




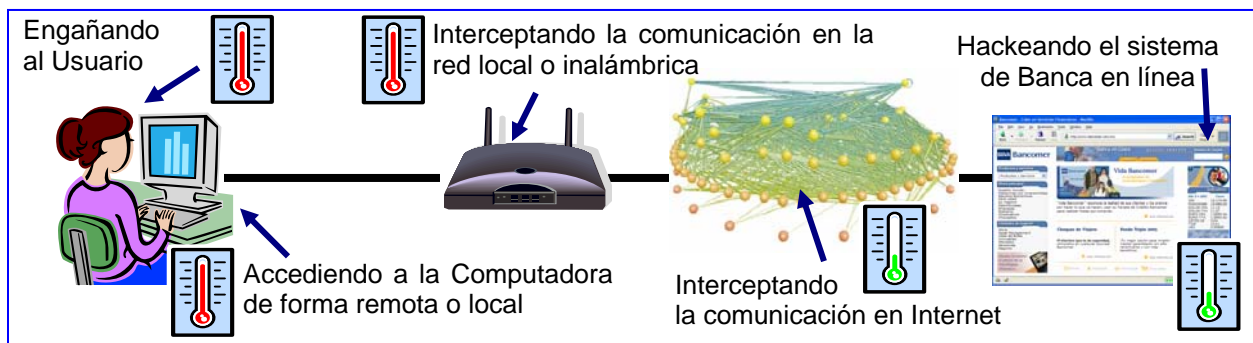
El número de fraudes por medios electrónicos ha crecido de forma exponencial en los últimos años. Bandas organizadas y ladrones astutos han usado Internet como un nuevo medio para atacar y defraudar a usuarios, empresas e instituciones.

Defenderse de este tipo de ataques es difícil cuando se desconoce la forma de proceder y de pensar de los atacantes. Con algunas medidas sencillas de precaución se puede reducir mucho el riesgo.

El objetivo principal del atacante normalmente va a ser tener acceso a las cuentas bancarias o número de tarjeta de crédito de la víctima para poder transferir dinero o hacer cargos de forma ilícita. Para ello puede atacar en diferentes lugares.

	Alto Riesgo o Muy Frecuente
	Riesgo Medio o Poco Frecuente
	Bajo Riesgo o Muy Poco Frecuente

Puntos Principales de Ataque



Actualmente los principales riesgos de fraude se concentran del lado del usuario final.

Engañando al Usuario

En una acción también conocida como “ingeniería social” el defraudador busca hacerse pasar por el Banco o por una persona o entidad conocida para engañar al usuario. Con el engaño pretende robar información confidencial o instalar un programa. Algunas de las tácticas más comunes son:

Phishing – Mandar un correo electrónico falso que parece ser del banco para pedir información de su tarjeta o cuenta de banco. Estos correos normalmente redirigen al usuario a un sitio de Internet que puede ser una copia exacta del sitio del Banco.



Sugerencia: El Banco no le va a enviar a usted ningún correo con vínculos directos a la página ni solicitándole información. Si tiene cualquier duda, diríjase directamente a la página del Banco o llame a atención al cliente.

Engaño Telefónico – También pueden hablar haciéndose pasar por un ejecutivo del Banco o de algún otro lado conocido para pedir información confidencial, número de tarjeta o incluso el usuario y contraseña.



Sugerencia: Nunca de información bancaria a un desconocido que le llame por teléfono. Si es algo importante, pídale su teléfono y márquele de regreso para asegurar que sea quien dice ser.

Engaño para ejecución de un Programa – También es muy común que el atacante envíe un archivo por correo electrónico o por mensajería instantánea que parezca ser otra cosa (una foto,

un video, un documento) para engañar al usuario a que lo abra. Es frecuente también que este tipo de programas ocultos los suban a redes peer-to-peer como Napster, Kazaa, eDonkey o Gnutella. Al abrir el archivo se ejecuta un instalador que introduce un troyano o puerta trasera a la computadora de la víctima. Generalmente manda un mensaje de error ficticio. De ese momento en adelante, el atacante tendrá acceso total e irrestricto a la computadora remota como si estuviera sentado frente a ella. Puede ver toda la información del disco duro, ejecutar programas, espiar al usuario e incluso conectarse al Banco para hacer transacciones.



Sugerencia: Nunca abra archivos adjuntos que usted no solicitó, aun cuando parezca venir de una fuente confiable. Mantenga su antivirus prendido y actualizado.

Engaño por Navegación en Internet – Una técnica común para introducir troyanos o spyware es por medio de descargar de forma automática aplicaciones cuando uno entra en un sitio Web. Hay aplicaciones que se instalan automáticamente sin solicitar confirmación del usuario utilizando fallos del navegador o aprovechándose de que no tiene criterios de seguridad adecuados. Una vez instalados puede ser muy difícil quitarlos, terminando en ocasiones con la necesidad de reinstalar el equipo. Estos programas les permiten a los defraudadores conseguir información personal y confidencial, incluyendo las contraseñas de acceso al sistema del banco.



Sugerencia: nunca diga que sí a la instalación de software desde Internet al menos que confíe totalmente en la fuente. Trate de no navegar en sitios de dudoso origen ni seguir ligas no solicitadas. Si sospecha tener spyware instalado no accese a Banca en línea hasta no haberlo removido. Y de nuevo, mantenga su antivirus prendido y actualizado.

Hackeando la Computadora de forma Local o Remota

Hay ataques directos a la computadora que permiten al defraudador instalar herramientas de control remoto o de espionaje. Hay ataques locales (cuando tiene acceso directo a la computadora) o remotos (utilizando la red local o Internet para acceder y manipular el equipo).

Acceso Directo a la Computadora

Cuando el atacante tiene acceso directo a la computadora, puede agregar dispositivos físicos como grabadoras del teclado que son pequeños cilindros que se instalan entre el cable del teclado y la computadora y que permiten guardar todo lo que el usuario escriba, incluyendo contraseñas. También puede instalar troyanos, puertas traseras o aplicaciones para espiar al usuario.



Sugerencia: nunca use una computadora pública o poco confiable para conectarse a Banca en línea. Preste su computadora solamente a personas a quienes les tenga mucha confianza. Cuando deje la computadora desatendida siempre déjela solicitando contraseña y bajo ninguna circunstancia le dé su contraseña de acceso a nadie. Es una buena práctica que el protector de pantalla pida contraseña.

Acceso Remoto a la Computadora

Al estar conectado el usuario a Internet de forma directa o a una conexión de red local, un atacante puede manipular remotamente las aplicaciones y servicios de la computadora del usuario para intentar controlarla. Hay muchos fallos de los sistemas operativos y aplicaciones comerciales que permiten que un atacante tome control remoto de una computadora. Una vez que el atacante logra transferir y ejecutar sus programas, puede controlar de forma total el equipo permitiéndole instalar troyanos, puertas traseras o spyware.



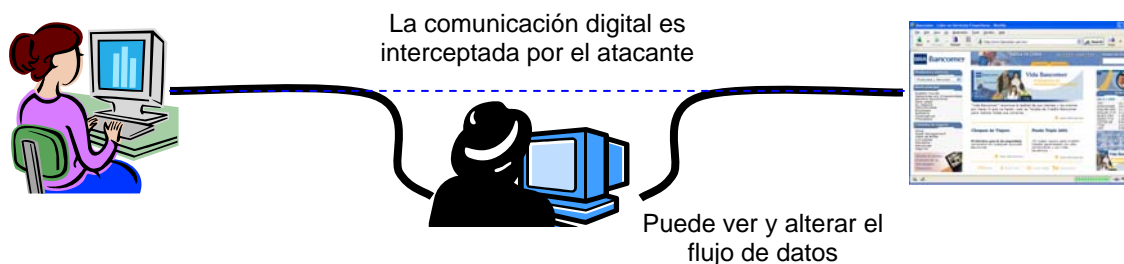
Sugerencia: Tener un firewall personal instalado y prendido en todo momento. Constantemente actualice y parche todos los programas que tenga instalados. Desinstalar o apagar todos los programas o servicios que no utilice. Estar pendiente de cualquier funcionamiento anómalo de su computadora.

Interceptando la Comunicación en la Red Local o Inalámbrica

La comunicación entre su computadora y el banco puede ser interceptada por un atacante que se conecte a la misma red que usted. Al estar conectados en la misma red puede desviar tráfico para interceptar la comunicación con el banco o incluso sus correos electrónicos, mensajes instantáneos, etc. Es importante por ello considerar el nivel de confianza que tiene en la red a la que se conecta.

Ataque de “man-in-the-middle”

En este ataque que en inglés significa “hombre en medio” el defraudador se coloca entre el sitio del banco y la computadora del usuario. Toda la información que viaja de ida y vuelta entre el banco y el usuario puede ser vista y modificada por la computadora del atacante.








El defraudador por lo tanto, podría interceptar una transacción y poner su propio número de cuenta, antes de que la información llegue al Banco. Este tipo de ataque se realiza sobre todo en la red local



Sugerencia: Si en cualquier momento el navegador le manda un aviso de que el certificado no es válido al intentar entrar al portal del Banco, **NO se conecte**, su sesión podría estar siendo interceptada.

Redes Hostiles – Riesgo de Interceptación

Entre más pública sea la red a la que se conecte más probabilidad hay de que su comunicación pueda ser interceptada.

	Computadoras de uso Público (cafés Internet, universidades, etc.)
	Redes Inalámbricas Públicas (hoteles, aeropuerto, restaurantes, etc)
	Redes Inalámbricas Privadas pero desprotegidas* (casa, oficina, universidad, etc.)
	Redes Privadas Cableadas o Inalámbricas Protegidas (casa u oficina)
	Computadora Personal conectada directo a Internet (con firewall personal) (vía MODEM, ADSL, MMDS)

*Las redes inalámbricas se pueden acceder por medio de antenas, por lo que si no está protegida (cifrando la comunicación), cualquier persona ajena se puede conectar, espiar la transferencia de información o hacer mal uso.

Sugerencia: Para acceder a Banca en línea o a información confidencial como puede ser su correo electrónico, sólo conéctese a través de redes privadas confiables como puede ser la red

de su oficina o la de su casa. Es también una buena práctica conectar la computadora directamente a Internet por MODEM o por algún servicio de banda ancha. En el caso de la conexión directa, no olvide asegurarse de tener instalado y prendido un firewall personal. Y si cuenta con una red inalámbrica, asegúrese de que este protegida al agregarle un cifrado WEP. Si cuenta con una VPN cifrada hacia su trabajo, utilícela siempre para garantizar un canal seguro. Esto mitiga casi totalmente el riesgo, aún en redes hostiles.

Intercepción de Comunicación en Internet o Hackeo del Sistema Bancario

Aun cuando este tipo de ataques se han llegado a dar esporádicamente en el mundo, es muy poca la incidencia y la probabilidad de que sucedan. El esfuerzo de muchos expertos está enfocado en prevenir este tipo de ataques y garantizar la legitimidad y seguridad de las transacciones de los clientes bancarios.



Sugerencia: Si se detecta cualquier anomalía en el comportamiento del sistema es mejor proceder con precaución. El área de servicio al cliente con gusto le responderá cualquier pregunta que pudiese surgir.

Sugerencias de Seguridad para Viajeros

- No utilice redes hostiles para conectarse al Banco o a cualquier sitio donde le pida un usuario y contraseña confidenciales.
- Siempre deje encendido su firewall personal.
- Mantenga su antivirus prendido y actualizado.
- Utilice contraseñas complejas de inicio (al encender) y otra diferente para entrar a Windows.
- Agregue la opción de contraseña en el protector de pantalla.
- Guarde un respaldo completo en un lugar seguro.
- Mantenga siempre su computadora con usted.
- Si tiene una VPN cifrada hacia su trabajo, utilícela siempre para garantizar un canal seguro. Esto mitiga casi totalmente el riesgo, aún en redes hostiles.

¿Cómo escojo una contraseña buena?

Algo importante de considerar es que los ataques que se hacen a las contraseñas se realizan de forma automatizada. Es decir, el atacante va a probar usando diccionarios con todas las palabras, en varios idiomas y combinándolas con números. Por lo tanto, para protegerse de ataques contra su contraseña se recomienda:

1. Hacer una contraseña compleja de más de 8 caracteres y que contenga una combinación de minúsculas, mayúsculas, números y caracteres especiales. Un ejemplo de una contraseña difícil sería "Kr\$Qt2p?".
2. Las contraseñas más críticas, como la Bancaria, no la use en ningún otro lado. De forma que si alguien tiene acceso a su contraseña del correo electrónico, no pueda con ella transferir dinero después.
3. Para recordar su contraseña más fácilmente, trate de pensar en una frase y no en una palabra. Es más fácil hacer contraseñas buenas si utiliza una frase y luego la abrevia. Por ejemplo: piense en "¡Los 3 reyes Magos traen más dinero!" y conviértala en algo como "L3rMt+\$!".

¿Qué es un Hacker?

El término originalmente se usaba para describir a una persona ingeniosa y hábil en la programación, configuración y manipulación de tecnología. El término en inglés se usa todavía hoy con este sentido. Sin embargo, en los últimos años, la prensa ha utilizado el término como sinónimo de criminal cibernético, desvirtuando con ello el significado original. Hoy se clasifican los Hackers en:

White Hats (de sombrero blanco) que son motivados por el reto tecnológico. Estos hackers ayudan a mejorar la seguridad al descubrir nuevos fallos y reportarlos a los fabricantes y a la comunidad.

Black Hats (de sombrero negro) cuyo objetivo es el beneficio personal. Este otro tipo de hacker va a usar sus descubrimientos y habilidades para causar daño, robar información o hacer fraude.

¿Qué es el Spyware?

El spyware es un término que abarca muchos tipos de programas hostiles. Estos tienen como funcionalidad recopilar información del usuario y enviarla al creador. El tipo de información que recopilan depende mucho del spyware instalado, pero puede ir desde hábitos de navegación en Internet, hasta todos lo que haya escrito el usuario (incluyendo contraseñas). El spyware más sofisticado tiene funcionalidad de Troyano.

¿Qué son los Troyanos?

Se conoce como troyanos a programas hechos por atacantes para abrir un acceso remoto a una computadora. Se les dice troyanos por su similitud al “caballo de Troya”. Muchas veces la víctima es engañada para instalar este tipo de programas al enviarlos en un correo electrónico o descargándolos desde un sitio Web. Al instalarse abren una “puerta trasera” para que el atacante gane control remoto total e irrestricto sobre la computadora de la víctima.

¿Cómo limpio mi computadora de spyware y troyanos?

Hay muchas aplicaciones enfocadas en eliminar este tipo de infecciones. En algunos casos, los antivirus comienzan a incluir esta funcionalidad. Las mejores aplicaciones para eliminar spyware y troyanos se enumeran a continuación (algunas son gratuitas).

Microsoft Antispyware	www.microsoft.com
SpyBot Search & Destroy	spybot.safer-networking.de
BPS Spyware/Adware Remover	www.bulletproofsoft.com
Aluria's Spyware Eliminator	www.aluriasoftware.com
Ad-aware 6	www.lavasoftusa.com

¿Cómo instalo un firewall personal?

Windows XP ya cuenta con un firewall que está prendido por default a partir de la instalación del SP2. Este firewall es suficiente para la mayoría de los usuarios. Si se utiliza una versión de Windows anterior a XP, algunas de las mejores opciones disponibles son:

Norton Personal Firewall	www.symantec.com
ZoneAlarm Pro	www.zonelabs.com
Sygate Personal Firewall PRO	smb.sygate.com