GUÍA PARA PRESERVAR LA SEGURIDAD EN DISPOSITIVOS MÓVILES

Con la llegada y posicionamiento de la era post PC —en la que los protagonistas son los teléfonos inteligentes, las tabletas y otros dispositivos de la gama móvil— las posibilidades de comunicación y productividad de manera rápida, flexible y eficaz en todos los ámbitos profesionales se han incrementado notablemente. No obstante, esta nueva era con todas sus ventajas, trae consigo una serie de problemas que van desde la extrema dependencia al terminal hasta la pérdida de activos digitales e información privada o profesional, y en esto último se centra el presente documento.

Los informes emitidos por diversas compañías del sector de la seguridad informática, muestran que un alto porcentaje de los ataques y/o delitos en entornos móviles llegan a consumarse por negligencia o desconocimiento por parte del usuario. Asimismo, existe una falta de conciencia en la sociedad con respecto a la naturaleza del terminal, y es que, en concreto, se trata de un pequeño computador susceptible a ser atacado y vulnerado, por lo que sin la adopción de medidas básicas en materia de seguridad el atacante podría contar con posibilidades inéditas para delinquir. Por tanto, el presente escrito busca informar, orientar y guiar al usuario de tecnologías móviles, en la adopción de mecanismos para proteger sus datos e información personal; y con ello, extraer los reales beneficios del equipo para su vida.

Consejos prácticos para proteger los dispositivos móviles

Los siguientes consejos pueden ser aplicados en cualquier dispositivo móvil y sistema operativo; sin embargo, se enfatiza la necesidad de adoptarlos en los teléfonos inteligentes, ya que actualmente cuentan con una mayor cuota del mercado con respecto a otros tipos de equipos. Es importante mencionar que los siguientes consejos de seguridad pueden no surtir el efecto deseado si el usuario no está alineado con ellos y toma conciencia que la seguridad, principalmente, depende de él. En todo caso y ante la duda, usar el sentido común antes de ejecutar alguna acción y asimismo recopilar la información respectiva.

1. Bloquear el dispositivo mediante una contraseña o número de identificación personal (PIN)

Es la primera medida práctica a tomar y, probablemente, la más importante. El contar con una contraseña o número de identificación personal en nuestro equipo es crucial para mantener nuestros datos seguros, ya que impedirá el acceso inmediato a cualquiera que manipule el terminal y en caso de pérdida o robo del mismo, la utilización de un PIN podría inhabilitarlo. Ahora bien, no sólo es importante contar con una contraseña o número de identificación personal, también lo es elegirla adecuadamente. Diversos estudios realizados en el campo de la seguridad informática muestran que muchos usuarios seleccionan contraseñas simples en su estructura (0000, 1111, 9999), posibilitando así que el atacante las adivine. Por tanto; una contraseña robusta no debe repetir caracteres y, en la medida de lo posible, deberá incluir y alternar letras y números**.** Finalmente; para complementar la seguridad que provee el PIN, es pertinente activar la opción “Bloqueo periódico del dispositivo”.

2. No almacenar información confidencial y/o realizar copias periódicas de seguridad de los datos

Dada la dinámica a la que está expuesto un dispositivo móvil lo recomendable es no almacenar información confidencial o personal en él, puesto que en caso de ataque, robo o pérdida, ésta podría ser explotada con fines negativos. En caso de almacenar información sensible, que sea la menor posible y como medida de seguridad realizar copias periódicas de ésta, lo que además de salvaguardarla le otorgará un mejor rendimiento al equipo.

3. Mantener el sistema operativo actualizado

El sistema operativo móvil (Android, iOS, BlackBerry OS, Windows Phone, etc.) es el equivalente al sistema operativo para computadores (Microsoft Windows, Mac OS X, Unix, GNU/Linux, MINIX, etc.); es decir, es la plataforma informática que sirve de nexo para que el usuario utilice el *hardware* (parte física del equipo) y ejecute o administre diversas aplicaciones. Ahora bien, el sistema operativo cumple un rol fundamental y su importancia aumenta en función de la masificación y producción de dispositivos que lo usen. Sin embargo; la experiencia recogida en diversos entornos de computación, muestra que una considerable cantidad de problemas surgidos se deben a errores en las líneas del código que gobierna al sistema operativo, más que a fallos en el *hardware*; asimismo, dichos errores pueden estar directamente asociados o repercutir en la seguridad del terminal, dejándolo en una situación delicada frente a posibles ataques. Por consiguiente y como medida preventiva y correctiva, se recomienda actualizar periódicamente, a la última versión estable, el sistema operativo del equipo móvil (previo resguardo de datos). Esta práctica además de combatir potenciales problemas de seguridad, permitirá obtener un mayor rendimiento a nivel de aplicaciones y de *hardware*.

4. Instalar aplicaciones móviles desarrolladas por fuentes de confianza

Luego de adoptar y ejecutar los tres primeros consejos de esta guía se podrán instalar las aplicaciones móviles (*Apps*). Es importante enfatizar que actualmente existen tres tipos de aplicaciones móviles, las cuales son: nativas, web e híbridas. El presente documento se enfoca en las nativas, ya que por ahora son las más demandadas y las que le otorgan una mejor experiencia al usuario. Por lo tanto; una aplicación móvil nativa es un programa informático diseñado y desarrollado para funcionar en un dispositivo móvil. Cada *App* cumple una tarea específica y las hay para todas las necesidades y gustos. Así pues, es factible encontrar una gran cantidad de aplicaciones, categorizadas en: arte, salud, deporte, educación, estilo de vida, ocio, etc.

El siguiente paso es localizar la aplicación deseada y para ello existen centros de *Apps* que las agrupan en un entorno común para que el usuario las seleccione, descargue e instale. Por lo general, estos centros son lanzados por los desarrolladores de sistemas operativos móviles y ofertan al público los programas de forma gratuita. El ejercicio que se recomienda es visitar estos centros de confianza a fin de descargar, o si fuese el caso, comprar un determinado programa. En esta parte del proceso el sentido común juega un papel fundamental, ya que antes de descargar e instalar el *software* (con mayor razón si se realiza una compra), es necesario tomar en cuenta la

valoración otorgada a la *App*, así como leer la política de privacidad y los comentarios vertidos por otros usuarios con respecto a ésta. Por ejemplo, si una aplicación determinada solicita para su instalación y posterior uso, acceder a información de carácter personal, el sentido común nos preguntará: ¿Por qué son necesarios mis datos personales? Por lo que surge una duda, y ante cualquier duda se recomienda no descargar la aplicación.

5. Activar: WiFi, Bluetooth y los servicios de geolocalización, sólo para usarlos

Si bien, en ocasiones es recomendable conectar el dispositivo a una red WiFi a fin de administrar eficientemente el plan de datos contratado, dicha conexión debe realizarse de forma manual (desactivar la opción de conexión automática) y siempre a una red segura. Sólo se considera segura una red WiFi, si está dotada de diversos mecanismos para preservar la autenticación, el acceso y la privacidad, dentro de la misma. En este sentido, una red segura podría ser la de un centro de labores, puesto que es administrada por un profesional que vigila el correcto funcionamiento de ésta. Una red de casa puede ser segura si es que cuenta con mecanismos de seguridad adicionales a los instalados por el proveedor de Internet. Asimismo y tal y como lo confirman los grupos de delitos telemáticos de la policía, las redes WiFi de: cafeterías, centros comerciales, aeropuertos, hoteles, etc., bajo ningún concepto son seguras y constituyen el blanco perfecto para los atacantes, por lo que se recomienda evitar conectar el equipo a estos entornos. Si la red no es segura, se deberá usar la red de datos (3G, 4G) del operador móvil, ya que el tráfico entre las torres celulares y los dispositivos, por lo general, está cifrado.

Práctica similar es la que se recomienda en el caso de Bluetooth, y es que en ocasiones los equipos están configurados para que otros terminales se conecten automáticamente usando esta tecnología, lo que podría permitir a un usuario copiar información personal. Lo recomendable es activar Bluetooth sólo cuando sea necesario.

Por último y no menos importante, es evitar instalar o desactivar las aplicaciones que utilicen el servicio de geolocalización. Actualmente son muchas las *Apps* que para usarlas solicitan la activación de este servicio, y en realidad no hay razón para aceptar tal condición, puesto que los datos del usuario podrían ser filtrados o compartidos con terceras personas.

6. Abrir y cerrar correctamente las sesiones de las cuentas utilizadas

Los constantes casos de suplantación (*Phishing*) son denunciados con frecuencia por los grupos de delitos telemáticos de la policía. En estos, el atacante falsifica la dirección electrónica (URL) del sitio para capturar la información de inicio de sesión de la víctima y sacar partido de ella. Por lo que antes de iniciar sesión en alguna cuenta se precisa verificar la URL del sitio, la misma que deberá incluir el protocolo seguro de transferencia de hipertexto (https) en la estructura que yace en la barra de direcciones. Asimismo lo recomendable en estos casos es descargar la aplicación oficial del sitio en cuestión, sólo así se garantizará el acceso adecuado.

Análogamente, el cierre de sesión debe ser el correcto, de lo contrario y si el terminal cayera en manos de un delincuente, éste podría acceder a cada una de las cuentas

con sólo conectarse al sitio web de la entidad correspondiente. En tal sentido, se debe finalizar sesión en la página web mediante el botón destinado a dicha función y no simplemente cerrando el navegador. Sea una red social, correo electrónico, servicio de almacenamiento y con mayor razón si se trata de una entidad bancaria o de comercio electrónico; el cierre de sesión es clave en la seguridad.

7. Borrar los correos electrónicos y/o mensajes de texto no solicitados

Por lo general, el delincuente usará alguna técnica de falsificación e ingeniería social, por ejemplo *Smishing* o *Phishing* para intentar capturar las credenciales de inicio de sesión del usuario; por tanto, la primera medida es evitar pulsar: enlaces, enlaces abreviados o archivos adjuntos incluidos en la comunicación, así ésta provenga de un supuesto amigo o de una entidad bancaria y; desde luego, jamás responder o enviar información personal. En este sentido se recomienda contactar directamente con la entidad o persona emisora del mensaje, siempre que esto sea posible, para validarlo.

Lo mejor que se puede hacer una vez recibido un: SMS, MMS o correo electrónico de dudosa procedencia, es borrarlo de inmediato.

8. Instalar un AntiMalware para dispositivos móviles, si fuera necesario

Si bien, por lo general se usa el término Antivirus para referirse a la aplicación de seguridad capaz de detectar y neutralizar distintos tipos de amenazas informáticas, lo exacto es denominarla AntiMalware, ya que este *software* no sólo protege a los dispositivos de virus, sino también de: *spyware*, troyanos, gusanos; es decir, de *malware*. Ahora bien, la instalación y uso de este tipo de programas depende de varios factores, como: la actividad en Internet, el sistema operativo, el uso de aplicaciones, etc. En tal sentido, un dispositivo con sistema operativo iOS podría no necesitar ser complementado con un AntiMalware, debido a que menos del 1% de *malware* existente va dirigido a esta plataforma, razón por la cual Apple declara que se puede prescindir de este tipo de aplicaciones en sus dispositivos. Por otro lado, el sistema operativo Android se ubica en un contexto distinto puesto que se trata del sistema operativo más usado en el mundo, en tanto que más del 80% del *malware* tiene como objetivo vulnerar este sistema. Por último, la actividad en Internet también es determinante de cara a adquirir un AntiMalware, y es que si el terminal es utilizado para acceder y descargar *software* sólo y exclusivamente en portales oficiales y de confianza, el usuario podría estar, casi siempre, seguro.

En resumen, la decisión de instalar un AntiMalware depende de cada persona en función de su actividad en la Red; sin embargo, es conveniente recalcar que estas aplicaciones, en la mayoría de casos, aportan un grado más de seguridad y tranquilidad debido a que incluyen funcionalidades adicionales como: gestión de privacidad, bloqueo a distancia o sistema antirrobo. Asimismo, existen versiones gratuitas por si el factor económico fuese un impedimento para usarlas, las mismas que pueden ser descargadas de las tiendas oficiales de aplicaciones.

Consideraciones Finales

El presente escrito sirve de guía en la implementación de una configuración razonable de seguridad para un dispositivo móvil, ayudando así a preservar la información de cualquier usuario de esta tecnología. En este sentido, complementar lo expuesto con otras prácticas es vital de cara a intensificar y/o personalizar el nivel de seguridad.

Sin embargo, el factor que marca la diferencia entre todos es el humano, por lo que la clave consiste en emplear el sentido común, permanecer alerta y desconfiar de páginas y proveedores de aplicaciones dudosas; pero especialmente, en tomar conciencia que nuestra vida no tiene que estar digitalizada en un dispositivo móvil.

Sergio Rentería Núñez