Google está desarrollando una nueva función de seguridad para Android que impide a los usuarios modificar configuraciones críticas mientras una llamada telefónica está en curso.

En particular, esta medida de protección contra fraudes impide que los usuarios habiliten la instalación de aplicaciones de fuentes no verificadas y otorguen permisos de accesibilidad. El portal *Android Authority* fue el primero en informar sobre esta novedad.

Si un usuario intenta realizar estos cambios durante una llamada, recibirá la siguiente notificación:
«Los estafadores suelen solicitar este tipo de acciones durante conversaciones telefónicas, por lo que se ha bloqueado para tu seguridad. Si alguien desconocido te indica que lo hagas, podría tratarse de un fraude.»

Asimismo, la función evita que las aplicaciones obtengan permisos de accesibilidad mientras la llamada está en curso.

Actualmente, esta característica está disponible en la Beta 2 de Android 16, que fue lanzada a principios de esta semana. Con esta actualización, se busca dificultar un método frecuentemente utilizado por delincuentes informáticos para propagar software malicioso.

Esta estrategia, conocida como *telephone-oriented attack delivery* (TOAD), consiste en enviar mensajes de texto a posibles víctimas, instándolas a llamar a un número al generar una sensación de urgencia falsa.

El año pasado, el *NCC Group* y el Centro Nacional de Ciberseguridad de Finlandia (*NCSC-FI*) revelaron que los ciberdelincuentes estaban distribuyendo aplicaciones fraudulentas mediante una combinación de mensajes SMS y llamadas, engañando a los usuarios para que instalaran malware como *Vultr*.

Esta nueva función llega después de que Google ampliara las restricciones en la configuración del sistema para incluir más permisos, con el propósito de evitar que las aplicaciones instaladas fuera de la Play Store accedan a información sensible.

Además, la empresa ha implementado una opción para bloquear automáticamente la instalación de aplicaciones potencialmente peligrosas en regiones como Brasil, Hong Kong, India, Kenia, Nigeria, Filipinas, Singapur, Sudáfrica, Tailandia y Vietnam, con el fin de combatir las estafas digitales.