
# Compras en línea de forma segura

Se acerca la temporada navideña. Pronto, millones de personas buscarán comprar los regalos perfectos y muchos de nosotros compraremos en línea. Desafortunadamente, los ciberdelincuentes también estarán activos, creando sitios web de compras falsos y otras estafas de compras en línea para robar tu información o dinero. Descubre cómo puedes encontrar buenas ofertas sin convertirte en una víctima.

## Tiendas online falsas

Los delincuentes crean tiendas online falsas que imitan el aspecto de sitios reales o utilizan nombres de tiendas o marcas conocidas. Cuando buscas las mejores ofertas en línea, es posible que te encuentres en uno de estos sitios falsos. Al comprar en dichos sitios web, puedes terminar con artículos falsificados o robados, o es posible que tus compras nunca se entreguen. Sigue los siguientes pasos para protegerte:

- Cuando sea posible, compra en tiendas en línea que ya conoces, en las que confías y con las que has hecho negocios anteriormente. Coloca estas tiendas en línea en tus marcadores.
- Sospecha de los anuncios o promociones en motores de búsqueda o redes sociales que sean significativamente más bajos que los que ves en las tiendas en línea establecidas. Si un trato parece demasiado bueno para ser verdad, puede ser una estafa.
- Ten cuidado con los sitios web que no tienen forma de contactarlos, formularios de contacto rotos o que usan direcciones de correo electrónico personales.
- Sospecha si un sitio web se parece a uno que has usado en el pasado, pero el nombre de dominio del sitio web o el nombre de la tienda es diferente. Por ejemplo, puedes estar acostumbrado a comprar en Amazon, cuya dirección de sitio web es www.amazon.com, pero terminar en un sitio web falso que se ve similar, pero tiene la dirección de sitio web www.amazonshoppers.com.
- Escribe el nombre de la tienda en línea o su dirección web en un motor de búsqueda para ver lo que otros han dicho al respecto. Busca términos como "fraude", "estafa", "nunca más" y "falsificación".
- Protege tus cuentas en línea utilizando una contraseña única y segura para cada una de tus cuentas. ¿No recuerdas todas tus contraseñas? Considera almacenarlos todos en un administrador de contraseñas.

## Estafadores en sitios web legítimos

Mantente alerta incluso cuando compres en sitios web confiables. Las tiendas en línea a menudo ofrecen productos vendidos por terceros (diferentes personas o empresas) que pueden tener intenciones fraudulentas. Estos destinos en línea son como los mercados del mundo real, donde algunos vendedores son más confiables que otros.

- Verifica la reputación de cada vendedor antes de realizar el pedido leyendo sus reseñas.
- Ten cuidado con los vendedores que son nuevos en la tienda en línea, que carecen de reseñas o que venden artículos a precios inusualmente bajos.

- Revisa la política de la tienda en línea sobre compras de dichos terceros.
- En caso de duda, compra artículos vendidos directamente por la tienda en línea, no por terceros vendedores que participan en su mercado en línea.
- Incluso con proveedores legítimos, asegúrate de comprender la garantía del vendedor y las políticas de devolución antes de realizar tu compra.

## Pagos en línea para compras

Revisa periódicamente los extractos de tu tarjeta de crédito para identificar cargos sospechosos. Si es posible, habilita la opción para notificarte por correo electrónico, mensaje de texto o aplicación cuando se realiza un cargo. Si encuentras alguna actividad sospechosa, infórmalo a la compañía de tu tarjeta de crédito de inmediato. Utiliza tarjetas de crédito en lugar de tarjetas de débito para pagos en línea. Las tarjetas de débito toman dinero directamente de tu cuenta bancaria; si se comete un fraude, te resultará mucho más difícil recuperar tu dinero. Los servicios de pago electrónico o cartera electrónica como PayPal también son una opción más segura para compras en línea, ya que no requieren que reveles un número de tarjeta de crédito al proveedor. Evita los sitios web que solo aceptan pagos en criptomonedas o requieren métodos de pago poco conocidos.

El hecho de que una tienda en línea tenga un aspecto profesional no significa que sea legítima. Si el sitio web te hace sentir incómodo, no lo uses. En su lugar, dirígete a un sitio conocido en el que puedas confiar o que hayas utilizado de forma segura en el pasado. Es posible que no encuentres esa oferta increíble, pero es mucho más probable que de esta manera evites ser estafado.

## Editor invitado

Mark Orlando es líder en seguridad que ha protegido redes de seguridad en el Pentágono, la Casa Blanca y muchos otros clientes del sector privado. Actualmente es CEO y cofundador en la firma de ciberseguridad Bionic y es instructor y autor de un curso en el Instituto SANS. [Twitter: @markaorlando]

## Recursos

**Creando contraseñas simples:** https://www.sans.org/newsletters/ouch/making-passwords-simple/
**Ingeniería social:** https://www.sans.org/newsletters/ouch/social-engineering-attacks/
**Smishing- Ataques a través de mensajería instantánea:** https://www.sans.org/newsletters/ouch/messaging-smishing-attacks/
**Estafas a través de redes sociales:** https://www.sans.org/newsletters/ouch/scamming-you-through-social-media/

**Traducido para la comunidad por:** Célica Martínez Aponte, UNAM-CERT