

Google amplía las funciones contra el robo de móviles Android

El robo de móviles Android está a la orden del día y lo mismo podemos decir de los iPhones de Apple. **Se cuentan por millones los hurtos o extravíos que se producen año tras año.** Un smartphone es un objetivo codiciado por los rateros su pequeño tamaño, la facilidad para su sustracción, su alto precio y las posibilidades de venta.

Teniendo en cuenta que hoy en día el móvil inteligente alberga casi toda nuestra vida digital, en caso de robo o extravío a la pérdida propia del dispositivo tenemos que unir el coste de que **terceros puedan acceder a nuestros datos** profesionales, financieros o personales, además de dejarnos ‘vendidos’ si acceden a nuestras contraseñas y servicios. Y ya no solo los propios del móvil, ya que éste tipo de dispositivos suele usarse para la seguridad de los accesos de otros, por ejemplo a la hora de la doble autenticación.

Más y mejores funciones contra el robo de móviles Android

Si el usuario debe poner medidas para [evitar el robo o extravío del dispositivo físico](#), otra parte de la ecuación es prevenir, dificultar o impedir que los ladrones accedan a los datos de los teléfonos robados.

Google anunció anoche una importante actualización de su sistema de protección antirrobo para Android, con nuevas herramientas y configuraciones diseñadas para dificultar el acceso y la explotación de smartphones robados por parte de delincuentes. Las actualizaciones, detalladas en el [blog oficial de seguridad de Google](#), **amplían las protecciones existentes de Android e incorporan defensas más robustas y controles de usuario más flexibles.**



Para contrarrestar las amenazas de que terceros accedan a datos confidenciales y los fraudes de identidad y financieros que pueden conllevar, Google está implementando múltiples funciones de protección que funcionan antes, durante y después de un robo.

La actualización se centra en un **bloqueo de autenticación**

fallida renovado. Introducida previamente en Android 15 , esta función ahora cuenta con su propio interruptor en la configuración de [Android 16](#), lo que te permite decidir si tu teléfono se bloquea automáticamente tras repetidos intentos incorrectos de introducir el PIN o la biometría. Esto te da mayor control sobre la eficacia de la defensa de tu teléfono contra intentos de fuerza bruta sin comprometer la seguridad.

Google también está reforzando la **seguridad biométrica** en toda la plataforma. La función de 'Verificación de Identidad' se ha ampliado para aplicarse a todas las aplicaciones y servicios que utilizan la Solicitud Biométrica de Android (la ventana emergente que solicita tu huella dactilar o rostro para confirmar tu identidad), incluyendo aplicaciones bancarias de terceros y gestores de contraseñas. Esto significa que, incluso si un ladrón logra eludir la pantalla de bloqueo, se enfrentará a una barrera biométrica adicional antes de acceder a aplicaciones sensibles.

En cuanto a la recuperación, Google ha mejorado **Remote Lock**, una herramienta que permite bloquear un dispositivo perdido o robado desde un navegador web ingresando un número de teléfono verificado. La compañía agregó un desafío de seguridad opcional para garantizar que solo el propietario legítimo pueda iniciar el bloqueo remoto, una importante protección contra el uso indebido.

MUY COMPUTER