NOTA DE PRENSA. N.° 154-2023

Mi celu seguro: ¿qué medidas preventivas puedo tomar para proteger mi información personal ante un posible robo de celular?

- Como medidas de seguridad, se aconseja activar el código PIN del chip, desactivar el acceso al puerto USB y guardar la clave del sistema operativo en un lugar seguro.

El celular se ha convertido en una billetera digital. En el equipo móvil no solo guardamos información valiosa, sino también lo utilizamos para realizar diversas operaciones bancarias. Por eso, es necesario tomar diversas acciones preventivas a fin de proteger nuestros datos personales y dinero ante un posible robo de nuestro celular, informó el Organismo Supervisor de Inversión Privada en Telecomunicaciones (OSIPTEL).

En el marco de la campaña Mi celu seguro, la directora de Atención y Protección del Usuario del OSIPTEL, Tatiana Piccini Antón, recomendó, como medida preventiva de seguridad, **activar el código PIN de la tarteja SIM (chip)** de nuestro celular para que no sea usada en otro dispositivo.

Para ello, añadió que debemos ingresar a configuración o ajustes desde el celular y buscar la opción “bloqueo de tarjeta de tarjeta SIM” o “pin de la SIM”. Luego, debemos digitar el pin de cuatro dígitos, según la empresa operadora (para Movistar es 1234; Entel, 1234; Claro, 1111, y Bitel, 0000). Una vez realizado este paso, debemos seleccionar “cambiar el pin de la tarjeta SIM” e ingresar un núevo código de 4 dígitos.

Otra acción preventiva es **desactivar el acceso al puerto USB** a fin de evitar que los ciberdelincuentes manipulen el software de nuestro celular. Para la depuración USB en Android, debemos ir a “ajustes”, “opciones de desarrollador” y “desactiva: depuración por USB”.

La representante del ente regulador también aconsejó **guardar la clave de nuestra cuenta vinculada al sistema operativo** (Google para Android y iCloud para iPhone) en un lugar seguro, nunca en nuestro teléfono. “En caso nos roben el equipo móvil, podremos ingresar y bloquear el celular. De esta manera, evitaremos que el ladrón acceda a nuestra información y datos”, mencionó Piccini Antón.

Más consejos de seguridad

Como acciones preventivas, además, podemos crear contraseñas seguras en bancos y aplicaciones con combinaciones de letras, números y símbolos; así como copias de seguridad regulares, y anotar el código IMEI del equipo en un lugar seguro y no divulgarlo. Este código de 15 dígitos se puede ubicar en la parte posterior del celular o en la bandeja de soporte del SIM *card*, o marcando *#06# desde el celular.

También podemos activar un segundo factor de autenticación para el desbloqueo del celular (código adicional, huella dactilar, entre otros), mantener el equipo móvil actualizado de activirus y parches de seguridad al día, verificar las URL de los sitios web

y analizar los permisos otorgados al momento de descargar las aplicaciones. Por último, seamos precavidos. No confiemos en llamadas, mensajes o links de redes sociales.

Los interesados pueden ingresar a https://sociedadtelecom.pe/landing/miceluseguro/ para obtener más información sobre la campaña **Mi celu seguro** del OSIPTEL.

Lima, 27 de diciembre de 2023