

EN MÉXICO PREVÉN PÉRDIDAS POR 68 MMDP

30 mil millones de intentos en 2023, para robo de contraseñas

Internautas, blanco de quienes buscan un beneficio económico: F5 Networks

CHRISTOPHER CALDERÓN
ccalderon@elfinanciero.com.mx

Durante 2023, los cibercriminales enfocaron sus esfuerzos en la vulneración de contraseñas y robo de credenciales para acceder a infor-

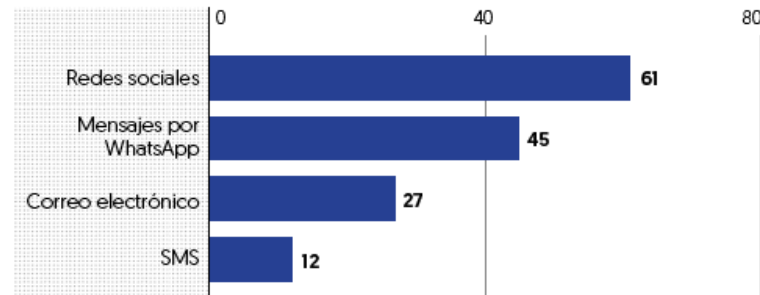
mación valiosa de los mexicanos, dando como resultado al menos 30 mil millones de intentos de ciberataques de este tipo, reveló un estudio de la empresa de ciberseguridad F5 Networks.

Como mínimo, las personas usamos al menos 40 aplicaciones en nuestro dispositivo celular, en donde más del 90 por ciento requieren de una contraseña para activar sus funciones, de ahí que el año pasado, en México debieron existir al menos

Peligro

Durante 2023, hubo al menos 30 mil millones de intentos de ciberataques para robo de contraseñas y credenciales en México.

■ % Método de robos de contraseña más comunes en México, 2023



Fuente: F5 NETWORKS

entre 20 mil y 30 mil millones de ataques para vulnerar las contraseñas de los mexicanos”, comentó Abel Orzuna Hernández, gerente de Territorio Digital en F5 Networks.

Agregó que a medida que la tecnología y los aplicativos con Inteligencia Artificial o que introducen a los usuarios al Metaverso avanzan, el número de aplicaciones que utilizan los mexicanos crece, por lo que el promedio podría llegar a las 67 aplicaciones en los próximos 2 años,

lo que haría aún más vulnerables a los mexicanos en caso de no tener protocolos adecuados para proteger sus contraseñas.

“El problema es que la vulneración de contraseñas y robo de credenciales para acceder a información valiosa que derive en su uso fraudulento obteniendo principalmente ingresos económicos seguirá en aumento y no dudo que los 30 mil millones de intentos que vimos en 2023, los superemos fácilmente en

2024”, advirtió Abel Orzuna.

En este sentido, el estudio realizado por F5 Networks revela que para este año dicho cibercrimen podría llegar a generar pérdidas a los mexicanos por más de 68 mil millones de pesos.

Ante esto el experto recomendó que tanto empresas, industrias y usuarios de internet, deben tomar medidas necesarias para evitar ser víctimas de este cibercrimen.

En cuanto a los ataques más comunes, el ejecutivo de F5 Networks, destacó que el *phishing*, los mensajes de correo fraudulentos y los mensajes por WhatsApp que simulan ser una empresa conocida y con buena reputación para engañar y conseguir información privilegiada, son algunas de las estrategias o ataques más utilizados por los cibercriminales.

El *phishing* o suplantación de identidad es muy empleado para aprovecharse de las vulnerabilidades. Este cibercrimen les permite aplicar la manipulación para que sus víctimas realicen acciones que aumenten el riesgo de sus sistemas.