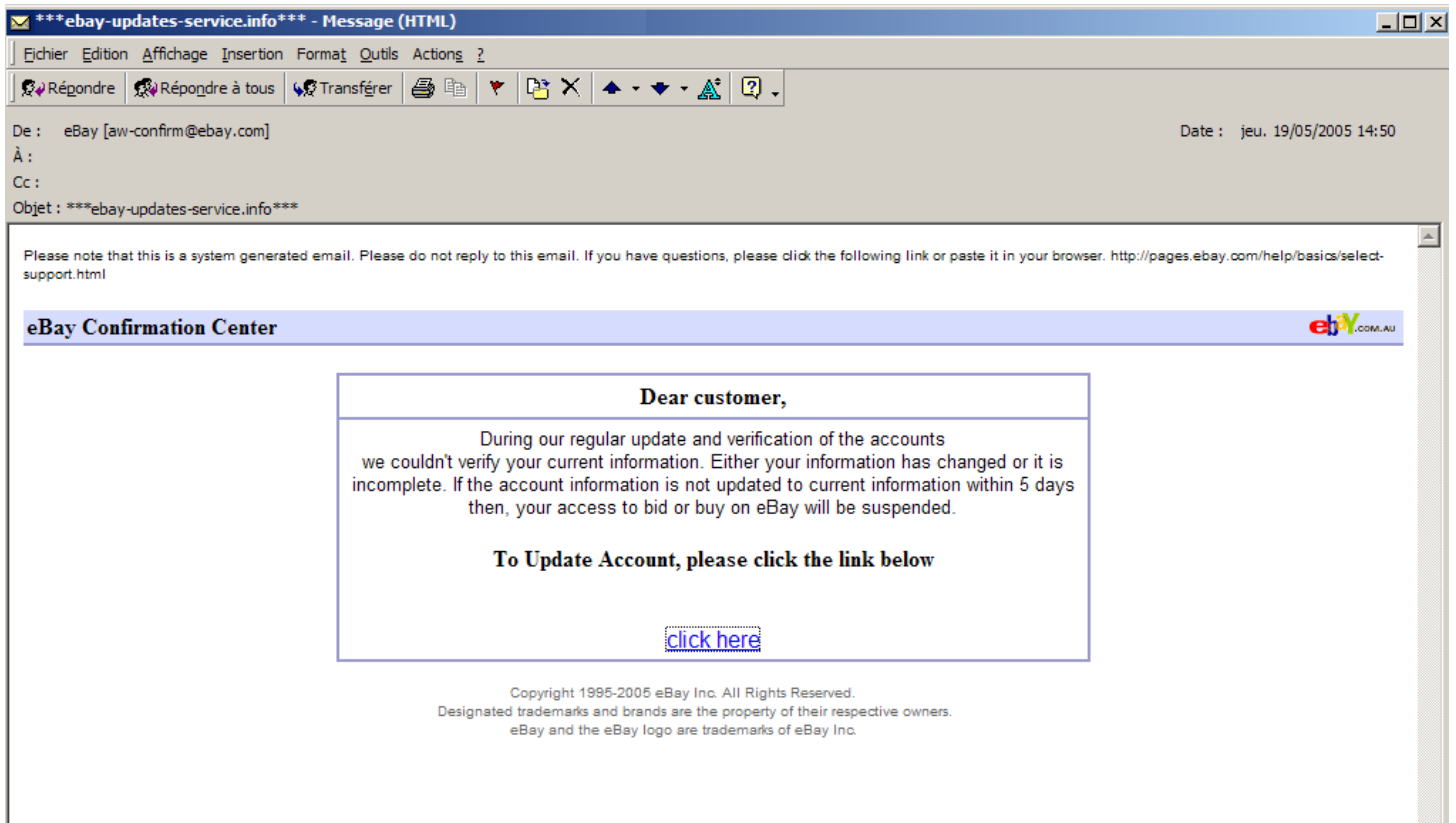


1. Le message, son aspect général :



2. La technique utilisée :

Ce cas de phishing est basé un lien html « [click here](#) » vers :

http://www.pearland.co.id/ws/eBayISAPI.dll?SignIn&co_partnerId=2&pUserId=&siteid=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=&ru=&pp=&pa2=&errmsg=&runame=&ruparams=&ruproduct=&sid=&favorit enav=

Dont l'adresse IP associée est déterminable via « tracert » :

```
X:\>tracert www.pearland.co.id
```

```
Tracing route to pearland.co.id [203.130.242.45]
```

L'analyse de l'IP 203.130.242.45 utilisée avec Whois aboutit à un site hébergé en Indonésie :

```

inetnum: 203.130.224.0 - 203.130.255.255
netname: TELKOMNET
descr: PT TELEKOMUNIKASI INDONESIA
descr: Jln Japati No 1
country: ID
admin-c: MR39-AP
tech-c: IS49-AP
remarks: service provider
mnt-by: APNIC-HM
mnt-lower: MAINT-TELKOMNET
status: ALLOCATED PORTABLE
remarks: -+-+-+
remarks: This object can only be modified by APNIC hostmaster
remarks: If you wish to modify this object details please
remarks: send email to hostmaster@apnic.net with your organisation
remarks: account name in the subject line.
remarks: -+-+-+
changed: hm-changed@apnic.net 19980107
changed: hm-changed@apnic.net 20041214
source: APNIC

person: M Untung Rahardjo
nic-hdl: MR39-AP
e-mail: m_untung@telkom.co.id
address: Jl. Kebon Sirih No. 37 Jakarta
phone: +62-21-3160500
fax-no: +62-21-3160300
country: ID
changed: joedi@telkom.co.id 20040205
mnt-by: MAINT-TELKOMNET
source: APNIC

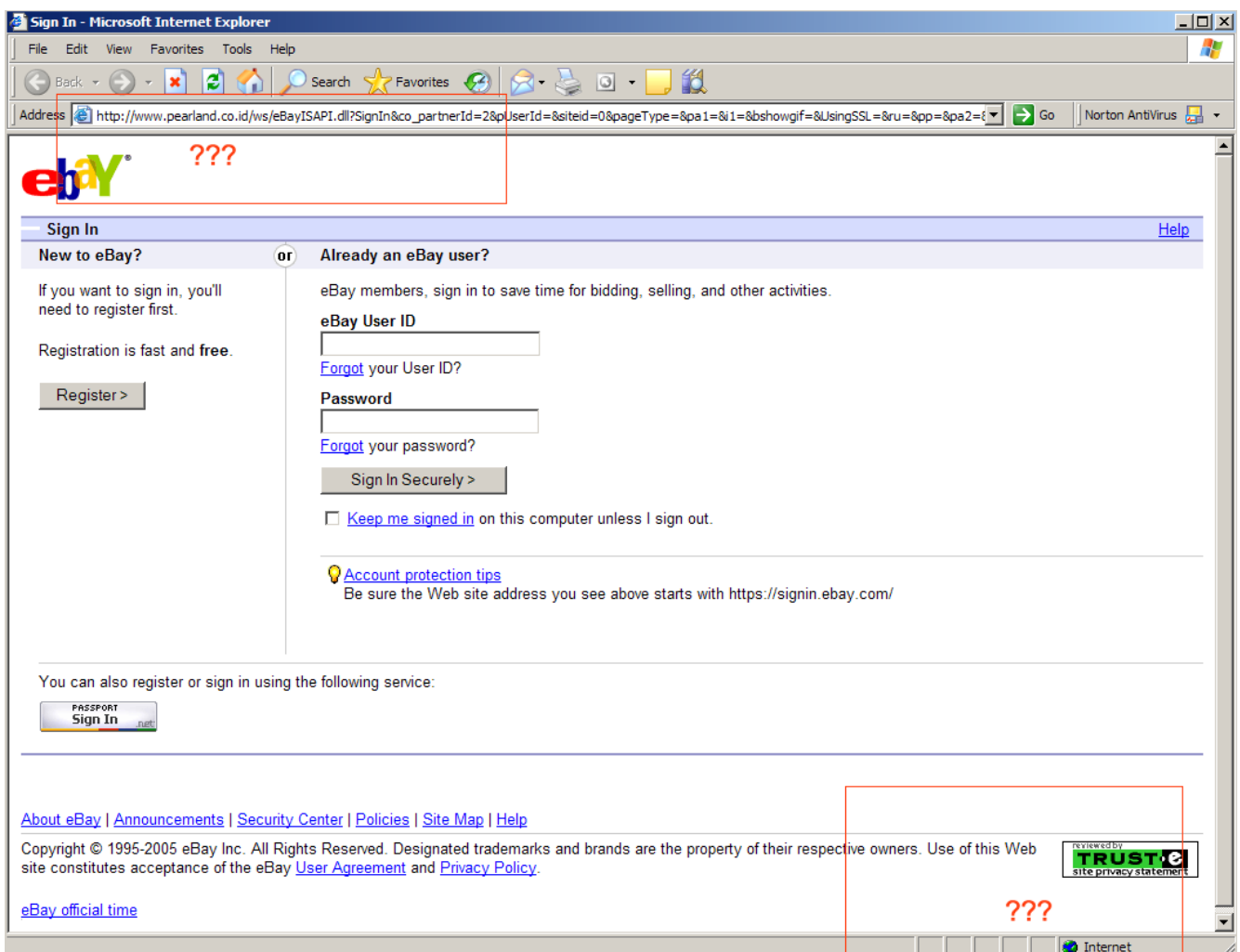
person: Iskandar Satyogo Prasetyo
nic-hdl: IS49-AP
e-mail: yogo@telkom.co.id
address: PT. TELEKOMUNIKASI INDONESIA
address: MULTIMEDIA DIVISION
address: Jl. Kebonsirih No.12 7th floor
address: Jakarta Indonesia
phone: +62-21-3860500
fax-no: +62-21-3861215
country: ID
changed: m_untung@telkom.co.id 20040729
mnt-by: MAINT-TELKOMNET
source: APNIC

```

3. Un cas de phishing visible :

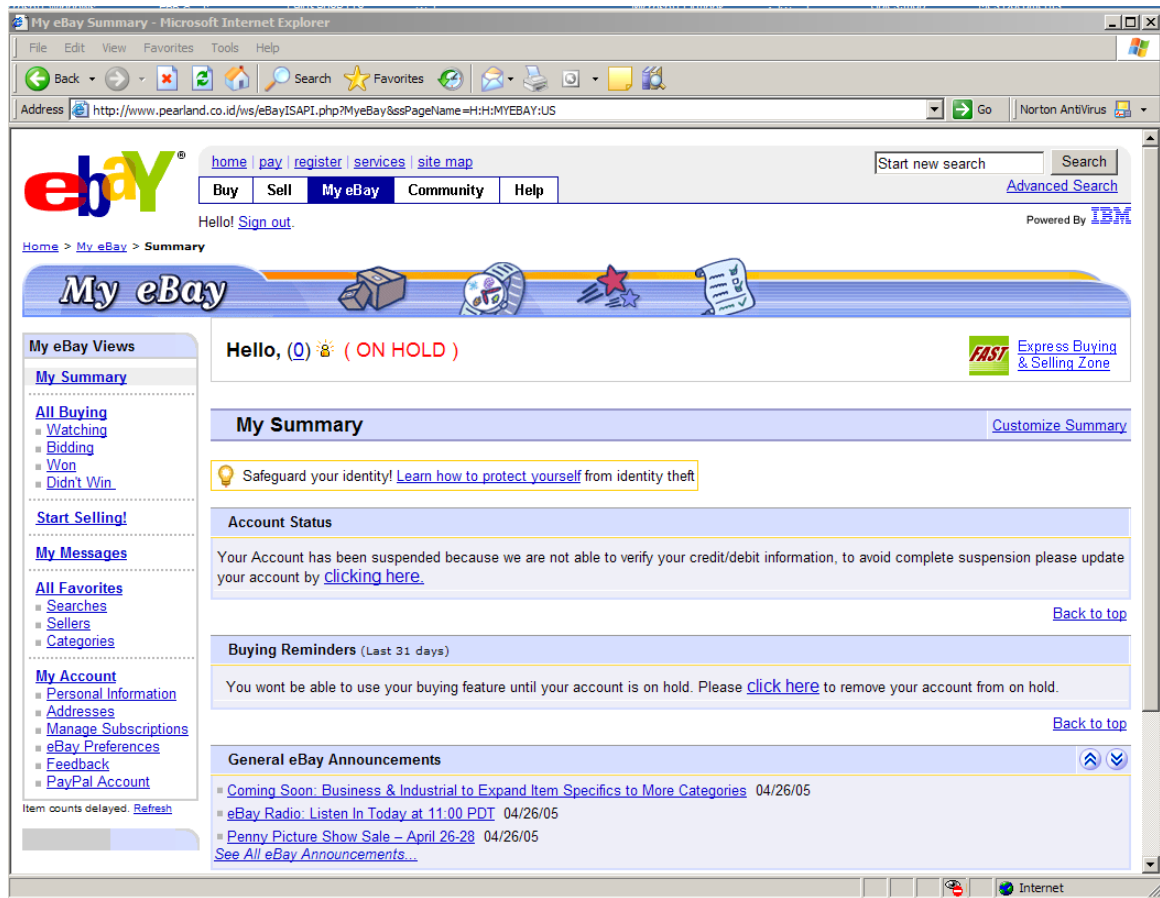
Les observations habituelles permettent de reconnaître la fraude :

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



4. Malheur au distrait car le graphisme reste « séduisant » :

Après avoir fourni les informations demandées, le distrait obtient une page d'accueil :



Et le distrait peut continuer à surfer sur ce pseudo site eBay :

