

El carterista del móvil: la ciberseguridad de los datos, en peligro

El robo de los dispositivos móviles se vuelve cada vez más lucrativo, no únicamente por el aumento de valor de los terminales, también porque son un punto de acceso a datos personales y bancarios. Datos y consejos para evitarlo

Alrededor de 8 de cada 10 europeos posee, por lo menos, un Smartphone. La penetración de estos dispositivos y su interconectividad abre la veda a los carteristas del móvil.

Y es que los teléfonos inteligentes suponen una gran fuente de datos personales e incluso bancarios, que son aprovechados por los ladrones o piratas informáticos en los momentos más inesperados. Tanto es así que, durante el año anterior, el Instituto Nacional de Ciberseguridad (INCIBE) se ocupó de más de 110.000 casos de ataques cibernéticos.

Uno de los ejemplos más populares de fraude es el phishing financiero, una suplantación de identidad que tiene como finalidad el acceso a información privada o bancaria y que, según expertos en softwares de seguridad, el registró llegó a alcanzar un ataque por segundo.

Los consejos de los expertos en seguridad digital

Uno de los consejos más útiles para evitar que los datos lleguen a las manos equivocadas es el conocimiento del número IMEI del terminal, que posibilitará su bloqueo en caso de tener cualquier sospecha. Para conocerlo, sólo hay que teclear *#06# y anotarlo en un lugar seguro.

Otro de los trucos que impedirán la sustracción indebida de datos es mantener al día las actualizaciones del software de los dispositivos. “Aunque normalmente todas las API’s de monetización están preparadas para integrarse en cualquier sistema operativo, si se mantiene el teléfono actualizado, se puede evitar ponerse en riesgo”, explica Carles Boronat, Responsable de Comunicación de Monsan, empresa tecnológica dedicada al desarrollo de plataformas de marketing móvil y de monetización móvil.

Trabas que aumentan la seguridad: Letra pequeña, huellas digitales y bloqueo automático

Proteger los datos personales y bancarios está en las manos del usuario y, también, en sus ojos. Tanto es así que, aunque algunos servicios ofrecen la información o letra pequeña de manera muy clara “hay piratas informáticos que, a través de apis, configuran aplicaciones fraudulentas que acaban repercutiendo en facturas elevadísimas”.

Por eso, comprobar la fiabilidad de terceros en cuanto se accede a un método de pago o a la descarga de una aplicación y “es tan fundamental como proteger el móvil con contraseña o limitar su acceso a través de huella digital”. Unas medidas de ciberseguridad que, unidas a la variedad de contraseñas y la desactivación de las cookies y auto-relleno de datos, “suponen una barrera entre los carteristas de

móviles y nuestros datos personales y bancarios”.

Datos de contacto:

Carles Boronat Muñoz

Comunicación Monsan

+34 685952754

Nota de prensa publicada en: [España](#)

Categorías: [E-Commerce](#) [Ciberseguridad](#)

NotasdePrensa

<https://www.notasdeprensa.es>