EL MERCURIO

Fecha: 29/04/2025 Audiencia: 320.543 Sección: CONTRAPORTADA
Vpe: $8.575.585 Tirada: 126.654 Frecuencia: SEMANAL
Vpe pág: $20.570.976 Difusión: 126.654
Vpe portada: $20.570.976 Ocupación: 41,69%

Autoridades llaman a desconfiar de este tipo de comunicaciones y nunca hacer clic en sus enlaces

Alza de fraudes por SMS: en lo que va del año casi se iguala a todos los detectados en 2024

De enero a la fecha, la Agencia Nacional de Ciberseguridad ha emitido 149 alertas por mensajes fraudulentos, mientras que en los 12 meses del año pasado la cifra llegó a 152. En los *smishing*, como se le llama a esta modalidad usada por los delincuentes, se asegura que es necesario pagar con urgencia una multa o deuda con el SII, entre otros.

ALEXIS IBARRA O.

"Casi todos los días me llegan mensajes avisando sobre puntos que van a expirar de tiendas y supermercados. Además de créditos aprobados, paquetes no entregados en Correos de Chile, mensajes con deudas en Tesorería y otros del SII", dice Álvaro Rodríguez.

No es el único. En el último tiempo se ha visto un incremento importante de estos mensajes, una verdadera avalancha de SMS que llaman la atención porque plantean una situación urgente: la pérdida de puntos, un ofertón que se acaba en poco tiempo, deudas que hay que solucionar al instante, etc.

"Hemos detectado un crecimiento en este tipo de fraudes de suplantación a instituciones y empresas. En el año 2024 publicamos 152 alertas con distintos mensajes fraudulentos relativos a bancos, tiendas y otras instituciones, mientras que en lo que va del año ya hemos emitido 149 alertas", dice Daniel Álvarez, director nacional de la Agencia Nacional de Ciberseguridad (ANCI). Es decir, en solo cuatro meses se ha detectado casi la misma cantidad de tipos de mensajes distintos que el año pasado. Cada uno de ellos es enviado a cientos de miles de personas.

El comisario Alan Constela, de la Brigada del Cibercrimen Metropolitana, dice que "estos mensajes que se están recibiendo en forma masiva son una modalidad de delito denominada *smishing*. Consiste en un mensaje de texto que los ciberdelincuentes envían a los usuarios acompañado de un link".

"El nombre es una mezcla de SMS y *phishing* que es una técnica de engaño (su nombre deriva de *fishing*, pescar en inglés, ya que se usa un anzuelo para engañar a las víctimas)", explica Fernando Abrego, CEO de Vedata Group, empresa tecnológica especializada en datos.

Él mismo, dice, recibe diariamente varios intentos de *smishing* que usan temas que asustan a la gente: cuotas pendientes, un paquete que no se puede entregar, una multa impaga, etc.

Dentro del mensaje se incluye un enlace que aparenta ser legítimo, pero que en realidad redirige a un sitio web falso diseñado para imitar al de la entidad suplantada, dice Leandro Cuozzo, analista de Seguridad en el Equipo Global de Investigación y Análisis para América Latina en Kaspersky.

"Estos sitios fraudulentos buscan engañar a la víctima para que ingrese información personal importante, como su RUT, claves bancarias, o datos de tarjetas de crédito. En algunos casos, también se solicita la descarga de aplicaciones maliciosas o archivos infectados que comprometen la seguridad del dispositivo", agrega.

"El fraude se concreta cuando la víctima entrega esa información, creyendo que está resolviendo algo urgente o importante, o cuando entrega dinero de forma voluntaria", explica Martina López, investigadora de Seguridad Informática en ESET Latinoamérica.

Según el director de la ANCI, este tipo de fraudes ocurre por diversos factores: "El aumento del uso del teléfono móvil como canal de comunicación, la facilidad con la que los ciberdelincuentes pueden suplantar a entidades legítimas, y el bajo costo de enviar mensajes. Además, muchas personas aún no están plenamente conscientes de los riesgos asociados al uso de tecnologías, lo que los convierte en un blanco fácil".

Con ayuda de IA

A pesar de ser una técnica antigua, López dice que ha ido evolucionando. "Hoy se usan textos generados por inteligencia artificial para crear mensajes más persuasivos y sin errores. Además, hay un uso más frecuente de enlaces acortados. Con ellos los cibercriminales evitan que se identifique el destino final y en algunos casos también se combinan con llamadas telefónicas que refuerzan la historia del mensaje, generando una presión adicional para que la persona actúe mucho más rápido".

La IA también ha ayudado a los cibercriminales a "la automatización de campañas a gran escala, incrementando su alcance y eficiencia. También se ha perfeccionado la generación de sitios falsos que imitan a la perfección a los originales, lo que refuerza el engaño y aumenta considerablemente las probabilidades de éxito del fraude", explica Cuozo.

Para evitar ser víctima, López dice que "hay que mantener una actitud crítica ante cualquier tipo de mensaje inesperado que contenga un enlace o solicite información".

La recomendación es jamás entrar a esos links "y en caso de que la oferta sea muy tentadora hay que entrar al sitio oficial de la tienda para ver si la oferta está en el sitio. En caso de ser víctima de este ilícito hay que recolectar la mayor cantidad de antecedentes y concurrir a la unidad policial más cercana al domicilio de la víctima", dice el comisario Constela.

JOSÉ LUIS RISSETTI

Todos los engaños que llegan por SMS tienen algo en común: llaman a una acción urgente. En el apuro, la persona cae con más facilidad. Por ello, sin entrar al link recibido, es clave chequear en la web de las empresas si la información es real.

Muerte del Papa es aprovechada por ciberdelincuentes

Tras el anuncio del fallecimiento del Papa Francisco surgieron campañas de desinformación en Instagram, TikTok y Facebook, en forma de imágenes falsas generadas por inteligencia artificial. Según Rafael López, ingeniero de seguridad en protección de correo electrónico en Check Point Software Technologies, estas campañas están diseñadas para atraer a los usuarios y captar su atención, incitándolos a buscar más información a través de motores de búsqueda o a hacer clic en enlaces dentro de las imágenes o publicaciones. Una vez que interactúan, los usuarios pueden ser redirigidos a sitios web fraudulentos con diversos fines maliciosos, desde el robo de datos hasta estafas financieras. "En un caso, el enlace estaba oculto en un sitio web que promovía noticias falsas sobre el Papa Francisco. Al hacer clic, el usuario era redirigido a una página falsa de Google que promovía una estafa con tarjetas de regalo, una táctica común para engañar a las personas y hacer que entreguen información o realicen pagos", añade López.

En otros sitios fraudulentos, se ejecutan comandos en segundo plano sin la interacción del usuario. Este tipo de *malware* recopila información como el nombre del equipo, sistema operativo, país, idioma, entre otros. Mientras más datos obtengan, más sencillo es hacer una estafa posterior.