¿Cómo se filtran las aplicaciones maliciosas en la Google Play Store?

A la hora de descargar una aplicación móvil, los expertos recomiendan hacerlo desde las tiendas oficiales. En otras palabras, evitar las plataformas de terceros. Sin embargo, el malware en Google Play es moneda corriente. ¿Cómo logran los programas maliciosos colarse en un entorno respaldado por un gigante y que, al menos en los papeles, promete garantías?

Un informe reciente de Kaspersky reveló que en lo que va de 2023 se descargaron más de 600 millones de herramientas maliciosas en la tienda oficial de Android. Según la firma especializada en ciberseguridad, ni siquiera una tecnológica superpoderosa como Google consigue frenar a los programas nocivos. Con ellos, espían a los usuarios, roban datos sensibles e invaden con anuncios no deseados, entre otras acciones perniciosas.

“Los usuarios tienden a pensar que la tienda oficial es segura para instalar aplicaciones (…) y que éstas son examinadas minuciosamente por los moderadores”, señalan al respecto en el reporte. “Sin embargo, hay que tener en cuenta que allí hay más de 3 millones de herramientas únicas y que revisarlas a fondo está más allá de los recursos de, incluso, una de las corporaciones más grandes del mundo”, añaden.

Tomando las alertas de Kaspersky como puntapié, Hipertextual conversó con especialistas y con representantes de Android para comprender cómo logran los piratas eludir las barreras de seguridad y filtrar malware en Google Play. Además, repasaremos una serie de claves para estar a salvo —cuanto sea posible— de los riesgos asociados a los programas maliciosos.

Con información de Hipertextual