RISCCO®
Risk & Business Consulting.
Internal Audit.

Antonio Ayala I.
VP Ejecutivo, RISCCO

26 de Abril de 2012

Riesgos, seguridad y medidas de protección para dispositivos móviles

Risk & Business Consulting.
Internal Audit.

Antonio Ayala I.
Vicepresidente Ejecutivo

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

www.riscco.com

“La venta de dispositivos móviles crecerá de 300Mi (2008) a 650Mi (2012).”

Gartner, Abril 2011

Mobile Communications Devices by Open Operating System

Entre Agosto 2010 y Diciembre 2011, los códigos maliciosos para dispositivos móviles aumentaron en un 2900%.

Marzo 2012

Kaspersky Laboratories

En Junio 2011, fue la primera vez que los usuarios de dispositivos móviles gastaron más tiempo utilizando aplicaciones móviles que navegando en Internet desde el mismo dispositivo.

Junio 2011

Flurry Mobile Apps Put the Web in their rear view mirror

Agenda

1. ¿Qué tan serio es el problema de fraudes en dispositivos móviles?

2. Riesgos de TI en servicios brindados a través de dispositivos móviles.

3. Rol del Ejecutivo frente a la adopción de dispositivos móviles como herramienta de trabajo

4. Reflexiones finales

¿Qué tan serio es el problema de fraudes en dispositivos móviles?

Realidad y no un mito

- La verdad es que es una comodidad bien berraca.
- Ocurre sólo a grandes corporaciones y gente de mucho dinero.
- Fraudes en servicios que utilizan dispositivos móviles es de millones de dólares.
- **Ya no hay que ser un gurú para hacer daño. "*downloadable kits*"**

RISCCO

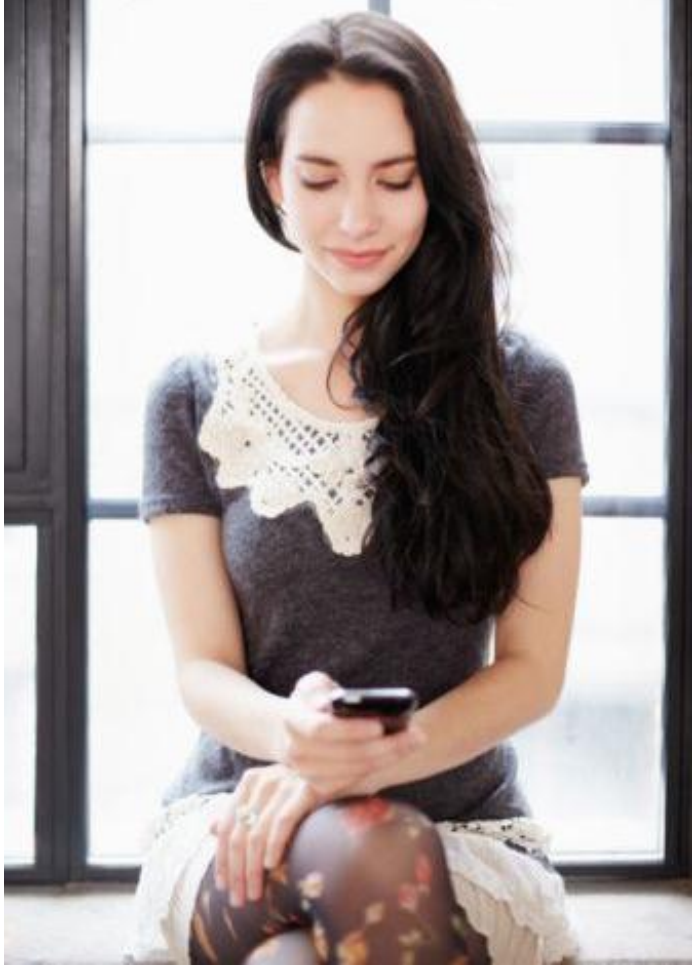
Realidad y no un mito

- Los usuarios de este tipo de tecnología son bastante “relajados” con la seguridad.
- Las bandas de terroristas han visto que es una oportunidad excelente para robar identidad.
- Aplicaciones en varias “apps stores” están infectadas.
- Para distribuir los códigos maliciosos las bandas utilizan SMS y Facebook.

Riesgos de TI en servicios a través de dispositivos móviles

Amenazas en dispositivos móviles

1. Amenazas basada en aplicaciones
2. Amenazas basadas en la Web
3. Amenazas de red
4. Amenazas físicas



1. Amenazas basadas en aplicaciones

- ✓ **Malware**
  (mensajes no solicitados o tener control remoto al dispositivo)
- ✓ **Spyware**
  (recolectar información como historia de llamadas, mensajes de texto, ubicación, etc.)
- ✓ **Amenazas de privacidad**
- ✓ **Vulnerabilidad de las aplicaciones**
  (permite al atacante aprovechar fallas de la aplicación para tener acceso al dispositivo.)

2. Amenazas basadas en Web

- ✓ **Esquemas de phishing**
  (Igual que las PCs, acceder sitios falsos para robo de credenciales)

- ✓ **Descargas de archivos maliciosos**
  (usualmente si que el usuario lo advierta)

- ✓ **Fallas en los navegadores**
  (Lo mismo que PC, toman ventaja de fallas del navegador)

3. Amenazas basadas de la red

- ✓ **Fallas de la red**
  (Fallas en el software de bluetooth, Wi-Fi)

- ✓ **Sniffer para redes inalámbricas**.
  (leer tráfico en texto legible en redes inseguras)

4. Amenazas físicas

- ✓ Robo o pérdida del dispositivo móvil.

"7 millones de celulares son extraviados o robados diariamente en el mundo"

Lookout Mobil Security

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 debería ser el rol del Ejecutivo frente la adopción de dispositivos móviles?

Rol del Ejecutivo

Los obvios:

1. Evaluar con mesura la adopción de dispositivos móviles como parte del servicios que se brinda. Ir de menos a más.

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

3. Solo bajar “apps” de fuentes confiables.

4. Prestar atención si el link donde ingresa el usuario y contraseña es realmente de la compañía que le interesa y no uno falso.

5. Asignar una contraseña a su dispositivo móvil.

Rol del Ejecutivo

6. Evaluación de riesgo para nuevas amenazas y la efectividad de controles implantados (anualmente).
7. Indague sobre integridad de bitácoras de transacciones desde dispositivos móviles utilizados a nivel corporativo.
8. Instale una herramienta de seguridad que verifique que las “apps” que está bajando sea libre de códigos maliciosos conocidos.
9. Actualizar con regular el sistema operativo de su dispositivo móvil.

¿ y con esas actividades es suficiente?

Sorry…pero que tal si te digo que no.

Reflexiones finales

1. Mida riesgos, implante controles y utilice los dispositivos.
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®
Risk & Business Consulting.
Internal Audit.