"Tus puntos van a caducar": Phishing, la tentadora estafa que llega por SMS y cómo no caer en ella

La dinámica de acumular puntos está presente en gran parte de los lugares donde se realizan compras. Retail, aerolíneas, combustibles, casas comerciales, entre otros.

Con este sistema, las compañías buscan fidelizar a su potencial clientela a cambio de beneficios. Las empresas ofrecen viajes, comida o artículos electrónicos a cambio de los puntos acumulados. Por lo mismo, es de esperarse que delincuentes cibernéticos intenten utilizar este método para engañar a las personas y robar información personal, como datos bancarios. Lee también...: Así es el "quishing": la estafa con código QR que usan los delincuentes por medio de multas falsas Desde un tiempo hasta ahora, decenas de personas han denunciado la llegada de mensajes de texto o correos electrónicos donde empresas como Copec, Latam o Movistar, avisan del vencimiento de puntos, por lo que llaman a canjearlos antes de que caduque el plazo. Al ingresar al link que suele traer este tipo de mensajes, pareciera no haber ningún error. De hecho, ni siquiera lucen como sitios falsos. Una vez en la web, aparecen tentadoras ofertas, casi imposibles de creer. Sin embargo, al momento de canjear el producto, el sitio pide los datos de una tarjeta bancaria para -generalmente- pagar el costo de envío del producto. Es ahí cuando ocurre la estafa. Todo lo anterior se conoce como Phishing, lo que en resumidas cuentas es una técnica que consiste en el envío de correos electrónicos o mensajes que suplantan la identidad de compañías para solicitan información personal y bancaria al usuario. ¿Y cómo no caer en estafas? El uso de Inteligencia Artificial hace mucho más difícil la tarea de identificar cuándo se está frente a una estafa. Pese a ello, José Lagos, director del diplomado en Ciberseguridad de UEjecutivos de la Facultad de Economía y Negocios de la Universidad de Chile, entregó algunos consejos para poder enfrentar estas situaciones. El académico inicia desde una primera base para comenzar reconocer una potencial estafa: ofertas demasiado buenas para ser ciertas. Por ejemplo, el sitio fraudulento de Copec ofrece teléfonos de últimos modelos por una cantidad muy reducida de puntos, junto con un envío que no supera los mil pesos. Lee también...: Visa informa que gracias a inversión tecnológica ha detenido miles de fraudes hechos con IA Otro punto que resalta José Lagos tiene que ver con los mensajes de texto que alertan, por ejemplo, el retraso en el pago de algo importante o un paquete que no se ha entregado, cuando en realidad no espero nada. Para distinguir una potencial estafa, el académico llama a fijarse en errores ortográficos o gramaticales en correos que dicen provenir de empresas, logos o imágenes de mala calidad, solicitud de información sensible como contraseñas, dirección personal, información financiera o información corporativa por parte de una supuesta compañía, entre otros. Consejos para evitar caer en Phishing · “Remitente desconocido, mal escrito o que no coincide con el que normalmente utiliza determinada empresa o servicio. Muchas veces, lo ciberdelincuentes intentan imitar a empresas legítimas, pero con pequeñas variaciones. · Mensajes de alerta o amenazantes que dicen cosas como “tu cuenta será bloqueada en 24 horas si no actualizas tu información” o “has ganado un premio, reclamalo ya”, buscan que actúes rápido sin pensar. · Que la URL del sitio web al que piden ingresar sea diferente a la

que normalmente se ingresa a través de Google o directamente en la barra". Por su parte, Daniel Álvarez Valenzuela, director de la Agencia Nacional de Ciberseguridad, sostiene que "es necesario que las personas estemos atentas y desconfiemos de cualquier mensaje no solicitado, especialmente si incluye enlaces o documentos que no esperamos". "Es importante fijarse en posibles errores de ortografía o redacción, y sobre todo, revisar cuidadosamente la dirección web a la que nos quiere dirigir. Muchos sitios de phishing imitan con gran precisión el diseño de páginas legítimas, por lo que verificar que la URL sea la oficial es clave", puntualizó el director del servicio. Finalmente, añadió que "en cualquier caso, la mejor recomendación es simple: nunca hagas clic en enlaces que te lleguen de forma inesperada".