Google anunció el jueves una versión mejorada de Navegación Segura para ofrecer protección en tiempo real de las URL, preservando la privacidad y evitando que los usuarios accedan a sitios potencialmente peligrosos.

> *«El modo de protección estándar para Chrome en escritorio e iOS verificará los sitios en tiempo real utilizando la lista de sitios maliciosos conocidos de Google almacenada en los servidores»,* explicaron Jonathan Li y Jasika Bawa de Google.
>
> *«Si sospechamos que un sitio representa un riesgo para ti o tu dispositivo, recibirás una advertencia con detalles adicionales. Al verificar los sitios en tiempo real, esperamos bloquear un 25% más de intentos de phishing».*

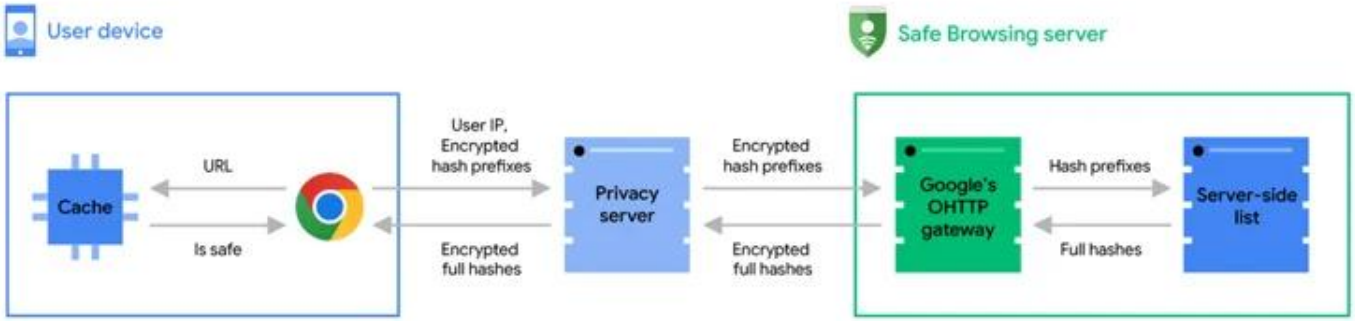
Hasta ahora, el navegador Chrome utilizaba una lista local de sitios peligrosos conocidos, que se actualizaba cada 30 a 60 minutos, y luego comparaba cada sitio visitado con esta lista utilizando un enfoque basado en hash.

Google reveló por primera vez sus planes de cambiar a verificaciones en tiempo real en el servidor, sin compartir el historial de navegación de los usuarios con la empresa, en septiembre de 2023.

El motivo del cambio, según el gigante de las búsquedas, se debe al rápido crecimiento de la lista de sitios web maliciosos y al hecho de que el 60% de los dominios de phishing existen por menos de 10 minutos, lo que dificulta su bloqueo.

> *«No todos los dispositivos tienen los recursos necesarios para mantener esta lista en crecimiento, ni siempre pueden recibir y aplicar actualizaciones con la frecuencia necesaria para beneficiarse de una protección completa»*, agregaron.

Por lo tanto, con la nueva arquitectura, cada vez que un usuario intenta visitar un sitio web, la URL se verifica con las cachés globales y locales del navegador que contienen URLs conocidas como seguras y los resultados de verificaciones anteriores de Navegación Segura, con el fin de determinar el estado del sitio.



En ausencia de la URL visitada en las cachés, se lleva a cabo una verificación en tiempo real mediante la transformación de la URL en hash completo de 32 bytes, que luego se reduce a prefijos de hash de 4 bytes, se cifra y se envía a un servidor de privacidad.

> *«El servidor de privacidad elimina posibles identificadores de usuario y transmite los prefijos de hash cifrados al servidor de Navegación Segura a través de una conexión TLS que mezcla las solicitudes con las de muchos otros usuarios de Chrome»,* explicó Google.

Posteriormente, el servidor de Navegación Segura desencripta los prefijos de hash y los compara con la base de datos del servidor para devolver los hashes completos de todas las URLs no seguras que coincidan con uno de los prefijos de hash enviados por el navegador.

Finalmente, en el lado del cliente, se comparan los hashes completos con los hashes completos de la URL visitada, y se muestra un mensaje de advertencia si hay coincidencia.

Google también confirmó que el servidor de privacidad es simplemente un relé HTTP Oblivious (OHTTP) operado por Fastly que se sitúa entre Chrome y el servidor de Navegación Segura para evitar que este último acceda a las direcciones IP de los usuarios, evitando así la correlación de las verificaciones de URL con el historial de navegación en Internet de un usuario.

> *«En última instancia, Navegación Segura ve los prefijos de hash de tu URL pero no tu dirección IP, y el servidor de privacidad ve tu dirección IP pero no los prefijos de hash. Ninguna parte tiene acceso tanto a tu identidad como a los prefijos de hash. Por lo tanto, tu actividad de navegación permanece privada»* , enfatizó la empresa.