LITORALPRESS

Fecha: 10-07-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: CIBERSEGURIDAD: LOS DESAFÍOS QUE ENFRENTA LA INDUSTRIA DE PREPAGO

Pág. : 28
Cm2: 669,8

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

CIBERSEGURIDAD: LOS DESAFÍOS QUE ENFRENTA LA INDUSTRIA DE PREPAGO

La mayor inclusión financiera que promete el impulso de las tarjetas de prepago no bancarias podría abrir las puertas para que los ciberdelincuentes pongan sus ojos en este segmento. Por ello, la industria ya está implementando diversas estrategias para proteger a sus usuarios.

POR MACARENA PACULL M.

Según el Panorama de Amenazas para América Latina realizado por Kaspersky, que analizó datos desde el 2021 hasta el 2023, los ataques de malware hacia computadores y dispositivos móviles han aumentado en un 617% y un 50% en cuanto a ataques de phishing y troyanos bancarios, respectivamente, siendo los sectores financiero y de gobierno los más afectados. Chile ocupa el sexto lugar en la región, con un total de 10,5 millones de intentos de ataque.

Como parte de las herramientas digitales de la industria financiera, las tarjetas de prepago también enfrentan complejidades en materia de ciberseguridad. De hecho, con el reciente fallo de la Corte Suprema que obliga a los comercios a aceptarlas de la misma manera que las tarjetas de crédito y débito, el uso de este medio de pago podría aumentar considerablemente, generando no solo una mayor inclusión financiera, sino también un mayor interés de parte de los delincuentes informáticos por vulnerarlas.

"Los riesgos aumentan en el segmento de usuarios que recién están incorporándose e iniciando su experiencia con el uso de metodologías prepago", advierte Néstor Strube, gerente general de ITQ Latam, destacando que los más expuestos pueden ser el público joven y también el de personas mayores. "Para todo el universo de usuarios es clave el mix de educación financiera, de ciberseguridad y de concientización respecto de los riesgos, trampas y acciones que jamás hay que hacer en la dinámica financiera del ciberespacio para así no ser víctimas de fraude", remarca.

En tanto, el segmento de pequeñas y medianas empresas también podría ser especialmente sensible a ataques al utilizar tarjetas prepagadas para gestionar gastos, dice Martina López, investigadora de Seguridad Informática de ESET Latinoamérica. "Estas pueden no tener los mismos recursos para invertir en ciberseguridad que las grandes empresas, haciéndolas más vulnerables a los ataques", agrega.

Amenazas crecientes

A juicio de Fabio Assolini, director del Equipo de Investigación y Análisis para América Latina en Kaspersky, desde el punto de vista de la ciberseguridad, la protección de una tarjeta de crédito, débito o prepagada no cambia mucho, y para todas es necesaria la adopción de las buenas practicas del PCI-DSS (sigla en inglés de Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago). De todas maneras, puntualiza que, "dependiendo del emisor, es más fácil para los estafadores obtener tarjetas prepagadas, incluso usando nombres de mulas de lavado de dinero o cuentas falsas. Acá es necesaria una atención, mejorando el proceso de 'KYC' (Know Your customer) o de onboarding para bloquear solicitudes maliciosas".

4 DE CADA 10 INTENTOS DE PHISHING SE DIRIGEN A DATOS FINANCIEROS, SEGÚN UN INFORME DE KASPERSKY.

El especialista de Kaspersky añade que los estafadores ya utilizan herramientas de inteligencia artificial (IA) para burlar este proceso, que muchas veces es basado en autenticación biométrica o reconocimiento facial. "Aun así, con la ayuda de la IA los malhechores logran abrir cuentas falsas usando datos de personas reales o ya muertas", detalla.

Frente a las crecientes amenazas, el rubro de las tarjetas de prepago en Chile ha avanzado significativamente en temas de ciberseguridad mediante la adopción de tecnologías y estrategias innovadoras.

"La inteligencia artificial y el aprendizaje automático se utilizan para analizar grandes volúmenes de datos en tiempo real, detectando patrones anómalos que podrían indicar actividades fraudulentas, lo que permite anticipar y mitigar ataques potenciales antes de que ocurran", dice Héctor Kaschel, CyberSecurity Practice Head Andina de Logicalis. A ello se suma el modelo de "confianza cero", que asegura una verificación continua de usuarios y dispositivos.

Kaschel explica que la industria ha implementado el cifrado de datos sensibles para proteger la información contra accesos no autorizados, y la tokenización, que reemplaza esos datos por tokens seguros que pueden ser utilizados en transacciones sin riesgo, así como también en monitoreo permanente.

Sin embargo, la educación financiera y en ciberseguridad es clave. El ejecutivo de Logicalis comenta que los actores del mercado están desarrollando programas de formación y campañas de concienciación para empleados y usuarios, con el fin de mejorar las prácticas de seguridad y prevenir fraudes. Para Martina López, de ESET, en tanto, las empresas deben adaptar sus estrategias de seguridad y educación, ofreciendo "materiales educativos accesibles, proporcionar soporte proactivo y desarrollar interfaces de usuarios que incorporen medidas de seguridad intuitivas y fáciles de usar".