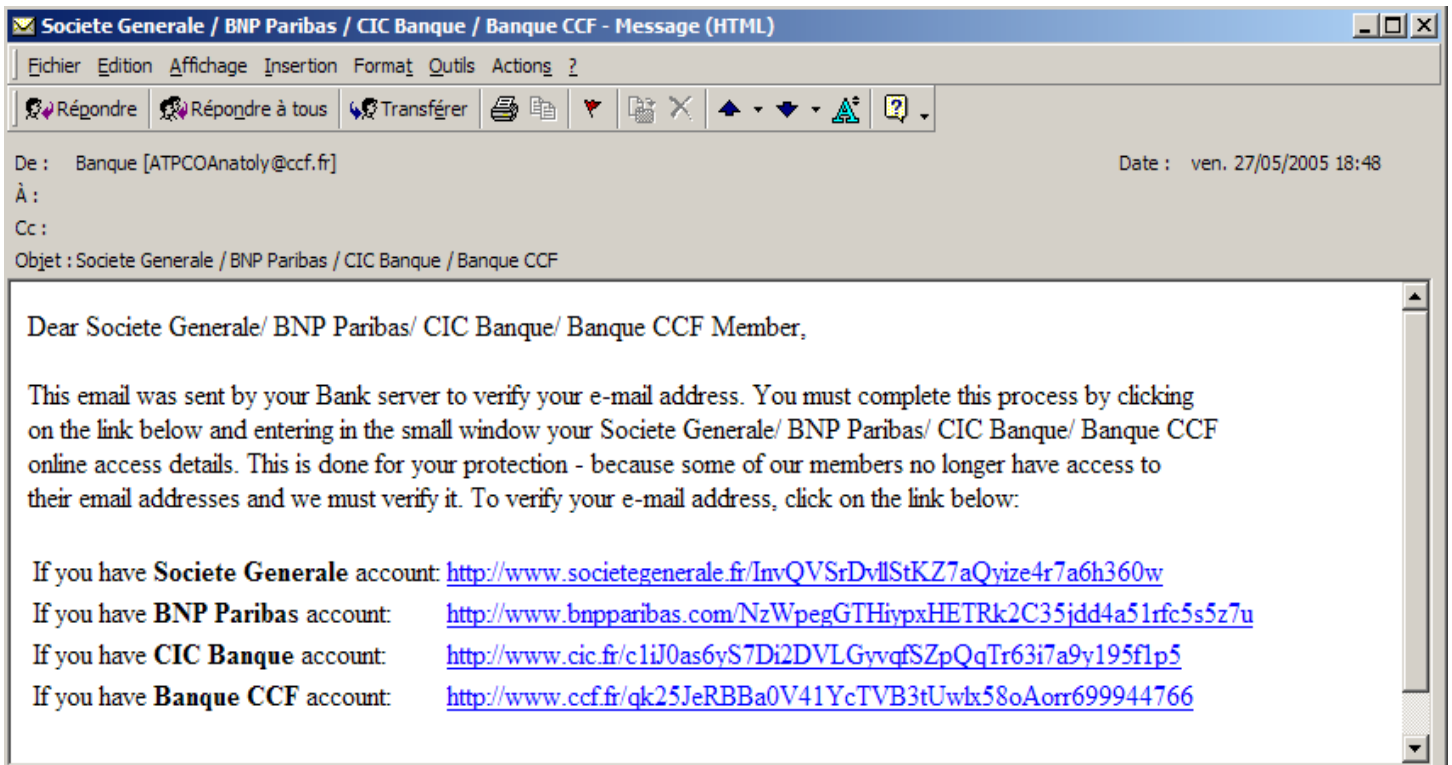


## 1. Le message, son aspect général :



## 2. La technique utilisée :

Ce cas de phishing est basé sur des liens à cliquer dont le code html associé est caractéristique :

- Usage de **code ASCII** pour masquer le site hostile,
- Usage de recherche **via le moteur Google** pour **dissimuler l'URL**.

On peut lire pour le lien BNP Paribas :

```
<tr>
  <td align=left>
    If you have <b>BNP Paribas</b> account:
  </td>
  <td align=left>
    <a href="http://www.google.nl/url?q=http://go.msn.com/HML/5/5.asp?
    target=http://%64ki%70a%70h%2e%44a%09%2E%52%55/"
    target=_blank>http://www.bnpparibas.com/BSafDNpTfthJviuSqQGY8J8vm1hact
    34v04</a>
  </td>
</tr>
```

Malgré ces astuces techniques, il reste peu probable qu'un tel email :

- rédigé en anglais,
  - émanant de banques françaises distinctes,
- puisse être interprété comme la demande authentique d'une de ces banques.

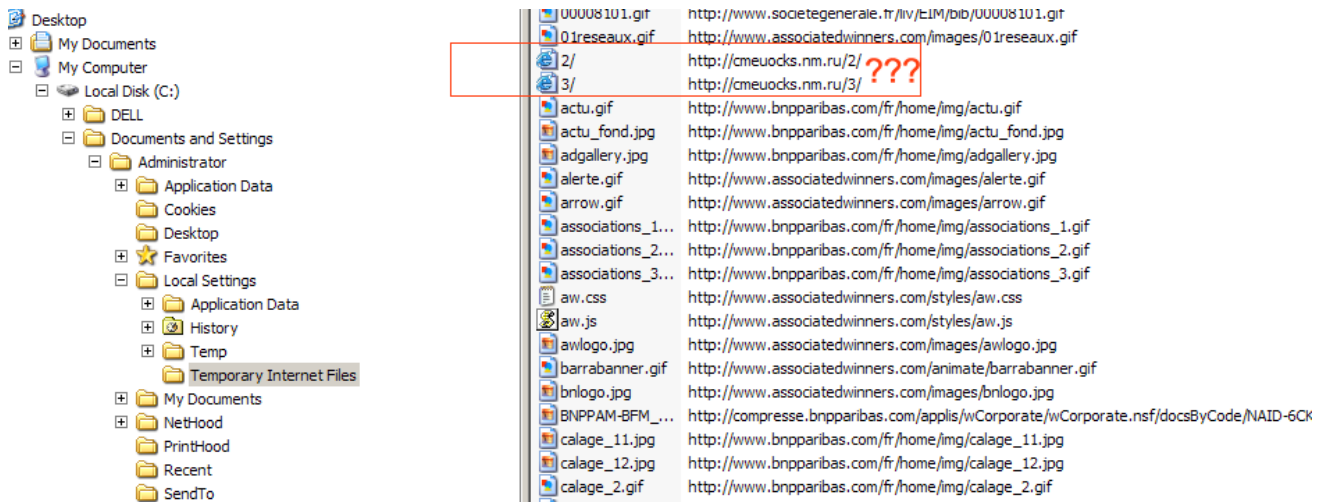
La nuisance de cet email est ainsi facile à soupçonner.

La page d'accueil du site caché par les codes ASCII :

- tente d'ouvrir une fenêtre qui à priori est bloquée par l'option « Pop-up Blocker » du browser IE,
- puis, redirige sur une page de la banque concernée.

La fenêtre Pop-up représente la tentative de phishing.

L'URL du site hostile reste visible dans les « Temporary Internet Files » de Windows (ceci même si l'option « Pop-up Blocker » a été activée) :



L'outil « nslookup » permet de repérer l'IP de ce site :

```

C:\WINDOWS\system32\cmd.exe - nslookup
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator>nslookup
Default Server: name.nordnet.fr
Address: 194.206.126.253

> cmeuock.nm.ru
Server: name.nordnet.fr
Address: 194.206.126.253

Non-authoritative answer:
Name: flock@ohs.newmail.ru
Address: 212.48.140.151
Aliases: cmeuock.nm.ru

>

```

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

```
inetnum: 212.48.140.144 - 212.48.140.159
netname: NEWMAIL-NET
descr: Network for Newmail mail services
country: RU
admin-c: AZ1254-RIPE
tech-c: AS23384-RIPE
status: ASSIGNED PA
remarks: Please send abuse reports to abuse@newmail.ru
mnt-by: AS6788-MNT
source: RIPE # Filtered
```

```
person: Andrey Zaletkin
address: 8, Gubkina str.,
address: Moscow, Russia
phone: +7 095 9382980
fax-no: +7 095 9382981
e-mail: zaletkin@nc.orc.ru
nic-hdl: AZ1254-RIPE
mnt-by: AS6788-MNT
source: RIPE # Filtered
```

```
person: Aleksandr Sinyakov
address: 8, Gubkina str.,
address: Moscow, Russia
phone: +7 095 9382980
fax-no: +7 095 9382981
e-mail: say@orc.ru
nic-hdl: AS23384-RIPE
mnt-by: AS6788-MNT
source: RIPE # Filtered
```

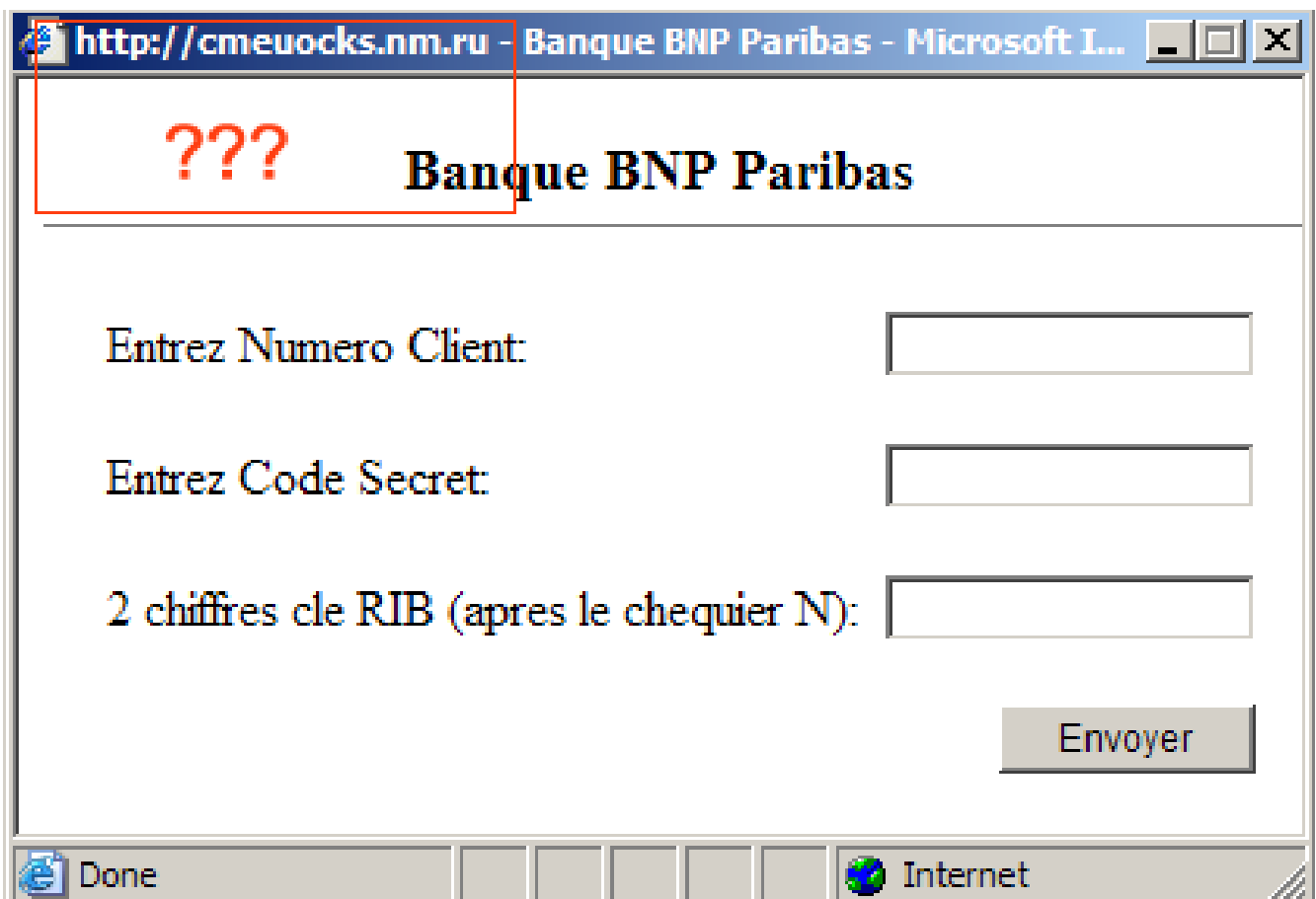
% Information related to '212.48.128.0/19AS6788'

```
route: 212.48.128.0/19
descr: Online Resource Center, ISP
origin: AS6788
mnt-by: AS6788-MNT
source: RIPE # Filtered
```

### 3. Un cas de phishing assez visible :

Les observations habituelles permettent de reconnaître la fraude :

- URL ne correspondant pas à la source (ici, BNP Paribas),
- Demande des identifiants de la carte à débiter dès la première page,
- Absence de clé SSL (icône zone sécurisée) pour un site HTTPS affiché.



#### 4. La redirection vers la banque visée :

Une redirection activée par la page d'accueil du site hostile, télécharge une page du site visé :

BNP PARIBAS | La banque d'un monde qui change - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://www.bnpparibas.com/>

BNP PARIBAS La banque d'un monde qui change

Contact English Plan du site Mentions légales Recherche

Le Groupe Actionnaires / Investisseurs Recrutement Mécénat Sponsoring

Actualités

27/05/05 : La Fondation BNP Paribas et le Prix du Jeune Ecrivain : favoriser l'émergence de jeunes aute...[suite >](#)

26/05/05 : L'Observatoire de la Réputation vient de rendre public son classement 2005 des entreprises d...[suite >](#)

05/27/2005 - 15:25 GMT

BNP Paribas	56.60	+1.34%	▲
CAC 40	4131.83	-0.13%	▼
DJ E.Stoxx50	3084.00	-0.07%	▼

Etudes économiques

A la une cette semaine:

- L'éditorial
- Paroles d'expert
- Focus sur ...

Particuliers En France A l'international

Banque Privée En France A l'international

Professionnels En France A l'international

Entreprises En France A l'international

Associations & Institutions

Accès à vos comptes

Services en ligne Infos utiles Contact

http://cmeuocks.nm.ru - Banque BNP Paribas - Microsoft I...

**Banque BNP Paribas**

Entrez Numero Client:

Entrez Code Secret:

2 chiffres de RIB (apres le chequier N):

Envoyer

Done Internet

## 5. Visite du site hostile :

En utilisant la syntaxe des pages hébergées, nous avons continué la visite le site hostile en demandant la page <http://cmeuocks.nm.ru/5/> avec un « 404 not found » en retour :

The screenshot shows a Microsoft Internet Explorer browser window with the address bar displaying <http://cmeuocks.nm.ru/5/>. The page content is in Russian and features a large "404 Not found" message. The page layout includes a navigation menu at the top, a main heading "ОТДЫХ И ПУТЕШЕСТВИЙ !!!", and several columns of text and links. The browser's address bar shows the URL and the Norton AntiVirus icon.

**Online Resource Center | 404 Not found - Microsoft Internet Explorer**

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Refresh Print Mail Print Mail Print Mail

Address <http://cmeuocks.nm.ru/5/> Go Norton AntiVirus

**Online Resource Center**

· Компания ОРЦ · Доступ в интернет · IP-телефония · Онлайн сервисы · Системная интеграция · Клиентам ·

**404 Not found**

**ОТДЫХ И ПУТЕШЕСТВИЙ !!!**

Лучшие предложения туристических компаний:

Россия	Болгария	Хорватия	Турция	Визы и паспорта
Прибалтика	Испания	Чехия	Крым	Авиабилеты
Франция	Кипр	Тунис	Абхазия	Экзотика
				Круизы

**Печать цифровых фото ONLINE!**

доставка	бесплатно*
10x15,11x15 см	6.50 руб.
15x20,15x21 см	15.00 руб.
20x27,20x30 см	25.00 руб.

**(095) 923-0863**  
**HTTP://FOTO.ORC.RU**

**Çairðàøèààiaÿ Ààìè òððàìèòà íà íàèàáá**

Àíçìíèí, àó òððàèèíó ìòè àáíàà ààðàíà èèè íàððàèè àáí òðííèèèè àóèààèè. Àíèè àó òààðáíó à ìðààèèóííòè òèàçàìíáí ààðàíà, òí àáííáÿ òððàìèòà òæà íà òóóáíòàòáò íà òàððààðà èèè àóèà íàððàèèáááá. Àèÿ òèíèà èíòàðàíòóðáè Ààí èíòòèàòèèè Àó ìæàòà àíííèóçááòóðÿ íàèè Èàðàèáí:

Èíèèè, ìòçóèà è àèàáí  
ìðç, Èèí, Èíèèè, ìòçóèà, Õèèóíó, Õíòí,  
...

Èííóòòàòó è ìððàòòèèèà  
Èííóòòàòó, ÈÈÈ, Ìíèèòòó, Ìòðàòòèè,  
Ìòèòòàòó, ...

Àóòèàáÿ òàòèèèà  
Àðàèòàòòèèèà, Èííàèòèíááó, Èóóèè,  
Ìòèàíííó, Õíèíàèèèèèè, ...

Ñàÿçó  
ÀON, Ìàèíàèè àèÿ òàèàòòíà, Ìàððàòòó  
òòèàíè òàÿçó, Ìòèòàòóà òàèàòòíó, ...

Ààòí-òòí  
Ààòòçàí-àíòè, Ààòííàèèè, Ààòííàèííó,  
Ìòèààæà Ìàèèí, ...

Àíà àèÿ àíà è ìòèà  
Àààòè, Èíòàòòàò, Ìàààèó, Ìèà, ...

Àèçíà è ÿèííèèà  
Ààíèè, Èíàáíòèèèè, Ìàààèèèèííó,  
Ìòàòòèàíèèà, Õíòàíèèÿ, ...

Ìòèçàíàíòàí è òíèèòèè  
Ìàòòàíàíèèà, Ìíèèàòòèè, Èàèèàìà,  
Èàííò, Ìòèòèèèèèèòòàí, ...

Ìàðçàíàíèèà è èàòòàòà  
Ààèàííèè, Èààòàòóà ààáíòòòà,  
Ìáó-àíèà, Ìíèèè òàáíòó, Ìíèèòèíèèÿ, ...

Õóòèçí è ìàóò  
Ààèàèèèèòòó, Àíòóòèà òòààèèè,  
Àííòèèèòó, Ìàáóð ó òòÿ, Èàííèèíàíèèà  
Ìáçàíà, Õóòèçí, ...

Ìíòòò  
Ìííòòèèíóà èèèóá, Õíààòó àèÿ òíòòà,  
Õèòíáí, Õóòàíè, ...

Èòàííòà è çàìòàòà  
Àèàòà, Èííàòòèèà è ìàòòòèàòòèè,  
Ìààèèèíèèèà òàòòó, ...

Àííòà è ìàóò  
Àíòíèèí, Çíàèííòòàà, Èèòó, Èèèóá,  
Ìíààòèè, Èàçàèà-àíèÿ, ...

· Компания ОРЦ · Доступ в интернет · IP-телефония · Онлайн сервисы · Системная интеграция · Клиентам ·

УЧАСТНИК TOP 100 Rambler's

SpyLOG

Я 14000

Copyright © 2003, Online Resource Center

## 6. Actions engagées

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