LITORALPRESS

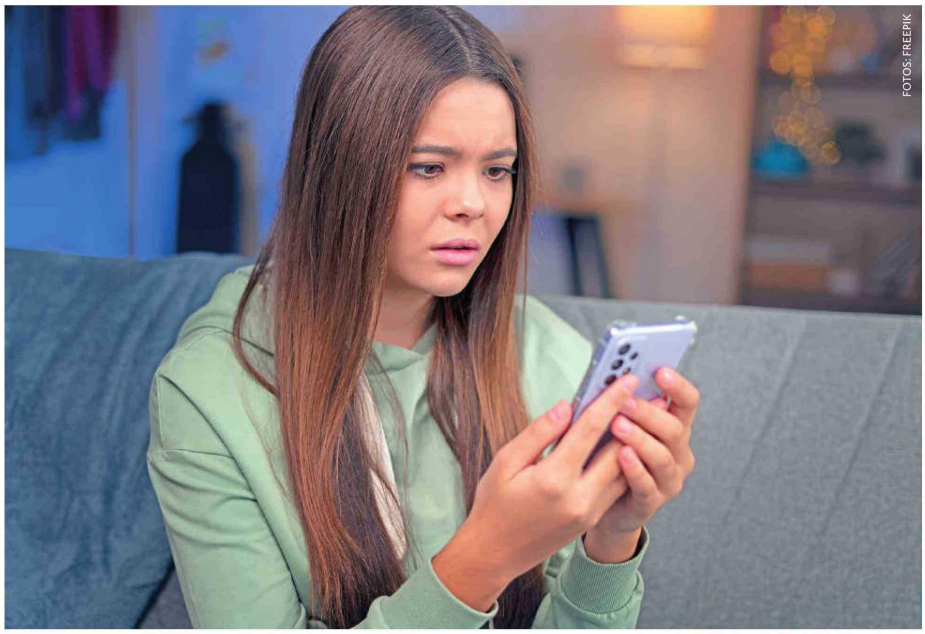
Fecha: 08-08-2025
Medio: Publimetro
Supl. : Publimetro
Tipo: Noticia general
Título: Consejos para evitar fraudes a través de mensajes

Pág. : 11
Cm2: 627,0

Tiraje: 84.334
Lectoría: 382.227
Favorabilidad: No Definida

fayerwayer FW

Precaución. En los fraudes cibernéticos como el smishing es importante que el usuario se mantenga alerta al ser el último eslabón en la cadena de prevención.



FOTOS: FREEPIK

Consejos para evitar fraudes a través de mensajes

Erika Padrón
Metro World News

El smishing es un tipo de ataque que se envía a través de mensajes de texto o SMS fingiendo que provienen de una empresa legítima, con la finalidad de engañar a los usuarios para obtener información confidencial y realizar estafas.

"Nuestra recomendación es mantenerse alerta y vigilante de las tácticas que se utilizan en estas estafas para saber cómo evitarlas". "Recientemente hemos visto un incremento de fraudes por mensajes SMS hacia nuestros usuarios. En nuestro caso, trabajamos para ofrecer conexiones seguras y bloquear ataques a nuestros clientes; sin embargo, en la cadena de prevención nuestros usuarios juegan un papel clave para cerrarle la puerta a los defraudadores", comenta Erick Armas, Chief Security Officer en AT&T México.

Mensualmente, los protocolos de ciberseguridad de esta compañía bloquean millones de mensajes detectados como spam, sin embargo, los sistemas no son infalibles y los usuarios podrían recibir mensajes maliciosos.

Toma en cuenta los siguientes consejos para identificar mensajes SMS fraudulentos:

● Provienen de remitentes desconocidos.
Si recibes un SMS de un número desconocido o de una empresa a la que no se lo solicitaste, es posible que sea fraude. NO lo abras.

● Crean un ambiente para realizar acciones urgentes
Los defraudadores suelen crear una sensación de urgencia y generar confusión para que la víctima actúe rápidamente sin pensar y dé clic a un enlace malicioso. Estos mensajes incluyen frases como:

"Su cuenta ha sido bloqueada, confirme sus datos aquí: [enlace falso]"

"Usted ha ganado un premio. Para reclamarlo, haga clic en este enlace"

"Hay actividad sospechosa en su cuenta. Verifique ahora"

● Ofrecen descuentos o préstamos fáciles.
Particularmente en temporadas de ofertas, como el último trimestre del año, los defraudadores envían mensajes con descuentos increíbles u ofreciendo préstamos o tarjetas de crédito con condiciones muy atractivas.

● Solicitan información confidencial.
A menos que el usuario esté seguro del origen, la recomendación es no responder a estos mensajes.

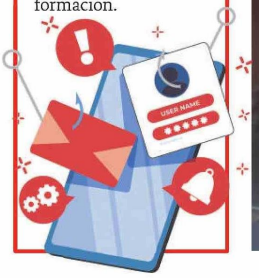
OTRAS ESTRATEGIAS

Recientemente, usuarios reportaron haber recibido mensajes para redimir puntos para recibir recompensas.

Es preciso informar que compañías como esta no cuenta con programas de puntos para canjear recompensas. Estos mensajes son falsos

RECUERDA

- Los fraudes a través de mensajes de texto o SMS, conocidos como smishing, van en aumento.
- Se trata de mensajes que aparentan provenir de bancos, servicios de paquetería o instituciones oficiales, con enlaces que redirigen a sitios falsos para robar tu información.



Otros consejos

- No abras enlaces sospechosos. Si el mensaje te pide entrar a una página para "verificar tu cuenta", ignóralo. Los bancos nunca solicitan datos sensibles por SMS.
- No compartas información personal. Jamás proporciones datos como tu NIP, número de tarjeta o contraseñas vía mensaje.
- Verifica la fuente. Si tienes dudas, contacta directamente a la institución desde sus canales oficiales.
- Bloquea y reporta. Usa las funciones de tu celular para bloquear al remitente y reportar el número como spam.
- Activa la verificación en dos pasos en tus aplicaciones y servicios digitales para mayor seguridad.

"Mántente alerta de estas situaciones que te pueden poner en riesgo especialmente en épocas de ofertas y descuentos".

AT&T MÉXICO.