

1. Le message, son aspect général :

La technique utilisée est un lien à cliquer « [clicking here](#) »:

De : SouthTrust Bank

A :

Date : 14/07/2005 01:37

Objet: Customer notice - instructions for client



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.

Les journaux de notre passerelle contiennent des traces intéressantes :

...

X-mxGuard-Sender:

X-mxGuard-Virus-Info: Infected [**HTML.Phishing.Bank-22**]

Cette tentative est donc parfaitement par ClamAV (antivirus “libre” applicable entre autre à une passerelle SMTP)

2. L'ergonomie du site « piège » :

SouthTrust Banking Details Confirmation - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Address <http://210.221.118.61:680/rock/st/> Go Norton AntiVirus

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

SouthTrust 210.221.118.61 ???

Banking Details Confirmation

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.

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.

Confirm

VeriSign Secure Site
Click to verify

Copyright © 2005 SouthTrust. All Rights Reserved

Internet

L'ergonomie peut paraître celle de SouthTrust. Les points suivants attirent l'attention :

- l'absence de session HTTPS,
- l'adresse 210.221.118.61 obscure,
- et surtout, la demande des identifiants de la carte de crédit sur une page d'accueil !

3. Le Whois renvoie vers un site en Corée :

Whois 210.221.118.61 ?

inetnum: 210.220.128.0 - 210.223.255.255
netname: KRNIC-KR
descr: KRNIC
descr: Korea Network Information Center
country: KR

inetnum: 210.221.118.0 - 210.221.118.255
netname: THRUNET-INFRA-KR
descr: Thrunet Co., Ltd.
descr: Thrunet IDC B/D, 1338-5, Seocho-2dong, Seocho-ku
descr: SEOUL
descr: 137-072
country: KR
admin-c: IA14558-KR
tech-c: IM18428-KR

4. Les actions engagées :

- Rédaction de ce document,
- Remontée au niveau « .org » effectuée.