Google agrega un período de espera de 24 horas para la instalación de apps no verificadas mediante métodos no oficiales para reducir el malware y estafas

Google anunció el jueves un nuevo “flujo avanzado” para la instalación externa de aplicaciones en Android que impone un periodo obligatorio de espera de 24 horas antes de instalar apps provenientes de desarrolladores no verificados, con el objetivo de equilibrar la apertura del sistema con mayores niveles de seguridad.

Estos cambios surgen en el contexto de una política anunciada el año pasado por la compañía, que exige que todas las aplicaciones de Android estén registradas por desarrolladores verificados para poder instalarse en dispositivos certificados. Según explicó, esta medida busca identificar más rápidamente a actores maliciosos y evitar la distribución de software malicioso.

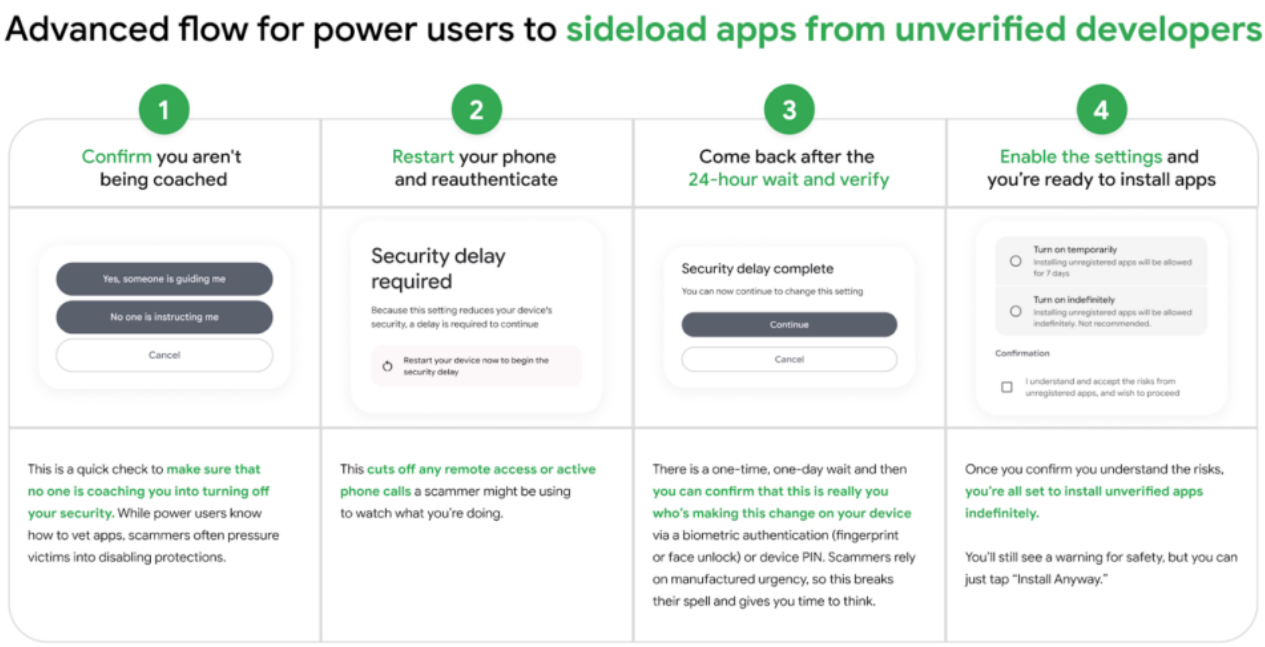
Esto también contempla situaciones en las que ciberdelincuentes engañan a usuarios para que instalen aplicaciones externas y les concedan permisos elevados, lo que podría permitir desactivar Play Protect, la herramienta antimalware integrada en todos los dispositivos Android certificados por Google.

Sin embargo, los requisitos obligatorios de registro han generado críticas por parte de más de 50 desarrolladores y tiendas de aplicaciones, entre ellos F-Droid, Brave, Electronic Frontier Foundation, Proton, The Tor Project y Vivaldi. Estos señalan que las medidas podrían generar fricción, elevar barreras de entrada y plantear preocupaciones sobre privacidad y vigilancia, especialmente ante la falta de claridad sobre qué datos personales deben proporcionar los desarrolladores, cómo se almacenarán, protegerán o utilizarán, y si podrían ser solicitados por gobiernos o procesos legales.

Como respuesta a estas preocupaciones, Google destacó que este nuevo flujo avanzado permite a usuarios experimentados seguir instalando aplicaciones de desarrolladores no verificados mediante un proceso único que incluye los siguientes pasos:

- Activar el modo desarrollador en la configuración del sistema.
- Confirmar que la acción se realiza de forma voluntaria y sin influencia externa.
- Reiniciar el dispositivo y volver a autenticarse para evitar que un atacante supervise las acciones del usuario.

- Esperar 24 horas y confirmar nuevamente la decisión mediante autenticación biométrica o PIN.
- Instalar aplicaciones de desarrolladores no verificados, ya sea de forma indefinida o durante un periodo limitado de siete días.



«Durante ese periodo de 24 horas, creemos que resulta mucho más difícil para los atacantes mantener su ataque,» señaló Sameer Samat a Ars Technica. *«En ese tiempo, probablemente puedas darte cuenta de que tu familiar no está realmente detenido o que tu cuenta bancaria no está siendo atacada.»*

Google también indicó que planea ofrecer cuentas gratuitas de "distribución limitada" que permitirán a desarrolladores aficionados y estudiantes compartir aplicaciones con hasta 20 dispositivos sin necesidad de *«proporcionar una identificación oficial ni pagar una tarifa de registro.»*

Cabe destacar que este proceso no aplica a instalaciones realizadas mediante Android Debug Bridge (ADB). Las cuentas de distribución limitada y el flujo avanzado estarán disponibles en agosto de 2026, antes de que entren en vigor los nuevos requisitos de verificación de desarrolladores al mes siguiente.

«Sabemos que un enfoque único no funciona para un ecosistema tan diverso como el nuestro,» afirmó Google. *«Queremos asegurarnos de que la verificación de identidad no sea una barrera de entrada, por lo que ofrecemos diferentes opciones adaptadas a distintas necesidades.»*

Este anuncio coincide con la aparición de un nuevo malware para Android llamado Perseus, que está atacando activamente a usuarios en Turquía e Italia con el objetivo de tomar el control de los dispositivos (DTO) y cometer fraudes financieros.

En los últimos cuatro meses, se han identificado al menos 17 familias de malware para Android en circulación, entre ellas FvncBot, SeedSnatcher, ClayRat, Wonderland, Cellik, Frogblight, NexusRoute, ZeroDayRAT, Arsink (y su variante mejorada SURXRAT), deVixor, Phantom, Massiv, PixRevolution, TaxiSpy RAT, BeatBanker, Mirax y Oblivion RAT.