PERIÓDICO	PAGINA	FECHA	SECCIÓN
24 HORAS EL DIARIO SIN LIMITES	PP-3	05/10/2023	NACIONAL

AUMENTA 87% EL RIESGO DE FRAUDES EN LA WEB

Golpea a México ciberdelincuencia

Las estafas van desde falsas ofertas de trabajos por WhatsApp, engaños por correo electrónico hasta amenazas directas para extorsionar, de acuerdo con registros de expertos. Los timadores se aprovechan del desconocimiento sobre el uso de datos personales y el modus operandi para engañar a la gente, haciéndose pasar por instituciones bancarias, empresas o incluso presentándose abiertamente como criminales, quienes exigen dinero para no actuar contra la víctima MÉXICO P. 3

EN MÉXICO AUMENTÓ 87% RIESGO DE ESTAFAS POR INTERNET: EXPERTOS

Entre promesas y amenazas, atacan los ciberdelincuentes

Alerta. Por correo electrónico, el phishing es una de las formas más socorridas por criminales para obtener datos de sus víctimas

RODRIGO CEREZO Y ARTURO RIVERA

En la Era Digital los ciberdelincuentes aprovechan la confianza y el desconocimiento de la gente para realizar fraudes y estafas por Internet, haciéndose pasar por instituciones bancarias, empresas o incluso presentándose abiertamente como criminales, pasando por engaños, promesas... Y amenazas.

De acuerdo a especialistas, las estafas van desde ofrecer trabajos por mensajería de WhatsApp y Telegram hasta amenazas directas por parte de supuestos hacker, exigiendo dinero para no actuar contra la víctima.

El especialista de la firma checa de ciberseguridad Avast, Luis Corrons, destacó que los riesgos de ciberestafas en México aumentaron 87% en la primera mitad de 2023, respecto al mismo periodo en el año anterior.

Para que las estafas funcionen, uno de los pasos que realizan los ciberdelincuentes es obtener datos de sus posibles víctimas.

Apenas este año, de acuerdo a la compañía de software israelí Perception Point, se detectó una operación de phishing denominada "Caimán manipulado", dirigida principalmente a los ciudadanos de México.

"La campaña intentó obtener acceso a las cuentas bancarias de las víctimas mediante ataques de phishing utilizando archivos adjuntos maliciosos. Los investigadores obtuvieron casi 40 millones de direcciones de correo electrónico objetivo de la campaña".

De acuerdo con la multinacional tecnológica IBM, el phishing es la forma más común para engañar, presionar o manipular a las personas para compartir información confidencial, mediante correos electrónicos, mensajes de texto, llamadas telefónicas o sitios web fraudulentos.

"Los ataques de phishing con éxito a menudo implican la usurpación de identidad... basa su éxito en tácticas de error humano y presión. El atacante normalmente se hace pasar por una persona u organización en la que la víctima confía (por ejemplo una compañía)", detalla la empresa en su sitio web.

Además, diversas plataformas han visto vulneradas sus bases de datos, exponiendo correos, contraseñas, nombres de usuarios y direcciones IP, como ocurrió en junio de 2020 con la empresa Yotepresto, con sede en Jalisco.

"La plataforma mexicana de préstamos yotepresto.com sufrió una violación de datos. Más de 1.4 millones de clientes se vieron afectados por la infracción que reveló direcciones de correo electrónico y IP, nombres de usuario y contraseñas almacenados", destaca el Centro Nacional de Ciberseguridad de República Dominicana.

Dicho centro cuenta con una herramienta virtual, en la que al ingresar el correo electrónico del usuario muestra si éste ha sido comprometido y cuántas veces a lo largo de los años, conforme a alertas internacionales.

SEXTORSIÓN

"Hola. Soy un hacker profesional y he logrado hackear tu sistema operativo. Actualmente he obtenido acceso completo a su cuenta. Además, estuve monitoreando en secreto todas tus actividades y observándote durante varios meses", dice un correo enviado en inglés a una de las víctimas.

Por supuesto, el mensaje va subiendo de tono cuando el presunto hacker menciona que ha "realizado una recopilación de videos, que muestra en el lado izquierdo escenas tuyas masturbándote felizmente, mientras que en el lado derecho muestra el video que estabas viendo en ese momento".

Para finalmente llegar a la extorsión: "Esto es lo que debes hacer: transferir el equivalente en Bitcoin de 600 dólares a mi cuenta", dice el correo enviado por *dlashondaky@mail4y.com*.

De acuerdo con la firma Avast, este método es conocido como sextorsión, en el que estafadores afirman contar con material íntimo de la víctima y exigen un pago exprés.

Y mientras que algunos de los criminales envían correos de forma masiva esperando que algunas de las víctimas caigan, otros buscan comprobar si la cuenta está activa para proceder a otro nivel de estafa.

"Te mande un email a .....@hotmail.com pero no sé si te llego... si este email te llega como spam/correo no deseado te pediría si sos tan amable que lo pases a bandeja de entrada, así te vuelvo a enviar la consulta para que te llegue correctamente", dice otro correo, enviado a la víctima desde *avisos@em.mypsx.net*.

En nuestro país, se estima que 7 de cada 10 organizaciones mexicanas han sufrido un ciberataque, sin embargo, debido a la falta de reportes por parte de las empresas, no se cuenta con una cifra oficial que precise el número de casos, señalaron especialistas.

"Es muy difícil saber esto, porque la única gente que puede saber en qué nivel estamos son los ciberdelincuentes (...) muchas organizaciones no van a reportar sus ataques por temas de reputación, por lo tanto, esa estadística no se puede tener al cien por ciento", explicó Enrique Herrera, fundador de Cyberimox.

Pese a la falta de reportes por parte de organizaciones, aseguró que las estadísticas posicionan a México como el país con más ciberataques en Latinoamérica.

"En primer lugar está Brasil, en segundo México con un 23%, Colombia, Perú y el resto de Latinoamérica. Esas son las estadísticas que hoy en día se tienen en temas de ciberseguridad", explicó Herrera durante el foro Info Security México, realizado este miércoles.

Al respecto, detalló que el 59% de los ciberataques se realizan a través del correo electrónico y phishing.

Por su parte, Jorge Osorio, vocero de Infosecurity México, aseguró que este grupo de estafadores, no necesariamente hackers, "son grupos organizados. Hemos visto, por ejemplo, empresas que se hacen pasar por otras empresas de préstamo de dinero, por ejemplo, por alguna fintech", refirió en entrevista con **24 HORAS**.

¿FUISTE VÍCTIMA DE UN DELITO EN LA RED?

Estos son los pasos que recomienda la Guardia Nacional ante la delincuencia por Internet:

1. Respalda la evidencia (mensajes, correos electrónicos y fotos) haciendo capturas de pantalla y copiando direcciones electrónicas
2. Presenta la denuncia correspondiente ante el Ministerio Público.
3. Llama al 088, donde la Guardia Nacional brinda orientación para realizar la denuncia ante el Ministerio Público.
4. Guarda el número de folio de atención para darle seguimiento.