Ciberestafas: Si es muy bueno para ser verdad, probablemente no lo sea

Andrea López | Redacción Nacional con información de Tec Review

Lo más probable es que en algún momento hayas escuchado la frase **‘si es demasiado bueno para ser cierto, probablemente no lo sea’. Cuando se trata de ofertas o promociones en línea, te recomendamos hacer caso a tal expresión y desconfiar.**

Dmitry Bestuzhev, director de Investigación y Análisis de **Kaspersky Lab** para América Latina, coincide, y **explica por qué**.

*“**Existen cada vez más casos y muchas formas de hacer fraude** a través de una campaña en línea. En la mayoría de los casos, **el objetivo de los autores de éstas es el dinero de los usuarios**”*, afirma en entrevista con CONECTA.

/>>

Por ejemplo, desde el año pasado, **algunas universidades mexicanas se han visto afectadas por la propagación de supuestos descuentos en sus colegiaturas**.

“¡Garantizado!”, “Colegiaturas al 80%”, “Este es un trámite totalmente legal”, anuncian campañas que circulan en redes sociales.

“Esto está creciendo muy rápido”, asegura Ignacio Hernández, director de Control Interno y de la Contraloría del Tecnológico de Monterrey. ***“Es por eso que debemos ser más preventivos*”.**

De acuerdo con Hernández Navarro, **estos terceros ofrecen a pagar al estudiante, por ejemplo, sólo el 80% de su mensualidad.**

*“Es decir, **si yo normalmente pago 10 pesos de colegiatura, les doy a ellos 8 pesos y los estafadores pagan los 10 pesos a la institución. ¿Cómo? Utilizando una tarjeta clonada o apócrifa**”*, detalla.

Incluso, **las personas que están detrás de estas campañas pueden solicitarle al alumno datos de cuentas personales para completar la transacción.**

*“**Tenemos que reforzar también la cultura del cuidado de estas cuentas o información.** De otra manera le estamos dando las ‘llaves’ a un tercero para que haga lo que quiera”*, aseveró.

Hernández aclaró que l**as campañas de descuentos que se han identificado no cuentan con logos de las instituciones afectadas** y que, en la mayoría de los casos de los que se tiene registro, **la transacción se da de manera electrónica, solicitando pagos con tarjetas de crédito.**

“Yo les recomiendo que no se dejen engañar y que no utilicen diferentes medios de pago de colegiaturas a los que ellos mismos ya conocen. Este es un acto ilícito y no ético por lo que puede ser causante de un proceso legal”.

¿Cómo evitar las ciberestafas?

El experto de Kaspersky Lab dio algunas **recomendaciones para evitar caer en ciberfraudes**.

Una forma realmente eficaz de evitar este tipo de estafas es, en primera instancia, **acercarse directamente al comercio para consultarles la veracidad de la oferta. Posteriormente, fijarse en los métodos de pago.**

“Los sistemas de pagos en línea, como PayPal, nos ofrecen cierta seguridad”, afirma Bestuzhev, ya que evitan que tengas que ingresar datos bancarios, protegen las compras, monitorean transacciones fraudulentas y revisan los sitios con los que trabajan antes de aceptarlos.

También puede ser útil **contar con una tarjeta virtual o una cuyos fondos sean asignados por el usuario**, es decir, *“si sabes que quieres comprar algo de 60 dólares, sólo le agregues los 60 dólares, no más”*, aconseja el experto. **Así, si el cibercriminal quiere hacer más cargos, no le será posible.**

“Evita utilizar tarjetas de crédito o de débito en las que tengas guardado el dinero que usas todos los días para comprar comida, transportarte o pagar la renta”.

También, Bestuzhev recomienda **no hacer negocios o tratos informales vía plataformas de mensajería instantánea o redes sociales, ya que éstos no te ofrecen ningún tipo de garantía o seguridad.**

Los engaños de los ciberdelincuentes

Por más cuidadoso que seas con tus datos personales y bancarios, así como de qué tipo de e-mails abres o que información reenvías vía plataformas de mensajería instantánea o redes sociales, **existen formas más complejas de robar información o bien de cometer un acto ilícito y no ético.**

*“Por ejemplo, **te pueden enviar un mensaje por Whatsapp o puedes ver cierta publicación en Facebook de que, por ejemplo, se están regalando boletos para un evento de tu interés**”,* detalla Bestuzhev.

“Uno puede pensar: si no lo reenvío o no le doy click a un link no corro riesgo. Sin embargo, lo que puede estar haciendo el cibercriminal es despertar un falso interés en los usuarios que los lleve a buscar la promoción u oferta en internet”.

Si este es el caso, lo más seguro es que **la persona lo ‘googleará’ con ciertas palabras clave en mente que lo lleven hasta un sitio en donde le espera la verdadera trampa. Incluso, en algunos casos, sitios legítimos pueden estar comprometidos.**

Otra modalidad es enviar campañas por Messenger (de Facebook) e incluso Skype. *"Te pueden llegar mensajes de personas que no están en tu lista de contactos"* dice Bestuzhev.

"Y no sólo puede tratarse de formas de obtener directamente datos personales o bancarios, sino también propagar malware. Basta con que se infecte una persona para que el ataque llegue a todos sus contactos".

Ya caí, ¿ahora qué hago?

Si ya caíste en una ciberestafa, lo primero que debes hacer es llamar a tu banco para bloquear tus tarjetas de inmediato.

Esto no puede esperar porque, *"**si piensas 'llamo mañana', probablemente para mañana ya sea muy tarde. Realmente el criminal no necesita ni siquiera horas para hacer un cargo**"*, advierte el especialista de Kaspersky Lab.

Algunas instituciones bancarias, como American Express, ofrecen herramientas como protección contra cargos no reconocidos y compras protegidas. Además, cuentan con sistemas que les permiten identificar patrones de consumo y recibir alertas en caso de que se registre un movimiento extraordinario.

"Si notamos cualquier compra que no sea acorde a tu estilo de vida o consumo regular, o si se dá en algún sitio inusual, te contactamos de inmediato para verificar si deseas realizar dicha compra", afirma Santiago Fernández, director general de American Express México.

Por ello también te recomendamos acercarte a tu banco para informarte de los servicios y respaldos con los que cuentas en este sentido.

Fernández añade que, **en caso de que ya hayas hecho un pago a una campaña que sospechas es fraudulenta, *"basta con reportar el cargo****. El tiempo máximo permitido para hacerlo es de 90 días a partir de la fecha de corte donde aparezca la compra no reconocida"*.

El siguiente paso es cambiar todas tus contraseñas. pero ten cuidado al hacerlo de un equipo infectado.

"Si defines nuevos passwords en un equipo que posiblemente esté infectado, el cibercriminal aún tendrá acceso a ellos. Podemos incluso cambiarlos cada hora y, si este es el caso, no servirá de nada".

Así, **lo mejor es asegurarse de que el equipo no está comprometido y, mientras tanto, hacer el cambio desde otro en el que confiemos.**

Después, se debe, de preferencia, **notificar al comercio real, por ejemplo en el caso de las universidades a las autoridades de las mismas. También es necesario denunciar a la policía.**

*"Aunque probablemente archiven el caso y no harán gran cosa, **esto sirve para sembrar un precedente**",* dice Bestuzhev.

"*Tras esto, **lo ideal es darlo a conocer en redes sociales para alertar a otros".***

*"Recomiendo especialmente en Twitter, porque Facebook, por ejemplo, es una comunidad más cerrada. **Si uno lo publica en Twitter lo puede leer prácticamente cualquiera***", concluyó.