

Cada vez son más frecuentes las prácticas delictivas en las compras por internet. Para tratar de evitarlas, hay que conocer algunos conceptos.



El **PHISHING** es una técnica con la que te muestran una web conocida para engañarte y que facilites contraseñas o datos personales que luego utilizarán o venderán a terceros para cometer otros fraudes.



Links · [Cómo identificar un phishing](#)



Las **WEB FALSAS** son páginas que simulan ser un comercio online cuando en realidad se trata de un fraude, ya que detrás de la web no existe ningún soporte comercial.



En las **ESTAFAS POR CORREO ELECTRÓNICO** los estafadores tratan de acceder por distintos mecanismos (malware, etc.) al tráfico de mensajes entre el comercio y su distribuidor, haciéndose pasar por los distribuidores legítimos del comercio, induciendo a este último a realizar los pagos por la compra de la mercancía a cuentas bancarias o sistemas de dinero virtual controlados por ellos.



En los **DELITOS CONTRA LA PROPIEDAD INDUSTRIAL E INTELECTUAL** debes extremar la prudencia respecto de las ofertas de productos de lujo o marcas de gama alta, y en relación con los sitios que ofrecen la posibilidad al usuario de descargarse de modo indiscriminado y sin garantías discos, películas, series de televisión, libros y otros productos similares de modo gratuito, ya que podría tratarse de productos obtenidos sin la autorización de los titulares de los derechos de autor.



La **COMPRA-VENTA ONLINE DE SEGUNDA MANO** también puede entrañar riesgos de fraude, ya sea en la propia identidad del vendedor y/o del comprador, la descripción de las características del producto, el precio de venta o los mecanismos de contacto.



Links · [Servicios compraventa y subastas](#)

CONSEJOS Y RECOMENDACIONES

- **SOSPECHA DE MENSAJES ALARMISTAS O QUE LLAMEN TU ATENCIÓN** con el fin de que accedas a un enlace o descargues un fichero adjunto de manera inminente.
- **NO RESPONDAS A CORREOS ELECTRÓNICOS O MENSAJES QUE TE SOLICITAN TUS DATOS PERSONALES** (por ej., bancarios). Pregunta a quien te solicita los datos o acude a la AEPD, las Fuerzas y Cuerpos de Seguridad del Estado, INCIBE, etc.
- **SI SE REALIZAN COMPRAS FRAUDULENTAS CON TU TARJETA**, debes efectuar la correspondiente denuncia y reclamar la devolución de los cargos efectuados. Anula las tarjetas en caso de pérdida o sustracción.
- **COMPRA EN PÁGINAS OFICIALES Y/O DE CONFIANZA O CON REPUTACIÓN Y PRESTIGIO** consolidado. Desconfía de las gangas. No compres si la tienda no te ofrece información sobre la empresa que hay detrás (titular, NIF/CIF, domicilio fiscal, etc.), condiciones de venta, devoluciones o reclamaciones, y referencias legales (aviso legal, políticas de privacidad, etc.)
- Denuncia si existen razones fundadas de que el producto adquirido se trata de una **FALSIFICACIÓN**.
- **ASEGÚRATE DE QUE TE DESCARGAS LA APP OFICIAL**. Comprueba quién es la entidad que figura como desarrollador de la aplicación, así como la política de privacidad. Antes de descargarla, revisa los permisos que te solicita y valora si son necesarios para el funcionamiento que ofrece.
- **CONSULTA LOS COMENTARIOS Y LA VALORACIÓN** de los usuarios **ANTES DE INSTALAR UNA APP** o comprar a través de ella. Te pueden ayudar a identificar si es fraudulenta o de mala reputación.
- Si vas a comprar o vender a través de un servicio de **VENTA ONLINE DE SEGUNDA MANO**, infórmate sobre quien es el comprador/vendedor antes de aceptar el pago. Utiliza un método de pago conocido. Sospecha si ofrecen más dinero del que se pide en el anuncio. No adelantes dinero.

SI QUIERES SABER MÁS



Links · [Evita fraudes en falsas tiendas online \(I de II\)](#)

Links · [Evita fraudes en falsas tiendas online \(II de II\)](#)

Links · [Yo no compraría en una tienda online si...](#)

Links · [Cómo identificar estafadores online en páginas de anuncios](#)

Links · [¿Será fiable esta página?](#)

Links · [Identificando timos y otros riesgos en servicios de mensajería instantánea](#)

Links · [Apps para dispositivos móviles ¿nos podemos fiar de todas?](#)

Links · [Apps y robo de información](#)

Links · [Por qué evitar apps que requieren de muchos permisos para su uso](#)