En la conferencia de desarrolladores de I/O 2019 de Google, la compañía anunció su plan para introducir dos nuevas características de privacidad orientadas a la seguridad en las siguientes versiones de su navegador Web Chrome.

Como un intento por permitir que los usuarios bloqueen el seguimiento en línea, Google anunció dos nuevas características, las cookies SameSite mejoradas y la protección de huellas digitales, que Google ofrecerá de antemano en el navegador web en el transcurso del año.

Las cookies, también conocidas como cookies HTTP o cookies de navegador, son pequeños archivos de información que los sitios web almacenan en las computadoras, que juegan un papel importante en la mejora de la experiencia en Internet.

Las cookies son creadas por un navegador web cuando un usuario carga un sitio en particular, lo que ayuda al sitio a recordar información sobre la visita, como información de inicio de sesión, idioma, elementos del carrito de compras, entre otros.

Sin embargo, las cookies también están siendo utilizadas ampliamente para identificar a los usuarios y hacer un seguimiento de las actividades, no solo en el sitio web que emitió una cookie, sino también en cualquier sitio de terceros que incluya un recurso compartido por el mismo sitio, por ejemplo, las cookies utilizadas para la retargetación de anuncios y publicidad comportamental.

Debido a que actualmente no existe forma estándar de identificar o categorizar cómo los sitios web utilizan las cookies, todas las cookies que se utilizan para diferentes propósitos tienen el mismo aspecto que los navegadores y al eliminarlas, se desconectará de todos los sitios y se restablecen las preferencias en línea.

Las cookies mejoradas de SameSite ofrecen más control a los usuarios

Aunque la compañía lo reconoce, Google tiene previsto modificar la forma en que funcionan las cookies en distintos sitios por medio de Internet, lo que facilita a los usuarios del

navegador Chrome bloquear o eliminar todas las cookies de terceros sin perder información y la configuración de inicio de sesión.

En una publicación detallada, Google explica un nuevo mecanismo que los desarrolladores de sitios web deben seguir en los próximos meses para especificar explícitamente qué cookies en sus sitios pueden funcionar en todos los sitios web y se pueden utilizar para hacer un seguimiento de los usuarios.

El nuevo mecanismo se basa en el atributo de cookie SameSite que ofrece a los desarrolladores tres opciones diferentes para controlar el comportamiento, y más transparencia para los usuarios, revelando si una cookie del navegador es para el mismo sitio o para distintos.

Los desarrolladores de sitios web pueden optar por una mayor seguridad al establecer el valor del atributo SameSite en «estricto» o «laxa», que limita una cookie a las solicitudes del mismo sitio, o en «ninguno» cuando se requiere explícitamente que esté disponible para sitios cruzados.

La nueva actualización limitaría las cookies entre sitios a las conexiones HTTPS y también dificultaría que los sitios maliciosos aprovechen las vulnerabilidades entre los sitios.

> *«Este cambio también tiene un beneficio de seguridad importante para los usuarios, ya que protege las cookies de inyecciones de sitios cruzados y ataques de divulgación de datos como Specter y CSRF (falsificación de solicitudes en sitios múltiples) de forma predeterminada. También anunciamos nuestro plan para eventualmente limitar las cookies entre sitios a las conexiones HTTPS, brindando importantes protecciones de privacidad adicionales para nuestros usuarios»,* explicó Google.

Con el lanzamiento de Chrome 76, Google también permitirá que los usuarios establezcan el comportamiento predeterminado para que su navegador defina si debería aceptar o rechazar

las cookies entre sitios cuando visita un sitio web.

Nuevas protecciones contra las huellas dactilares del navegador

Además de las cookies, la identificación del navegador también es una técnica común y altamente precisa que utilizan los sitios web para identificar y rastrear a los usuarios individuales en todos los sitios web sin su conocimiento.

La huella digital del navegador es una forma muy efectiva de identificar con precisión a los usuarios por medio de la recopilación de una gran gama de datos acerca de sus dispositivos por medio de las API del navegador y luego combinarlos para calcular y asignar un valor único a cada navegador que pueda ser rastreado en Internet.

En la conferencia de desarrolladores de I/O 2019, Google también anunció que Chrome dificultará la identificación de huellas dactilares del navegador al reducir las formas en que se pueden tomar huellas digitales pasivamente en los navegadores de Internet.

> *«Debido a que las huellas digitales no son transparentes ni están bajo el control del usuario, se produce un seguimiento que no respeta la elección del usuario. Esta es la razón por la que Chrome planea restringir de forma más agresiva las huellas digitales en la web»*, dijo Google.

Sin embargo, Google reconoce que tanto las cookies entre sitios como las huellas digitales se utilizan más allá del simple rastreo de los usuarios en línea y que la compañía está *«comprometida a trabajar en el ecosistema web para entender cómo Chrome puede seguir apoyando estos casos de uso positivos y construir una mejor web»*.