Consejos Sobre Compras en Intranet

- Compruebe las normas de la tienda minorista en Internet sobre devoluciones y reembolsos, así como lo que ocurre si hay algún problema con el artículo comprado.
- Pague con un método de pago seguro. Por ejemplo, las tarjetas de crédito o los sistemas de pago seguro en línea ofrecen protecciones adicionales.
- Si un vendedor exige el pago mediante transferencia bancaria, tarjeta regalo o criptomoneda, deténgase y busque otro vendedor. Los estafadores suelen preferir estos métodos de pago porque son difíciles de rastrear.
- Cuando compre en sitios de segunda mano, no le compre a un vendedor que solicite el pago desde una fuente distinta a la del sistema del sitio. Si un consumidor hace esto, las protecciones del mercado frente al fraude se pierden y es probable que el cliente no reciba el artículo y no pueda optar a un reembolso.
- Cuando venda artículos por Internet, nunca acepte más dinero que el del valor de compra acordado.
- Si le compra a una tienda minorista nueva, consulte con la Oficina de Buenas Prácticas Comerciales (BBB, por sus siglas en inglés) para determinar si otros clientes han presentado reclamos en su contra.

Oficina de la Fiscal General Estafas a Simple Vista:

Estafas de Comercio Electrónico

Visite <u>MyFloridaLegal.com</u> para obtener consejos para los consumidores o para presentar un reclamo.

Denuncie el fraude llamando al

1-866-9-NO-SCAM (1-866-966-7226)

Consulte otros recursos de Estafas a Simple Vista en: MyFloridaLegal.com/ScamsAtAGlance

> Oficina de la Fiscal General PL-01 The Capitol Tallahassee, FL 32399-1050

> > MyFloridaLegal.com



Las compras en línea son una manera práctica de conseguir grandes ofertas desde la comodidad de casa. Pero mientras navega por Internet, tenga cuidado con los estafadores que buscan aprovecharse de usted, obtener su información personal y dejarlo expuesto a pérdidas financieras. Conforme la tecnología avanza, conocer estos sistemas lo ayudará a mantenerse a salvo de las Estafas de Comercio Electrónico.

Estafas por Falta de Entrega

???

Hay dos tipos de estafas por falta de entrega en las compras por Internet: cuando un vendedor acepta el pago, pero apenas tiene contacto con el comprador y nunca entrega el producto, y cuando un estafador lanza una amplia red de correos electrónicos de errores de envío para intentar engañar a los consumidores, normalmente después de que ya han realizado el pago.

En el primer caso, un estafador puede proporcionar un número de seguimiento falso e ignorar los intentos de contacto del consumidor y así robarse el dinero.

En el segundo caso, un estafador enviará un correo electrónico de error de envío alegando que es necesario actualizar la información para que el producto se entregue de manera correcta, todo ello para robar información personal y financiera y dinero.

Para evitar una estafa en la entrega, investigue la reputación del vendedor y lea las opiniones de otros clientes. Utilice servicios de mercado en línea establecidos y de buena reputación, y considere la posibilidad de utilizar servicios de depósito en garantía u opciones de pago que retengan los fondos hasta recibir el producto.

Mensajes de Correo Electrónico de Phishing



Los estafadores suelen utilizar mensajes de correo electrónico para engañar a sus víctimas para que proporcionen información personal o instalar programas maliciosos en sus dispositivos. Lo que puede parecer un correo electrónico legítimo de un comercio minorista conocido solicitando verificar información personal para resolver un problema de cuenta, podría ser en realidad un correo electrónico de phishing de un estafador.

Desconfíe cuando alguien le envíe un correo electrónico solicitando información personal o lo inste a tomar medidas inmediatas. Compruebe si la dirección del remitente presenta variaciones sospechosas o errores ortográficos en el nombre de la empresa o la dirección web. En lugar de hacer clic en los enlaces de los correos electrónicos, escriba manualmente la dirección del sitio web del comercio minorista en el navegador.

Estafas de Sobrepago



Una estafa de sobrepago se dirige a los vendedores a través de anuncios o subastas en línea. Un estafador compra el artículo, pero envía un pago por un importe superior al precio de venta acordado y, a continuación, solicita el reembolso del sobrepago. El vendedor devuelve los fondos, pero el método de pago original resulta ser fraudulento. En algunos casos, el vendedor pierde tanto el artículo como los fondos.

Cuando venda por Internet, verifique de forma independiente la información de su comprador. Nunca acepte un pago, especialmente un cheque, por un importe superior al precio de venta y verifique siempre la autenticidad de los pagos antes de efectuar cualquier devolución. Utilice plataformas de pago seguras que ofrezcan a los vendedores protección para las transacciones en línea

Tiendas en Linea Falsas



Si una tienda en línea ofrece precios muy rebajados en artículos populares de electrónica o artículos de diseño, es posible que la tienda minorista sea falsa. Si compra en un sitio web falso, el cliente puede recibir productos falsificados o de calidad inferior, o peor aún, tal vez no reciba el producto. Si una oferta parece demasiado buena como para ser verdad, probablemente no lo sea.

Investigue la empresa y compruebe si tiene reseñas, valoraciones y reclamos en el sitio web de la Oficina de Buenas Prácticas Comerciales: www.BBB.org. Verifique la información de contacto de la tienda, incluida la dirección física y el número de teléfono. Si decide hacer una compra, utilice una tarjeta de crédito, ya que puede ofrecerle una mayor protección al consumidor.

Robo de Identidad



El robo de identidad se produce cuando alguien utiliza, o intenta utilizar, la información personal de otra persona para cometer fraude. Al comprar por Internet, facilitar sus datos a un sitio web impostor o a un estafador que simule ser un representante del servicio de atención al cliente puede dar lugar a un robo de identidad. Los delincuentes utilizan la información de las víctimas para abrir cuentas y realizar compras fraudulentas.

Cuando compre en Internet, solo comparta información personal en sitios web seguros. Un navegador seguro exhibe "https" o el símbolo de un candado en la barra de direcciones. Desconfíe de los pedidos no solicitados de información personal por correo electrónico. Supervise de manera periódica los estados de cuenta y los informes de crédito para detectar actividades sospechosas. Solicite un informe de crédito gratuito a través del sitio web autorizado por el gobierno en AnnualCreditReport.com.