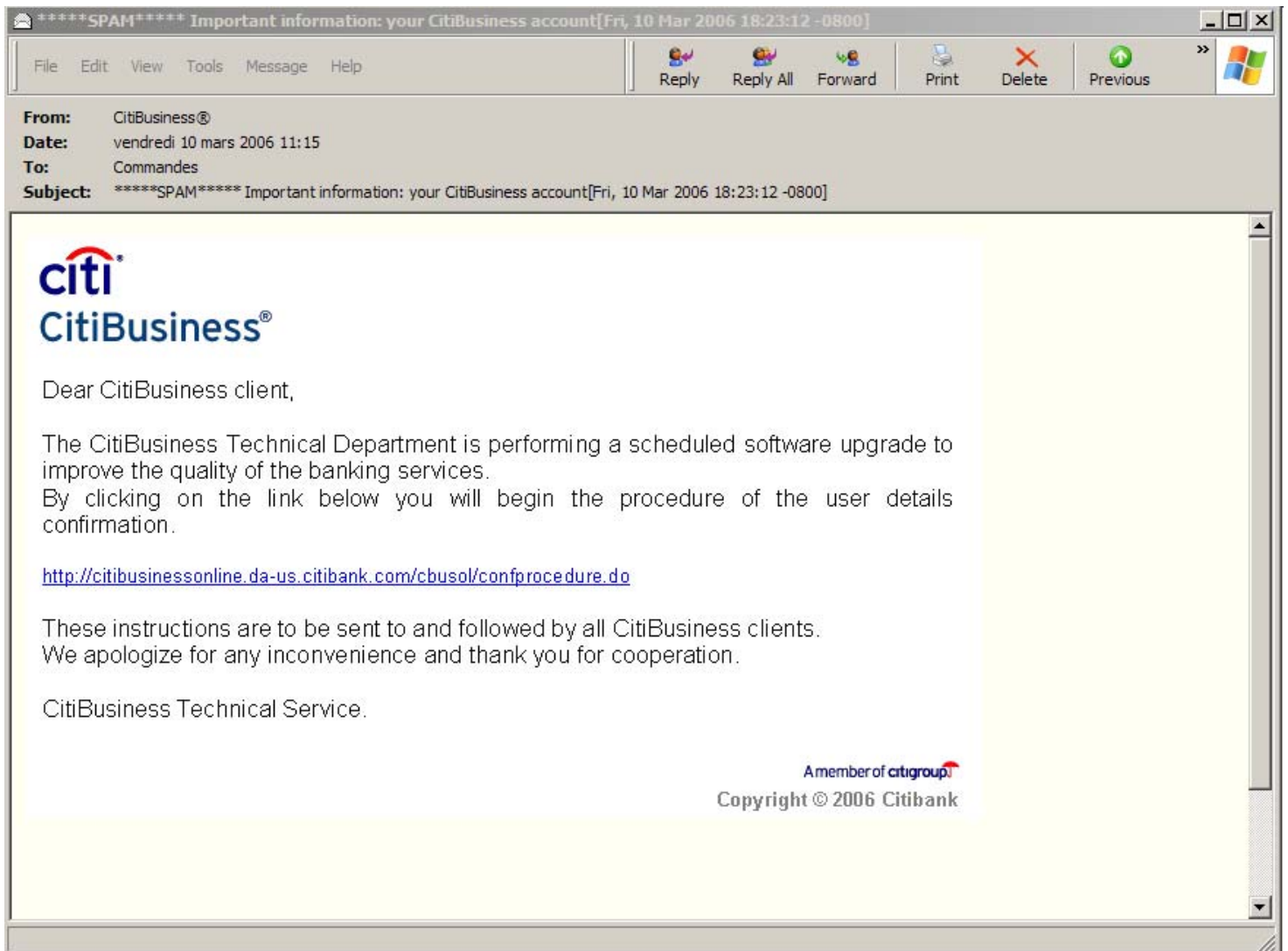


## 1. Le message, son aspect général :

Le vendredi 10 mars, les clients de Citibank ont été visés par une tentative de phishing :



## 2. La technique utilisée

La technique est celle d'un lien à cliquer associé à une image et l'examen du code html associé permet de lire le lien caché :

```
<BODY bgcolor="#FFFFFF" text="#66A2DF">
<a href=http://citibusinessonline.da-us.citibank.com.dlinfo.tv/r1/cb/>
</a>
</p>
<p><font color="#FFFFFF4">"Oh dear Jesus, the doctor is in! baseman advantage He knew that
smell a deadly mixture of dirt and face-powder.</font></p>
<p><font color="#FFFFFF0">Paul could not see the Smokey's eyes because of the sunglasses, but the tilt of
his head expressed moderate puzzlement. homeenglish. I didn't really care, as long as they played fair. He
couldn't stop shivering. For one bottle! Something had happened when he was asleep, someone had come, or
perhaps Annie had had a change of heart or mind. "She paused, not quite panting but breathing hard, looking at
him hard, as if inviting him to just dare and tell her different. anxious</font></p>
</BODY>
```

On remarquera les textes « surréalistes » affichés en caractères blancs (donc invisibles !).

Lors de nos essais, l'adresse IP utilisée pour héberger le piège s'est avérée être **211.97.71.213** et le lien nous a retourné la page suivante :

CitiBusiness Online - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://citibusinessonline.da-us.citibank.com.dlinfo.tv/r1/cb/> Go

**citi**  
CitiBusiness® Online

Home User Guide citi.com

Client details confirmation page. For enrolled CitiBusiness Online users only!  
We kindly request you to complete all the mandatory fields, if mandatory fields are left blank, you will see a note requesting you to complete missing fields.

First Name

Last Name

Credit/Debit Card (if you have)

Social Security Number (SSN)

Mother's Maiden Name (MMN)

Date Of Birth (DOB)

Enter Business Code: 7000-0000-

0 1 2 3 4 5 6 7 8 9

Back Clear

The business code contains 16 digits and begins with '70000000'

User ID (3 digits):

Password:

E-Mail:

Enter

Citibank, N.A., Citibank, F.S.B., Citibank (West), FSB, Citibank Texas, N.A. Member FDIC.  
www.citi.com

bill payment  
Citi Promise  
Online

VeriSign  
Secured  
VERIFY

Member of Citigroup  
CitiGroup LENDER  
Citigroup Privacy Promise  
Terms, conditions, accounts and services

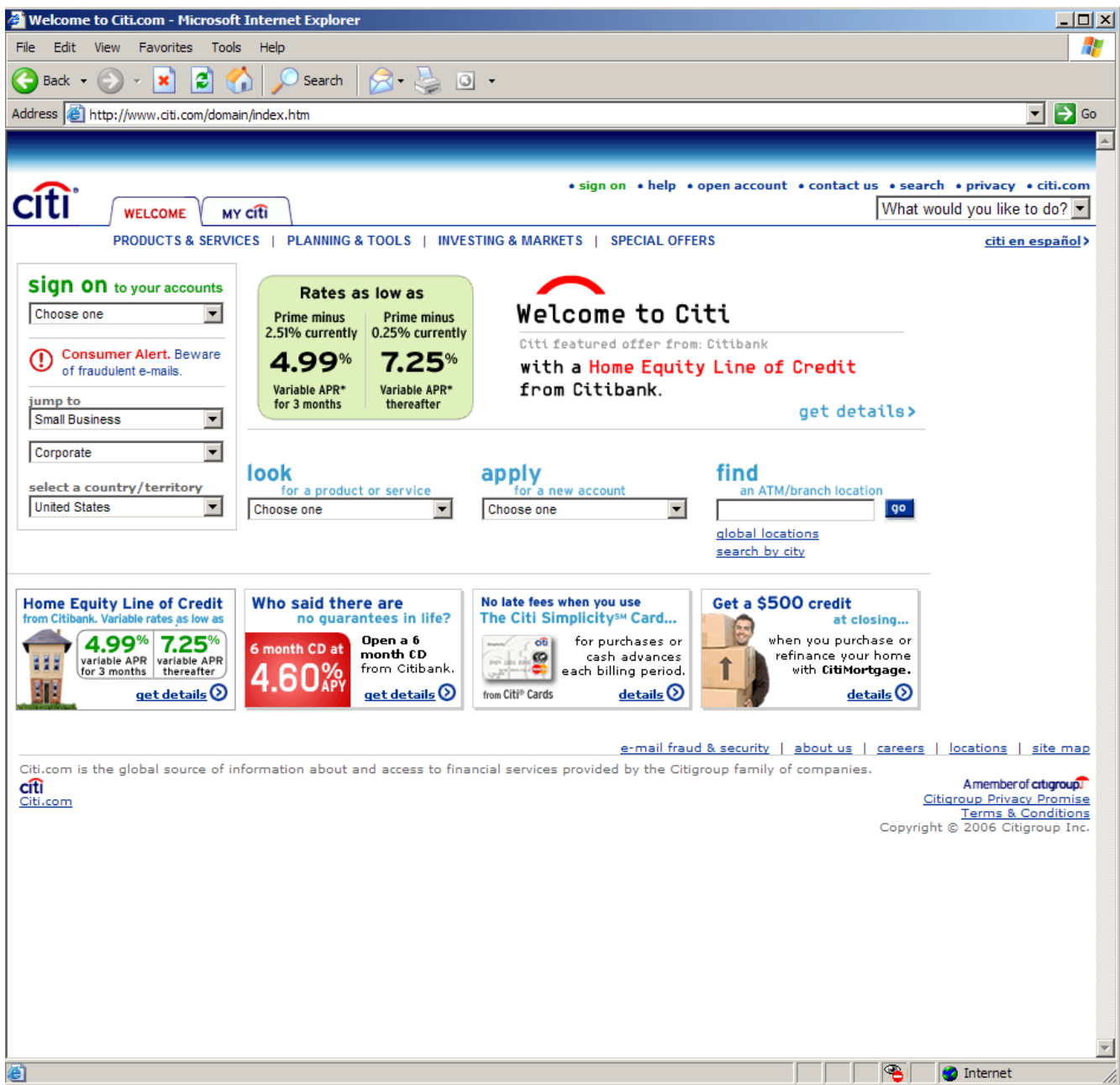
Done Internet

Les caractéristiques restent assez classiques :

- Pas de session sécurisée HTTPS,
- Un nom de domaine proche du nom réel,
- Des informations confidentielles dès la page d'authentification.

Mais, la nouveauté est la reproduction de « la calculette html » pour saisir le « Business Code » ce qui renforce la crédibilité du phishing.

Après avoir renseigné tous les champs, une redirection vers le site Web original est automatique. Le but est d'essayer de leurrer un internaute distrait ...



Globalement, l'ensemble est soigné et va jusqu'à effectuer un contrôle de présence des réponses :

## CitiBusiness® Online

Client details confirmation page. For enrolled CitiBusiness Online users only!

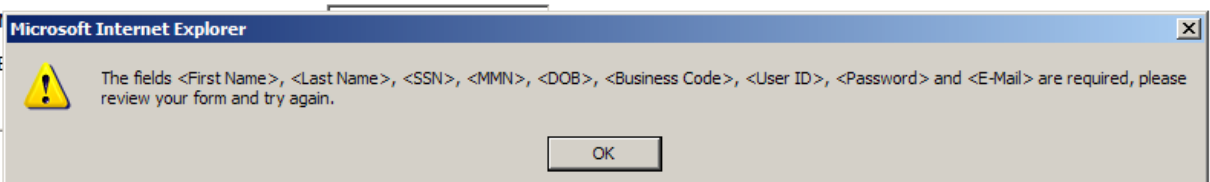
We kindly request you to complete all the mandatory fields, if mandatory fields are left blank, you will see a note requesting you to complete missing fields.

First Name	<input type="text" value="Rene"/>
Last Name	<input type="text" value="Bernard"/>
Credit/Debit Card (if you have)	<input type="text" value="145782157444"/>
Social Security Number (SSN)	<input type="text" value="14512145"/>

Mother's Maiden

Date of Birth (DOB)

Enter Business



### 3. Localisation de l'origine du phishing :

Le Whois permet de savoir qui se cache derrière l'IP **211.97.71.213** et le domaine **<http://citibusinessonline.da-us.citibank.com.dllinfo.tv/>** :

#### Whois 211.97.71.213 ?

```
inetnum:      211.90.0.0 - 211.97.255.255
netname:      UNICOM
descr:        China United Telecommunications Corporation
descr:        No.133,Taiyun Building,Xidan North Street
descr:        Xicheng District,Beijing,China
country:      CN
admin-c:      UCH1-AP
tech-c:       UCH1-AP
mnt-by:       APNIC-HM
mnt-lower:    MAINT-CN-CNNIC-UNICOM
status:       ALLOCATED PORTABLE
changed:      hm-changed@apnic.net 20041203
source:       APNIC

person:       Wenhui Zhang
address:      China Internet Information Center (CNNIC)
address:      No.4,South Fourth street,Zhongguancun,Haidian
address:      Beijing,100080
address:      P.R.China
country:      CN
phone:        +86-10-62553604
fax-no:       +86-10-62559892
e-mail:       whzhang@cnnic.net.cn
nic-hdl:      WZ2-CN
mnt-by:       MAINT-CNNIC-AP
changed:      ipas@cnnic.net.cn 20020408
source:       CNNIC
```

#### whois citibusinessonline.da-us.citibank.com.dllinfo.tv ?

```
Authoritative Answer: No
Recursion Available: Yes
Truncated (partial answer): No
```

```
Answer:
A-record for citibusinessonline.da-us.citibank.com.dllinfo.tv.:
  IP address = 211.97.71.213
  TTL = 11 Hours, 44 Minutes, 28 Seconds
```

### 4. Actions engagées

- La publication de ce document,
- Ce cas a été reporté au niveau « .org ».