BUENAS PRÁCTICAS DE SEGURIDAD PARA LOS DISPOSITIVOS MÓVILES

CONSEJOS Y MEDIDAS PREVENTIVAS PARA LIMITAR LA EXPOSICIÓN AL RIESGO DE EXTRAVÍO DE DATOS SENSIBLES MEDIANTE CAMPAÑAS DE PHISHING Y/O INFECCIÓN DEL DISPOSITIVO A CAUSA DE MALWARES Y TROYANOS

1. Hacer uso de contraseñas robustas, inclusive para el desbloqueo / acceso al terminal (ver Anexo)

2. Realizar copias de seguridad del dispositivo movíl de forma periódica de cara a preservar los datos importantes

3. Evitar de liberar y/o manipular componentes del dispositivo móvil en sitios / tiendas no oficiales en la que no se ofrece ningún tipo de garantía

4. Instalar software original en lugar de software pirateado

5. Poner atención a los mensajes (SMS o Mail) así como llamadas desde numeros desconocidos o desde fuentes que no sean de confianza donde se soliciten datos personales, bien sea vía telefónica y bien sea mediante enlaces en los que no es posible determinar de forma clara y evidente el dominio de los mismos

6. Configurar debidamente el dispositivo mediante las opciones del sistema operativo de cara a evitar que se instalen aplicaciones procedentes de fuentes desconocidas.

7. En caso de robo del dispositivo denunciarlo y llamar al operador para bloquear la SIM y el terminal. Si se dispone del servicio de "*Borrado Remoto de la Información*" hacer uso de él.

8. No activar el bluetooth del móvil cuando no es necesario hacer uso del mismo así como evitar de realizar conexiones a dispositivos bluetooth desconocidos;

   Solicitar siempre autorización cuando alguien esté intentando conectar con su dispositivo.

   Asegúrese de activar el bluetooth en modo "*oculto*" evitando además emparejamientos (*asociaciones*) en lugares públicos, ya que los ataques mediante este canal de comunicación son multiplices (*ej.* *Bluejacking* , *Bluebugging*, *Bluesnarfing*, *etc..).*

9. Activar las conexiones a internet a través de la Wi-Fi sólo cuando sea necesario usarlas y evitar de conectarse a puntos de accesos desconocidos, ya que toda información, incluida la de tipo confidencial como conversaciones, contraseñas, datos bancarios, etc.. puede ser interceptada por el dueño del punto de acceso mediante el cual Usted está intentando conectarse a internet.

10. Desconectar o salir de la navegación desde aquellos servicios web que requieran contraseña antes de cerrar el navegador.

11. Cuando el sistema operativo notifique que está disponible una nueva versión de este así como cuando notifique la disponibilidad de nuevas actualizaciones sobre las aplicaciones instaladas en el dispositivo, aceptar e instalar las mismas, puesto que en la mayoría de las veces dichas actualizaciones, además de añadir funcionalidades, corrigen fallos de seguridad y evitan posibles infecciones derivadas por la presencia en el móvil de aplicaciones vulnerables.

12. En caso de querer deshacerse del dispositivo móvil se aconseja borrar el contenido del mismo de cara a evitar que la información persistida en este, llegue en manos de terceros.

    Ej. agendas, sms, fotos, cuentas de correo, aplicaciones que dan acceso a redes sociales, tiendas online o pasarelas de pago, caché y contraseñas almacenadas en el navegador

    Se aconseja por lo tanto formatear el dispositivo así como se aconseja que, siempre y cuando el sistema operativo lo permita, se utilice por ello la funcionalidad de restablecimiento del estado original de fábrica del teléfono (restauración y borrado).

13. Desconfíe de correos en los que se estén solicitando sus datos biométricos, mediante el envío de fotos o vídeos.

QUÉ HACER CUANDO EL DISPOSITIVO HA SIDO INFECTADO O EXISTE LA SOSPECHA DE QUE LO ESTÉ

1. Analizar la presencia de ficheros o carpetas anómalas mediante el uso de un antivirus, de cara a poder determinar y eliminar eventuales virus presentes en el dispositivo

2. Debido a que los antivirus no siempre son capaces de detectar todo tipo de malware o troyanos, se aconseja al usuario restablecer el dispositivo al estado original de fabrica

3. Modificar las credenciales de acceso a las aplicaciones que se encontraban instaladas en el dispositivo previo su formateo y restablecer el estado de fábrica del mismo.

4. Revisar las aplicaciones que se pretenden reinstalar en el dispositivo, garantizando que son necesarias y que provengan de los Markets oficiales y que sean emitidas por desarrolladores de confianza;

   Así mismo aseverar que dichas aplicaciones estén pidiendo únicamente aquellos permisos sobre el dispositivo y sobre su información personal que sean estrictamente necesarios para con la funcionalidad que se pretende realizar tras la instalación de dichas aplicaciones.

ANEXO

- Antes de definir nuevas claves de acceso a sus aplicaciones, analizar el dispositivo mediante un antivirus de cara a detectar la presencia de eventuales malwares o troyanos que puedan haberse instalado en su dispositivo

- La longitud de las contraseñas no debe ser inferior a ocho caracteres. A mayor longitud más difícil será de reproducir y mayor seguridad ofrecerá.

- No se deben reutilizar contraseñas utilizadas en el pasado.

-Construir las contraseñas con una mezcla de caracteres alfabéticos (donde se combinen las mayúsculas y las minúsculas), dígitos e incluso caracteres especiales (@, ¡, +, &).

- Usar contraseñas diferenciadas en función del uso (por ejemplo no debe usarse la misma para una cuenta de correo que la usada para acceso a servicios bancarios).

- Un buen método para crear una contraseña sólida es pensar en una frase fácil de memorizar y acortarla aplicando alguna regla sencilla.

- Se deben cambiar las contraseñas regularmente.

- La contraseña no debe contener el nombre de usuario de la cuenta, o cualquier otra información personal fácil de averiguar (cumpleaños, nombres de hijos, cónyuges, ...). Tampoco una serie de letras dispuestas adyacentemente en el teclado (qwerty) o siguiendo un orden alfabético o numérico (123456, abcde, etc.)

- Se deben evitar contraseñas que contengan palabras existentes en algún idioma (por ejemplo “campo”). Uno de los ataques más conocidos para romper contraseñas es probar cada una de las palabras que figuran en un diccionario y/o palabras de uso común.

- No se deben almacenar las contraseñas en un lugar público y al alcance de los demás (encima de la mesa escrita en papel, etc…).

- No compartir las contraseñas en Internet (por correo electrónico) ni por teléfono. En especial se debe desconfiar de cualquier mensaje de correo electrónico en el que le soliciten las mismas o indiquen que se ha de visitar un sitio Web para comprobarla. Casi con total seguridad se tratará de un fraude.