

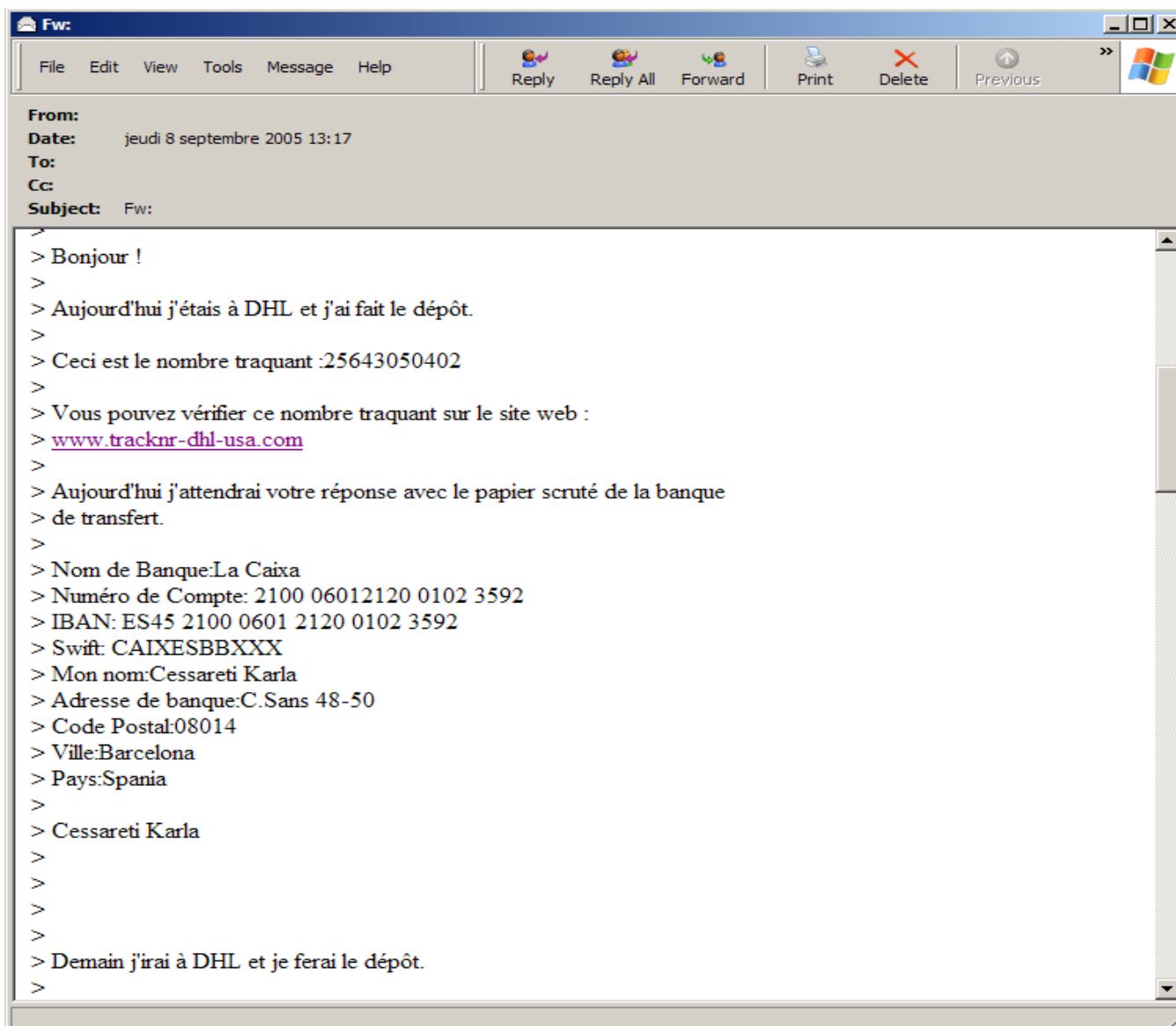
## 1. Le message, son aspect général :

Le cas décrit ici n'est pas la tentative usuelle de phishing mais une « arnaque » utilisant un site Web plagié (en l'occurrence celui de DHL USA). Nous ne reportons pas la partie privée de l'échange entre le vendeur et son acheteur potentiel mais seulement la mise en évidence du site plagié. Le schéma de « l'arnaque » est :

- Offre de vente d'un écran plasma à un prix très intéressant sur le site d'eBay.
- Négociation et vente par un échange d'emails directs. Le « pseudo » vendeur utilise un compte « générique » Yahoo pendant ces échanges : [ponconz@yahoo.com](mailto:ponconz@yahoo.com).
- Le vendeur effectue la livraison via DHL et produit son numéro DHL pour le tracking (**voir NOTE**).
- L'acheteur reçoit un email du site DHL pour confirmer qu'une livraison est en cours.
- L'acheteur constate sur le site DHL et le numéro de tracking que la livraison est en cours. Il suffit de suivre le lien sur le site de DHL pour suivre le colis.
- Puisque la livraison est en cours, le vendeur demande un paiement via son compte bancaire.
- L'acheteur peut donc payer « tranquillement » !

**NOTE** : l'arnaque est basée sur la reproduction du site DHL via une URL « plausible » :

- >
- > *Vous pouvez vérifier ce nombre traquant sur le site web :*
- > [www.tracknr-dhl-usa.com](http://www.tracknr-dhl-usa.com)
- >



Comme dans le phishing, la technique utilisée est celle du lien « à cliquer ».

La page Web suivante sera appelée: [www.tracknr-dhl-usa.com](http://www.tracknr-dhl-usa.com)

**DHL: Home - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Address <http://www.tracknr-dhl-usa.com/> Go

Contact Us | Sitemap

**DHL** Ship Track Services About DHL Help

Welcome to DHL DHL USA Home ▶ DHL Global

▶ New export regulations. How DHL can help... view demo.

**Get it there** [Get a quote](#)

Origination Information

Sender's name

Destination information  
Fields marked with an asterisk (\*) are required.

Current recipients Enter receiver ID

Enter new recipient Country

Name

Postal code

[Next](#)

**Log in to DHL**

User ID

Password

[Log in](#)

[Forgot your Password?](#)

**Register**  
Registration is quick and easy. You'll save time when shipping.  
[Register now](#)

**Pickup & Drop-off**

- [Schedule a pickup](#)
- [Cancel a pickup](#)
- [Find drop-off locations](#)

**Track it**  
Enter up to 25 tracking numbers, one per line

[Track](#)

**DHL Small Business Center**  
Tips, tools, savings and other resources to get you where you want to go  
[Learn More](#)

**Tools**

- [What's new](#)
- [Fuel surcharge](#)
- [Transit Times](#)
- [International Shipping](#)

**News and service updates**

- [SED Regulation Update](#)
- [FDA Regulation Update](#)

**MLB.com**  
OFFICIAL EXPRESS DELIVERY AND LOGISTICS PROVIDER OF MAJOR LEAGUE BASEBALL®  
TM® MLB 2005

[DHL Global](#) | [About DHL](#) | [Newsroom](#) | [Contact](#) | [Sitemap](#) | [Privacy Policy](#)  
Copyright © 2005 DHL International, Ltd. All Rights Reserved.

Internet

Il suffit de visiter le site de DHL USA : <http://www.dhl-usa.com/home/Home.asp> pour constater la similitude de l'ergonomie.

## 2. Identification du site hostile :

L'utilitaire nslookup montre l'hébergement chez Yahoo :

```

C:\WINDOWS\system32\cmd.exe - nslookup
Server: associatedwinners.com
Address: 10.0.0.2

Non-authoritative answer:
Name: tracknr-dhl-usa.com
Addresses: 68.142.234.50, 68.142.234.51, 68.142.234.52, 68.142.234.53
           68.142.234.54, 68.142.234.55

> set type=all
> tracknr-dhl-usa.com
Server: associatedwinners.com
Address: 10.0.0.2

Non-authoritative answer:
tracknr-dhl-usa.com internet address = 68.142.234.55
tracknr-dhl-usa.com internet address = 68.142.234.54
tracknr-dhl-usa.com internet address = 68.142.234.53
tracknr-dhl-usa.com internet address = 68.142.234.52
tracknr-dhl-usa.com internet address = 68.142.234.51
tracknr-dhl-usa.com internet address = 68.142.234.50
tracknr-dhl-usa.com nameserver = yns1.yahoo.com
tracknr-dhl-usa.com nameserver = ns9.san.yahoo.com
tracknr-dhl-usa.com nameserver = ns8.san.yahoo.com
tracknr-dhl-usa.com nameserver = yns2.yahoo.com
>

```

Lors de nos essais la première IP activée est **68.142.234.51**. Whois définit :

```

Domain Name..... tracknr-dhl-usa.com
Creation Date..... 2005-08-31
Registration Date... 2005-08-31
Expiry Date..... 2007-08-31
Organisation Name... John Wise
Organisation Address. 57 baston road
Organisation Address.
Organisation Address. Bromley
Organisation Address. BR27BD
Organisation Address. MO
Organisation Address. UNITED KINGDOM

Admin Name..... John Wise
Admin Address..... 57 baston road
Admin Address.....
Admin Address..... Bromley
Admin Address..... BR27BD
Admin Address..... MO
Admin Address..... UNITED KINGDOM
Admin Email..... obaradehash@yahoo.com
Admin Phone..... +34.02084622272

Tech Name..... YahooDomains TechContact
Tech Address..... 701 First Ave.
Tech Address.....
Tech Address..... Sunnyvale
Tech Address..... 94089
Tech Address..... CA
Tech Address..... UNITED STATES
Tech Email..... domain.tech@YAHOO-INC.COM

```

## 3. Actions engagées

- La publication de ce document,
- L'acheteur potentiel (qui n'a pas effectué le virement !) a porté plainte,
- Ce cas a été reporté au niveau « .org »