SOCIEDAD | NUEVAS TECNOLOGÍAS

Investigadores de la UVa advierten del peligro de la app que graba el iris del ojo

El palentino Amador Aparicio y el Grupo en Ingeniería de la Privacidad del Departamento de Informática analizan la aplicación móvil vinculada a Woldcoin, la empresa que ofrece criptomonedas a cambio de datos biométricos

CARLOS H. SANZ / PALENCIA

El pasado día 6, la Agencia Española de Protección de Datos (AEPD) prohibía a la empresa Worldcoin, tras recibir varias reclamaciones, seguir recogiendo datos biométricos durante, al menos tres meses. Unos días antes, en el centro comercial Río Shopping de Valladolid, centenares de jóvenes hacían cola para escanearse el iris del ojo a cambio de criptomonedas.

El creador de Worldcoin, el mismo de la inteligencia artificial ChatGPT, asegura que su intención es «crear una forma confiable de autenticar la identidad online de los seres humanos». Además, defiende también que su proyecto puede ser «un camino hacia una renta básica universal financiada por la IA».

Dinero -aunque sea digital- a cambio de estarse quieto unos segundos para que una aplicación grabe uno de los rasgos capaces de indentificar a una persona sin género de duda. A 3,4 millones de personas les ha convencido la propuesta, de ellos 360.000 en España.

Una propuesta demasiado bonita para ser verdad. Así al menos lo han creído el Grupo de Investigación en Ingeniería de la Privacidad del Departamento de Informática de la Universidad de Valladolid, del que forma parte el palentino Amador Aparicio.

El profesor de la Universidad de Valladolid y responsable de Ciberseguridad en la empresa Zunder ha rebuscado en las entraña de la aplicación *WorldApp* para examinar específicamente «el uso y el impacto de los permisos de Android que solicita la aplicación en la privacidad de los usuarios».

Cuando una persona decide participar, un dispositivo llamado Orb escanea su ojo y genera un código único e irreplicable llamado Irishash, el cual se guarda en la cadena de bloques (*blockchain*). A cambio, recibe unas criptomonedas llamadas worldcoin (WLD) que al cambio son uno 30 euros. Ese dinero digital se puede utilizar a través de una aplicación móvil llamada *WorldApp* que permite pagos, transferencias o compras tanto en criptomoneda como en activos tradicionales.

Amador Aparicio y el Grupo de Investigación en Ingeniería de la Privacidad han analizado el impacto esa app sobre la privacidad del usuario y, en concreto, «las implicaciones de ciertos permisos con respecto a la privacidad y la seguridad de los datos de los usuarios, como el acceso a la ubicación, contactos y archivos multimedia del dispositivo o información relacionada con los servicios de Google».

Este dispositivo llamado Orb escanea los ojos y genera un código único e irreplicable llamado Irishash. / STEVE JURVETSON

HASTA 23 PERMISOS. Amador Aparicio explica que la aplicación móvil de Worldcoin tiene un total e 23 permisos declarados, «de los cuales 10 son de tipo *dangerous*, es decir, que impactan en la privacidad de los usuarios; nueve de tipo normal y cuatro de otro tipo. «Hay uno en particular que permite a las aplicaciones acceder a los servicios proporcionados por Google en dispositivos Android, como Google Maps y Google Location Services. Este permiso esencial para aplicaciones que dependen de la funcionalidad de ubicación proporcionada por Google para ofrecer servicios como navegación, búsqueda de lugares y seguimiento de ubicación», detalla el profesor de la UVa.

Esto, para Aparicio, plantea «preocupaciones» porque «implica el acceso a servicios que pueden recopilar datos de ubicación del usuario». «Aunque el permiso otorga acceso a los servicios de Google y no directamente a los datos personales del usuario, estos servicios pueden recopilar información sensible sobre la ubicación del dispositivo y los patrones de actividad del usuario».

«Este es uno de esos permisos que se conceden durante la instalación de la aplicación móvil y que el usuario no puede modificar. De hecho, debe utilizarse con cuidado, ya que permite a una aplicación acceder a datos sensibles y servicios proporcionados por Google y, por lo tanto, los desarrolladores deben utilizar este permiso solo cuando sea absolutamente necesario y seguir las políticas y prácticas recomendadas por Google».

> La aplicación móvil tiene 23 permisos declarados, de los cuales **10 son de tipo 'dangerous'**

«Los usuarios deben estar informados sobre el uso de este permiso por parte de una aplicación y tener la opción de aceptar o denegar el permiso, ya que puede afectar su privacidad y seguridad», concluye el profesor de la UVa. Esta aplicación, según la investigación que ha llevado a cabo este grupo, puede tener acceso también a la lista de contactos, a la localización de los usuarios, a los archivos, a los vídeos, a las imágenes y a los archivos de audio de los usuarios.

Tras pasar *WorldApp* por la herramienta ApkFalcon para calcular su impacto sobre la privacidad de los usuarios, obtiene una nota de 2,8 puntos sobre 10 (máximo riesgo). No obstante, Amador Aparicio advierte de que los permisos que solicita WorldApp y que los usuario pueden gestionar le permiten conocer la ubicación de los usuarios, acceder a la cámara del dispositivo, a los contactos, al estado del teléfono, a los ficheros de audio, vídeo e imágenes almacenadas en los dispositivos externos conectados al teléfono».

«Todas estas categorías están clasificadas por Google como potencialmente intrusivas para la privacidad. Pero es que, además, la aplicación utiliza otros permisos que los usuarios no pueden gestionar y que permiten recopilar información sensible, lo que indica claramente que es dañina para los usuarios desde el punto de vista de su privacidad. Es necesario dar un paso más allá para tranquiliar a los usuarios: que estos sepan para qué se utiliza realmente su ubicación, por qué es necesario el acceso a su cámara, a sus ficheros de audio, vídeo, imágenes, o qué información personal se podría estar revelando cuando la app accede a los servicios de Google», concluye.

! DECLARACIONES

AMADOR APARICIO
PROFESOR DE LA UVA Y RESPONSABLE DE CIBERSEGURIDAD EN ZUNDER

«Los usuarios deben saber para qué se utiliza realmente su ubicación o por qué es necesario el acceso a su cámara, ficheros o qué información personal»

«El análisis de los permisos solicitados por esta app muestra que hay razones suficientes para cuestionarse si es tan respetuosa con la privacidad como sería deseable»