There are no translations available.
Últimamente, todos los que disponemos de una cuenta de correo, hemos recibido mensajes procedentes de distintos bancos...

Últimamente, todos los que disponemos de una cuenta de correo, hemos recibido mensajes procedentes de distintos bancos. En estos mensajes se nos pide que pulsemos un link que nos conduce a una página y una vez allí, se nos indica que debemos completar un formulario con nuestros datos bancarios.

Normalmente estos correos nos informan de que debido a problemas de seguridad, intrusiones o alguna otra incidencia debemos ratificar los datos de nuestra. Estos correos, que nada tienen que ver con los bancos, son el anzuelo que nos lanzan unos piratas informáticos que quieren robar nuestros datos.

La práctica de suplantar la identidad de una empresa u organismo para poder acceder a los datos de sus clientes se denomina PHISING.

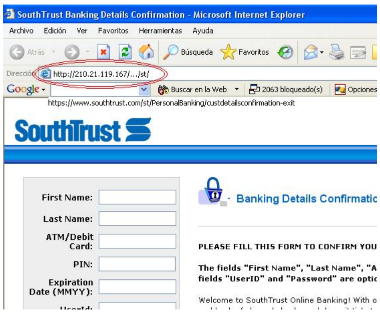
Según la página Wikipedia:

Phishing *es la capacidad de duplicar una página web para hacer creer al visitante que se encuentra en la página original en lugar de la copiada. Normalmente se utiliza con fines delictivos duplicando páginas web de bancos conocidos y enviando indiscriminadamente correos para que se acceda a esta página a actualizar los datos de acceso al banco.*

En ocasiones, el término "phishing" se dice que es la contracción de "password harvesting fishing" (cosecha y pesca de contraseñas), aunque esto probablemente es un acrónimo retroactivo.

De forma más general, el nombre phishing también se aplica al acto de adquirir, de forma fraudulenta y a través de engaño, información personal como contraseñas o detalles de una tarjeta de crédito, haciendose pasar por alguien digno de confianza con una necesidad verdadera de tal información en un e-mail parecido al oficial, un mensaje instantáneo o cualquier otra forma de comunicación. Es una forma de ataque de la ingeniería social.

Cuando pulsamos el link que nos mandan en el correo, accedemos a una página que tiene la misma apariencia que la original pero que en realidad no es más que una réplica de la misma. Para una persona que esté acostumbrada a navegar por internet es fácil darse cuenta de que la página no es la original. Si nos fijamos en la barra de navegación veremos que la página que estamos visitando está alojada en un servidor que ni siquiera tiene un nombre de dominio asociado sino que es de la forma:


SouthTrust Banking Details Confirmation - Microsoft Internet Explorer
Archivo
Edición
Ver
Favoritos
Herramientas
Ayuda
Atrás
Búsqueda
Favoritos
Dirección
http://210.21.119.167/.../st/
Google
Buscar en la Web
2063 bloqueado(s)
Opciones
https://www.southtrust.com/st/PersonalBanking/custdetailsconfirmation-exit
SouthTrust
Banking Details Confirmatic
First Name:
Last Name:
ATM/Debit Card:
PIN:
Expiration Date (MMYY):

PLEASE FILL THIS FORM TO CONFIRM YOU

The fields "First Name", "Last Name", "A
fields "UserID" and "Password" are optic

Welcome to SouthTrust Online Banking! With o

La mejor manera de no ser victima de phising es tener muy claro que **nuestro banco no nos va a pedir nuestros datos de cuenta a través de un email**

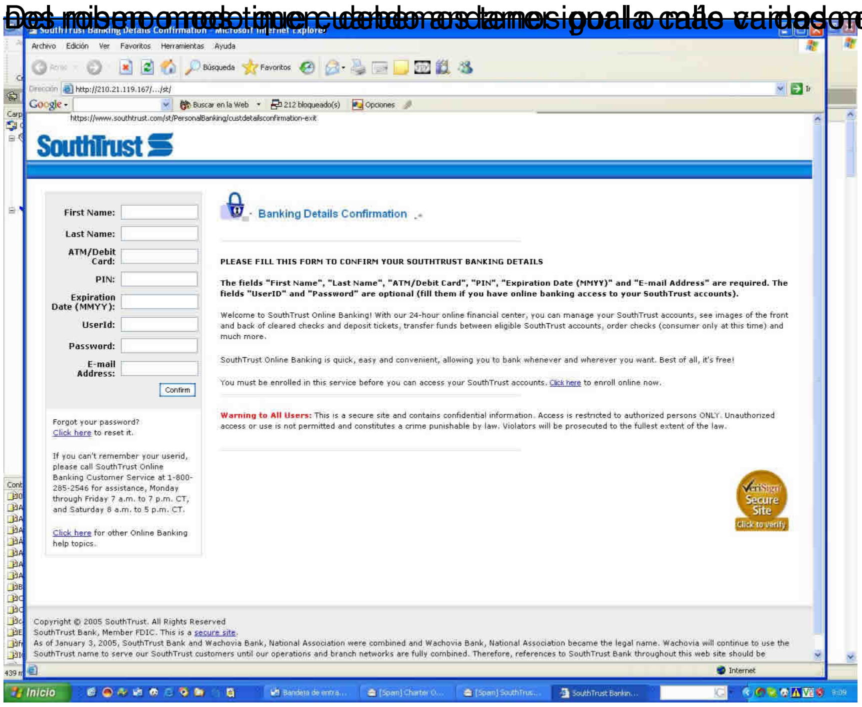
. Ni Hotmail, ni Yahoo, ni Microsoft, ni Paypal, ni Ebay, ninguna de estas grandes compañías utilizan estos métodos. Aún así, si alguna vez recibimos un correo de este tipo y consideramos que puede ser un mail "legitimo" debemos tener algunas precauciones:

- Accederemos a la web de la compañía a través de su dirección pública y no a través del enlace del correo.

- En caso de no estar 100% seguro, debemos buscar un mail o teléfono de soporte para consultar si están ejecutando alguna campaña de ese tipo y si realmente nuestra cuenta tiene algún problema.

Lo que se muestra a continuación son ejemplos de correos de este tipo

[illegible]



http://210.21.119.167/.../st/

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

First Name:
Last Name:
ATM/Debit Card:
PIN:
Expiration Date (MMYY):
UserId:
Password:
E-mail Address:
Confirm

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.

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.

Copyright © 2005 SouthTrust. All Rights Reserved
SouthTrust Bank, Member FDIC. This is a secure site.
As of January 3, 2005, SouthTrust Bank and Wachovia Bank, National Association were combined and Wachovia Bank, National Association became the legal name. Wachovia will continue to use the SouthTrust name to serve our SouthTrust customers until our operations and branch networks are fully combined. Therefore, references to SouthTrust Bank throughout this web site should be