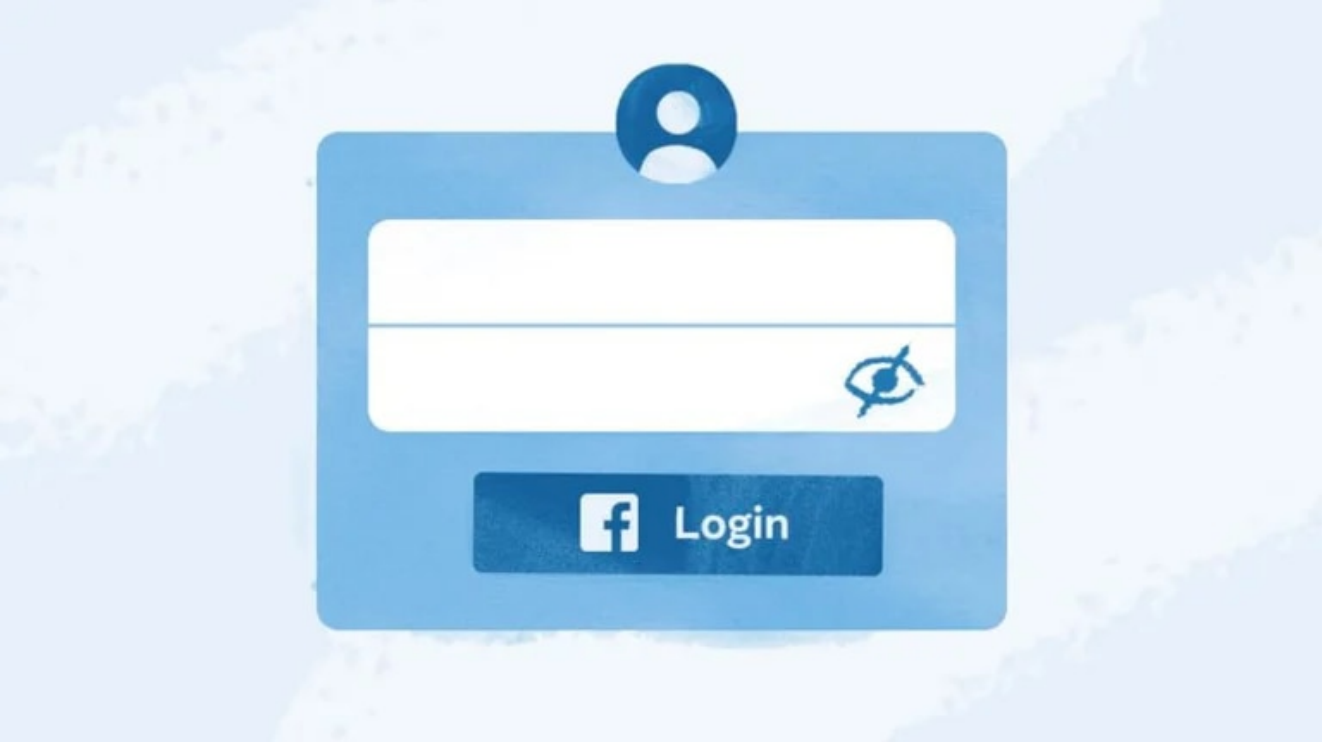
Las 3 preguntas que todo usuario de Facebook debe hacerse para reconocer aplicaciones maliciosas

09/10/2022



La empresa de tecnología **Meta** realizó un trabajo de vigilancia informática y pudo identificar un total de 400 aplicaciones en la **App Store** y **Play Store** que amenazaban la ciberseguridad de millones de usuarios alrededor del mundo debido a que, a través de ellas, operaban cibercriminales que infiltraban **malware** a los dispositivos de sus víctimas para robar información.

Esta investigación realizada durante el último año, dio como resultado no solo la identificación de estas amenazas sino que, por medio de un trabajo coordinado junto a **Google** y **Apple**, estas fueron eliminadas de las tiendas de aplicaciones para evitar que se produzcan más **ciberataques** en contra de los usuarios.

Durante una entrevista exclusiva con Infobae, **David Agranovich**, director de Security Policy en **Meta** a nivel global, compartió tres preguntas que Meta invita a que las personas se hagan cada vez que intenten **descargar una aplicación** para reconocer cuándo esta es en realidad una app maliciosa.

¿Tiene sentido que esta app se conecte a Facebook?

En primer lugar, los usuarios deben preguntarse si la aplicación que se ha descargado realmente necesita la información que ofrece una vinculación con **Facebook** u otras cuentas en redes sociales para poder operar con normalidad.

Los usuarios deben preguntarse si tiene sentido que una aplicación solicite ingresar a Facebook antes de ser utilizada. REUTERS/Dado Ruvic/Illustration

Según la información indicada por Agranovich, entre las **400**

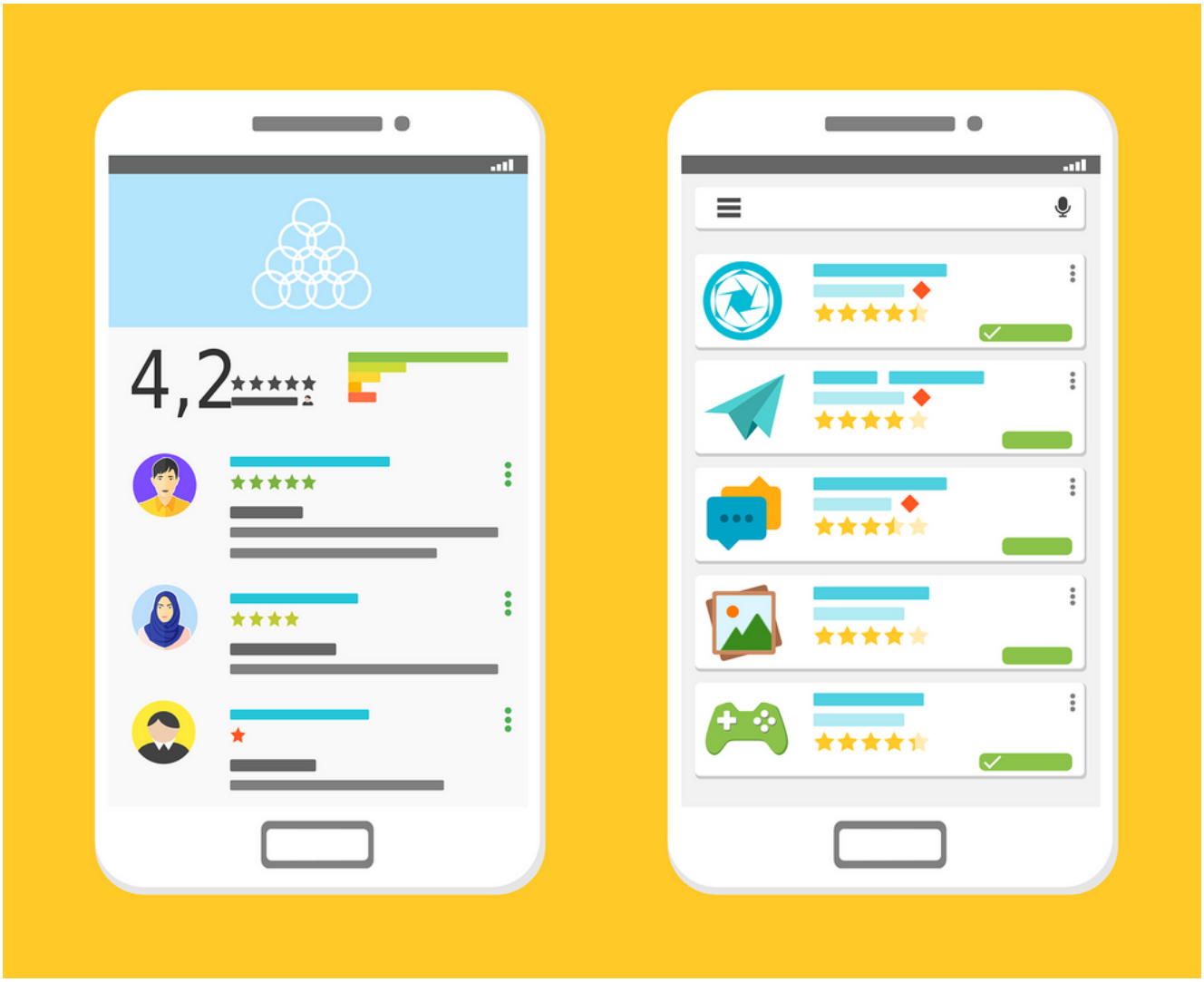
aplicaciones que fueron eliminadas de las tiendas de **Google** y **Apple**, se identificó que el 42.6 % de ellas cumplían la función de editor de fotos, 15.4 % estaban relacionadas con usos de trabajo, 14.1 % con usos del dispositivo, 11.7 % eran juegos, 11.7 % decían se VPNs y 4.4 % eran de salud y estilo de vida.

Sin embargo, entre todas estas aplicaciones también se pudo ver que algunas solicitaban que los usuarios la conecten a **Facebook** antes de utilizarla. “Si una persona descarga una **aplicación** de linterna, pero antes de poder usarla esta me dice que necesito iniciar sesión con Facebook. Eso es probablemente algo sospechoso”, indicó Agranovich.

¿Cuál es la reputación de la aplicación?

En las tiendas de aplicaciones, ya sea en **App Store** o en la **Google Play Store**, las personas podrán encontrar una serie de comentarios sobre cómo la app que instalan es útil, cómo funciona y qué posibles fallas pueden presentar.

Según comentó a Infobae el representante de **Meta**, estas son importantes para poder conocer si una aplicación es potencialmente maliciosa o no. Para Agranovich, es muy importante que los usuarios lean algunas de las **reseñas negativas** que tienen las aplicaciones.



Los usuarios deben leer las reseñas negativas de las aplicaciones en busca de alguna que pueda indicar que la app que se intenta descargar es maliciosa. (Bitdefender)

“En alguna de ellas podrían incluso aparecer personas que, de forma explícita, dicen que consideran que la **aplicación** es una estafa o que no hace lo que dice”, afirmó.

¿La app parece muy buena para ser verdad?

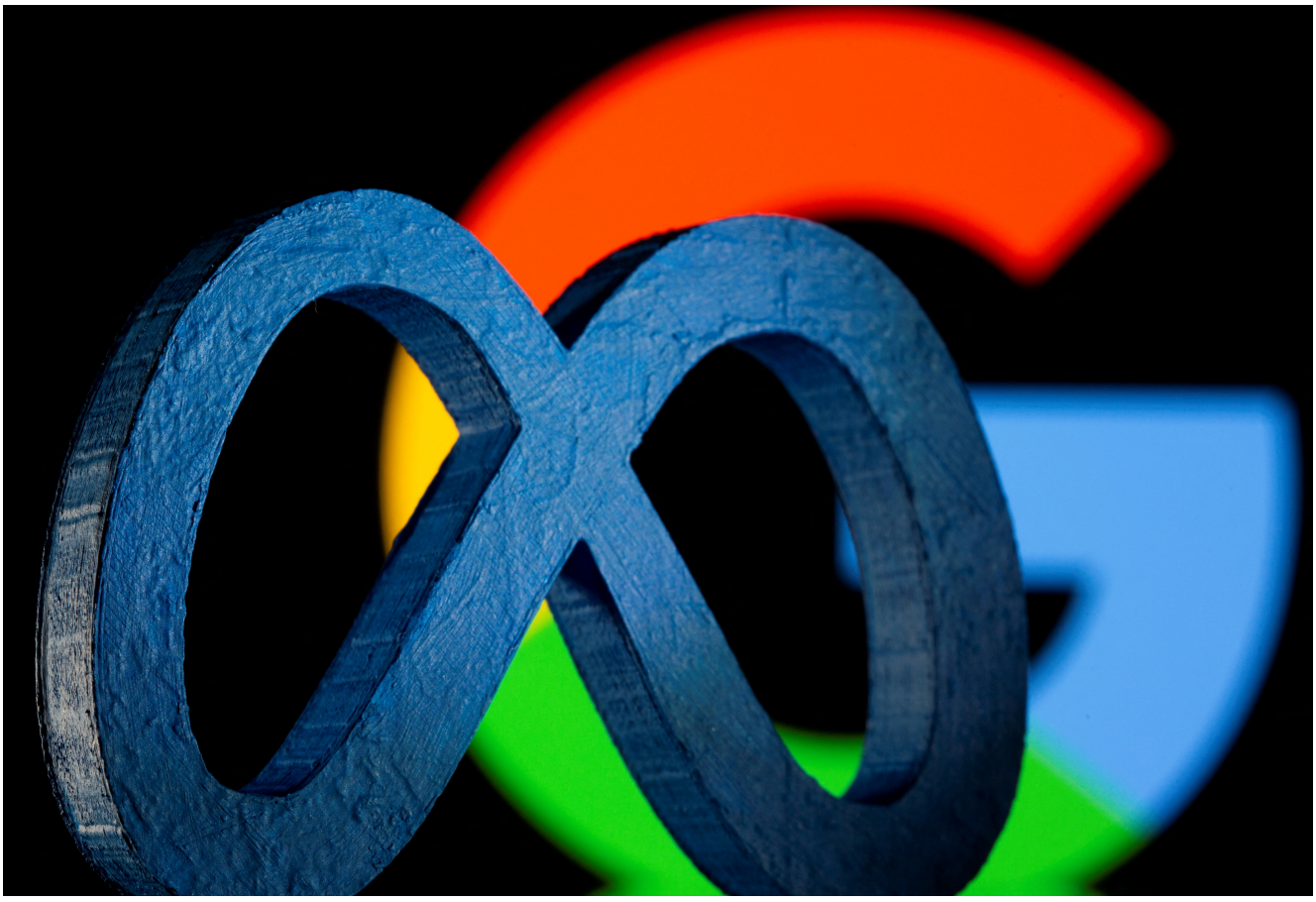
Las aplicaciones maliciosas también intentarán convencer a los usuarios de que descargarlas es bueno, por lo que ofrecen **funciones** que podrían parecer exageradas o engañosas. David Agranovich también considera que esto podría ser visto por los usuarios como una mala señal sobre las intenciones de

la **app**.

“Si la aplicación está prometiendo funcionalidades que son muy buenas para ser ciertas como nuevas capacidades dentro de las plataformas de **Meta**, entonces es probable que tenga otra intenciones”, aseguró a Infobae.

Coordinación con Apple y Google

El trabajo de investigación de Meta implicó también el esfuerzo de equipo junto a **Apple y Google** para poder eliminar estos actores maliciosos que usaban aplicaciones como fachada para sus intenciones.



Meta compartió los resultados de su investigación con Google y Apple para ayudar a las compañías a mejorar sus sistemas de seguridad y proteger a los usuarios. REUTERS/Dado Ruvic/Illustration/File Photo

Agranovich indicó a Infobae que este tipo de colaboraciones

entre empresas de la industria tecnológica es usual y que tiene el objetivo de **proteger a los usuarios**.

“Lo mejor que podemos hacer no solo es aumentar nuestras defensas, sino ayudar a que los compañeros en la industria lo hagan también, de modo que si estas amenazas ocurren en sus plataformas, estamos todos juntos trabajando para asegurarnos de que estos no puedan hacer lo que hacen”, aseguró.

Además, también dijo que estas colaboraciones no son extrañas y que, cuando otras compañías detectan actividad maliciosa, también comparten su información con Meta.

Cómo funcionan las aplicaciones maliciosas

Según la información recogida por **Meta** en su trabajo de investigación, estas aplicaciones son desarrolladas por **ciberdelincuentes** con la intención de extraer información de los dispositivos que lleguen a descargarlas.

Las aplicaciones son desarrolladas por ciberdelincuentes tienen la intención de extraer información de los dispositivos

que lleguen a descargarlas. (foto: 20Minutos)

Por lo general, estas aplicaciones indican tener **funcionalidades divertidas o útiles**, como editores de imágenes para crear dibujos animados o reproductores de música, y las publican en tiendas de **aplicaciones**.

Además, para esconder las evaluaciones negativas de las personas que han detectado la naturaleza maliciosa de estas aplicaciones, los desarrolladores pueden publicar **reseñas falsas** para hacer que las personas descarguen este **malware**. Es por esto que, según Agranovich, los usuarios deben revisar las reseñas desfavorables para las aplicaciones.

Una vez que una persona instala esta aplicación, esta puede solicitar "iniciar sesión con **Facebook**" antes de que puedan usar las funciones que promete. Si el usuario ingresa sus datos, el **malware** introducido en el dispositivo puede robar la **información** de acceso, como el **usuario y contraseña** usaros para el inicio de sesión.

En caso de que la información sea robada, los agresores entonces podrán tener acceso a la cuenta del usuario y usar la información que contiene en nuevas formas de ciberataque.

Fuente: Infobae