



# Consejos para realizar compras seguras en Internet

Las compras en línea presentan una oportunidad para que los consumidores compren prácticamente cualquier cosa de forma rápida y cómoda. No obstante, Internet tiene muchos anuncios falsos, sitios web fraudulentos y estafadores que intentan quitarle su dinero y no darle nada a cambio. Siempre y cuando se protejan, los consumidores pueden tener una experiencia de compra en internet segura.

---

*La investigación salvaguarda la protección.*

---

## Debemos conocer a quien le compramos

Su mejor protección al comprar es hacer negocios con empresas que conoce. No importa cuán impresionante sea el sitio web de una empresa, cuán convincente pueda parecer un vendedor por teléfono o cuán sincero pueda parecer un vendedor a domicilio, debe verificar la reputación de una empresa, si con certeza, usted no está familiarizado con la empresa, es importante comprobarlo

La investigación es el primer paso en la protección

- Consulte con amigos para ver si alguna vez han hecho negocios con la empresa.
- Consulte con la Oficina de Protección al Consumidor y *Better Business Bureau* en Wisconsin o el estado donde se encuentra el vendedor.
- Confirme la dirección física y el número de teléfono del vendedor. Al comprar con un proveedor extranjero, es posible que no tenga las mismas protecciones o no pueda hacer cumplir sus derechos tan fácilmente como cuando el proveedor está en los Estados Unidos.
- Haga una búsqueda en internet. Escriba el nombre de la empresa en su buscador con términos como "queja" (*complaint* en inglés), "estafa" (*scam* en inglés) o "revisión" (*review* en inglés). Es probable que si otros hayan tenido problemas con esta empresa, existan menciones al respecto.



## Comprenda el alcance del Internet

Si bien Internet ha ampliado enormemente las oportunidades de comprar desde casa, también ha aumentado las posibilidades de ser estafado. La identificación de un proveedor fraudulento en Internet puede resultar complicado. Con mucha facilidad se puede crear un sitio web llamativo o enviar lo que parece ser un mensaje de correo electrónico amigable.

Los vendedores en internet quieren conocer cuáles son sus hábitos de compra. Para lograr esto, ellos usan información que es sumamente valiosa para adaptarle la publicidad acorde a sus gustos, lo que a menudo resulta en que usted sea bombardeado con anuncios no deseados. Los proveedores de Internet utilizan "cookies" para enviar anuncios orientados a sus gustos e intereses. Una "cookie" es información que un sitio guarda en su computadora usando su navegador web. Los datos se pueden utilizar para crear un perfil de sus actividades en internet y conectarlo con la publicidad que verá en el futuro.

Mientras que los proveedores legítimos utilizan cookies para orientar sus anuncios, los estafadores las utilizan para atraer a los consumidores con ofertas increíbles de productos que ni siquiera tienen o que no venderán. Tenga cuidado con los anuncios y sitios web que ofrecen productos que están agotados en otros lugares. Si ve una oferta que parece demasiado buena para ser verdad, especialmente si se trata de un artículo raro o

difícil de encontrar, la mayoría de las veces se trata de una estafa.

Revise las cláusulas de devolución, reembolso y envío y gestión, u otros términos legales. Si no puede encontrarlos, pregúntele al vendedor dónde se encuentran en el sitio o pida que se los proporcione por escrito.

Imprima los términos. Debe imprimir y plasmar la fecha de la copia de los términos, condiciones, garantías, descripción del artículo, información de la empresa e incluso correos electrónicos de confirmación, y guardarlos con los registros de su compra.

## Proteja su privacidad

Solo debe proporcionar información personal si sabe quién recopilará la información y cómo se utilizará.

- No proporcione información financiera sobre su tarjeta de crédito u otra información a cambio de una tarjeta de regalo gratuita o de un alquiler vacacional.
- No proporcione su número de seguro social, número de licencia de conducir ni ninguna otra información personal que no sea necesaria para la transacción.
- No envíe su información por correo electrónico. El correo electrónico no es una forma segura de transmitir información personal.
- No haga clic en ningún enlace que aparezca. Las empresas legítimas no solicitan su información mediante mensajes emergentes en su pantalla.
- Consulte la cláusula de privacidad. Las empresas de renombre publicarán su cláusula de privacidad en su sitio web. Lea la cláusula y sepa cómo utilizarán su información.
- Utilice un navegador seguro al realizar pagos. No utilice *Wi-Fi* público para enviar información confidencial. Los llamados “*hot spots*” públicos no son seguros.
- Mantenga actualizado su antivirus, antispyware y su *firewall*.

## Cautela, ante todo

Garantice la entrega segura de su artículo. Si le preocupa que no esté en casa cuando se entregue su

paquete y que alguien pueda recogerlo, solicite a la compañía de envío que solicite una firma antes de dejar el paquete. Alternativamente, puede ser más seguro entregar el paquete a un amigo o familiar que estará en casa.

Inspeccione su compra. Tan pronto reciba su compra, dedique tiempo a revisarla. En caso de detectar algún problema, comuníquese con el vendedor de inmediato. Informe al vendedor por escrito sobre cualquier problema que tenga, solicite una reparación o un reembolso y guarde una copia de su correspondencia.

Proteja sus contraseñas al momento de realizar pedidos en Internet. No utilice la misma contraseña que utiliza para iniciar su computadora. Intente utilizar una contraseña diferente cada vez que cree una cuenta nueva con un sitio web.

## Aplicaciones de pago móvil

La popularidad de las aplicaciones de pago móvil ha aumentado, y los estafadores lo saben. Las aplicaciones de pago móvil como *Venmo*, *Cash App* o *Zelle* le permiten enviar y recibir dinero usando su teléfono inteligente, lo que hace que la transferencia de dinero sea rápida y conveniente.

Configurar una cuenta es fácil. Al agregar sus tarjetas de crédito y/o débito a una aplicación de pagos móviles, puede pagar bienes o servicios con su teléfono, con poca demora. Esta facilidad de uso los convierte en el método de pago preferido de los estafadores.

Los estafadores intentan que los consumidores tomen decisiones rápidas sin realizar una investigación adecuada. Aunque es rápido y sencillo, antes de enviar el dinero es importante hacer una pausa y evaluar cada situación. Tómese el tiempo para investigar al vendedor o a la persona a la que le enviará dinero.

Considere estas preguntas, antes de enviar dinero:

- ¿Se puede pagar utilizando un método diferente?
- ¿El precio es demasiado bueno para ser verdad?
- ¿Es esta realmente una oportunidad que no se puede perder?

## ¿Qué hacer si ha sido víctima de una estafa?

Si ha enviado dinero a un estafador, informe de la estafa a la aplicación de pago móvil y pídale que revierta la transacción y presénteles una queja con relación a la transacción fraudulenta. También debe comunicarse con su empresa prestamista para que se entere de si tienen alguna solución para transacciones fraudulentas. De no ser exitoso con estos pasos, presente una queja ante la Oficina de Protección al Consumidor.

*Para obtener más información visite nuestro sitio Web, o contáctenos:*

Wisconsin Department of Agriculture,  
Trade and Consumer Protection  
*Bureau of Consumer Protection*

2811 Agriculture Drive

PO Box 8911

Madison, WI 53708-8911

Correo electrónico: [DATCPHotline@wi.gov](mailto:DATCPHotline@wi.gov)

Sitio Web: [datcp.wi.gov](http://datcp.wi.gov)

Teléfono: (800) 422-7128

TTY: Marque 711 o llame al (800) 947-3529 antes de llamar a DATCP



USE ESTE CÓDIGO QR PARA  
PRESENTAR UNA QUEJA