Fecha: 11/04/2025 Audiencia: 320.543 Sección: ACTUALIDAD
Vpe: $8.358.047 Tirada: 126.654 Frecuencia: OTRAS
Vpe pág: $20.570.976 Difusión: 126.654
Vpe portada: $20.570.976 Ocupación: 40,63%

FRECUENCIA Y CANTIDAD DE ESTOS ATAQUES VA EN AUMENTO:

Educación a los usuarios, esencial para combatir la amenaza del *phishing*

La IA generativa ha incidido en la sofisticación de los mensajes usados para estafar, así como en su alcance, creando contenido en múltiples idiomas y estilos comunicacionales.

NOEMÍ MIRANDA G.

Mucho se ha dicho sobre que, dada la sofisticación que ha alcanzado la tecnología y el desarrollo de la inteligencia artificial (IA), las mayores amenazas de ciberseguridad vendrían por el lado de la explotación de potenciales brechas en los sistemas informáticos. Sin embargo, el principal riesgo hoy son las personas, que caen en la trampa de estafas como el *phishing* o son víctimas del robo de identidad.

Así señalan el Foro Económico Mundial (WEF) y la consultora Accenture en el informe "Perspectivas globales de ciberseguridad 2025", que revela que el 72% de los encuestados observó durante 2024 una mayor cantidad y frecuencia de esos tipos de ataques.

El hecho de que el *phishing* siga liderando las ciberamenazas no deja de llamar la atención de los especialistas. La explicación de la eficacia de esta estafa, que utiliza aplicaciones de uso común, como correos electrónicos, WhatsApp y mensajes de texto, es que los usuarios reciben sofisticados mensajes que explotan emociones básicas, como la empatía, el temor y la satisfacción; por ejemplo, el deseo de ayudar a alguien enfermo, la alegría de recibir un premio o el miedo a perder acceso a un sistema esencial, como el banco, comenta Claudio Ordóñez, director de Ciberseguridad de PwC Chile.

Alto retorno

Además, los estafadores han refinado sus métodos, usando la IA generativa para crear mensajes altamente personalizados y reproducir el estilo de comunicación de personas públicas o instituciones, con datos obtenidos de redes sociales o declaraciones oficiales. Nicolás Deino, director ejecutivo para la Industria Financiera de Accenture Chile, indica que, además, "la IA generativa facilita la creación de ataques en múltiples idiomas y los ciberdelincuentes pueden dirigirse a un público más amplio a menor costo".

EL MERCURIO

El *phishing* es de alto retorno de inversión para los delincuentes, ya que es un tipo de estafa de bajo costo, lo que explica su masividad.

Consejos para evitar las estafas

- **Mantenerse alerta:** siempre revisar los mensajes que piden información sobre inicios de sesión a cuentas personales. El *phishing* suele generar una sensación de urgencia para presionar la acción sin pensar de forma crítica.
- **Reconocer las señales:** los correos electrónicos de *phishing* suelen incluir lenguaje urgente, *links* sospechosos o solicitudes poco comunes. Se recomienda leer con cuidado, detectar faltas de ortografía sutiles y desconfiar de direcciones de *email* inusuales.
- **Proteger los datos:** nunca entregar información como nombre de usuario, contraseñas o códigos a personas que los piden por mensajes, correos o por teléfono.

FUENTE: Boise State University, Estados Unidos.

Otra de las razones es el alto retorno de inversión (ROI) del *phishing*: el costo de crear y enviar contenido a las potenciales víctimas, en comparación con las ganancias, sigue estando a favor de los ciberdelincuentes, señala Mike Price, *chief technology officer* de la empresa especializada en ciberseguridad ZeroFox.

Así como son la puerta de entrada de las amenazas, la mejor herramienta para combatir el *phishing* son las personas, las que deben contar con información para aprender a distinguir estos ataques. Las campañas de educación, por ende, son esenciales. Por una parte, como indica el estudio del WEF y Accenture, las empresas deben educar a sus clientes sobre estos riesgos y proporcionar canales de comunicación claros y seguros, y su fuerza laboral debe contar con las competencias necesarias para hacer frente al panorama dinámico de las ciberamenazas.

Pero los gobiernos también tienen responsabilidad. Para Claudio Ordóñez, "la ciberseguridad es un tema país; la educación de las personas debe utilizar diferentes medios y en distintas formas para lograr el objetivo de integrar la ciberseguridad a la cultura". El ejecutivo advierte que, por parte del Estado, debiese existir una campaña permanente en redes sociales, televisión y medios escritos.

Labor multisectorial

En paralelo, es imperativa la colaboración multisectorial, donde el Estado desempeñe un rol central, afirma Nicolás Deino: "La educación debe fomentar la capacidad de cuestionar la autenticidad del contenido en línea, porque —ante la proliferación de contenido generado por IA— es crucial que las personas tengan un reflejo de duda y cautela al interactuar en el entorno digital".

Desde una mirada macro, las *fintechs* son vitales, ya que "tienen la oportunidad de liderar la innovación en ciberseguridad, desarrollando e implementando soluciones creativas y ágiles para proteger sus plataformas y usuarios", detalla Deino. Y agrega que podrían intercambiar inteligencia sobre amenazas, colaborando entre sí y con otras entidades del sector: "La cooperación facilita una detección y respuesta más temprana y efectiva".

Finalmente, "en la medida en que las empresas dificulten el acceso a las cuentas sin autorización, se reducirá el ROI de los ataques de *phishing*, lo que sin duda contribuirá a desincentivarlos", destaca Mike Price.