LifeMatters®

Evitando Estafas

Las estafas fraudulentas vienen en todas las formas y tamaños. Aquí están algunas con las que te puedes encontrar:

- **Fraudes electrónicos (phishing o SMiShing).** Recibes un correo electrónico o un mensaje de texto pidiéndote que hagas clic en un enlace. El mensaje declara que debes actuar rápido o perderás el acceso a una cuenta o a un servicio. A menudo, el enlace te va a llevar a un sitio de pagos falso o va a descargar malware en tu dispositivo. A partir de ahí, el estafador puede robar tu información personal o incluso apoderarse de tu dispositivo.

- **Fraudes electrónicos dirigidos (spear phishing).** Recibes un mensaje de texto o un correo electrónico de alguien que se hace pasar por una amistad tuya o por un colega tuyo. Esta persona te pide que envíes dinero, pagues una cuenta, o le proporciones información personal privada o información de negocios privada. De nuevo, la verdadera intención es robar dinero o información o tener acceso a un dispositivo o a la red de una empresa.

- **Ingeniería social.** Los estafadores pueden estudiar tus redes sociales para hacer un fraude electrónico dirigido (ver punto anterior). También pueden utilizar esta información para tenerte como objetivo para estafas específicas, como ofertas de un trabajo de tus sueños, oportunidades de viajes, consolidación de deudas, o inversiones. Ten en mente que si algo suena muy bueno para ser cierto, probablemente lo es.

Estos consejos te van a ayudar a identificar y a evitar las estafas:

- Si recibes un correo electrónico sospechoso, revisa la dirección con mucho cuidado. A menudo, puede ser parecida (pero no exactamente igual) a la dirección oficial de correo electrónico de una empresa.

- Si el URL no tiene “https://” en el principio, puede tratarse de un sitio web no seguro o fraudulento.

- Si la petición sospechosa viene de alguien que tú conoces, verifica con él o ella por teléfono o en persona antes de tomar cualquier acción. Si el mensaje viene de una empresa con la que tienes tratos de negocios, llama o comunícate con ellos utilizando su sitio web oficial.

- Si recibes un correo electrónico fraudulento o un mensaje en el correo electrónico de tu trabajo o en el teléfono que utilizas en tu trabajo, sigue los procedimientos de tu empresa para reportar el atentado. En dispositivos personales, reporta o bloquea los correos electrónicos o los números telefónicos fraudulentos.

- Ten cuidado al publicar información que te identifique y otros detalles personales en los sitios de las redes sociales.

Si caes en la trampa de un fraude, LifeMatters te puede ayudar. Te ofrecemos ayuda 24/7/365 para manejar el impacto legal y financiero, incluyendo el robo de identidad.

1-800-634-6433

Asistencia con tu Vida, tu Trabajo, tu Familia, y tu Bienestar
mylifematters.com • 24/7/365
Llama por cobrar al **+1 262-574-2509** si llamas fuera de Norteamérica
Están disponibles servicios de traducción de TTY/TRS 711