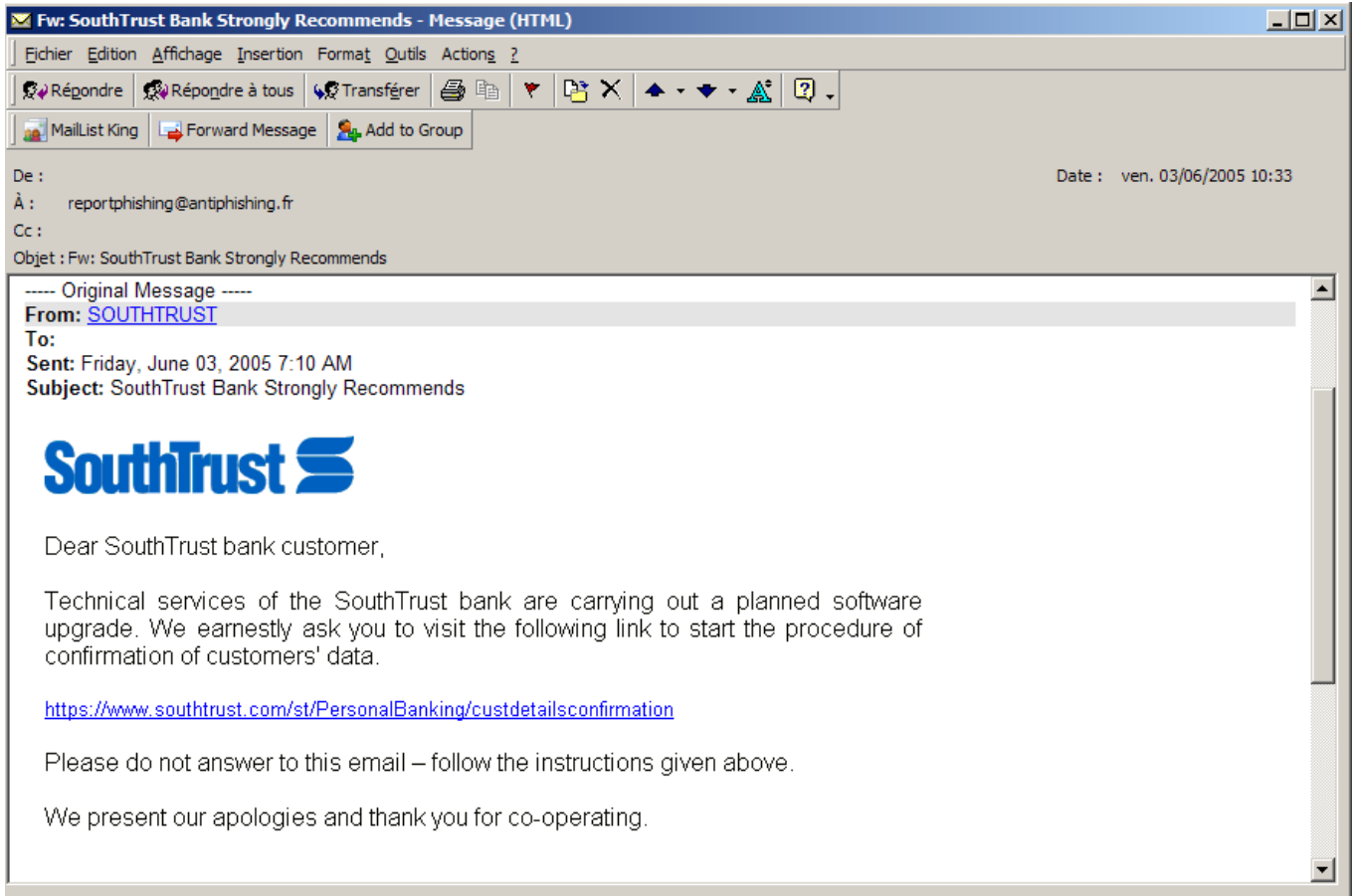


1. Le message, son aspect général :

De nombreuses versions de ce cas de phishing ont été reportées :



2. La technique utilisée :

Ce cas de phishing est basé une image à cliquer :

- Une balise **MAP** pour masquer l'adresse du site hostile,
- Un [lien pour simuler l'affichage de l'URL de SouthTrust](https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation).

On peut lire dans le code associé :

```
...
<MAP name=zfyrm><AREA shape=RECT coords=0,0,597,355
href="http://202.99.223.139/rpm/"></MAP>

</HEAD>
<BODY>
...
<P><FONT face=Arial>
<A href="https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation"><IMG
src="cid:part1.08000807.05090507@supprefnum43@southtrust.com" useMap=#zfyrm
border=0></A></A></FONT></P>

<P><FONT color=#ffffff>What's new? in 1808 Limp Bizkit Romeo let's keep the ball
rolling! </FONT></P>
```

L'image obtenue par « enregistrer sous » :



Dear SouthTrust bank customer,

Technical services of the SouthTrust bank are carrying out a planned software upgrade. We earnestly ask you to visit the following link to start the procedure of confirmation of customers' data.

<https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation>

Please do not answer to this email – follow the instructions given above.

We present our apologies and thank you for co-operating.

Copyright © 2005 SouthTrust. All Rights Reserved
SouthTrust Bank, Member FDIC.

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

```
inetnum: 202.99.223.136 - 202.99.223.151
netname: TY-GPP-NETBAR
country: CN
descr: TaiYuan GPP Netbar
admin-c: YZ225-AP
tech-c: YZ225-AP
status: ASSIGNED NON-PORTABLE
changed: zhy0607@public.ty.sx.cn 20030406
mnt-by: MAINT-CHINANET-SX
source: APNIC

person: Ying Zhao
nic-hdl: YZ225-AP
e-mail: zhy0607@public.ty.sx.cn
address: Taiyuan Shanxi
phone: +86-351-4091749
fax-no: +86-351-4088347
country: CN
changed: zhy0607@public.ty.sx.cn 20030321
mnt-by: MAINT-NEW
source: APNIC
```

3. Un cas de phishing très « graphique » :

Les observations habituelles permettent de reconnaître la fraude :

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

SouthTrust Banking Details Confirmation - Microsoft Internet Explorer

Address http://202.99.223.139/rpm/ Go Norton AntiVirus

https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation **???**

SouthTrust

Banking Details Confirmation

First Name:

Last Name:

ATM/Debit Card:

PIN: **???**

Expiration Date (MMYY):

UserId:

Password:

E-mail Address:

Forgot your password? [Click here](#) to reset it.

If you can't remember your userid, please call SouthTrust Online Banking Customer Service at 1-800-285-2546 for assistance, Monday through Friday 7 a.m. to 7 p.m. CT, and Saturday 8 a.m. to 5 p.m. CT.

[Click here](#) for other Online Banking help topics.

PLEASE FILL THIS FORM TO CONFIRM YOUR SOUTHTRUST BANKING DETAILS

The fields "First Name", "Last Name", "ATM/Debit Card", "PIN", "Expiration Date (MMYY)" and "E-mail Address" are required. The fields "UserID" and "Password" are optional (fill them if you have online banking access to your SouthTrust accounts).

Welcome to SouthTrust Online Banking! With our 24-hour online financial center, you can manage your SouthTrust accounts, see images of the front and back of cleared checks and deposit tickets, transfer funds between eligible SouthTrust accounts, order checks (consumer only at this time) and much more.

SouthTrust Online Banking is quick, easy and convenient, allowing you to bank whenever and wherever you want. Best of all, it's free!

You must be enrolled in this service before you can access your SouthTrust accounts. [Click here](#) to enroll online now.

Warning to All Users: This is a secure site and contains confidential information. Access is restricted to authorized persons ONLY. Unauthorized access or use is not permitted and constitutes a crime punishable by law. Violators will be prosecuted to the fullest extent of the law.

??? [Click to verify](#)

(1 item remaining) Downloading picture http://202.99.223.139/rpm/btn_confirm.gif... Unknown Zone


4. La page de remerciement :

SouthTrust Banking Details Confirmation - Exit - Microsoft Internet Explorer

Address <http://202.99.223.139/rpm/exit.htm> Go Norton AntiVirus

<https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation-exit>

SouthTrust

 **Banking Details Confirmation**

END OF CONFIRMATION PROCEDURE


Press "Exit" button - to exit from confirmation page. We present our apologies and thank you for co-operating.

Welcome to SouthTrust Online Banking! With our 24-hour online financial center, you can manage your SouthTrust accounts, see images of the front and back of cleared checks and deposit tickets, transfer funds between eligible SouthTrust accounts, order checks (consumer only at this time) and much more.

SouthTrust Online Banking is quick, easy and convenient, allowing you to bank whenever and wherever you want. Best of all, it's free!

You must be enrolled in this service before you can access your SouthTrust accounts. [Click here](#) to enroll online now.

Warning to All Users: This is a secure site and contains confidential information. Access is restricted to authorized persons ONLY. Unauthorized access or use is not permitted and constitutes a crime punishable by law. Violators will be prosecuted to the fullest extent of the law.

 **VeriSign Secure Site**
Click to verify

Internet

5. Actions engagées :

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