Las 4 claves para prevenir el robo de información en redes sociales como Twitter o Instagram

15/08/2022

Un comunicado emitido por **Twitter** en su Centro de Privacidad informó a los usuarios de la red social que fueron víctimas del robo de la información de aproximadamente 5,4 millones de cuentas dentro de la **plataforma** y, aunque no se filtraron públicamente sus contraseñas, esta información podría ser usada para cometer más ataques.

Es por ello que es necesario que todos los usuarios de **redes sociales**, dentro y fuera de Twitter, tomen en cuenta algunas recomendaciones de seguridad para evitar ser víctimas de cibercriminales o que su información sea usada con fines maliciosos.

Alerta contra el phishing

En el caso del robo de información como correos electrónicos y números de teléfono, estos pueden ser usados por cibercriminales para llevar a cabo campañas de **phishing** destinadas al **robo de los datos** de otros usuarios por medio de enlaces falsos. Es necesario extremar las precauciones con todo tipo de correos extraños o que pudieran ser sospechosos.

Los ciberdelincuentes intentarán engañar al usuario haciendo uso del nombre de una empresa o servicio de confianza para que de clic a un link fraudulento. (EFE/Sascha Steinbach)

No dar clic en un enlace enviado por correo es la decisión correcta aún si se trata de una supuesta entidad bancaria o un servicio conocido. La comunicación directa por medio de sus canales oficiales es la mejor opción para confirmar si las ofertas o premios ofrecidos por correo son reales.

Mantener la seguridad de las contraseñas

Usar **contraseñas diferentes** para todas las plataformas o redes sociales que requieran de accesos puede hacer la diferencia en caso de ser víctimas de **ciberataques** como el de **Twitter**. Un usuario con la misma clave en todas sus cuentas podrá recordar con facilidad cuál es, pero a su vez pone en riesgo su información, pues el robo de información en una de ellas, significa el robo en todas.

Si el usuario tiene contraseñas diferentes y todas son robustas (combinan mayúsculas, minúsculas, números y caracteres especiales), estará mucho más protegido ante posibles**robos de información**. El cambio periódico de contraseñas es una medida que mantiene lejos a los ciberdelincuentes.

Tener contraseñas diferentes y robustas (combinan mayúsculas, minúsculas, números y caracteres especiales) permite a los usuarios protegerse ante posibles robos de información. (El Androide Libre)

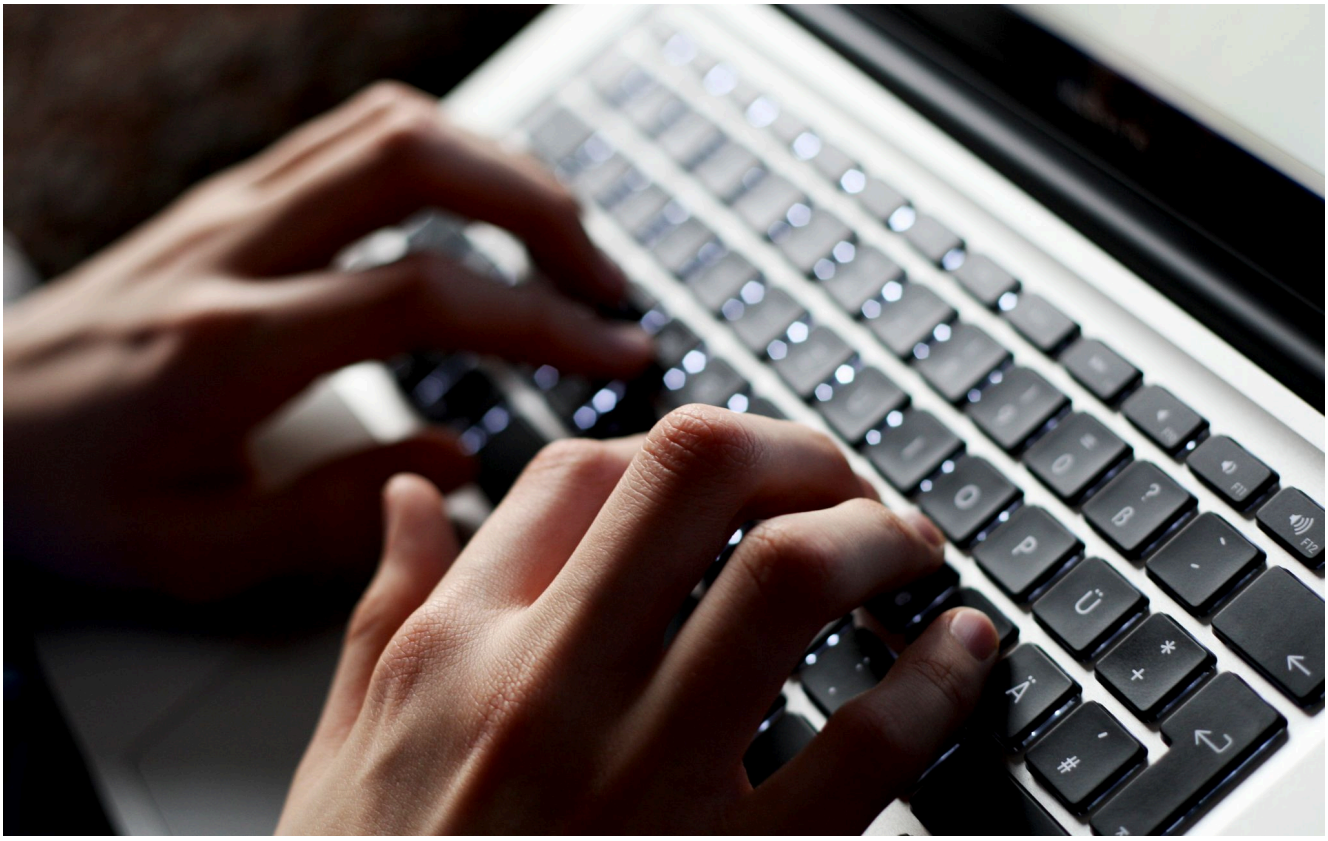
Activar la autenticación de doble factor

Si bien la contraseña establecida puede ser robusta y cambiada de manera periódica, una capa adicional de seguridad nunca está de más. La **autenticación de doble factor** obligará a quien desee acceder a la cuenta a escribir un código adicional solo disponible en el dispositivo personal del usuario.

Mantener actualizadas el dispositivo y las aplicaciones

Para evitar que un **cibercriminal** acceda a la información dentro de un dispositivo, es importante tener actualizadas todas las aplicaciones y herramientas que están instaladas en él. Muchas veces estas **actualizaciones** incluyen parches de seguridad que son importantes en caso de encontrarse vulnerabilidades de algún tipo.

Para Ivonne Pedraza, Territory Manager CCA de Check Point Software, empresa dedicada a la ciberseguridad, los ciberataques aumentan constantemente debido a la capacidad de **teletrabajo** de los usuarios y la cantidad de dispositivos que tienen a su disposición.



Ivonne Pedraza, Territory Manager CCA de Check Point Software, considera que los ciberataques aumentan debido a la capacidad de teletrabajo de los usuarios y la cantidad de dispositivos que tienen a su disposición. (Karl-Josef Hildenbrand/dpa)

“Los ciberdelincuentes no dejan de inventar formas novedosas de atacar y acceder a las cuentas de las redes sociales de los usuarios. Es imprescindible extremar las precauciones y que los usuarios protejan al máximo sus cuentas”, indicó.

Además, puntualizó que, para evitar que las empresas también sean víctimas de ciberataques, es preferible que los usuarios no ingresen a redes corporativas desde sus dispositivos personales.

Fuente: Infobae