

1. Le message, son aspect général :

L'email n'utilise pas un « appât » graphique mais s'appuie sur un nom de domaine « réaliste »:

De : <service@paypal.com>
Date : 3 juillet 2005 22:06:04 HAEC
À :
Objet : Unauthorized Access: (Routing Code: O201-W211-T090)

Dear Paypal User

???

You have added funstuff12@aol.com as a new email address for your PayPal account.

If you did not authorize this change or if you need assistance with your account, please contact PayPal customer service at:

<http://www.paypalonlineupdate.com/index.htm?cmd=login-run>

???

Thank you for using PayPal!
The PayPal Team

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, log in to your PayPal account and choose the "Help" link in the header of any page.

L'utilisation d'un email farfelu « funstuff12@aol.com » laisse toutefois deviner un envoi massif car ce compte « ajouté » n'est pas personnalisé.

Qui est www.paypalonlineupdate.com ?

```
Whois paypalonlineupdate.com ?
```

```
Answer:
```

```
A-record for paypalonlineupdate.com.:
```

```
IP address = 221.5.250.94
```

```
TTL = 3 Hours, 59 Minutes, 12 Seconds
```

```
NS-record for paypalonlineupdate.com.:
```

```
DNS server = ns2.nightdreamserver.com.
```

```
TTL = 3 Hours, 59 Minutes, 12 Seconds
```

```
NS-record for paypalonlineupdate.com.:
```

```
DNS server = ns1.nightdreamserver.com.
```

```
TTL = 3 Hours, 59 Minutes, 12 Seconds
```

Qui est 221.5.250.94 ?

Whois 221.5.250.94 ?

Answer:

```
inetnum:      221.5.128.0 - 221.5.255.255
netname:      CNCGROUP-CQ
descr:        CNC Group Chongqing province network
descr:        China Network Communications Group Corporation
descr:        No.156,Fu-Xing-Men-Nei Street,
descr:        Beijing 100031
country:      CN
admin-c:      CH455-AP
tech-c:       CH455-AP
remarks:      service provider
mnt-by:       APNIC-HM
mnt-lower:    MAINT-CNCGROUP-CQ
changed:      hm-changed@apnic.net 20030113
status:       ALLOCATED PORTABLE
source:       APNIC
```

2. La technique utilisée :

Cette tentative est un classique « lien à cliquer » associé à la reproduction des pages d'accueil du site plagié (sans usage d'une session HTTPS ...)

PayPal - Welcome - Microsoft Internet Explorer

Address http://www.paypalonlineupdate.com/index.htm?cmd=_login-run

Member Log In [Forgot your Password?](#)

Email Address

Password

Join PayPal Today
Now over 71 million accounts

[Learn more about PayPal Worldwide](#)

The Fast Way to Pay
Safe to Pay

PayPal is a global leader in online payments. [Find out more](#)

Good for Business
[Learn how](#) PayPal helps your business grow

Enterprise Solutions
[Learn more](#)

Buyers

Send money to anyone with an email address in 45 countries.
PayPal is [free to use](#).
Your information is kept [secure](#).

eBay Sellers

Free eBay tools make selling easier.
PayPal works hard to help [protect sellers](#).
PayPal simplifies [shipping and tracking](#).

Merchants

Accept credit cards on your website using PayPal.
Free merchant tools help grow your business.
Low fees make PayPal the affordable choice.

[About](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [Contact Us](#) | [User Agreement](#) | [Developers](#) | [Jobs](#) | [Buyer Credit](#) | [Referrals](#) | [Shops](#) | [Mass Pay](#)

PayPal, an eBay company

Powered By Sun Microsystems

Copyright © 1999-2005 PayPal. All rights reserved.
[Information about FDIC pass-through insurance](#)

TRUSTe
site privacy statement

PRIVACY
BBB OnLine

Done

3. Un essai pour révéler le phishing

Pour mettre en évidence, le phishing il suffit de se connecter sur un compte fictif pour obtenir, dans tous les cas, la demande des informations bancaires confidentielles !

Compte : perso

Mot de passe : perso

PayPal - Update Account - Microsoft Internet Explorer

Address: <http://www.paypalonlineupdate.com/formular.php>

???

Welcome Send Money Request Money Merchant Tools Auction Tools

Update Your Paypal Account

→ 1 Enter Your Information

Your Address Information - Begin building your profile by entering your name and address as you have it listed for your credit card or bank account.

First Name:

Last Name:

Address 1:

Address 2: (optional)

City:

State:

ZIP Code: (5 or 9 digits)

Country: - Choose a Country -





Home Telephone:

Work Telephone: (optional)

Credit Card - Update your credit card for your security ???

Bank Name:

Card Type:

Number on Credit Card:    

Expiration Date: 01 2005

Card Verification Number: (On the back of your card, find the last 3 digits) [Help finding your Card Verification Number](#) | [Using AmEx?](#)

ATM PIN Number: [Why is your PIN required?](#)

Next

[About](#) | [Accounts](#) | [Fees](#) | [Privacy](#) | [Security Center](#) | [Contact Us](#) | [User Agreement](#) | [Developers](#) | [Jobs](#) | [Buyer Credit](#) | [Referrals](#) | [Shops](#) | [Mass Pay](#)

PayPal, an eBay company

4. Actions engagées :

- La publication de ce document,
- L'information au niveau « .org » a été effectuée.