LITORALPRESS

Fecha: 23-01-2025
Medio: El Divisadero
Supl. : El Divisadero
Tipo: Noticia general
Título: Cómo reconocer y evitar las estafas cibernéticas

Pág. : 6
Cm2: 448,3

Tiraje: 2.600
Lectoría: 7.800
Favorabilidad: No Definida

Cómo reconocer y evitar las estafas cibernéticas más comunes

· Un mensaje de texto malicioso, un link en un correo sospechoso, la llamada de un supuesto ejecutivo que solicita datos personales o incluso Códigos QR que simulan ser confiables, son algunas de las amenazas que afectan a las personas. La empresa de tecnología y telecomunicaciones Entel, entrega consejos para identificarlos y enfrentarlos.

¿Has escuchado sobre el Smishing, el Vishing o el Phishing? Estos ciberataques son cada vez más comunes y pueden suceder a través de diferentes plataformas, como mensajes de texto, correos electrónicos, llamadas y códigos QR.

El gerente de Ciberseguridad de Entel, Rodrigo Hernández explica que "la mejor manera de evitar estas ciberamenazas, es reconociéndolas y saber cómo proceder en caso de que un usuario crea que se pueda tratar de una estafa o un link malicioso".

En esa línea, la empresa de tecnología y comunicaciones Entel explica cuáles son las más comunes, cómo opera cada una y cómo protegerse de estos ataques.

Smishing y Vishing

El Smishing, es una estafa similar al phishing, pero que se realiza a través de un mensaje de texto engañoso. En él los ciberdelincuentes se hacen pasar por entidades (como un banco, una tienda en línea, un proveedor de servicios, etc.) o personas que parecen confiables, para inducir al usuario a compartir información personal o financiera -como contraseñas, datos bancarios o números de tarjetas de crédito-; hacer clic en un enlace malintencionado; o descargar un virus malicioso que puede robar información o infectar el equipo. Estos mensajes parecen proceder de fuentes fiables y crean una sensación de urgencia, curiosidad o miedo como forma de manipulación.

Por otro lado, el Vishing, es un ciberataque donde los delincuentes se hacen pasar por empleados de una empresa a través de una llamada por teléfono para convencer a la víctima o el cliente, de compartir información personal o financiera. Por lo general, el delincuente tratará de ganar la confianza de la persona revelando datos personales como el nombre, la dirección o el lugar de trabajo. Luego, tratará de crear un sentido de urgencia en la solicitud para así aprovechar el miedo o emoción de la persona, esperando que se facilite data confidencial.

¿Cómo evitarlos?: siempre se debe verificar la autenticidad de los remitentes antes de entregar datos personales; dudar de solicitudes que vengan desde números desconocidos o anónimos; no hacer clic en archivos o enlaces sospechosos; desconfiar de ofertas demasiado buenas para ser verdad o de las solicitudes urgentes, ya que a menudo los estafadores intentan crear un sentido de urgencia en los mensajes, correos o llamadas, para que la víctima actúe rápidamente y sin pensar; y por último, jamás realizar pagos, transferencias, o entregar información personal sin antes validar en los canales oficiales de la empresa u organización correspondiente.

Estafas con código QR

También existen las estafas a través de códigos QR, que ocurren cuando los ciberdelincuentes manipulan estos códigos para engañar a las personas y obtener acceso a su información, robar dinero o instalar un malware (virus malicioso) en sus dispositivos. Normalmente, estos redirigen a sus víctimas a sitios web poco fiables donde se les solicita entregar datos personales, o realizar pagos fraudulentos a través de transferencias bancarias.

¿Cómo evitarlo?: antes de escanear, el usuario debe asegurarse de que el código provenga de una fuente confiable, no se debe confiar en códigos colocados en espacios públicos sin confirmación. Por otra parte, se recomienda activar la revisión previa de URL, ya que muchas aplicaciones de escaneo muestran la dirección a la que redirige el código QR. Es importante verificar que la dirección sea legítima antes de continuar y hacer clic. También es fundamental no confiar ciegamente en ofertas o mensajes urgentes. Si el código QR promete algo demasiado bueno o crea un sentido de urgencia, probablemente sea una estafa.

Para más consejos

"Desde Entel estamos permanentemente entregando recomendaciones en materia de ciberseguridad a nuestros clientes y usuarios a través de consejos, información y recomendaciones disponibles en nuestra web w2.entel.cl/concienciaentodas. Esto es parte de nuestra estrategia de Sostenibilidad Conciencia en Todas que a través de su eje Transformación Responsable, promueve espacios digitales seguros y el uso responsable de la red", señaló Hernández.

Desde la compañía sugieren que ante cualquier información sospechosa o de dudosa procedencia se acuda a los canales oficiales como la web www.entel.cl; la aplicación de Entel; al call center al "103"; y a los canales habilitados para personas mayores, donde podrán esclarecer dudas y confirmar si el contenido recibido es fidedigno.