Compras navideñas seguras en Internet:

Consejos para las compras navideñas por Internet:

BBB | Walmart

Ha llegado la época del año en que muchos de nosotros planeamos hacer al menos algunas de nuestras compras navideñas por Internet. Para su seguridad y la de los suyos, aquí van algunos consejos para detectar y evitar estafas.

Vendedores y páginas web desconocidos.

Si está interesado en comprarle a un vendedor nuevo o en una página web desconocidos, tómese el tiempo de investigar antes de comprar.

- **Si la oferta suena demasiado buena para ser verdad, probablemente lo es.** No compre solo por el precio. Precios demasiado buenos y artículos difíciles de encontrar son una señal de alarma de que la página web podría ser falsa.
- **No crea todo lo que ve.** Los estafadores son excelentes para imitar sellos oficiales, tipografía y otros detalles. El hecho de que una página web parezca oficial no significa que lo sea.
- **Dedique unos minutos a investigar una página web nueva:**
  - **Verifique la URL:** Los estafadores crean URL falsas que imitan nombres de marcas conocidas. Si se fija bien, normalmente podrá detectar una letra o algo incorrecto.
  - **Preste atención a la gramática incorrecta:** lea atentamente el contenido; es posible que detecte errores tipográficos y gramaticales, lo que indica que la página web se creó en poco tiempo.
  - **Investigue la antigüedad del dominio:** Los estafadores crean páginas atractivas en poco tiempo para atraer a sus víctimas antes de que la despubliquen. Las herramientas en línea pueden ayudarlo a averiguar cuánto tiempo lleva activo el dominio. Si se trata de una página web nueva, proceda con cautela.
  - **Busque información de contacto:** ¿Hay alguna forma de ponerse en contacto con la empresa (teléfono, correo electrónico, dirección, chat en línea)? Si la única información de contacto que encuentra es un formulario en línea, es una señal de alarma.
  - **Asegúrese de que es segura:** Busque el “https” en la URL (la s extra corresponde a “seguro”) y un pequeño icono de candado en la barra de direcciones.

“Piratas del porche.”

Cada año se roban millones de paquetes. Tome medidas para proteger sus entregas.

- **No deje paquetes desatendidos.** Cuando sea posible, no deje los paquetes entregados desatendidos durante largos periodos de tiempo. Si está esperando un paquete, intente programar la entrega cuando sepa que va a estar en casa.
- **Recoger en la tienda.** Si está comprando en línea un artículo en una tienda cercana a su domicilio, considere la posibilidad de recogerlo en la tienda. Las tiendas exigirán prueba de la compra o identificación antes de entregar los paquetes.
- **Utilice una cámara de seguridad.** Instalar un sistema de seguridad doméstico con cámaras o un timbre con cámara es una buena forma de disuadir del robo de paquetes, sobre todo si es bien visible. Considere la posibilidad de incluir un cartel que indique específicamente que el domicilio está vigilado.
- **Exija una firma.** Muchas empresas de reparto incluyen la opción de exigir una firma antes de dejar un paquete, lo que le permite tomar posesión física del artículo en cuanto se entrega.

Recuerde que las tarjetas de regalo son para regalar, NO PARA pagos no solicitados.

Las tarjetas de regalo pueden ser el regalo navideño perfecto para amigos o seres queridos, pero también pueden ser una señal de alarma de fraude.

- **Tenga cuidado con las personas que le piden que realice un pago no solicitado con una tarjeta de regalo.** Los estafadores piden a sus víctimas que les paguen con tarjetas de regalo porque es una forma cómoda de robar dinero y son difíciles de rastrear o recuperar. Las organizaciones legítimas nunca le pedirán que les pague con una tarjeta de regalo.
- **Utilice transacciones seguras y rastreables.** Evite pagar mediante transferencia bancaria, giro postal, tarjeta de regalo u otros métodos de pago no tradicionales.

Protéjase en las redes sociales.

Las estafas en las redes sociales aumentaron un 63 % en 2023.

- **Evite hacer compras rápidas mientras navega por las redes sociales.** Sea más consciente de sus compras en línea y evite las compras impulsivas.
- **Desconfíe de "amigos nuevos" que conoce en línea que le envían mensajes directos con oportunidades increíbles.** A veces, los estafadores se hacen pasar por conocidos o entablan una relación en línea antes de estafarlo.
- **Evite compartir demasiados datos personales en sus publicaciones en las redes sociales.** Estos datos pueden utilizarse para la ingeniería social/phishing.
- **No tome una decisión de compra basándose únicamente en los comentarios.** Asegúrese de ampliar su investigación más allá de los comentarios de los clientes antes de tomar una decisión de compra. Siempre investigue al vendedor y compre solo desde su sitio web o aplicación oficial.

Si cree que está siendo víctima de una estafa:

- **Mantenga la calma.** Si lo presionan para que tome una decisión rápida, resista la tentación sin importar cuán dramática sea la situación o cuán amenazante o intimidante suene la persona que llama.
- **No responda directamente.** No responda a llamadas, mensajes de texto o correos electrónicos no solicitados. En cambio, llame directamente a la empresa o a la persona para verificar que el mensaje o la llamada que recibió sean legítimos.
- **Vaya a la fuente o busque ayuda.** Comuníquese con la empresa a través de la información que ya tiene o que puede encontrar en su página web. En caso de duda, llame a su BBB® local para solicitar una segunda opinión. Si hizo una compra, siempre verifíquela y hágale el seguimiento mediante la app móvil o la página web de la empresa.
- **Nunca proporcione información personal (número de Seguro Social, números de cuenta/contraseñas, número de licencia, etc.) por teléfono, especialmente si la llamada fue inesperada.** Los estafadores pueden hacerse pasar por un representante de servicio al cliente de una empresa conocida, incluso falsificando una llamada (falsificando el nombre/organización en su identificador de llamadas). Si no está seguro, dé por finalizada la llamada o el chat y comuníquese directamente con el número de teléfono o la página web de servicio al cliente de la empresa.
- **Nunca pague por teléfono, especialmente si la llamada no fue solicitada.** Nunca haga un pago hasta que haya verificado todos los detalles con un tercero o a través del centro de llamadas o la página web oficial de la organización.
- **Nunca permita el acceso remoto a su computadora si alguien le ofrece soporte técnico.** Apague su computadora inmediatamente y busque soporte directamente de un proveedor de servicios de confianza.
- **Haga una búsqueda en nuestro BBB Scam Tracker℠.** Si sospecha de la situación, haga una búsqueda en el BBB Scam Tracker para ver si alguien más reportó una situación similar. El BBB Scam Tracker le permite buscar por correo electrónico, URL, número de teléfono y más.
- **Verifique la dirección de correo electrónico o la URL más de cerca.** Los estafadores usan direcciones de páginas web o correos electrónicos similares para que parezcan legítimos, pero si observa detenidamente, es posible que encuentre una letra o un número incorrecto.
- **Denuncie cualquier estafa al BBB Scam Tracker.** Reportar estafas ayuda a proteger a otros. BBB publica informes de estafas para que otros puedan evitar la estafa de la que fueron víctima.

HAZ TU PARTE.
COMPRE INTELIGENTEMENTE.
BBB.ORG/SHOPSMART

BBB | Walmart