¿Compras por Internet? Protéjase con estos consejos para prevenir 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 o lee.** Los estafadores son excelentes para imitar logotipos 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.
  - **Busque la fecha de creación de la página:** 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 activa la página. 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.

Ladrones de paquetes.

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.
- **Envíe sus compras a la tienda.** Si está comprando un artículo en línea 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 haga un pago con una tarjeta de regalo.** Los estafadores les 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 prepago, tarjeta de regalo u otros métodos de pago no tradicionales.

Protéjase en las redes sociales.

Aproximadamente el 82 % de los consumidores informaron haber perdido dinero cuando se comunicaron con un estafador a través de redes sociales.

- **Evite hacer compras rápidas cuando 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. Investigue siempre al vendedor y compre solo en la página web o app móvil oficial.

Detecte y evite los avisos de envío suplantados.

- **Vaya directamente a la fuente:** En lugar de hacer clic, abra una nueva ventana del navegador y vaya manualmente a la página web oficial de la empresa de envíos (p. ej., USPS.gov, UPS.com, FedEx.com).
- **Reastree el envío utilizando la página web real:** Utilice el número de rastreo que recibió en su confirmación de compra original para comprobar si hay problemas de envío legítimos en la página web oficial.
- **Desconfíe de las solicitudes de pago:** Las empresas de envíos legítimas no suelen exigir el pago inmediato de problemas de entrega mediante mensajes de texto no solicitados.
- **Verifique con el remitente:** Si le preocupa, comuníquese directamente con la tienda donde hizo la compra para verificar cualquier notificación de envío.

Si sospecha una estafa: qué tiene que hacer

- **Mantenga la calma.** No tome decisiones apresuradas, aunque el mensaje parezca urgente o amenazante.
- **No responda directamente.** Ignore las llamadas, mensajes de texto o correos electrónicos no solicitados; verifique la información utilizando datos de contacto confiables.
- **Vaya directamente a la fuente.** Comuníquese con la empresa utilizando información verificada o llame a su BBB® local para que lo asesoren.
- **Proteja su información personal.** Nunca comparta datos confidenciales por teléfono, especialmente si se trata de llamadas inesperadas.
- **No pague por teléfono.** Verifique todos los detalles a través de canales oficiales antes de hacer cualquier pago.
- **Evite el acceso remoto.** Nunca permita que un servicio de soporte técnico desconocido acceda a su computadora; contáctese con un proveedor de confianza.
- **Utilice el BBB Scam Tracker℠.** Haga una búsqueda para ver si otras personas han denunciado estafas similares.
- **Verifique las direcciones URL y los correos electrónicos.** Fíjese bien en los errores chicos que podrían indicar que se trata de una página web o un correo electrónico falsos.
- **Denuncie las estafas.** Ayude a otros consumidores denunciándolas en el BBB Scam Tracker℠.

PONGA DE SU PARTE. **COMPRE CON CUIDADO.**
BBB.ORG/SHOPSMART

BBB | Walmart