



Rabobank

Rabopass

Doble seguridad para su dinero

Rabobank Chile

¿Qué es Rabopass?



- Rabopass surge de la necesidad de entregar a nuestros clientes un sistema de doble autenticación, basado en:

Algo que usted **sabe** + Algo que usted **tiene**

Usted sabe **su clave** + tiene **su Rabopass**

Introducción a la Seguridad



“La información es un activo que, al igual que otros activos importantes para su negocio, tiene valor para la organización y consecuentemente necesita ser protegido apropiadamente.”

TRIADA DE LA SEGURIDAD



¿En qué consiste la tríada de la Seguridad de la Información?



- **Confidencialidad:**
Que la información sólo sea accesible para quien esté autorizado para ello.
- **Disponibilidad:**
Que la información esté disponible cuando se la requiera.
- **Integridad:**
Que la información no sea alterada.

Riesgos de la Información Personal



- La información personal, es decir, los **datos confidenciales** de una persona, no sólo pueden quedar expuestos por falta de resguardo en una empresa en donde ella sea cliente, sino también por **su propio desconocimiento** y/o negligencia.
- Así, por ejemplo, las personas pueden, sin saberlo, permitir que terceros accedan a sus **datos confidenciales** a partir de ser víctimas de técnicas de **ingeniería social**, que las llevan a revelar, por ejemplo, sus contraseñas. Esto puede darse, entre otros, a través de llamados telefónicos o correo electrónico, que simulan provenir desde una fuente confiable.

¿Qué es la Ingeniería Social?



- Es una práctica que busca **explotar la confianza de las personas para obtener información confidencial** o hacer que falten a las medidas de seguridad establecidas.
- Con este término se engloba una serie de tretas, artimañas y engaños elaborados cuyo fin es confundir al usuario o, peor todavía, lograr que comprometa seriamente la seguridad de sus sistemas.
- Aprovecha sentimientos tan variados como curiosidad, la avaricia, el sexo, la compasión o el miedo.

Seguridad de la Información: Problemas Actuales



- Un cliente de un banco puede realizar una transacción desde un computador en donde puede haberse instalado software que registra los datos que ingresa en el teclado (Usuario y Contraseña). Dichos datos pueden incluso ser rastreados remotamente, vía Internet. Ejemplo: Caso del cibercafé en Aeropuerto de Santiago.
- A partir del aumento de las transacciones electrónicas, el **robo de identidad** para cometer fraudes vía Internet se ha convertido en uno de los principales objetivos de los ciberdelincuentes. De hecho, se estima que los fraudes on-line aumentaron el 2007 en un 40% a nivel mundial.
- Por lo tanto, las formas de autenticación tradicional ya no son suficientes, haciéndose cada día más necesaria la **autenticación robusta** o de **doble factor**, en tanto minimiza los riesgos para los clientes y las propias empresas e instituciones financieras.

Algunas Cifras sobre Phishing...



- El Phishing tiene una “tasa de éxito” superior al Spam o correo electrónico no deseado. Mientras el Spam genera respuestas de un 1%, el Phishing alcanza aproximadamente un 5% de respuestas.
- Cada víctima de Phishing es estafada, en promedio, en 1.200 dólares.
- Hasta el año pasado, se consideraba que los fraudes electrónicos a nivel mundial ya acumulaban más de mil millones de dólares en pérdidas

Debilidades de Autenticación Simple



- Los procesos de autenticación de usuarios actuales, enfrentan los siguientes problemas o debilidades:
 - - Las personas ingresan claves fáciles de detectar.
 - Las personas escriben sus claves en lugares accesibles.
 - Las password o contraseñas pueden ser capturadas fácilmente por hackers (keylogger, hombre en el medio, troyanos, sitios falsos).
 - Las claves exigen ciertos niveles de seguridad: como cantidad de dígitos, códigos alfanuméricos, que dificultan recordarlas.

¿Qué es Autenticación Robusta?



- Autenticación Robusta es la combinación de dos o más factores de autenticación.
- Los factores de Autenticación son:
 - 1° Algo que se “sabe”:
 - ID de usuario, password, PIN
 - 2° Algo que se “tiene”
 - Token, smartcard
 - 3° Algo que se “es”
 - Biométrica (Voz, huella digital, escaneo de retina)

La Autenticación Robusta ayuda a resolver:



- Autenticación & Autorización
 - Determinar ¿Quién es?
 - Obtener un acceso correcto
 - Validar un proceso
- Integridad
 - Mantener la información completa y sin cambios
- No-Repudio
 - Asegurar que el proceso fue realizado por la persona autorizada
 - Prevenir la negación de su ejecución

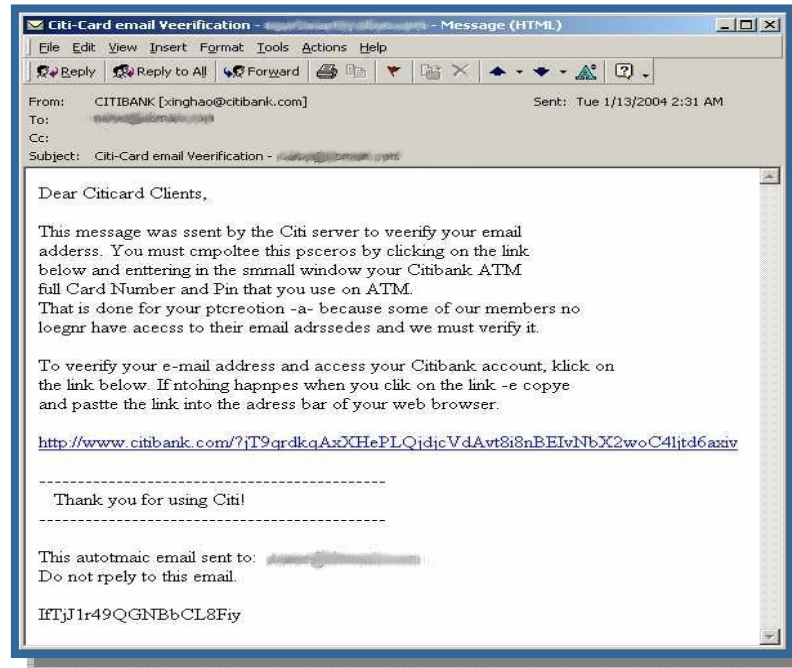
¿Qué es el Phishing?



- El 'phishing';
 - Es el envío masivo de mensajes electrónicos que fingen ser notificaciones oficiales
 - Busca obtener datos personales y bancarios de los usuarios
 - La finalidad es suplantar a una persona para realizar transacciones 'on line' fraudulentas
- ¿Cómo llegar a la víctima?
 - Primero envían spiders para capturar e-mails
 - Luego las validan enviando Spam con el mensaje "remuévanme de esta lista"
 - Creación de una lista válida
 - Arman un sitio Web falso hosteado en algún servidor vulnerable
 - Empieza "la pesca" de contraseñas y datos personales



Anzuelo...



- Envío masivo de correos
- Intentan bypassar los filtros Spam (por ej., reemplazando letras).
- Utilizan cadenas para que su víctima le envíe el mail a otras víctimas.

Camuflaje...



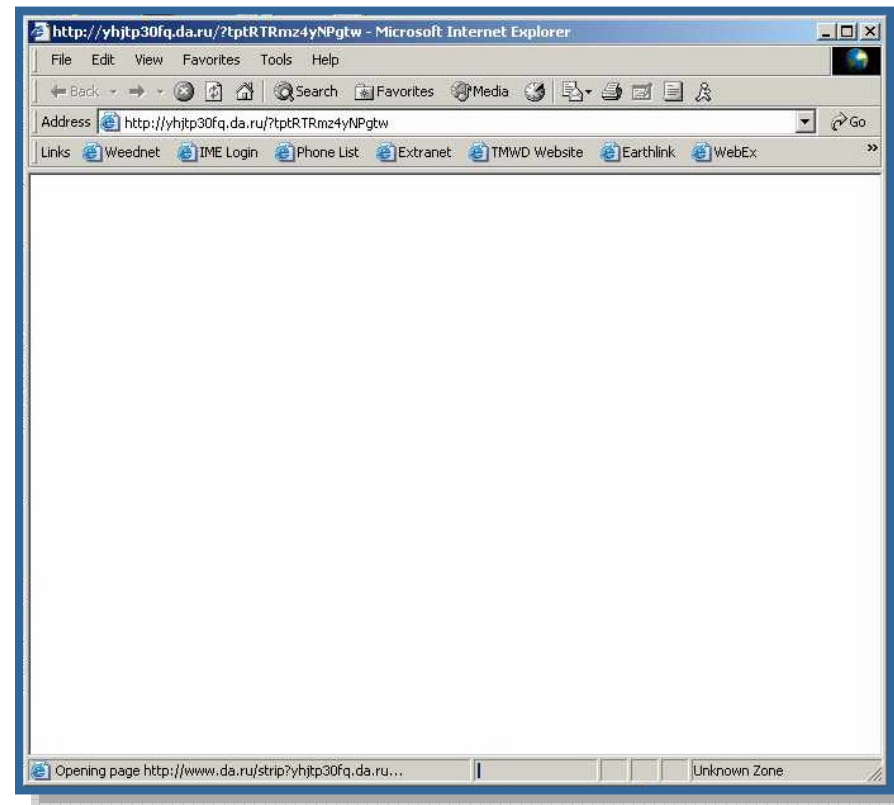
Rabobank

- Siempre utilizarán en el subject del correo información que aparenta ser de utilidad para la víctima.
 - También hay correos que se aprovechan de los sentimientos de las personas.
- [ATTENTION TO ALL SunTrust Bank CLIENTS](#)
 - [Temporary Account Suspension](#)
 - [CONGRATULATION CONGRATULATION CONGRATULATION!!!](#)
 - [Citizens Bank reminder: please update your details](#)
 - [CALL FROM SUDANESE REFUGEE](#)
 - [PayPal Important Warning Second Notice](#)
 - [fdic.gov URGENxk](#)
 - [Customer Notice - Instructions For Client](#)
 - [MESSAGE FROM AN ACCOUNTANT](#)
 - [WE CAN MAKE THIS WORK!!!!!!](#)
 - [Shawn John from Suntrust.com, alez](#)
 - [PLEASE HELP ME](#)
 - [BUSINESS TRANSACTION](#)
 - [UPDATE YOUR ACCOUNT RECORDS](#)
 - [Please Help the victim in Beslan!](#)

Carnada...



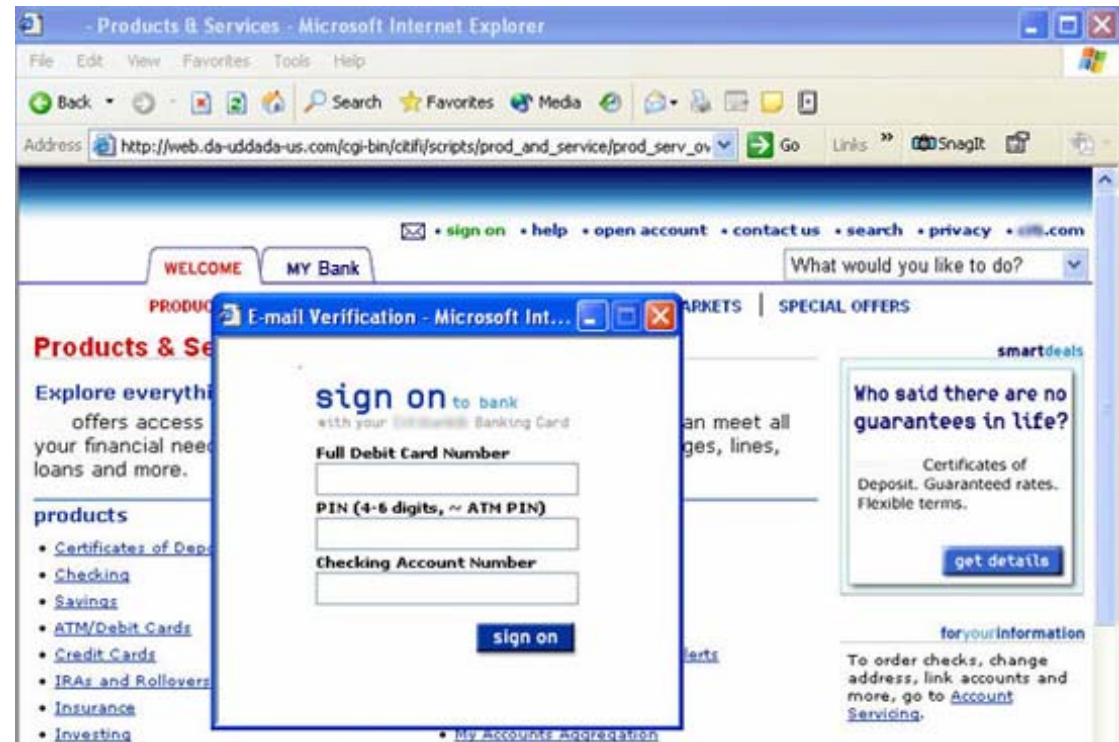
- Harán caer a sus víctimas haciéndolos pensar que han entrado en un sitio web original.



Recogiendo el anzuelo...



- La víctima ingresará datos confidenciales que serán utilizados en futuras suplantaciones de identidad.



- Recuerde:
 - El sistema que está implementando Rabobank Chile evita que sus clientes comprometan sus contraseñas, ya que son aleatorias y dinámicas

Rabopass



- Es un dispositivo de Autenticación Robusta.
- Su fabricante es VASCO Data Security International.
- Usado de forma masiva por Rabobank
- Características principales:
 - Dispositivo de seguridad altamente robusto
 - Requiere un PIN de acceso
 - Generador de códigos
 - Contraseñas o passwords aleatorias y dinámicas
 - Hermético



Tecnología Rabopass



- Rabobank utiliza la más avanzada tecnología de administración de claves de seguridad disponible en el mercado, que permitirá a sus clientes una conexión segura a www.rabobank.cl.
- Rabopass es la clave que le abre las puertas a www.rabobank.cl.
- Rabopass funciona sobre la base de una clave fija, la cual sólo el cliente conoce, reforzada con una segunda clave de carácter aleatorio.
- En conjunto permiten:
 - Ingresar a Banca en Línea.
 - Autorizar movimientos bancarios (transferencias, pagos, etc.).

Nivel de seguridad óptimo



- Rabopass permite conectarse a Banca en Línea y efectuar transacciones de forma segura en www.rabobank.cl
 - Eleva los niveles de seguridad actuales
 - Elimina la contraseña estática
 - Permite validar al usuario que realiza la transacción
 - Código generado en el Rabopass (Firma electrónica).
 - Por sus características, protege a los clientes y evita una transacción fraudulenta.
 - Un dispositivo por cada usuario
 - Todos generan códigos distintos
 - Tecnología probada y validada desde hace 15 años en prestigiosas empresas del mundo.

Seguridad de Rabopass



- ¿Es más seguro que la contraseña estática o actual?
 - La tecnología Rabopass es mucho más segura
 - El usuario dispone siempre de dos elementos para poder autenticarse
 - Se requiere un PIN de acceso que sólo el usuario conoce
 - Rabopass genera un único código, el cual cambia pasados unos segundos.
 - La contraseña estática siempre es la misma, por lo cual puede ser adivinada o crakeada.
 - Altamente vulnerable al Phishing
 - La contraseña generada por Rabopass:
 - Cambia constantemente (en segundos)
 - Válida para una sola sesión
 - Utiliza algoritmos de seguridad que evitan su predicción

Precauciones de seguridad



- Rabopass es un dispositivo altamente seguro pero, en tanto es operado por personas, se debe tener presente algunas consideraciones de seguridad adicionales
 - El usuario debe seguir tres normas básicas de uso:
 - Nunca revelar el PIN de acceso al Rabopass
 - El PIN de acceso siempre debe ser guardado separado del Rabopass
 - Nunca dejar abierto su computador y a vista de todo el mundo cuando se conecte
 - Precauciones de seguridad adicionales
 - Cuidados físicos
 - Mantener libre de altas temperaturas
 - Mantener libre de humedad
 - Mantener libre de golpes
 - Cuidados especiales.
 - Dejar fuera del alcance de los niños
 - Dejar fuera del alcance de todos los demás

Información de apoyo



- ¿Qué le puede pasar a Rabopass?
 - Extraviado
 - Perdido
 - Bloqueado el PIN (después de cinco intentos fallidos)
 - Bloqueado el acceso www.rabobank.cl
 - PIN vulnerado
 - PIN olvidado
 - Deteriorado por mal uso

Para todos estos casos se ha habilitado una Mesa de Ayuda

Mesa de ayuda: 800 47 6000



- Servicios que presta
 - Ayuda en uso de Rabopass.
 - Ayuda a solucionar problemas con el Rabopass.
 - Atiende las solicitudes de Reposición o entrega de Rabopass.
 - Atiende servicios de Bloqueo del Rabopass ante su pérdida u olvido de PIN.
- Horarios de atención
 - Servicio de atención normal
 - Lunes a viernes de 08:30 a 18:00 horas (todo tipo de requerimientos)
 - Días y horarios no hábiles.
 - Servicio de emergencia (Bloqueos de Rabopass)

Conclusiones



- Rabobank tiene 15 años de experiencia en estándares de seguridad para Banca en Línea.
- Rabopass funciona tanto para acceder a la página web del Banco, como para autorizar transferencias de fondos, siendo Rabobank el único banco en Chile, que administra ambas claves con el mismo dispositivo.
- El **800 47 6000** está exclusivamente disponible para cualquier necesidad que tengan nuestros clientes respecto del Rabopass.
- Existe un mini sitio, accesible desde www.rabobank.cl, con abundante información disponible acerca de Rabopass.
- La migración de nuestros clientes a este nuevo sistema terminará el 31 de Marzo de 2008.



Rabobank

Rabopass

Doble seguridad para su dinero

Rabobank Chile