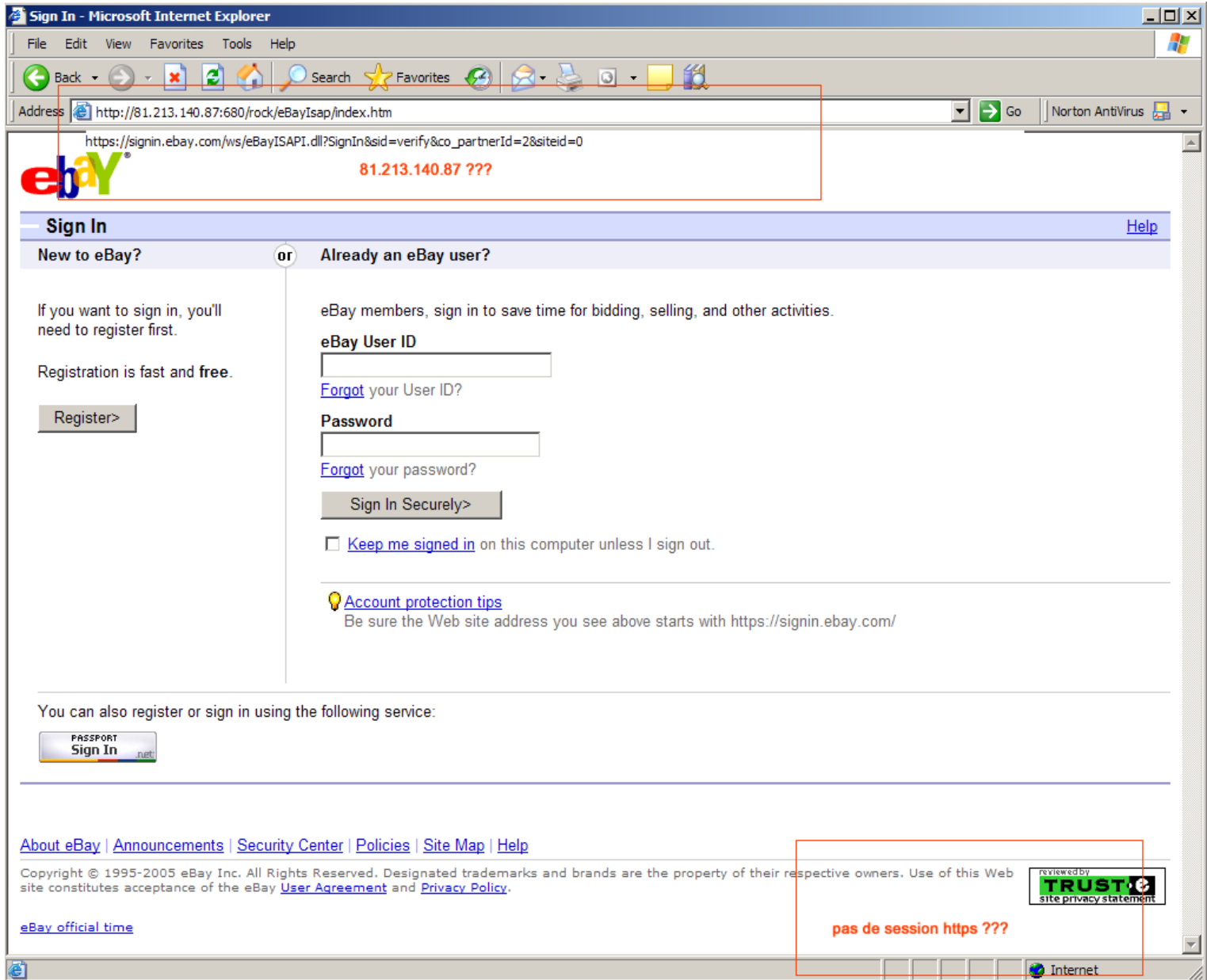
```
<A HREF="https://signin.ebay.com/ws/eBayISAPI.dll?SignIn&sid=verify&co_partnerId=2&siteid=0">  
<map name="rceyrbx">  
<area coords="0, 0, 646, 569" shape="rect" href="http://81.213.140.87:680/rock/eBayIsap/index.htm">  
</map>  
<img SRC="http://www..... &Body=2" border="0" usemap="#rceyrbx">  
</A>
```

```
<p><font color="#FFFFFF0">Oscar Powerball Denisse Richards into account do not </font></p>
```

La signature [en bleu](#) fera peut-être sourire ?

L'utilisation d'une image avec MAP est largement répandue dans les essais de phishing.

2. L'ergonomie du site « piège » :

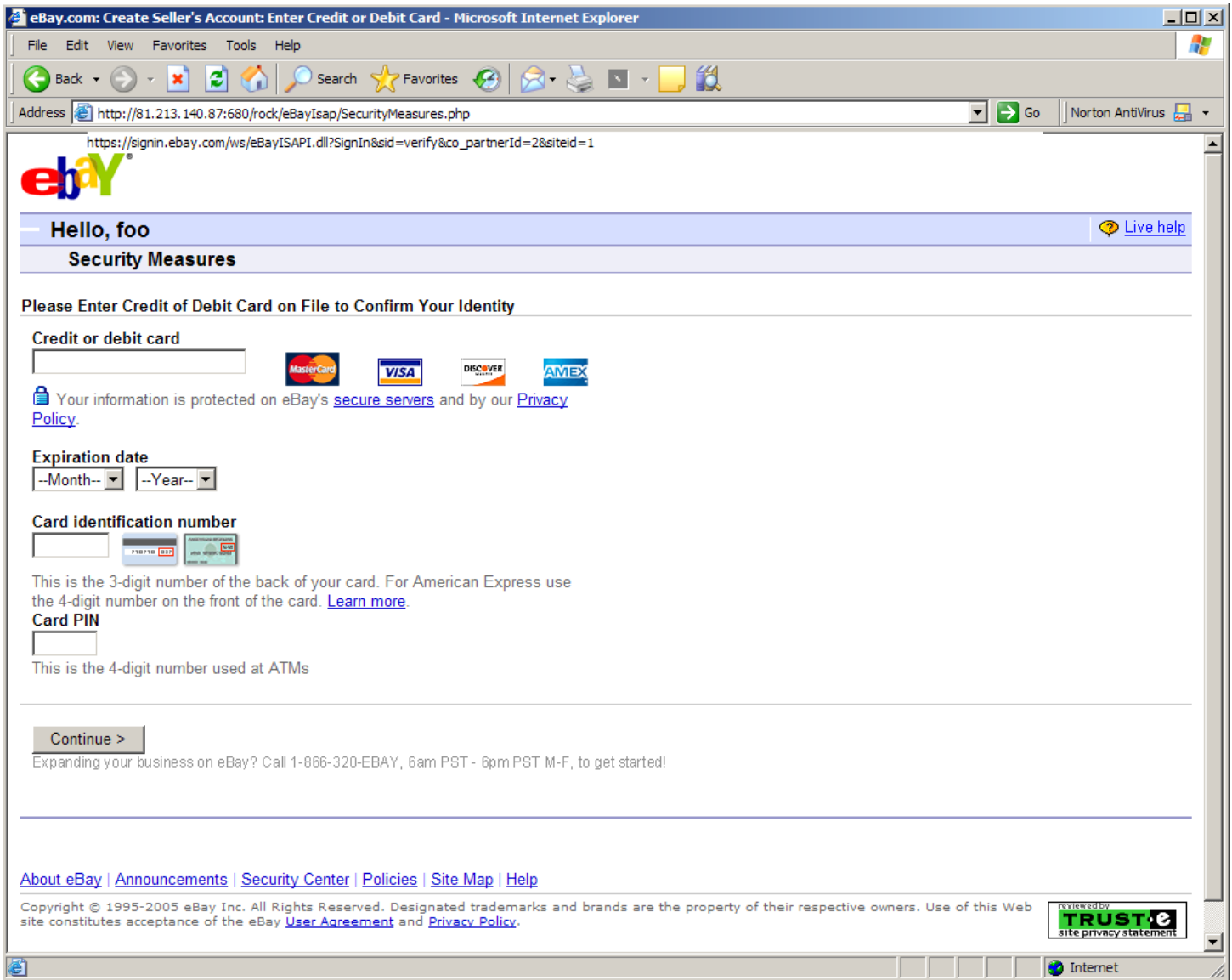


L'ergonomie peut paraître celle d'eBay mais les points suivants attirent l'attention :

- l'absence de session HTTPS,
- l'adresse **81.213.140.87** étrange.

3. Test des pages suivantes :

Nous avons essayé le classique : « *compte=foo ; password=foo* » pour tester les pages suivantes.



Malgré un effort graphique, l'absence de session HTTPS reste la signature du phishing.

4. Le Whois renvoie vers un site en Turquie :

Whois 81.213.140.87 ?

inetnum: 81.213.140.0 - 81.213.140.255
netname: TurkTelekom
descr: **ADSL-ALC-Izmir-Static Pool**
country: tr
admin-c: TTBA1-RIPE
tech-c: TTBA1-RIPE
status: ASSIGNED PA
mnt-by: as9121-mnt
source: RIPE # Filtered

role: TT Administrative Contact Role
address: Turk Telekom
address: Bilisim Aglari Dairesi
address: Aydinlikevler
address: 06103 ANKARA
phone: +90 312 313 1950
fax-no: +90 312 313 1949
e-mail: abuse@ttnet.net.tr
admin-c: BADB3-RIPE
tech-c: ZA66-RIPE
tech-c: ZA196-RIPE
tech-c: LA109-RIPE
tech-c: NO638-RIPE
nic-hdl: TTBA1-RIPE
mnt-by: AS9121-MNT
source: RIPE # Filtered

route: 81.213.128.0/17
descr: TurkTelecom
origin: AS9121
mnt-by: AS9121-MNT
source: RIPE # Filtered

5. Les actions engagées :

- Rédaction de ce document,
- Remontée au niveau « .org » effectuée.