Vishing: la nueva cara del fraude telefónico en Chile

Los **fraudes telefónicos** en el país están viviendo una mutación tecnológica que alarma a autoridades y expertos. Un estudio de la Universidad de Chile junto al SERNAC reveló que el "vishing" —modalidad de phishing basada en llamadas telefónicas, donde delincuentes se hacen pasar por familiares o instituciones confiables— ya concentra el 71% de los fraudes de tipo phishing en Chile, según los reclamos recibidos por el servicio.

La modalidad deja atrás los clásicos correos mal redactados o llamadas evidentemente sospechosas. Hoy, los estafadores pueden articular guiones cada vez más sofisticados e incluso apoyarse en herramientas de inteligencia artificial capaces de clonar voces con alto grado de precisión, imitando a un hijo, un ejecutivo bancario o un funcionario público. El resultado es un nivel de realismo que desarma incluso a los más prevenidos. El estudio advierte que se trata de un salto cualitativo en la forma en que operan estos delitos, donde la confianza del usuario se convierte en la principal vulnerabilidad.

Julio Farías, cofundador de compañía especializada en experiencia de cliente e inteligencia artificial aplicada a contact centers, apunta a un vacío crítico: la falta de protocolos claros en las comunicaciones legítimas de empresas e instituciones. "Cuando no existe una forma predecible de contacto, los delincuentes tienen vía libre para imitar

cualquier interacción", señala. Según el experto, muchas organizaciones replican prácticas impersonales —mensajes grabados, solicitudes de datos sensibles sin contexto— que terminan siendo indistinguibles de una estafa.

El estudio también subraya un déficit de alfabetización digital en la población. La naturalidad con que los chilenos responden a llamadas automatizadas o de centros de contacto (contact centers), sin cuestionar su origen, aumenta la exposición al riesgo. En ese sentido, Farías insiste en que la seguridad no puede seguir tratándose como un elemento externo a la experiencia del cliente: "Hoy el usuario espera eficiencia, pero también confianza. Y esa confianza solo se construye con comunicaciones verificables y transparentes".

Desde el SERNAC advierten que el impacto de estas estafas no es solo económico, sino también emocional. Las víctimas, engañadas a través de la voz de un supuesto ser querido o de un funcionario que aparenta urgencia, suelen experimentar altos niveles de angustia, culpa y desorientación después del fraude. Por ello, la recomendación es tajante: ante cualquier llamada sospechosa, cortar de inmediato y verificar la información directamente con la institución, usando canales oficiales como números publicados en sitios web o aplicaciones bancarias.

El llamado es especialmente urgente para sectores como la banca, las aseguradoras, los servicios públicos y las telecomunicaciones, que concentran la mayoría de los contactos con usuarios. El estudio plantea que estas industrias deben establecer políticas de contacto claras y reconocibles —por ejemplo, definir qué datos nunca se solicitan por teléfono y cómo se confirma la identidad del ejecutivo— y difundirlas masivamente para que los clientes sepan cómo distinguir lo real de lo falso.

Farías coincide en que la prevención debe ser parte integral del diseño de los servicios, y no una reacción posterior al

fraude. “Las organizaciones que pongan la seguridad al centro de la experiencia de cliente no solo protegerán a sus usuarios, también fortalecerán su reputación en un entorno donde la confianza es clave”, sentencia. El desafío, advierte, es doble: educar proactivamente al usuario y, al mismo tiempo, implementar mecanismos de autenticación en tiempo real que cierren la puerta a los estafadores.