



Una falla de seguridad de Facebook habría expuesto fotos de 6,8 millones de usuarios

Infobae.- Facebook reveló que una nueva vulnerabilidad en el sistema podría haberle brindado, a aplicaciones de terceros, acceso a fotos de **6,8 millones de usuarios**. Y no se trata de fotografías subidas a la plataforma sino de imágenes no publicadas.

Este bug estuvo vigente durante 12 días de septiembre y se suma a otras fallas anunciadas por Facebook en el último tiempo, como una vulnerabilidad comunicada en noviembre que habría expuesto datos personales de usuarios; y otra informada en octubre que afectó a 30 millones de miembros de la comunidad virtual.

Esta nueva falla hizo que 1.500 aplicaciones tuvieran acceso a millones de imágenes de usuarios. A veces puede ocurrir que un

persona comience a subir una foto pero no termine de publicarla porque pierde la conexión, se olvida de completar la carga o simplemente se arrepiente de hacerlo.

Esa imagen que se comienza a subir queda guardada en el sistema para que, si el usuario así lo desea, pueda terminar de hacer la publicación luego. El problema es que esas imágenes quedaron expuestas a raíz de este bug.

"Lamentamos que esto haya pasado", publicó Facebook en su blog. "La semana próxima estaremos publicando herramientas para desarrolladores de apps que les permitirán saber qué usuarios de sus apps podrían haber estado afectadas por este bug. Trabajaremos junto con esos desarrolladores para borrar las fotos de los usuarios afectados", se lee en el comunicado.

Quienes hayan sido afectados por esta falla, deberían ver una alerta en su cuenta de Facebook. La empresa recomienda también que los usuarios verifiquen que fotos podrían haber compartido a través de apps en las cuales utilizaron su perfil de Facebook para iniciar sesión.

El primer gran escándalo de seguridad surgió con Cambridge Analytica y desde ese entonces la compañía ha estado en la mira y se han detectado otros tantos incidentes que exponen información privada de los usuarios.

Fuente: **Infobae**