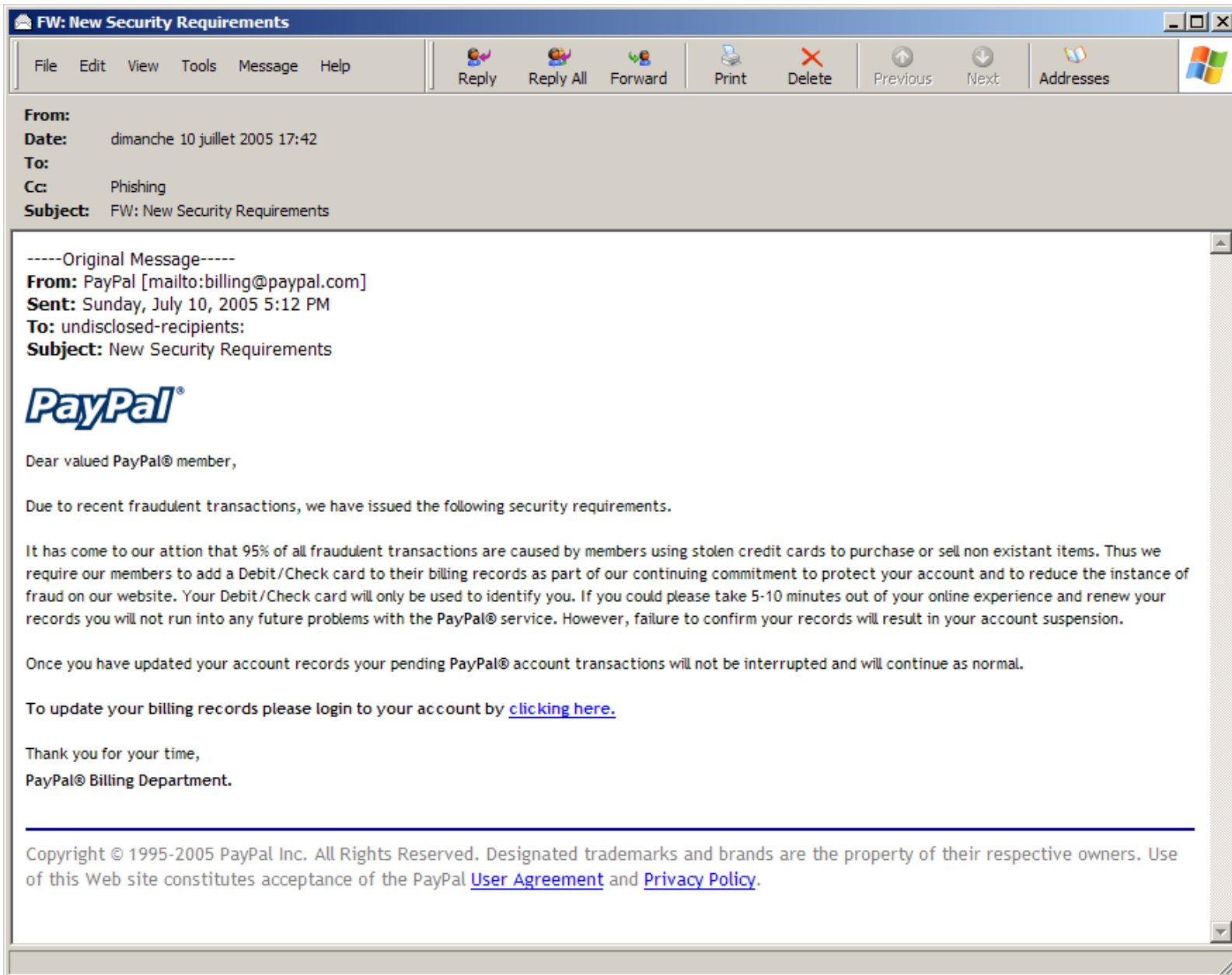


## 1. Le message, son aspect général :

La technique utilisée est un lien à cliquer « [clicking here](#) »:



Mais lors de nos essais, il semble que le site de phishing ait été désactivé ! Les divers journaux de notre passerelle contiennent malgré tout quelques traces intéressantes :

```
...  
X-mxGuard-Sender:  
X-mxGuard-Virus-Info: Infected [HTML.Phishing.Auction-47]
```

Cette tentative est donc parfaitement par ClamAV (antivirus "libre" applicable entre autre à une passerelle SMTP)

## 2. Le header du message tel qu'il figure dans notre passerelle :

Received: from ... ESMTP(SMTPD32-8.15) id A1121203EE;  
Sun, 10 Jul 2005 17:38:58 +0200  
Received: from ... with SMTP id EE9992561D;  
Sun, 10 Jul 2005 17:40:25 +0200 (CEST)  
Reply-To:  
From:  
To: [reportphishing@antiphishing.fr](mailto:reportphishing@antiphishing.fr)  
Cc:  
**Subject: FW: New Security Requirements**  
Date: Sun, 10 Jul 2005 17:42:50 +0200  
Message-ID:  
MIME-Version: 1.0  
Content-Type: multipart/alternative;  
boundary="====\_NextPart\_000\_0007\_01C58576.CAE29810"  
X-Priority: 3 (Normal)  
X-MSMail-Priority: Normal  
X-Mailer: Microsoft Outlook IMO, Build 9.0.6604 (9.0.2911.0)  
X-MimeOLE: Produced By Microsoft MimeOLE V6.00.2900.2527  
Importance: Normal  
  
X-mxGuard-Info: Processed by associatedwinners.com  
X-mxGuard-Spool-ID: 4112001203eealb5  
X-mxGuard-Sender:  
X-mxGuard-Virus-Info: Infected [**HTML.Phishing.Auction-47**]  
  
X-Note: This message has been scanned for spam and viruses by  
Associated Winners  
  
This is a multi-part message in MIME format.  
  
====\_NextPart\_000\_0007\_01C58576.CAE29810  
Content-Type: text/plain;  
charset="iso-8859-1"  
Content-Transfer-Encoding: 8bit  
  
-----Original Message-----  
From: PayPal [mailto:billing@paypal.com]  
Sent: Sunday, July 10, 2005 5:12 PM  
To: undisclosed-recipients:  
Subject: New Security Requirements  
  
...  
  
====\_NextPart\_000\_0007\_01C58576.CAE29810--

### 3. Une visite sur le site de ClamAV ([www.clamav.net](http://www.clamav.net)) :

Via le moteur de recherche de ClamAV, nous avons recherché les « virus » connus par ClamAV et associés à la signature d'une tentative de phishing :

425 hits for 'HTML.Phishing'

## ClamAV Virus Database Search

Search for:   begins with  contains  exact  regex

Case-sensitive search:  Yes  No

Search database(s):  Daily  Main

Display results:  Database  File  Virus Name  Signature

---

### Search results:

main.cvd HTML.Phishing.Auction-47

1 hit for 'HTML.Phishing.Auction-47'

---

## ClamAV Virus Database Search

Search for:   begins with  contains  exact  regex

Case-sensitive search:  Yes  No

Search database(s):  Daily  Main

Display results:  Database  File  Virus Name  Signature

---

## Search results:

main.cvd HTML.Phishing.Bank-2 (Clam)  
main.cvd HTML.Phishing.Bank-3 (Clam)  
main.cvd HTML.Phishing.Bank-14 (Clam)  
main.cvd HTML.Phishing.Bank-17 (Clam)  
main.cvd HTML.Phishing.Bank-30 (Clam)  
main.cvd HTML.Phishing.Bank-1  
main.cvd HTML.Phishing.Bank-4  
main.cvd HTML.Phishing.Auction-1  
main.cvd HTML.Phishing.Auction-2  
main.cvd HTML.Phishing.Bank-5  
main.cvd HTML.Phishing.Bank-6  
main.cvd HTML.Phishing.Bank-7  
main.cvd HTML.Phishing.Bank-8  
main.cvd HTML.Phishing.Bank-9  
...  
main.cvd HTML.Phishing.Auction-84  
main.cvd HTML.Phishing.Auction-85  
main.cvd HTML.Phishing.Bank-257  
main.cvd HTML.Phishing.Bank-259  
main.cvd HTML.Phishing.Bank-258

425 hits for 'HTML.Phishing'

## 4. Les traces de nos essais dans notre serveur de DNS :

Peu d'informations utiles car la résolution DNS a été désactivée !

Les traces du serveur de DNS:

-----  
16:14:34 Request from 192.168.111.3 for A-record for [paypal-signin03.com](http://paypal-signin03.com).  
16:14:34 Sending request to [66.33.238.172](http://66.33.238.172) ([ns294.paypal-signin03.com](http://ns294.paypal-signin03.com).) for A-record for paypal-signin03.com.  
16:14:35 Sending request to [216.196.137.147](http://216.196.137.147) ([ns3498.paypal-signin03.com](http://ns3498.paypal-signin03.com).) for A-record for paypal-signin03.com.  
16:14:35 -> Duplicate request ignored - still working on original.

Whois [66.33.238.172](http://66.33.238.172) ?

-----  
OrgName: epix Internet Services  
OrgID: EPIX

Address: 100 CTE Dr.  
City: Dallas  
StateProv: PA  
PostalCode: 18612  
Country: US

NetRange: 66.33.224.0 - 66.33.255.255  
CIDR: 66.33.224.0/19  
NetName: EPIX-5BLK  
NetHandle: NET-66-33-224-0-1  
Parent: NET-66-0-0-0-0  
NetType: Direct Allocation  
NameServer: NS-1.EPIX.NET  
NameServer: NS-2.EPIX.NET

Whois 216.196.137.147 ?

-----  
OrgName: Fuse Internet Access  
OrgID: FIAI  
Address: 209 W. Seventh St.  
Address: MS 121-550  
City: Cincinnati  
StateProv: OH  
PostalCode: 45202  
Country: US

NetRange: 216.196.128.0 - 216.196.255.255  
CIDR: 216.196.128.0/17  
NetName: FUSE-NET-BLK-2  
NetHandle: NET-216-196-128-0-1  
Parent: NET-216-0-0-0-0  
NetType: Direct Allocation  
NameServer: NS1.FUSE.NET  
NameServer: NS2.FUSE.NET

## **5. Les actions engagées :**

- Rédaction de ce document « à la gloire » de ClamAV,
- Pas de report au niveau « .org » car trop d'informations.