RISCCO®
Risk & Business Consulting.
Internal Audit.

Antonio Ayala I.
VP Ejecutivo, RISCCO

18 de Noviembre de 2011

Riesgos potenciales de seguridad al implantar banca móvil.


RISCCO®
Risk & Business Consulting.
Internal Audit.

“En el 2011 se duplicará el número de amenazas a dispositivos móviles comparadas con las del 2010.”

Septiembre 2011

Estudio realizado por IBM X-Force

“Android se ha convertido en la plataforma número uno para códigos maliciosos”

Octubre 2011

Kaspersky Laboratories

“En USA, el 75% de los fraudes bancarios a pequeñas y medianas empresas, ocurre vía la banca en línea.”

Abril 2011

Estudio reliazado por Guardian Analytics y Ponemon Institute.

FFIEC considera que la autenticación de un solo factor, como único mecanismo, es inadecuado para transacciones que involucren acceso a información del cliente o el movimiento de fondos a terceros.

2006

***FFIEC** (Federal Financial Institutions Examination Council)*

Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and Office of Thrift Supervision.

“80% de las organizaciones no cuentan con un Oficial de Seguridad de Información a tiempo completo”

Julio 2011

Estudio Seguridad y Privacidad de Datos
UTP y RISCCO

Agenda

1. ¿Qué tan serio es el problema de fraudes en servicios en línea?
2. Riesgos de TI en servicios de banca móvil
3. ¿Cuál debería ser el rol del Ejecutivo Bancario frente a la adopción de banca móvil ?
4. Reflexiones finales

¿Qué tan serio es el problema de fraudes en servicios en línea?

RISCCO

Realidad y no un mito

- La verdad es que es una comodidad a muy alto precio.
- Ocurre sólo a grandes corporaciones y gente de mucho dinero.
- Fraudes en banca en línea es un negocio de millones de dólares y en pujante crecimiento.
- **Ya no hay que ser un gurú para hacer daño. "*downloadable kits*"**

RSA online Fraud Report

Sale Ítem	Underground Price
Logins Online Banking	$50 - $1,000 per account, depending on the account type and balance.
‘Fulls’ Data Sets	$5 - $20 per set
Fraudulent Phone Calls	$10 - $15 per call

Fuente:RSA Fraud Report August 2010

¿Cómo ocurre un fraude en línea?

1. Identificar Víctimas
2. Instalar código malicioso
3. Banca en línea
4. Colectar /transmitir datos
5. Transferir fondos

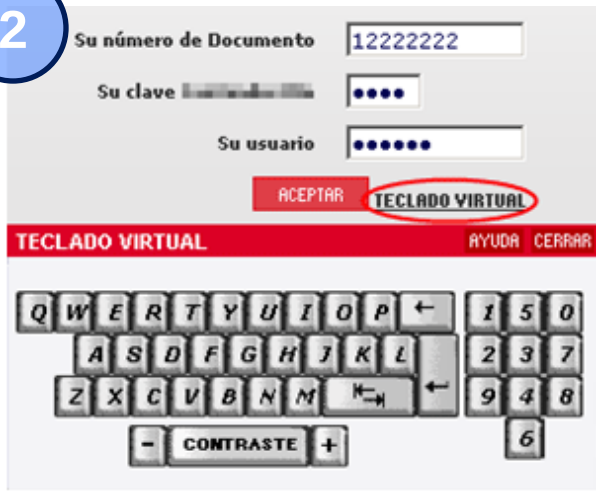
Fuente: FBI, IC3, SS, FS-ISAC

RISCCO

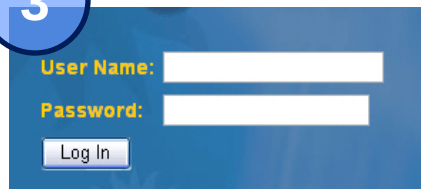
Evolución – Autenticación servicios en línea

1

2



3



Biométricos
Out-of-Band Aut.
IP Geo Location
Customer Verification

4

User + Pass +
Multifactor +

Fraud Prevention Sol.

Proactive monitoring Sol.

RISCCO

Riesgos de TI en servicios de banca móvil

RISCCO

Conceptualización del Riesgo Móvil

Cliente

Red GSM

Banco

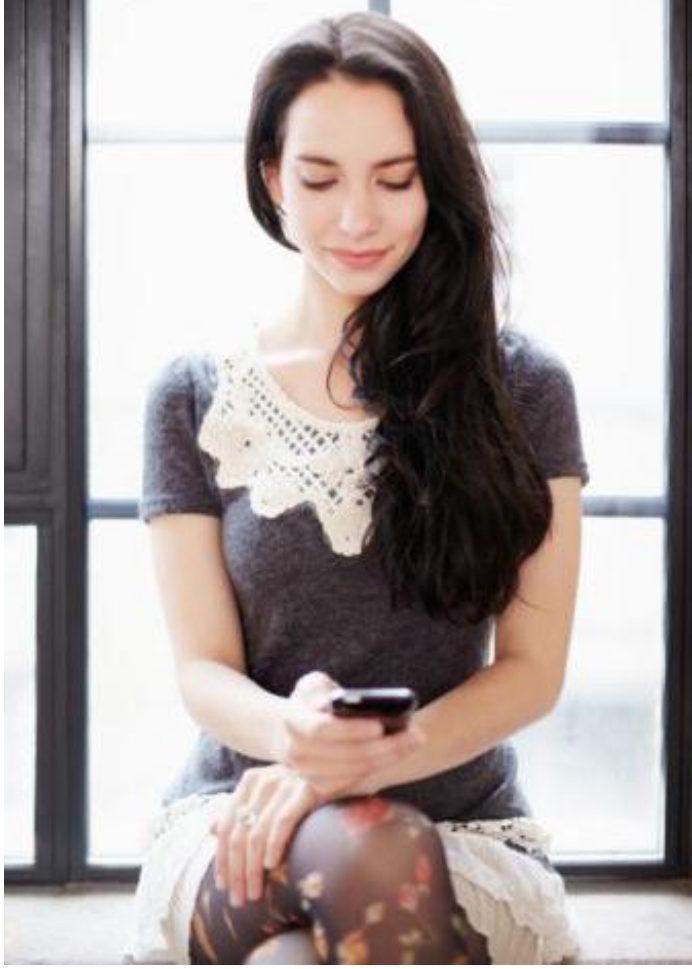
Servidor Banco

Base de Datos Banco

RISCCO

Riesgos de aplicaciones móviles

- Robo o pérdida del teléfono
- Robo de credenciales de acceso.
- Que el no buen diseño de aplicaciones permita se almacene en el teléfono datos sobre:
  - ✓ Historial de pagos
  - ✓ Datos parciales de tarjetas de crédito
  - ✓ Credenciales de acceso



Impacto

Los obvios:

a) Pérdida de dinero de usuarios (personas y organizaciones)

b) Daño a la imagen/reputación de la institución

c) Demandas legales

d) Incumplimiento regulatorio

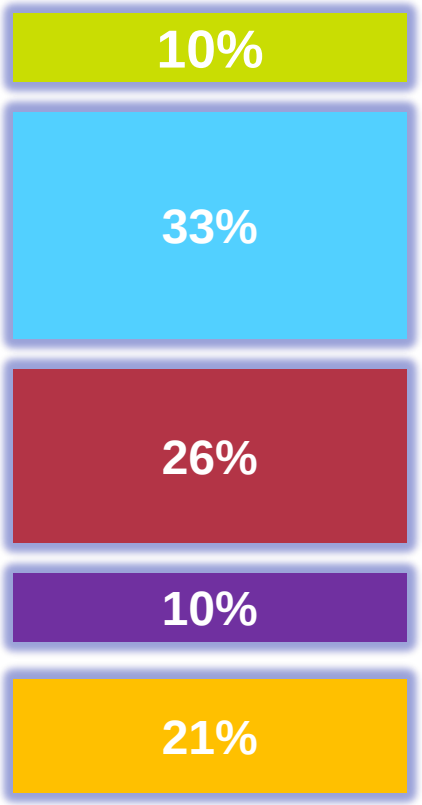
Los no tan obvios:

a) Pérdida de clientes

b) Minar la confianza de ese tipo de servicio en el mercado

¿Cuál es la consecuencia más seria de un fraude o intención de fraude en línea, con respecto a su banco?

43% se van a otro Banco



- **Terminan la relación con el Banco**
- **Buscan otro Banco para los servicios primarios**
- **Disminuye la confianza en la habilidad del Banco para banca en línea**
- **Incrementa la confianza en el Banco**
- **No afecta la relación con el Banco**

Fuente: 2011, Business Banking Trust Study – Guardian Analytics – Ponemon Institute

¿Cuál debería ser el rol del Ejecutivo Bancario frente la adopción de banca móvil?

Rol del Ejecutivo Bancario

Los obvios:

1. Evaluar con mesura la adopción de la banca móvil. Ir de menos a más.

2. Cumplir los acuerdos bancarios sobre seguridad y banca electrónica.

    1. Riesgo
    2. Cumplimiento
    3. Seguridad

3. Fortalecer los mecanismos utilizados para educar a los clientes.

Rol del Ejecutivo Bancario

Los no tan obvios:

1. Evaluación de riesgo para nuevas amenazas y la efectividad de controles implantados (anualmente)
2. Evalúe el método de autenticación utilizado (One size fits all approach).
3. Defina criterio para qué tipo de transacciones serán realizadas desde el teléfono (no crear pagos programados desde el móvil por ejemplo)
4. Indague sobre integridad de bitácoras de transacciones desde teléfonos móviles.
5. Evalúe el nivel de integridad de las bitácoras de auditoría de las transacciones en línea.

¿ y con esas actividades es suficiente?

Sorry…pero que tal si te digo que no.

Reflexiones finales

1. Mida riesgos, implante controles, brinda el servicio.
2. El riesgo existe y es real.
3. La confianza de los clientes hoy día es muy volátil.
4. Existe el marco legal/regulatorio para realizar demandas.
5. La educación y concienciación al cliente es clave, pero no podemos descansar en ella.

RISCCO

Antonio Ayala I.
Vicepresidente Ejecutivo

t: +507 279-1410
c: +507 6675-0644
f: +507 279-0729
e: aayala@riscco.com

www.riscco.com


RISCCO®
Risk & Business Consulting.
Internal Audit.