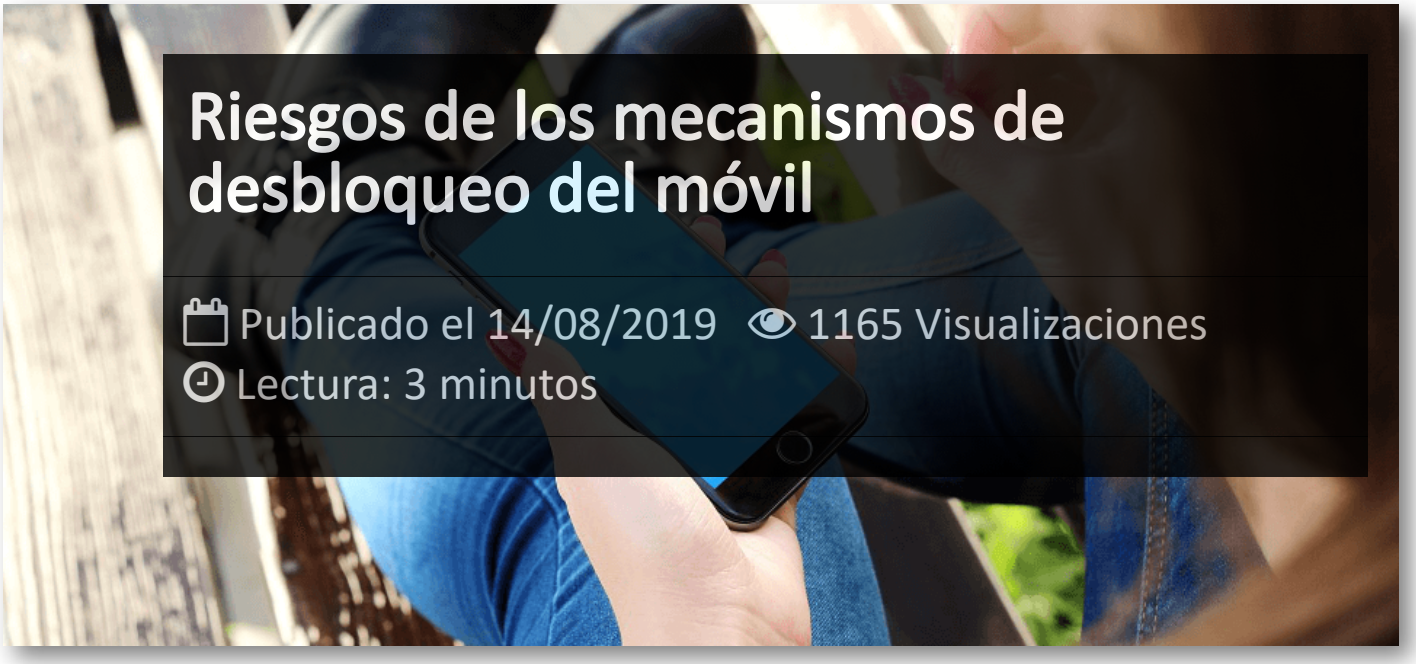
< Riesgos de los mecanismos de desbloqueo del móvil - Blog de Tecnología e Informática >



Actualmente disponemos de varios sistemas de desbloqueo en los smartphone, desde los tradicionales códigos PIN numéricos hasta los más recientes ejemplos de reconocimiento biométrico.

A pesar del alto nivel tecnológico que poseen estos mecanismos que aportan seguridad al móvil, estos presentan algún riesgo de seguridad que es interesante conocer.

Código PIN

Es el método de desbloqueo más habitual y más antiguo, normalmente de cuatro dígitos. Se recomiendan que para fortalecer la seguridad de esta medida es necesario evitar códigos fáciles como **1234** y elegir números con los que no se tenga ninguna relación personal, evitando fecha de nacimiento o de aniversario.

Dibujar un patrón

Otro método parecido al del PIN es el de dibujar un patrón en la pantalla para proceder al desbloqueo. También se trata de un método seguro si se siguen algunos consejos básicos como que la dirección del patrón no sea de izquierda a derecha, ni de arriba hacia abajo, ni dibujando la inicial del nombre.

Sin embargo, y a pesar de estas precauciones, en ambos casos no tendremos nada que hacer si el móvil es hackeado, ya que existen aplicaciones diseñadas para acceder a los sistemas operativos, sorteando sin problemas contraseñas de seguridad como estas.

Huella dactilar

El caso de la huella dactilar es uno de los modos de bloqueo más seguros ya que no existen dos huellas dactilares idénticas. No obstante, el peligro se encuentra en las huellas digitales, que son huellas artificiales o falsas que pueden llegar a coincidir hasta en un 65 por ciento de las veces con las reales.

Este tipo de hackeo es posible porque los escáneres empleados en los teléfonos, al registrar la huella, leen las distintas partes y fotografían hasta diez imágenes de ellas. De esta manera, si solo una parte de la huella coincide con una de esas imágenes, resulta suficiente para tener acceso al dispositivo.

Reconocimiento facial

Otro sistema de reconocimiento biométrico es el reconocimiento facial, que se basa en el uso de la cámara frontal y de sensores infrarrojos. Un ejemplo es el sistema FaceID de Apple, que la compañía recoge que tiene una probabilidad de error de tan solo uno entre un millón. No obstante, fiabilidad de este mecanismo no es completa.

Debido a que la cámara examina y memoriza los rasgos principales pero no siempre es capaz de capturar toda la profundidad de la cara, esta podría identificar una imagen impresa en alta calidad del mismo rostro como el propio usuario.

De hecho, un estudio publicado por la asociación de consumidores de los Países Bajos (Consumentenbond) ha analizado 60 modelos de smartphone y ha determinado que 26 de ellos, de fabricantes como *Huawei*, *Xiaomi* y *Motorola* -entre otros-, no son seguros y han podido desbloquearlos con una fotografía.

Escáner del iris

El escáner del iris es otra alternativa de identificación biométrica que funciona con un emisor de infrarrojos y la aparición de dos puntos en la pantalla que indican al usuario hacia dónde dirigir la mirada para verificar el reconocimiento. El problema de este método es que si la luz del sol da directamente al sensor, tardará demasiado o no funcionará.

De modo que el reconocimiento de iris es bueno, como complemento, no como único sensor biométrico.

Artículos Relacionados

Cómo ver videos de YouTube sin publicidad y sin pagar YouTube Premium con KMPlayer

Cómo solicitar y descargar toda la información que WhatsApp tiene sobre mi

El mejor truco de seguridad para tu móvil

WhatsApp crea una nueva función para liberar espacio de tu dispositivo móvil

Y tú, ¿ Qué opinas ?

Agregar Comentario

0 Comentarios