EQUIFAX®

Seguridad Movil:
Identificación de amenazas y recomendaciones.

Seguridad móvil: identificación de amenazas y recomendaciones

Elaborado por: Alicia Baldeón, Information Security Officer de Equifax Ecuador

Equifax es una firma global de Big Data, Analítica y Alta Tecnología. Líder mundial en ciberseguridad, reconocida por Gartner Control Maturity Benchmark, la publicación más importante en materia de ciberseguridad, como la firma de mayor madurez en seguridad de la información entre las 11 industrias más relevantes del mundo.

Algunas cifras del contexto:

Al cumplirse un año de la pandemia por el COVID-19 en Ecuador, las transacciones realizadas en los canales digitales tuvieron un aumento del 113% anual entre febrero de 2020 y febrero de 2021.

Si bien, estas cifras representan una dinamización de los servicios financieros digitales, también implican un desafío en términos de seguridad, pues así como la tecnología avanza también lo hacen los riesgos y las modalidades de ciberdelitos.

Principales amenazas a la seguridad móvil:

Malware Bancario: El malware móvil basado en la banca va en aumento, ya que los hackers buscan comprometer a los usuarios que prefieren llevar a cabo todos sus negocios desde sus dispositivos móviles.

Ransomware móvil: El ransomware, "bloquea" datos importantes del usuario, como documentos, fotos, mediante el cifrado de la información y luego exige el pago de un rescate.

Spyware móvil: Es cargado como un programa en el dispositivo, supervisa tu actividad, registra tu ubicación y sustrae información crítica, como nombres de usuario y contraseñas de cuentas de correo electrónico o sitios visitados.

Malware MMS: Los creadores de malware también buscan maneras de aprovechar la comunicación basada en texto como una forma de distribuir malware.

Troyanos: Los troyanos de SMS siembran el caos financiero mediante el envío de mensajes SMS a números con tarificación especial de todo el mundo.

¿Cómo evitar, identificar y eliminar malware, spyware de tu dispositivo móvil ?

Evitar

- Descargar aplicaciones que no sean verificadas por desarrolladores.
- Navegadores inseguros. Mejor hacerlo con Safari, Firefox o Google.
- Descargar archivos de dudosa procedencia.

- No tener un antivirus o antimalware activo que sea verificado.
- Usar el teléfono sin que tenga un firewall activo.

Identificar

- Cambios de ajustes y permisos sin su consentimiento.
- Si las apps nativas han sido sustituidas por otras.
- Gasto desmesurado de la batería. Puede ser señal de una intromisión.
- Gasto injustificado de datos móviles (Internet).
- Detectar un rendimiento anómalo en el teléfono.
- Verificar la instalación de aplicaciones sin permiso.

Eliminar

- Minimizar las estafas y proteger el teléfono con aplicaciones de escaneo, análisis, limpieza y eliminación de malware y spyware, seguridad contra ransomware, etc., el mismo que desinstalará/eliminará las amenazas.

¿Cómo actuar frente a una suplantación de identidad o robo?

Frente a la suplantación de identidad:

- Reportar al banco o entidad correspondiente.
- Bloquear cuentas bancarias.
- Establecer el monto máximo de transferencia.

Frente al robo del celular:

- Bloquear remotamente el terminal.
- Reportar a la operadora móvil.
- Denunciar robo a las autoridades.

Frente a la clonación del chip:

- Verificar señal del dispositivo.
- Reportar a la operadora y al banco.
- Bloqueo del número.

Recomendaciones para la seguridad móvil

Cifrado de datos: Garantiza la seguridad del Smartphone. Protege la información privada contra robos o amenazas. Aumenta la confidencialidad de tu dispositivo.

Contraseñas seguras: Usar combinaciones de letras en mayúsculas y minúsculas, junto con números y símbolos. Cambiar la contraseña cada cierto intervalo de tiempo para evitar riesgos.

Permisos de aplicaciones: Verificar permisos de acceso a la cámara, micrófono, contactos. Controlar que documentos o información está utilizando la aplicación.

Usar una conexión VPN: Añade una capa extra de seguridad cifrando los paquetes que se transmiten. Se conecta y desconecta fácilmente.

Verificación de dos pasos: Potencia la seguridad de los smartphone. Evita que alguien entre sin permiso a una cuenta nuestra. Fácil configuración.