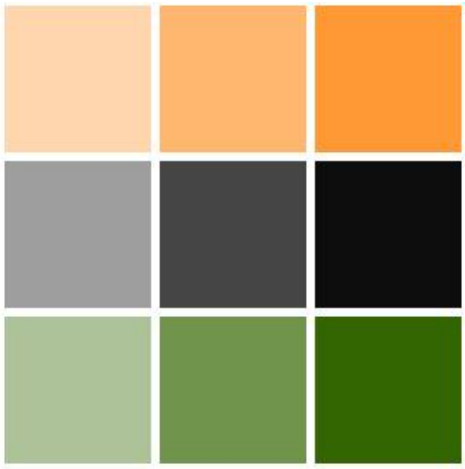
Teléfonos inteligentes, un nuevo riesgo de privacidad y protección de datos en las corporaciones.

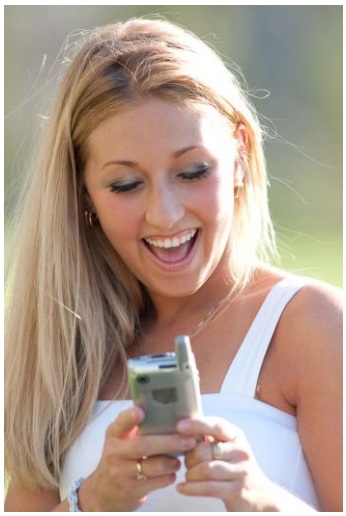


La utilización de teléfonos inteligentes ha creado en las corporaciones e instituciones del Estado riesgos de privacidad y protección de datos. Los riesgos, implicaciones y consejos de seguridad en su uso son abordados en este punto de vista.

En este punto de vista

Introducción

Los teléfonos inteligentes (smartphones), como por ejemplo Blackberry, Nokia y IPhone, por mencionar solo algunas marcas, se han convertido en mucho más que un dispositivo para realizar una llamada telefónica. Han pasado a ser para muchos, una herramienta de trabajo y un buen negocio para sus fabricantes.



- ✓ Las ventas de teléfonos inteligentes alcanzaron los 1,211 millones de unidades en el 2009 (según un estudio de Febrero 2010 de la casa de investigación de tecnología *Gartner Group*).

- ✓ Apple vendió 8.7 millones de unidades de teléfonos IPhone en el último trimestre de 2009 en comparación con solo los 3.4 millones de computadoras Mac que vendió durante el mismo período.

Los teléfonos inteligentes nos permiten ahorrar costos al comunicarnos con sistemas de mensajería instantánea como por ejemplo, Google Talk o Yahoo! Messenger. Enviar y recibir mensajes tipo SMS o MMS, guardar y escuchar música, videos, fotos, estar conectado a redes sociales, por mencionar sólo algunas de las ventajas.

Desde la visual corporativa, son literalmente una herramienta de trabajo para recibir y enviar correos electrónicos, revisar y modificar documentos, navegar por Internet, tener a mano la agenda y contactos, conectarnos a la red de datos de la organización donde laboramos, entre otros.

Los teléfonos inteligentes permiten que los clientes de bancos en Panamá puedan conocer el saldo de sus cuentas o recibir mensajes de texto cuando se realizan transacciones con su tarjeta de crédito. Estas computadoras en miniatura han pasado de ser un artículo de lujo a más bien una herramienta de trabajo casi imprescindible, de gran poder, pero sobre todo muy convenientes.

Cuando la conveniencia implica riesgos

Al momento de escribir este artículo (Marzo 2010) en Panamá circulaba un mensaje alertando entre amistades que utilizan el servicio Blackberry Messenger, que un número de PIN específico era de un "Hacker" y que no lo aceptará bajo ninguna circunstancia. Cierto o no, es común ver que a nivel corporativo el Departamento de Riesgo o de Seguridad de Información no establecen controles suficientes para proteger la información confidencial almacenada en estos equipos.

En 2008, un alto asesor del Primer Ministro inglés Gordon Brown en un viaje oficial a China, perdió en un incidente confuso su Blackberry. La diplomacia británica acusó a los servicios de inteligencia Chinos de tal evento. ¿Por qué? Muy probablemente para acceder a información privilegiada del Gobierno Británico que debía tener el teléfono en mención.

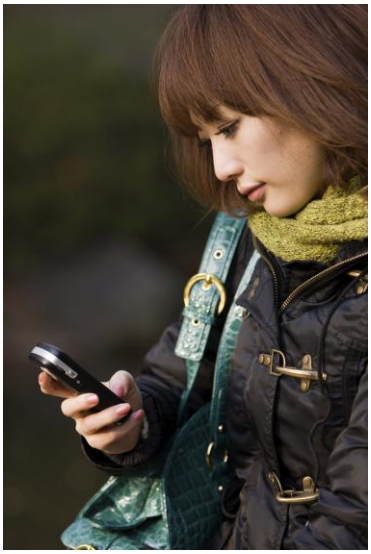
El conveniente tamaño de estos dispositivos es su principal amenaza. Un estudio de la casa *Credent Technologies* realizado en Londres reflejó que en los taxis fueron olvidadas 3,000 *notebooks*. Esta cifra parece mínima comparada con los cerca de 55,000 teléfonos inteligentes olvidados durante el mismo periodo.

Existe la falsa creencia en muchas organizaciones que, como quiera los *emails* enviados y recibidos desde el teléfono "viajan" en forma cifrada (encriptada), la información contenida en el teléfono es segura. Pues permítanme informarle que no es así. Es cierto que el correo puede "viajar" de manera segura, pero una vez lo lea en su teléfono y baje algún documento, la información podría ser accedida fácilmente salvo que haya adoptado algunas prácticas de seguridad.

Los teléfonos inteligentes están expuestos al menos a riesgos como:

- ✓ Virus y Malware
- ✓ Worms y troyanos
- ✓ Ataques tipo *phishing*

Estos son típicamente diseminados a través del correo electrónico o a través de mensajes tipo SMS o MMS.



Valore qué representaría para su organización que el VP de Ventas, pierda el teléfono donde tenía las estimaciones de ventas para lo que falta del año fiscal, o un documento en *word* sobre los resultados operativos del último trimestre o un *email* con las bases parac comprar la compañía competidora. Estos ejemplos son documentos que cada día residen más en los teléfonos inteligentes y menos en las computadoras. Si su corporación adolece de buenas prácticas de seguridad en el uso de este tipo de dispositivos, la información podría ser accedida fácilmente por un ladrón con el simple hecho de tener el teléfono, sin que sea necesario utilizar ningún programa o técnica de *hacking* para acceder su información.

Muy probablemente usted puede estar pensando que su corporación tiene un control para en caso roben un equipo, el Departamento de Tecnología pueda remotamente eliminar los datos de su teléfono. Si al ladrón sólo le interesa el teléfono, su control será efectivo. Sin embargo, si el hurto obedece a un tema de espionaje, no seamos ingenuos, el ladrón sabe que lo primero que tiene que hacer es quitarle la batería al equipo y/o ir a un lugar donde no haya señal del operador. Para esto, créame que no hay que ir al Cerro Fábrega en Bocas del Toro, solo trate de hacer una llamada desde el nivel dos o tres de estacionamientos que estén por debajo del nivel de la calle en un edificio.

Las corporaciones deben tener presente que la responsabilidad relacionada con proteger la privacidad de los datos personales de sus clientes, en ningún momento excluye a los teléfonos inteligentes, ¿cierto?

Por alguna razón, los riesgos que impone a las organizaciones el uso de este tipo de dispositivos, generalmente no son ni dimensionados ni atendidos por el Departamento de Riesgo o Seguridad de Información en su justa perspectiva. Hoy día, en caso que no esté al tanto, existe una creciente industria de productos de seguridad para este tipo de dispositivos. Esto incluye, programas anti-virus, firewall, programas para encriptar los datos, entre otros. Ahora bien, por mientras, el adoptar buenas prácticas de seguridad en su uso es un buen comienzo.

Consejos de seguridad al utilizar teléfonos inteligentes

A continuación, resumimos algunos consejos y buenas prácticas para el uso de teléfonos inteligentes. La mayoría de los teléfonos tienen disponibles estás opciones, lo que sucede es que las personas no las activan.

1. **Asigne una contraseña o *password* al equipo**

   Bastante obvio, pero la mayoría de las personas no lo hacen por la incomodidad que representa digitarlo cada vez que necesite utilizar el teléfono.

2. **Encripte los datos almacenados en el equipo**

   Nuevamente, que el correo electrónico corporativo pueda viajar de forma encriptada hacia/desde el teléfono no significa que una vez los datos residan en el teléfono, estén encriptados. Habilite la opción de encriptación, preferiblemente la más fuerte.

3. **Deshabilite las opciones Bluetooh y Wi-Fi si no las necesita**

   Un número importante de ataques a los teléfonos inteligentes se da por tener habilitada la opción de Bluetooh. Es cierto que es muy conveniente para transferir archivos pequeños y/o conectarnos a otros dispositivos, pero al mismo tiempo, permite a terceros con herramientas apropiadas acceder al teléfono sin que el dueño lo advierta.

   Si debe utilizar la opción de Bluetooh, puede definir para qué dispositivo desea tenerla habilitada (por ejemplo manos libres). Además, restrinja la opción que permite a otros dispositivos "descubrir" su teléfono. En caso de que usted necesite conectarse a otros dispositivos, podría hacerlo manualmente.

   Con relación a las redes Wi-Fi, esto es para conectarse remotamente a su red corporativa o tener acceso a Internet desde parques o espacios públicos. Es preferible que no la utilice salvo en su organización hayan establecido mecanismos muy seguros para acceder a la red corporativa desde su teléfono.

4. **Evite almacenar contraseñas o *password*s de servicios en línea**

Evite almacenar contraseñas de acceso a servicios en línea en el teléfono. Si es necesario, siga las recomendaciones No. 1 y No. 2. Además, algunos teléfonos permiten a los usuarios guardar sus contraseñas de forma segura utilizando un programa que viene instalado de fábrica. Ahora bien, si no es estrictamente necesario, mejor no guarde esa información en el teléfono.

5. **Elimine los datos de forma segura al cambiar de equipo**

   Si va a utilizar un nuevo equipo y el anterior estuvo con usted por algún periodo de tiempo considerable, borre de forma segura "wipe" los datos mantenidos en el teléfono antes de regalar o desechar el teléfono.

Los consejos anteriores, para la mayoría de los casos, serían suficientes para reducir el riesgo de pérdida de información, pero existe una recomendación adicional que puede también considerar.

6. **Instale programas de seguridad adicionales de ser requerido**

   Dependiendo de la criticidad de datos que almacene el teléfono, de la información enviada-recibida en los correos electrónicos, si accede a páginas web desde el teléfono o si tiene que conectarse a la red corporativa desde el teléfono, muy probablemente necesite considerar instalar programas antivirus, firewall o similares. Indague con el Oficial de Seguridad de Información de su organización sobre la conveniencia o no, utilizando un enfoque basado en riesgo.

El evitar su uso es no querer adaptarse a nuevos tiempos . Utilícelo de forma segura, tenga presente los riesgos que conlleva y no piense que es solo un teléfono para hacer llamadas de voz.

* * *

Independencia. Integridad. Conocimiento. Credibilidad.

RISCCO es una compañía independiente dedicada de manera exclusiva a la consultoría en riesgo, negocios, fiscal, tributaria y auditoría interna.

Para mayor información sobre el contenido de este documento o conocer más sobre la forma cómo estamos ayudando a las organizaciones a enfrentar sus desafíos en materia de administración de riesgo, riesgos de tecnología, riesgos fiscales o auditoría interna, por favor contáctenos.

info@riscco.com

Teléfono: +507 279-1410

RISCCO
Ave. Ricardo J. Alfaro
Panamá, Rep. de Panamá

www.riscco.com