

# Seguridad Móvil

## Percepción desde el Operador

Nelson Enrique Bermudez Moreno

Colombia Móvil SA ESP-Tigo

Enero 2012

# Agenda

- Fraudes comunes aplicables a servicios móviles ofrecidos por el operador
- El reto de la seguridad para el cliente en su móvil
- El desafío: los OS de los móviles como ecosistema
- Tips de Seguridad desde la experiencia del operador.
- Experiencia de aplicaciones seguras: Banca Móvil

# El mundo móvil y el fraude

- El Operador Móvil ofrece medios de acceso a diversidad de servicios a través de la terminal móvil.
- Los servicios van desde la voz, hasta conexiones móviles de datos y voz sobre Internet
- Capacidad de servicios a medida de los usuarios
- Los principales servicios aplicados a Colombia son: Voz, SMS y Datos.
- La oferta básica atractiva al usuario, mantiene al móvil como parte fundamental de la propuesta de valor.
- Las redes en Colombia están innovando rápidamente a las tecnologías comerciales de punta

# El mundo móvil y el fraude

- Las oportunidades de fraude aparecen debido, en gran medida, a la curiosidad del usuario.
- La idiosincrasia del cliente en Colombia lo lleva a buscar la forma mas barata de uso
- La gran cantidad de los fraudes focalizan los esfuerzos en planes prepago usando la oferta disponible.
- Los productos desarrollados por los operadores incluyen la evaluación de riesgo.
- Caso Mundial de Futbol Sub-20



# El mundo móvil y el fraude

- Hay fraudes asociados a voz, ejemplo Bypass
- Los SMS son usados como forma de atraer victimas de estafas.
- En Datos, el hosting usando como salida de internet un modem: Phishing, SPAM.



# El mundo móvil y el fraude

- Bypass: Esquema de terminación de llamadas por rutas no legales, especialmente aplicado a llamadas entrantes internacionales, servicios de VOIP y trafico a países “transito”. Baja calidad de servicio, impacto en finanzas del operador
- Smishing: Fraude por mensajes de texto. Clásico: “Te regalamos un carro .....”. Nuevas formas: “Necesito minutos recárgame a este numero”. La imagen del operador entra en vilo
- Phishing: “Clásica”: El uso de computadores con módems de internet móvil. “Nueva”: Creación de servidores web en móviles.
- SPAM: Apoyado en redes esclavas, desde un móvil o computador con modem realiza el envío.

# La Seguridad del móvil y el usuario

- El objetivo del operador es mantener la reputación de su servicio: qué tan atractivo es para el fraudulento.
- Las condiciones del contrato buscan evitar la mala utilización del servicio: Evitar abusos del servicio, cumplir con las disposiciones legales.



# La Seguridad del móvil y el usuario

- La clave para evitar que el fraude sea negocio tiene dos frentes:
  - Prevenir los abusos y evitar la ocasión
  - La educación de los suscriptores.



# La Seguridad del móvil y el usuario

- La prevención: Tanto operadores como reguladores, Privados (banca, transportes, servicios), proveedores y fabricantes deben buscar las sinergias para poder minimizar el impacto de las fallas de seguridad



# La Seguridad del móvil y el usuario

- La educación debe empezar con la alfabetización digital
- Buscar que el usuario sea consciente de usar correctamente la tecnología.
- Enseñar a reconocer formas de fraude y de robo de datos
- Difundir información sobre las formas de fraude de manera eficiente de cara al cliente, gran ejemplo: la banca con el tema de phishing



# La Seguridad del móvil y el operador

- Cumplir con las disposiciones de autoridades de regulación y legales para evitar la proliferación de actividades inseguras
- Blindar la infraestructura que el usuario tiene a disposición para mantener el servicio ofrecido
- Evitar que malas practicas de uso proliferen en sus suscriptores.



# El desafío de los OS en los celulares

- Se están conformando 3 grandes mundos de sistemas operacionales en móviles:
  - Apple iOS
  - Google Android
  - Microsoft Windows Phone



# El desafío de los OS en los celulares

- Prever que los recursos de sistemas operativos tales como las aplicaciones, funcionalidades y software sean confiables en seguridad.
- Caso Blackberry: El túnel desde el usuario hasta la salida de Internet de RIM
- Confiabilidad de las aplicaciones en las Tiendas de aplicaciones. Como en los vinos: Certificación de origen.



# Tips de Seguridad desde la experiencia

- En el uso de servicios de voz y SMS:
  - Los SMS legales de servicios siempre tendrán un identificador de 3 a 5 dígitos o letras como *sender*. Nunca como números telefónicos reales.
  - Nunca contestar SMS o realizar llamadas a números cuya identificación no sea clara para el usuario: puede estar recargando o dando recursos a delincuentes.
  - Las llamadas internacionales entrantes que aparecen procedentes de números locales tienen el peligro de ser grabadas o monitoreadas por delincuentes.

# Tips de Seguridad desde la experiencia

- En su internet móvil (teléfono o modem):
  - En caso de robo o pérdida, dar aviso inmediato al operador para evitar su uso en prácticas delictivas, denunciar ante las autoridades para evitar problemas futuros.
  - En caso de aplicaciones descargadas de Tiendas, evitar aplicaciones cuyo origen no sea reconocido por el administrador de la tienda ó que tengan mala calificación de los usuarios
  - Siempre leer los comentarios de los usuarios sobre la aplicación a la que se va descargar. Tener desconfianza de las aplicaciones con muchos comentarios positivos que tengan calificaciones con frases cortas.

# Ejemplo de desarrollo seguro: Banca Movil

- Llega a Colombia en 2006 de mano de Gemalto, Redeban y Tigo
- La transacción se realiza por medio de SMS
- La comunicación es segura entre la SIM card y el banco. El banco y la SIM descriptan la información por medio de la aplicación de banca móvil.
- La información esta encriptada usando 3DES



## REFLEXIÓN



**Ministro TIC Colombia** @DiegoMolanoVega

Tenemos q mejorar la educación de los internautas porq ellos aceptan cosas q no saben implicaciones #darksideofconnectivity

4

RETWEETS



4:59 AM - 25 Jan 12 via Twitter for BlackBerry® - Details

Reply Retweet Favorite

La clave de la seguridad para los usuarios de servicios móviles, se basa en la educación continua en las tecnologías. En la manera responsable en que todos los miembros del ecosistema de tecnología enseñen a sus usuarios

**Gracias!!!**