



Compra de forma más segura a través de internet

ÍNDICE

1. Presentación
2. ¿Qué es la ciberseguridad? ¿Y por que es tan importante?
3. Los 10 consejos básicos para comprar de forma segura por internet
4. Protege adecuadamente tu dispositivo y utiliza una red de confianza
5. Utiliza los servicios de una tienda online de confianza
6. Alerta ante posibles fraudes en las compras por internet
7. Que medios de pago son los más seguros para comprar o contratar online
8. Cómo configurar mi cuenta de usuario de una forma segura para comprar o contratar online.
9. Bibliografía

Presentación

La **ciberseguridad** es esencial en nuestro día a día, especialmente cuando realizamos compras o contratamos servicios por Internet.

Proteger nuestros datos personales y financieros evita fraudes, robos de identidad y pérdidas económicas. A través de este webinar aprenderás a identificar sitios web seguros, utilizar métodos de pago confiables y reconocer señales de riesgo. Comprar online puede ser cómodo y rápido, pero solo si lo hacemos de forma responsable.

La seguridad digital empieza con pequeñas acciones y buenos hábitos en la red.



¿Qué es la Ciberseguridad? ¿Y porqué es tan importante?

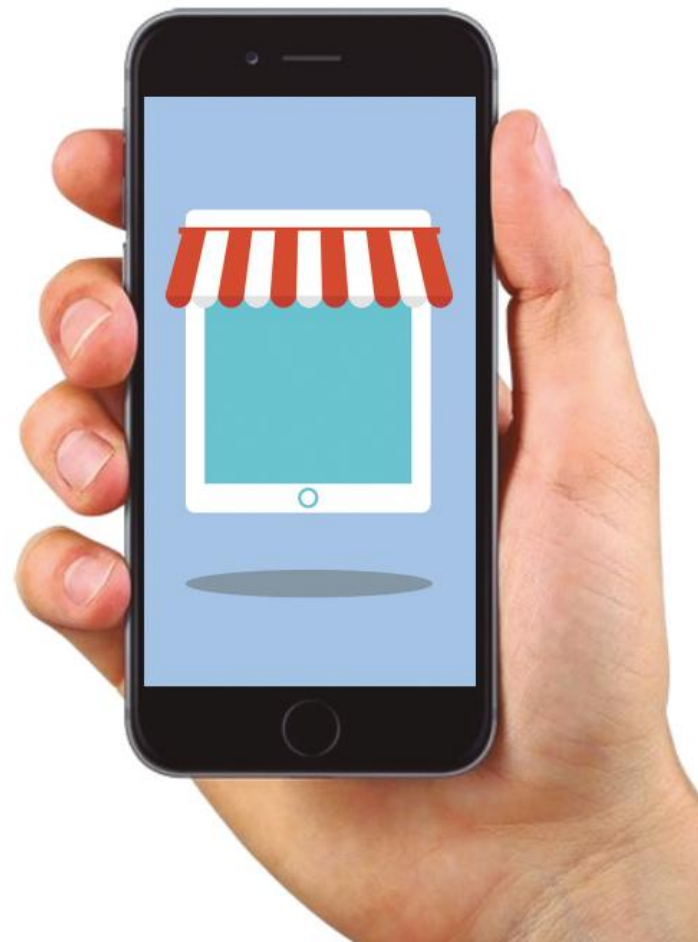
La **ciberseguridad** es el conjunto de medidas y prácticas que protegen nuestros dispositivos, datos y conexiones frente a ataques o fraudes digitales. Es importante porque cada día compartimos información personal y financiera en la red. Sin una buena protección, somos vulnerables a robos, suplantaciones o estafas. La ciberseguridad no depende solo de la tecnología, sino también de nuestras decisiones al navegar. **Mantenernos alerta es la mejor defensa.**



Los 10 consejos básicos para comprar



-  — 1. Realiza tus compras en páginas que te inspiren confianza
-  — 2. Asegúrate de que en la web aparece identificado el responsable de la tienda online y su ubicación
-  — 3. Comprueba que la tienda online es segura y te proporciona toda la información que necesitas sobre consumo y tratamiento de datos personales
-  — 4. Si te es posible, utiliza una tarjeta de uso exclusivo para realizar pagos online
-  — 5. Desconfía de las ofertas demasiado atractivas, ya que podrías estar ante una web fraudulenta
-  — 6. No olvides comprobar que tus dispositivos están configurados correctamente y la conexión a internet es segura antes de proporcionar tus datos personales o tus datos de pago
-  — 7. Nunca envíes dinero en efectivo para completar una compra. Elige con cuidado el medio de pago
-  — 8. Recuerda que los comercios con sellos de confianza ofrecen mayores garantías
-  — 9. Puedes desistir de una compra o contrato sin tener que dar explicaciones en los 14 días posteriores
-  — 10. Si desistes o haces uso de la garantía, ello no debe tener coste alguno para ti, y esto incluye los gastos de envío





— Para realizar compras online en un entorno seguro, es fundamental utilizar una conexión a internet de confianza y que el dispositivo que se use esté debidamente configurado y protegido para evitar que los datos intercambiados entre el usuario y la tienda online se vean comprometidos.



CONSEJOS Y RECOMENDACIONES

- **INSTALA UNA HERRAMIENTA ANTIVIRUS** y analiza tu dispositivo para detectar posibles amenazas. Si está infectado, puedes poner en riesgo la compra y los datos personales aportados.



• Herramientas antivirus gratuitas
• Síntomas de los dispositivos infectados

- **REVISAS LOS PROGRAMAS Y LAS APPS INSTALADAS** en tu dispositivo. Elimina todas las que no utilices. Cuantas más tengas más difícil será mantenerlo actualizado y protegido.



• Cómo proteger los dispositivos y la información que contienen

- **CONFIRMA QUE EL SISTEMA OPERATIVO, PROGRAMAS Y APLICACIONES ESTÁN ACTUALIZADAS** Así evitaras que un delincuente tome el control de tu dispositivo y ejecute acciones maliciosas sin tu conocimiento.



• La importancia de las actualizaciones
• Consecuencias de no instalar las actualizaciones

- **EVITA EL USO DE ORDENADORES, TABLETAS Y TELÉFONOS INTELIGENTES PÚBLICOS O COMPARTIDOS** para realizar compras online.



• Consideraciones a tener en cuenta al utilizar ordenadores públicos
• Cómo actuar en caso de hacer uso de un dispositivo público

- **NO COMPRES UTILIZANDO UNA RED WIFI PÚBLICA.** Terceros pueden interceptar tus comunicaciones. Configura tu router WiFi para que los intrusos no puedan conectarse a tu red.



• Protege tus dispositivos
• Riesgos de usar redes WiFi públicas
• Cuándo utilizar redes WiFi públicas
• Medidas básicas de configuración de redes WiFi
• Cómo asegurar la red WiFi en siete pasos
• Cómo proteger la red WiFi de casa

CONSEJOS Y RECOMENDACIONES

- No utilices los servicios de una tienda online que no te dice **QUIÉN ES SU RESPONSABLE**.
- **LA INFORMACIÓN LEGAL QUE DEBE FACILITARTE LA TIENDA** es fundamental para saber ante quien reclamar en caso de tener algún problema. Debe informarte además de la identidad de su responsable, de para qué va a tratar tus datos y cómo puedes ejercitar tus derechos. Es necesario que te facilite una dirección de correo electrónico u otro medio para que puedas acceder a conocer toda la información que necesites.
- **LA TIENDA SOLO PUEDE UTILIZAR TUS DATOS PERSONALES** para los fines de los que te hayan informado. Si alguno de los fines no guarda relación directa con la gestión de tu compra, contratación o consulta, en el momento en que te solicitan tus datos deben ofrecerte la posibilidad de oponerte a los otros fines.
- **EL COMERCIO ONLINE DEBE INFORMARTE DE LA POSIBILIDAD DE EJERCITAR LOS DERECHOS** ARCO y otros derechos previstos en el Reglamento General de Protección de Datos y cómo puedes hacerlo (sobre el alcance de estos derechos, ver Ficha 6).

 *• Derechos ARCO y nuevos derechos del Reglamento*
Links *• Modelos para ejercer los derechos ARCO*

- **LOS MENORES DE 14 AÑOS NO PUEDEN HACER COMPRAS ONLINE**, sólo sus representantes legales pueden hacerlo en su nombre.

 *• Tú decides en Internet*
Links

- **AL ACCEDER A UN COMERCIO ELECTRÓNICO ES POSIBLE QUE SE DESCARGUEN COOKIES EN TU DISPOSITIVO**. Son ficheros que se almacenan cuando navegas por Internet y que pueden utilizarse para diversos fines. Algunos pueden ser intrusivos, como realizar perfiles en función de tu navegación en Internet o mostrar publicidad basada en tu comportamiento. En estos casos deben informarte sobre su uso y dejarte elegir si las aceptas o no.

 *• Guía sobre el uso de las cookies*
Links

- **SI LA WEB** donde vas a comprar **TE MUESTRA EN EL NAVEGADOR UN ICONO EN FORMA DE CANDADO** y la URL empieza por **HTTPS**, a priori es una página en la que puedes confiar.

 *• Información sobre el candado que aparece en los navegadores*
Links *• Cómo comprobar certificados digitales*

- **COMPRUEBA QUE LA TIENDA ONLINE TIENE UN SELLO DE CONFIANZA**. Eso es porque está adherida a un código de conducta y suelen ofrecer a los consumidores procedimientos alternativos de resolución de conflictos sencillos, rápidos y cómodos. Uno de más conocidos en España es **CONFIANZA ONLINE**

Alerta ante posibles fraudes en las compras por internet

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.



• 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.

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.



Observar el aspecto visual

Una web mal construida y poco atractiva puede ser debido a que se ha hecho con prisas y/o tratando de copiar el estilo de una tienda oficial.



Monitorizar opiniones

Antes de comprar un producto revisaremos las opiniones de otros usuarios haciendo una búsqueda por Internet.

© Comprobar información legal empresa

El NIF de la empresa y otros datos como la razón social o los datos de contactos son necesarios para identificar a una tienda online fiable.

€ Fijarse en los precios

Deben hacernos sospechar los precios demasiado bajos con respecto a las tiendas oficiales o al precio de mercado.

Recomendaciones "Buenas prácticas del cibernauta"



Comprobar certificado SSL **ON**

Las tiendas online fiables tendrán una conexión segura por HTTPS y contarán con un certificado de seguridad.

Leer condiciones y políticas **GDPR**

Seamos conscientes de las condiciones del servicio que se nos está ofreciendo, así como de las políticas de privacidad de la plataforma. Esta información suele incluirse dentro del "Aviso legal" de la web, y debemos sospechar si no lo vemos por ningún lado.

\$ Analizar pagos permitidos

Evitaremos páginas que, aunque contengan los logos de muchos métodos de pago online, a la hora de la verdad solo permiten transferencias a depósitos y pagos con tarjeta.

★ Contrastar reputación en la red

Un rápido vistazo por Internet, buscando por el nombre de la empresa o del vendedor, nos dirá si nos encontramos ante una estafa o fraude.



El tipo de pago a utilizar es una de las mayores preocupaciones cuando se realizan compras online. Aún son muchos los que desconocen las distintas alternativas de pago disponibles, qué ventajas o inconvenientes aporta cada una y cuál ofrece mayor seguridad. También es importante saber cómo se gestionan los datos bancarios que te solicitan para realizar el pago.



— **PAGO EN EFECTIVO.** Son servicios que no debes utilizar ya que están diseñados para realizar transferencias de dinero, incluso de forma anónima, resultando imposible identificar quién es el emisor y el receptor. Aunque este sistema no supone un intercambio de datos bancarios entre vendedor y comprador, en caso de problemas con la compra (producto que no llega, defectuoso o incorrecto) será difícil reclamar el dinero.



— **PAGO CONTRA REEMBOLSO.** Es un método muy seguro porque pagas después de recibir el producto, has abierto el paquete y compruebas que el pedido es correcto.



— **PAGO POR TRANSFERENCIA BANCARIA.** La principal ventaja es que no necesitas introducir ningún dato en el sitio web, sólo ingresar el dinero de tu compra en la cuenta que te facilite el vendedor. Tiene riesgos de seguridad especialmente en caso de transferencias internacionales, ya que el dinero será difícil de recuperar una vez abonada en la cuenta del receptor. Si el titular de la cuenta receptora del dinero no autoriza la devolución del importe, habría que acudir a la vía judicial.



— **PAGO CON TARJETA.** Es el medio de pago más extendido. Es un sistema muy seguro cuando la tienda online utiliza una pasarela de pago ofrecida por un banco que será quien verifique la autenticidad de la tarjeta y protegerá los datos del cliente. Si te es posible, se recomienda utilizar una tarjeta de uso exclusivo para realizar pagos online.



— **PAGO A TRAVÉS DE INTERMEDIARIOS DE CONFIANZA.** Se utiliza a una tercera empresa de confianza, por ejemplo PayPal, que será quien gestione los datos bancarios tanto del vendedor como del comprador y se encargue de formalizar los pagos. El usuario solo necesita disponer de una cuenta en PayPal y configurar en ella su tarjeta de crédito.



CONSEJOS Y RECOMENDACIONES

- Nunca compres ni contrates **CUANDO TE SOLICITEN QUE PAGUES EN EFECTIVO**.
- **LAS OPERACIONES DE PAGO POR TRANSFERENCIA** sólo se considerarán autorizadas cuando el ordenante haya dado el consentimiento para su ejecución.
- **NO SE DEBEN FACILITAR NUNCA DATOS DE LA TARJETA DE CRÉDITO** si la web no dispone de certificado digital y no cifra las comunicaciones (https).
- **CUANDO EL IMPORTE DE UNA COMPRA HAYA SIDO CARGADO FRAUDULENTA O INDEBIDAMENTE** utilizando el número de tu tarjeta de pago, exige la inmediata anulación del cargo.
- Ahora bien, **SI LA COMPRA HA SIDO EFECTIVAMENTE REALIZADA POR TI**, como titular de la tarjeta, y salvo que la exigencia de devolución sea consecuencia de haber ejercido el derecho de desistimiento, deberás resarcir al vendedor por los daños y perjuicios ocasionados por la anulación del cargo de la tarjeta.
- **ANTES DE REALIZAR LOS PAGOS** mediante una tercera empresa de confianza, asegúrate de leer las condiciones de uso del servicio y utilizar una contraseña segura para acceder al mismo.

Configurar cuenta usuario de forma segura



Muchas tiendas online te obligan a crear una cuenta de usuario, solicitando tu nombre y apellidos, dirección de recepción del pedido, domicilio para registrar la factura, datos de la tarjeta de crédito, etc.

Debes proteger el acceso a esa información y por ello es muy importante que utilices **CONTRASEÑAS SEGURAS**. Hacerlo impedirá que otros puedan adivinarlas, accediendo a tus datos o utilizándolas fraudulentamente.



Links

- ¿Por qué son tan importantes las contraseñas?
- Cómo generar contraseñas seguras (video)
- Por qué no utilizar la misma clave para distintos servicios
- Cómo prevenir el robo de contraseñas
- Cómo utilizar un gestor de contraseñas



Una contraseña segura no garantiza totalmente la seguridad de tu cuenta. Por eso, si la tienda online te ofrece la opción de activar la doble verificación no dudes en aceptarla, ya protegerás mejor tus datos personales. Cuando actives la **DOBLE VERIFICACIÓN** (bien durante el proceso de login/registro o durante el proceso de formalización de la compra) la tienda o el servicio online te va a solicitar un PIN, código o clave adicional que previamente habrá enviado al dispositivo que le hayas indicado (por ejemplo, en tu teléfono móvil). Se trata de un código que sólo vais a conocer tú y la tienda. La compra no se va a hacer efectiva hasta que no introduzcas el código.



Links

- Verificación en dos pasos, ¿qué es y cómo me puede ayudar?
- Añade una capa de seguridad extra a la cuenta de usuario



Si se te olvida la contraseña de acceso a la cuenta de la tienda online donde vas a tramitar una compra, los servicios online te van a permitir recuperarla. El mecanismo utilizado con más frecuencia por estos servicios es la **RECUPERACIÓN DE CUENTA**, utilizando el envío de una nueva contraseña a la dirección de correo electrónico que le hayas facilitado. También puede hacerte preguntas de seguridad.



DESPUÉS DE REALIZAR UNA COMPRA ONLINE, posiblemente en tu cuenta de usuario se han memorizado datos como nombre, apellidos, dirección de envío, dirección de facturación, histórico de compras, etc., así como la información relativa a la forma de pago. Si has elegido pagar con tarjeta de crédito los datos que van a guardar son: tipo de tarjeta, número, fecha de caducidad y CVV. Si te proponen guardar estos datos para futuras compras, valora si es necesario, ya que quizás no vuelvas a comprar en esa tienda. Siempre es más seguro borrarlos y facilitarlos nuevamente que dejar tus datos personales en cada tienda online en la que compres.



En las **COMPRAS A TRAVÉS DE APPS** hay que extremar las medidas de seguridad, sobre todo si el terminal donde está configurada la app de compra online tiene tus datos personales, incluidos los bancarios. Piensa que si por algún motivo alguien tiene acceso al terminal, puede realizar compras en tu nombre.

CONSEJOS Y RECOMENDACIONES

- Las contraseñas deben tener una **LONGITUD MÍNIMA DE OCHO CARACTERES** que combine letras mayúsculas, minúsculas, números y caracteres especiales (símbolos).
- **NUNCA UTILICES COMO CONTRASEÑAS PALABRAS SENCILLAS** en cualquier idioma que se puedan encontrar fácilmente en el diccionario.
- **NO ELIJAS CONTRASEÑAS QUE HAGAN REFERENCIA** a tu nombre, tu mascota, lugares significativos, fechas de nacimiento o de otros eventos especiales, etc.
- **EVITA CONTRASEÑAS** formadas únicamente a partir **DE LA CONCATENACIÓN DE VARIOS ELEMENTOS**. Por ejemplo: "Marco1978" (nombre + fecha de nacimiento).
- **NO USES** ninguna de **LAS SIGUIENTES CONTRASEÑAS**, ni similares: 123456, 123456789, qwerty, 12345678, 111111, 1234567890, 1234567, password, 123123, 987654321.
- **NUNCA UTILICES LAS MISMAS CONTRASEÑAS** para servicios diferentes.
- Al recuperar una contraseña a través del correo electrónico, asegúrate de que **LA CONTRASEÑA DE ACCESO AL CORREO SEA SEGURA** y diferente a la que facilitaste en la cuenta de la tienda online. Si el servicio lo permite en su configuración, utiliza un correo alternativo al utilizado en el proceso de registro para la recuperación de la contraseña.
- Al recuperar una contraseña a través de pregunta secreta, **COMPRUEBA QUE LAS RESPUESTAS** no estén basadas en información verídica y sean fáciles de recordar.
- Intenta **NO ALMACENAR INFORMACIÓN FINANCIERA EN CUENTAS DE USUARIO** que no estén correctamente configuradas en materia de seguridad (contraseña segura, doble verificación).
- **NO OLVIDES CERRAR LA SESIÓN AL FINALIZAR LA COMPRA**; evitarás que terceros accedan a ella.
- **ESTABLECE UN BLOQUEO DE PANTALLA** del dispositivo con el menor tiempo de espera posible para restringir el acceso a las funcionalidades del dispositivo, incluyendo las apps.
- **INTENTA CONFIGURAR TU DISPOSITIVO** para que solicite introducir un código PIN antes de descargar cualquier aplicación, tanto si es de pago como si no. Con esta acción evitarás que un tercero instale o utilice aplicaciones sin tu consentimiento.



- ◇ **INCIBE – Instituto Nacional de Ciberseguridad**
Información práctica, guías y avisos sobre seguridad digital.
👉 <https://www.incibe.es>

- ◇ **OSI – Oficina de Seguridad del Internauta (INCIBE)**
Consejos para proteger tus datos y navegar de forma segura.
👉 <https://www.osi.es>

- ◇ **AEPD – Agencia Española de Protección de Datos**
Normas, derechos y buenas prácticas sobre privacidad digital.
👉 <https://www.aepd.es>

- ◇ **Policía Nacional – Seguridad en Internet**
Alertas sobre fraudes, ciberestafas y denuncias online.
👉 https://www.policia.es/_es/tupolicia_seguridadinternet.php

Gracias

