Un hackeo a la plataforma Wattpad expuso los datos de 271 millones de usuarios

23/07/2020

La plataforma de publicación de textos Wattpad fue víctima de un ciberataque que afectó a más de 271 millones de usuarios, cuyos datos han aparecido en el mercado negro. Wattpad es una plataforma social donde se reúnen lectores y escritores de todo el mundo. Según datos de la web, conecta a 80 millones de personas que dedican 23.000 millones de minutos al mes en este espacio.

La empresa de ciberseguridad Cyble detectó una brecha de seguridad en Wattpad, y la venta de un archivo con los datos obtenidos a cambio de 10 bitcoins (unos 100.000 dólares). Posteriormente, los investigadores de la compañía encontraron el archivo con **120GB de datos en uno de los foros de hackeo, compartido de forma gratuita, como explican en una publicación en su blog oficial.**

Según explicaron, se trata de un archivo con información de más de 271 millones de usuarios, procedente de un ataque sufrido por la plataforma en junio, que expuso **credenciales, nombres completos, fechas de nacimiento y contactos, entre otros datos.**

Los ciberdelincuentes ofrecieron la información obtenida en foros.
Por su parte, Wattpad compartió esta información en su blog oficial: “A partir de nuestra investigación, hasta la fecha, podemos confirmar que no se accedió a información financiera, historias, mensajes privados o números de teléfono durante este incidente. Wattpad no procesa la información financiera a través de nuestros servidores afectados, y las contraseñas de

los usuarios activos de Wattpad se procesan de forma criptográfica. **Por precaución, y como es común en estas situaciones, estamos restableciendo las contraseñas y aconsejando a los usuarios que cambien las contraseñas en otros sitios si utilizan la misma contraseña".**

Los riesgos

Si bien en el informe se detalla que no se divulgó información financiera, ni mensajes privados, la filtración de información personal podría ser utilizada por ciberatacantes de varios modos. **En primer lugar es importante que el usuario cambie las contraseñas que utilizó no sólo en el sitio afectado sino en todos los demás. Y que no emplee el mismo password en todos los sitios porque de verse afectado uno de ellos, los ciberatacantes podrían emplear esa información en todas las otras plataformas donde el usuario tiene cuenta.**

Por otra parte, la información puede ser empleada por el atacante para orquestar engaños basados en ingeniería social. A veces los ciberdelincuentes envían correos o mensajes diciendo que saben tal o cual dato para extorsionar al usuario y lograr que les depositen dinero a cambio de no develar supuesta información confidencial.

Desde la empresa de ciberseguridad Cyble compartieron las siguientes medidas de precaución

Nunca comparta información personal, incluida información financiera por teléfono, correo electrónico o SMS

Utilice contraseñas seguras y aplique la autenticación de múltiples factores siempre que sea posible

Controle regularmente sus transacciones financiera y si nota alguna transacción sospechosa, comuníquese con su banco de inmediato.

Active la función de actualización automática de software en

su computadora, dispositivo móvil y otros equipos conectados.

Use un paquete de software de seguridad de Internet y antivirus en sus dispositivos conectados, incluyendo PC, computadora portátil, móvil

Cómo saber si mis datos fueron expuestos en alguna filtración de datos

Existen dos sitios que recolectan información sobre las múltiples filtraciones de datos que surgen a raíz de vulnerabilidades y otras fallas de seguridad en varios sitios o aplicaciones. Para verificar si tu correo figura en alguna de esas filtraciones, podés ingresar tu mail en **Have I been pawned** o **Firefox Monitor.**