Instagram dejará usar la cuenta de Google para proteger cualquier chat

26/02/2023

Meta está probando la opción de realizar la restauración de los chats de Instagram con ayuda de Google usando el servicio **Drive**, donde también se garantizaría una seguridad con la encriptación de extremo a extremo, es decir que los chats solo los ven el emisor y receptor.

Asimismo, se anunció que se continúa trabajando en la creación de un **PIN** para acceder de forma segura a los mensajes; lo que significa que hay dos formas de protección, el resguardo en Google y el acceso con una contraseña.

Autenticación en dos pasos

En Configuración de la cuenta con la opción “Privacidad y seguridad”, estará “**Autenticación en dos pasos**” y luego “App

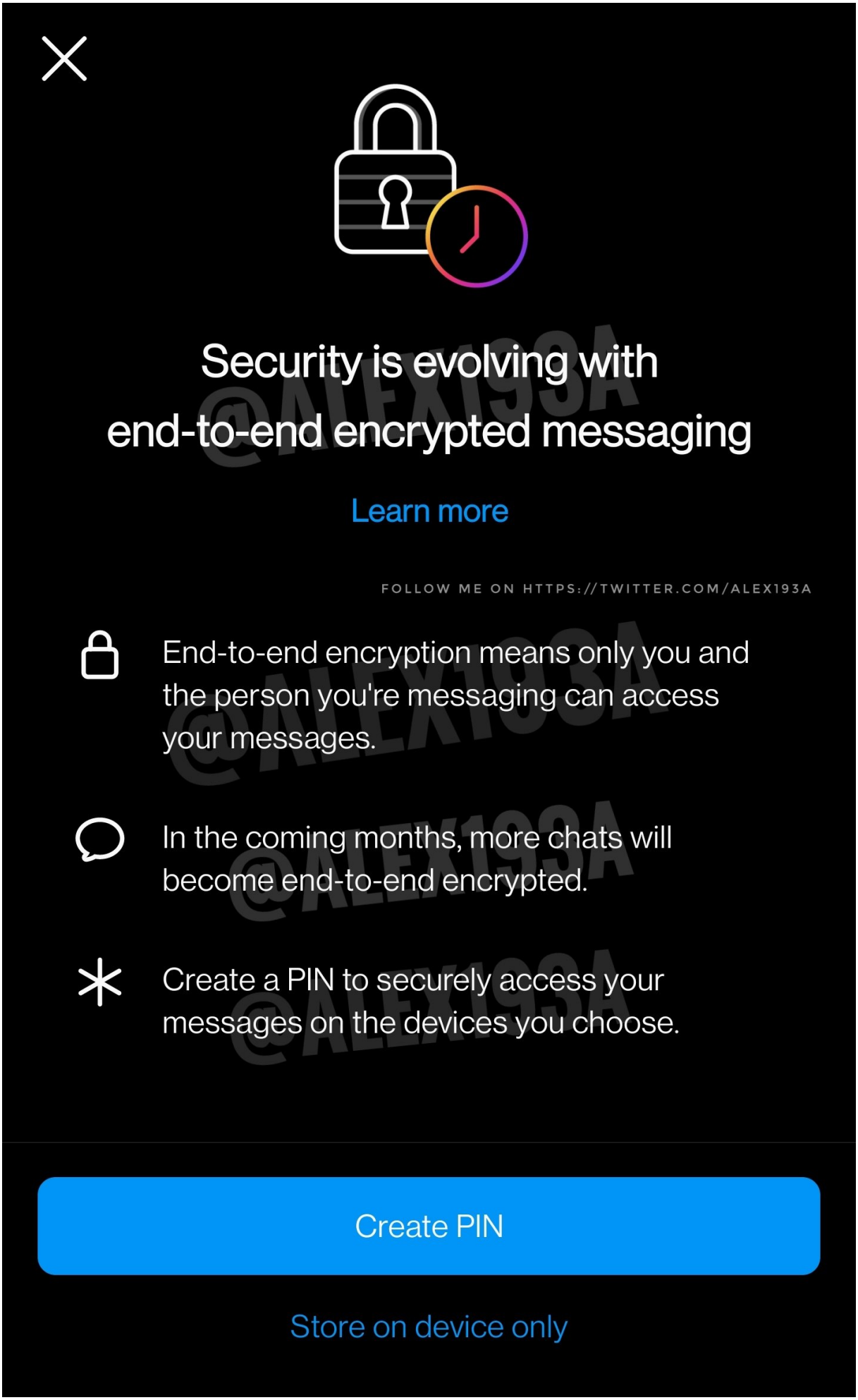
de autenticación” donde se podrá descargar una app como **Duo Mobile** o **Google Authenticator** para obtener códigos de acceso.

“Recomendamos este método de seguridad, ya que puede agregar varios dispositivos conectados a una cuenta para que todos puedan obtener códigos de inicio de sesión”, indicaron.

Otro de los métodos disponibles en la app es “Mensaje de texto”, ya que con el número de celular, se enviará un código para acceder a la cuenta.

Y como última opción de seguridad está “**WhatsApp**”, al darle clic se activa el método de seguridad de la aplicación de mensajería que entrega un código de inicio de sesión cada vez que se quiera ingresar a Instagram.

Después de activar la autenticación en dos pasos se podrán ver solicitudes de inicio de sesión y eliminar dispositivos de confianza.


Security is evolving with
end-to-end encrypted messaging
Learn more
FOLLOW ME ON HTTPS://TWITTER.COM/ALEX193A
End-to-end encryption means only you and the person you're messaging can access your messages.
In the coming months, more chats will become end-to-end encrypted.
Create a PIN to securely access your messages on the devices you choose.
Create PIN
Store on device only

Los

usuarios pueden obtener automáticamente los chats encriptados de extremo a extremo en cualquier dispositivo que inicie sesión en su cuenta de Google.

Recomendaciones

Ahora bien, desde la aplicación advierten que los dispositivos de confianza son todos los aparatos con los que ya haya iniciado sesión usando la autenticación en dos pasos. “No se debe tocar Confiar en este dispositivo si está usando uno público o compartido al que puedan acceder otras personas que no conozca”.

Código QR

Otra de las acciones que tiene la red social es que permite a los usuarios compartir contenido de la plataforma por medio de **códigos QR,** lo que aplica para publicaciones, ubicaciones y reels.

Con la ampliación del alcance de los códigos, que en un principio solo estaban disponibles para empresas, los usuarios podrán generarlos desde el menú de tres puntos, y en la versión de escritorio de Instagram se tiene que agregar ‘/qr’ al final de la url (instagram.com/infobae/qr).

Fuente: Infobae