BOLETÍN MENSUAL DE CONNECTICUT CONSUMER PROTECTION

Volumen 1/Número 5/Diciembre de 2024

ALERTA DE ESTAFAS

Qué son: Estafas relacionadas con organizaciones benéficas

Cómo funcionan: Durante la temporada de fiestas, los estafadores se hacen pasar cada vez más por organizaciones benéficas legítimas que piden donaciones. Estos estafadores disfrazan su identidad para presionarlo a que realice una donación rápida a la organización fraudulenta mediante dinero en efectivo, tarjetas de regalo, transferencias de dinero o cualquier otro método sospechoso.

Cómo puede protegerse:

Siempre verifique y confirme la autenticidad de una solicitud de beneficencia realizando una investigación independiente sobre la organización. Pida a quienes le llamen para solicitar donaciones su número de registro, documente cada donación y nunca pague con dinero en efectivo, tarjetas de regalo ni transferencias bancarias.

Las compras en línea son cómodas. Pero en esta temporada de fiestas, tenga cuidado con los estafadores.

En diciembre, las ventas de comercio electrónico se disparan debido a las compras de regalos navideños.

Pero el año pasado, la Federal Trade Commission (FTC, Comisión Federal de Comercio) informó más de 368 000 quejas de fraude relacionadas con compras en línea, el segundo tipo de queja de fraude más frecuente en los Estados Unidos. Uno de cada cuatro estadounidenses informó haber perdido dinero debido a una estafa, con una pérdida promedio de $500.

A medida que los delitos cibernéticos se vuelven más sofisticados y más difíciles de detectar, resulta más importante que nunca ser un comprador inteligente y protegido durante esta temporada de fiestas.

Algunos consejos de seguridad para compras en línea:

- **Revise las políticas de devolución:** lea la política de devolución o cambios del sitio, ya que las principales tiendas minoristas como Amazon y Target están endureciendo sus políticas debido al aumento del fraude en las devoluciones.
- **No se deje engañar por las buenas ofertas:** pueden aparecer anuncios emergentes de productos populares a precios sospechosamente bajos. Si la oferta parece demasiado buena para ser real, es probable que no lo sea. No haga clic en anuncios sospechosos.
- **Tenga cuidado con los productos fraudulentos:** sitios desconocidos intentarán vender imitaciones de productos o juguetes falsificados, que a menudo están mal etiquetados y contienen piezas pequeñas o toxinas. Compre únicamente en tiendas minoristas de confianza.
- **Verifique la URL:** controle que el sitio web comience con “https”. La “S” significa que el sitio es seguro. Verifique la

SOLICITUDES DE CHARLAS

¿Desea que el DCP dé una charla a su organización o presente una mesa en su evento? Póngase en contacto con Catherine Blinder al correo electrónico Catherine.Blinder@ct.gov para enviar una solicitud.

Contacto

Connecticut Department of Consumer Protection

450 Columbus Boulevard,

Suite 901

Hartford, CT 06103-1840

Línea principal: (860) 713-6100

(de 8:30 a. m. a 4:30 p. m.)

Consumer Complaint Center

(860) 713-6300

Línea gratuita: (800) 842-2649
De 8:30 a. m. a 4:30 p. m.
Correo electrónico:

DCP.complaints@ct.gov

VISÍTENOS EN LÍNEA
CT.GOV/DCP

gramática en todo el sitio web. Use la herramienta Safe Browsing de Google para asegurarse de que el sitio web sea seguro.

- **Lea las reseñas.**
- **Use una tarjeta de crédito:** las tarjetas de crédito ofrecen más protección que las tarjetas de débito. Según la ley federal, usted puede cuestionar cargos no autorizados a su tarjeta de crédito. Evite aplicaciones como PayPal, Venmo y Zelle para pagos en línea. Utilice este método únicamente con personas que conozca y en quienes confíe.
- **Compre en tiendas locales:** comprar localmente puede evitar que sea víctima de una estafa en línea.

Qué hacer si es víctima de una estafa en línea:

1. Denuncie la estafa lo antes posible ante el Department of Consumer Protection (DCP, Departamento de Protección del Consumidor), ante la Federal Trade Commission y ante el departamento de policía local.
2. Comuníquese con su banco o emisor de la tarjeta de crédito para cuestionar los cargos. Es posible que puedan cancelar el cargo.
3. Cambie las contraseñas de todas sus cuentas en línea.

Tenga cuidado con el *smishing*

Los intentos de *smishing* ocurren cuando los estafadores envían mensajes de texto haciéndose pasar por un servicio de entrega para engañar a los destinatarios a fin de que ingresen información personal.

Mientras espera que se entreguen sus paquetes, es posible que reciba un mensaje de texto que parece ser de USPS o FedEx que dice: “Su paquete se ha retrasado; confirme su código postal mediante el enlace”.

Si recibe un mensaje como este, no haga clic en el enlace, utilice la función “Denunciar correo no deseado” y bloquee el número. Si envió o está esperando un paquete y aún no está seguro, llame al número de atención al cliente del servicio de entregas.

¿Se nos pasó algún consejo? ¿Quiere saber más sobre algún tema? Envíenos un correo electrónico a DCP.Communications@ct.gov.