LITORALPRESS

Fecha: 29-01-2025
Medio: El Mercurio
Supl. : El Mercurio - Chile Tecnológico
Tipo: Noticia general
Título: Cómo reconocer las estafas cibernéticas más comunes

Pág. : 6
Cm2: 485,5

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

EDUCACIÓN DIGITAL:

Cómo reconocer las estafas cibernéticas más comunes

Los ataques de ingeniería social, como el *phishing*, *smishing* y *vishing*, siguen siendo las principales preocupaciones de organizaciones y particulares en materia de ciberseguridad. Aquí, Entel entrega consejos para identificarlos y enfrentarlos.

BÁRBARA LICHNOVSKY

Entre julio de 2023 y julio de 2024, las estafas mediante *phishing* aumentaron 140% en América Latina, según un reporte de Kaspersky. Este tipo de ciberataque, usualmente ejecutado por correo electrónico, busca engañar a las personas para hacer que compartan datos confidenciales.

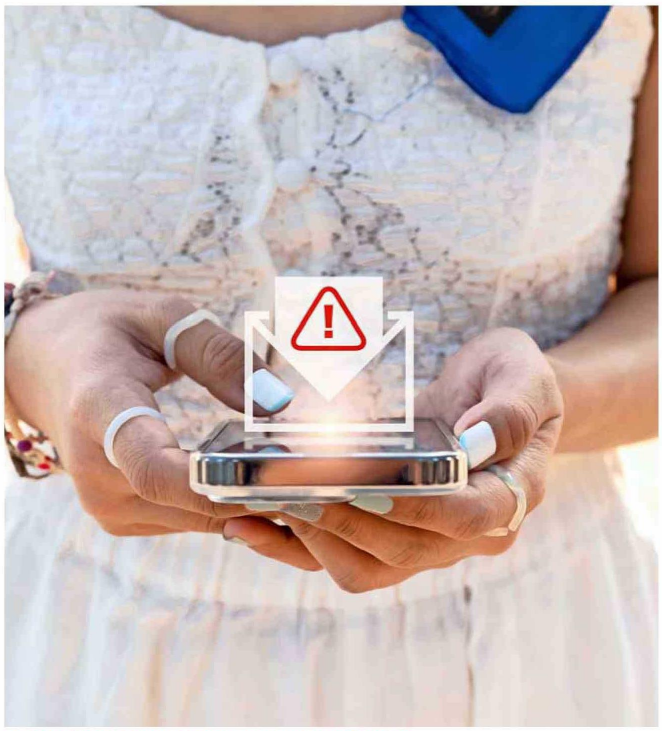
El nivel de penetración tecnológica mundial ha permitido que este y otros delitos de ingeniería social sean cada día más comunes, por lo que reconocerlos y "saber cómo proceder en caso de que un usuario crea que se pueda tratar de una estafa o un *link* malicioso" es fundamental, dice Rodrigo Hernández, gerente de Ciberseguridad de Entel.

DISTINTAS PLATAFORMAS

El *smishing* es un fraude similar al *phishing*, pero que se realiza a través de un mensaje de texto (SMS) engañoso. En él, los ciberdelincuentes se hacen pasar por entidades bancarias, tiendas en línea, proveedores de servicios, etc., o personas que parecen confiables, para inducir al usuario a compartir información personal o financiera. Al hacer clic en un enlace fraudulento o descargar un virus malicioso, le roban sus datos o infectan el equipo.

También está el *vishing*, en el que los cibercriminales, a través de llamadas telefónicas, dicen ser empleados de una empresa determinada para convencer a la víctima de compartir información personal o financiera. Por lo general, el delincuente tratará de ganar la confianza de la persona revelando datos como el nombre, la dirección o el lugar de trabajo. Luego, intentará crear un sentido de urgencia en la solicitud para así aprovechar el miedo o emoción de la persona, esperando que se facilite data confidencial.

Otra estafa común es la de código QR, que ocurre cuando los delincuentes manipulan esta herramienta para engañar a las personas y obtener acceso a su información, robar dinero o instalar un *malware* (virus malicioso) en sus dispositivos. Normalmente, el QR redirige a su víctima a sitios web poco fiables donde se les solicita entregar datos personales o realizar pagos fraudulentos.



EL *SMISHING* ES UNA ESTAFA SIMILAR AL *PHISHING*, pero que se realiza a través de un mensaje de texto (SMS) engañoso.

A QUÉ PONERLE OJO

En cuanto al *smishing* y al *vishing*, 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, y desconfiar de ofertas demasiado buenas para ser verdad o de las solicitudes urgentes, ya que los estafadores intentan crear un sentido de urgencia en los mensajes, correos o llamadas para que la víctima actúe rápido y sin pensar. Además, jamás se deben realizar pagos o entregar data personal sin antes validar en los canales oficiales de la empresa u organización correspondiente.

Entel cuenta con un canal de SMS oficial (casilla verificable), donde el remitente de estos mensajes figura de manera predefinida como "ENTEL" y no como un número desconocido. Estos mensajes no pueden responderse.

Con respecto a las estafas con código QR, antes de escanear, el usuario debe asegurarse de que este provenga de una fuente confiable y no arriesgarse con códigos colocados en espacios públicos sin confirmación. Además, se recomienda activar la revisión previa de URL, ya que muchas aplicaciones de escaneo muestran la dirección a la que redirige el código QR. También es fundamental no confiar ciegamente en ofertas o mensajes urgentes.

"CONCIENCIA EN TODAS"

Como parte de su estrategia de sostenibilidad "Conciencia en Todas", Entel está permanentemente promoviendo espacios digitales seguros y el uso responsable de la red entre sus clientes y usuarios, señala Rodrigo Hernández, gerente de Ciberseguridad de la compañía. Para más información y recomendaciones, visite **w2.entel.cl/concienciaentodas**.