Seguridad en Internet

UNAE

GENERALITAT VALENCIANA
Conselleria d'Economia Sostenible, Sectors Productius, Comerç i Treball

Seguridad en Internet

Internet es, en la actualidad, una forma fundamental de comunicación para la mayoría de las personas, especialmente a través de **dispositivos móviles como smartphones y tablets**.

Pero es imprescindible **conocer los principales riesgos y peligros** que se corren al usar Internet, y las medidas de protección para evitarlos.

Virus y software malicioso

Los virus informáticos son **programas de software dañino**, creados para entrar en un ordenador o dispositivo sin permiso o conocimiento del usuario, y tienen la capacidad de replicarse a sí mismos, continuando así su propagación.

La mayoría pueden causar **graves daños o afectar negativamente el rendimiento de un sistema**, reducir la memoria, destruir datos o dañar archivos, e **incluso robar información** como contraseñas o datos financieros, registrar pulsaciones de teclado, enviar *spam* a los contactos de correo electrónico y hasta tomar el control del equipo. En la actualidad, las **vías más habituales de transmisión** de los virus son la descarga de archivos infectados, navegar por sitios que no son seguros y el correo electrónico.

Para proteger los equipos y terminales es conveniente seguir ciertas recomendaciones de seguridad:

- **Instalar un buen antivirus**, actualizarlo de forma periódica y tener **siempre activado el cortafuegos** (*firewall*).

- **Realizar copias de seguridad frecuentemente**, para recuperar los datos si el sistema se infecta.
- **Tener contraseñas fuertes y robustas y no usar la misma para todo**, pues si los hackers la descubren se ponen en peligro todos los datos y accesos.
- **No abrir correos, enlaces o páginas web** sospechosas.
- **No instalar software de origen desconocido** o que solicite la **desactivación del antivirus**.
- **Analizar cualquier pendrive o tarjeta de memoria** antes de usarlos.
- **Actualizar el navegador web** periódicamente, porque las nuevas versiones corrigen problemas de seguridad.
- Si el navegador web advierte que una **página no es segura, cerrarla inmediatamente**.
- **No aceptar fotos ni archivos recibidos de desconocidos** por correo electrónico u otras vías.
- Si el equipo sufre un ataque, **cambiar todas las contraseñas después de limpiarlo**.

Comercio electrónico

El comercio electrónico es uno de los servicios de la sociedad de la información que ha experimentado un **mayor crecimiento en los últimos años**. Según datos de la CNMC, la **facturación del primer trimestre de 2018 ha aumentado un 32.8% interanual**, hasta alcanzar los **8.974 millones**

de euros, con **más de 156 millones de transacciones**, de las que el **52,7% se realizaron en webs españolas**. Los **sectores de actividad con mayores ingresos** han sido las agencias de viajes y operadores turísticos, con el 14,9% de la facturación total; el transporte aéreo, con el 10,8% y las prendas de vestir, en tercer lugar, con el 6,1%.

Por eso los usuarios deben estar bien informados, ya que la **confianza y la seguridad son esenciales en el entorno digital.** Con este objetivo la **Agencia Española de Protección de Datos (AEPD)**, el **Instituto Nacional de Ciberseguridad (INCIBE)**, la **Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN)** y **Policía Nacional** han elaborado conjuntamente una **Guía práctica sobre compra segura en Internet**, de la que se recogen algunas recomendaciones.

Para realizar **compras online en un entorno seguro**, la primera precaución es **no conectarse a través de una red Wifi pública** para realizar transacciones en las que haya intercambio de datos bancarios o acceso a pasarelas de pago.

A continuación hay que **comprobar la información legal del comercio online**, que permite saber con quién se va a contratar y ante quién reclamar en caso necesario. Se deben

facilitar, entre otros datos, la denominación completa de la entidad, dirección postal y de correo electrónico, número de identificación fiscal y datos de inscripción en el Registro Mercantil, el plazo de conservación de los datos personales, la identificación del Delegado de Protección de Datos y los derechos que asisten al usuario. En caso de duda, se puede **consultar la titularidad del dominio asociado a la página web**.

Hay que tener en cuenta que **los menores de 14 años no pueden prestar su consentimiento** para que los comercios online recojan y traten sus datos personales, por lo que son sus representantes legales - padres o tutores - quienes deben hacerlo en su nombre.

Antes de facilitar datos personales (nombre, dirección, DNI, datos bancarios o de tarjetas) al comprar o contratar, se debe comprobar que la página web o aplicación móvil utiliza el **protocolo de comunicación segura *https***, que cifra la información para que no pueda ser interceptada. Además, deben disponer de un **certificado de seguridad** emitido por organismos independientes. El usuario debe comprobar, por tanto, que el navegador muestre el **icono de un candado** y que la **URL o dirección comience por *https***.

Si se contrata o compra a través de **aplicaciones móviles**, o ***apps***, es aconsejable configurarlas para que sea necesario introducir un **PIN o una contraseña para realizar pagos**,

para impedir que sean usadas por terceros sin consentimiento del dueño.

Finalmente, los comercios online están obligados a **guardar secreto profesional sobre los datos personales** de los usuarios, incluso después de finalizar la relación comercial. En consecuencia, no podrán hacerse públicos los datos personales de los visitantes y clientes sin su consentimiento expreso, y la vulneración de esta obligación puede **denunciarse ante la Agencia Española de Protección de Datos**.

Compraventas de segunda mano

Cada vez son más frecuentes los servicios online de compraventa de productos de segunda mano, que actúan como **intermediarios entre el comprador y el vendedor**, mediante anuncios en la web. Sin embargo, hay que tener ciertas precauciones para evitar fraudes:

- El **comprador** debe buscar información sobre el vendedor, especialmente comentarios o valoraciones de otros usuarios; descartar anuncios que sólo contengan fotos genéricas o descripciones que no coincidan con el producto, o que parezcan traducciones automáticas; y no aceptar nunca métodos de pago como Western Union o Money Gram.
- El **vendedor** también puede informarse sobre el comprador antes de realizar el envío; exigir un medio de pago seguro y no adelantar dinero, ni aceptar compensaciones del precio mediante Western Union o Money Gram; y sospechar si se ofrece más dinero del que se indica en el anuncio.

En caso de **duda o falta de garantías**, se recomienda cancelar el proceso.

Medios de pago

Una de las **mayores preocupaciones de los usuarios** al realizar compras online se refiere a los medios de pago, por lo que hay que conocer las ventajas e inconvenientes que presentan.

- **Pago en efectivo**: no es un medio seguro para realizar compras online, pues no queda constancia de quién envía y recibe el dinero, por lo que dificulta mucho poder reclamar en caso de problemas o fraudes.
- **Pago contra reembolso**: supone el pago en efectivo cuando se recibe el producto y se comprueba que es correcto, por lo que es más seguro para el comprador, pero muchas tiendas online no lo admiten, pues no asumen el riesgo de enviar un producto que no se ha pagado o que el comprador no se encuentre en su domicilio.
- **Transferencia bancaria**: se envía el dinero desde una cuenta bancaria a otra, por lo que no es necesario dar datos bancarios a la tienda online, pero tampoco lo admiten muchas.
- **Pago con tarjeta de débito o crédito**: es la modalidad más utilizada, y sólo se facilitan estos datos. Debe comprobarse que la operación se realiza a través de una pasarela de pago seguro, y en caso de uso fraudulento o

indebido, su titular puede exigir la anulación del cargo. También es recomendable usar tarjetas específicas para realizar pagos online. No se pueden exigir al consumidor gastos o cuotas adicionales por su uso.

- ***PayPal***: es una forma segura y sencilla de realizar pagos en Internet y enviar o recibir dinero a familiares o conocidos, que utilizan unos **200 millones de personas** en todo el mundo y se acepta en **202 países**. Funciona a través de una cuenta creada con el correo electrónico y una contraseña, vinculada de forma segura a una cuenta bancaria o tarjeta de crédito, por lo que no hay que introducir estos datos cuando se realice un pago. Además, este sistema supone una **garantía para el usuario**, pues si el comprador no recibe el producto o no coincide con la descripción del vendedor, se devuelve íntegramente el importe de la compra, e incluso el de compras no autorizadas, previa la oportuna reclamación.

Finalmente, la mayoría de tiendas online permiten **almacenar la información de la forma de pago** utilizada para futuras compras, especialmente cuando se trata de tarjetas (tipo, número, fechas de caducidad y CVV), pero esto supone un riesgo en caso de que utilice la cuenta una **persona no autorizada o sea *hackeada***, por lo que el usuario debe valorar si prefiere eliminar esos datos.

Pagos con móvil

Pagar con el móvil se está convirtiendo en algo cada vez más habitual, a través de la **conectividad NFC** y aplicaciones como Apple Pay, Android Pay, Google Pay, Samsung Pay, Bizum, Twyp, Wallet, etc.

Derecho de desistimiento

En las compras online el consumidor dispone de un **plazo de 14 días naturales desde la recepción del producto, o desde la fecha de celebración si se trata de servicios,** para poder desistir del contrato celebrado, notificándolo a la otra parte **sin necesidad de alegar ninguna causa y de forma gratuita**. Pero **si no se informa al usuario de este derecho**, ni se le entrega el **documento de desistimiento**, el plazo se **amplía a 12 meses**.

Una vez ejercido este derecho, el comercio online debe **devolver todas las cantidades pagadas por el consumidor**, sin demoras indebidas y antes de 14 días naturales desde que el consumidor comunicase el ejercicio del derecho de desistimiento.

Se **excluyen** de este derecho de desistimiento:

- Billetes de avión y tren, reservas de hotel, entradas de conciertos, o alquiler de vehículos.
- Alimentos y bebidas servidos a domicilio.
- Productos fabricados a medida o personalizados.
- Soportes de datos de audio, vídeo o programas informáticos desprecintados.
- Contenidos digitales online, si ya se ha iniciado la descarga o la emisión en tiempo real.
- Contratos de reparación o mantenimiento urgentes, una vez acordado el precio.

- Productos comprados a particulares.

Garantía de bienes de consumo.

Aparte del derecho de desistimiento, en el que no hay que alegar ningún motivo, a los productos comprados online también se les aplica la **garantía de los bienes de consumo**. La garantía en la compra de **productos nuevos es de dos años**, pero durante los **primeros seis meses** se presume que existe defecto de fabricación o falta de conformidad del producto, salvo prueba en contrario. Además, puede existir una **garantía comercial** que supere aquél plazo. Los **productos de segunda mano tienen un plazo de garantía de un año**, salvo pacto entre las partes.

En todo caso, el consumidor puede optar entre la **reparación o sustitución gratuita del producto** o, de no ser estas posibles, una **rebaja del precio** o la **resolución del contrato con devolución del importe** pagado, salvo que sean imposibles o desproporcionadas.

Confianza online

Para garantizar la confianza del consumidor en las empresas dedicadas al comercio electrónico, la Administración pública ha creado un distintivo que sólo pueden exhibir **las empresas adheridas a un código de conducta**, destinado a mejorar los derechos legalmente reconocidos al consumidor. Además, ostentar este distintivo supone que la empresa está adherida al **Sistema Arbitral de Consumo**, una vía de resolución extrajudicial de conflictos que pone al servicio del consumidor una vía rápida, sencilla gratuita y eficaz para resolver las reclamaciones que pueda plantear.

Reclamaciones

Los **órganos administrativos competentes en consumo** estatales, autonómicos o locales, pueden tramitar las reclamaciones cuando se produzcan incumplimientos de protección de los consumidores y usuarios en estos ámbitos territoriales. Si la reclamación versa contra empresas que tengan su sede en otros **Estados miembros de la Unión Europea, Noruega e Islandia**, se pueden tramitar a través del **Centro Europeo del Consumidor**. También se puede acudir a las **Asociaciones de Consumidores y Usuarios**.

Si se trata de reclamaciones sobre protección de datos personales, es competente la **Agencia Española de Protección de Datos (AEPD)** y se pueden presentar a través de su **sede electrónica**.

Delitos informáticos

Los **fraudes cometidos a través de Internet** son los delitos informáticos más frecuentes, el 75%, seguidos por las **amenazas y coacciones en redes sociales**, con el 14% y los **delitos de tipo sexual y contra el honor**, con el 1,6%, Y durante el año **2017 las denuncias aumentaron un 22%**.

El principal problema es que no **se conocen los límites en Internet**, no se sabe hasta dónde pueden llegar los usuarios y se asimilan como normales comportamientos que, en realidad, son delictivos, como el acoso, y además existe una **sensación de falsa impunidad o anonimato en la red**.

En la actualidad, los fraudes en Internet más habituales son el ***phising*** (se suplantan páginas web de bancos, empresas e incluso Administraciones para engañar a las víctimas y que faciliten sus datos o contraseñas, que se utilizan para cometer la estafa), el ***carding*** (realizar cargos fraudulentos contra una tarjeta de crédito hasta que el titular la anule) y el ***pharming*** (se suplanta el nombre de dominio - o DNS - de una web legal para reconducir al usuario a otra falsa).

Además, están tipificados en el **Código Penal** otros delitos como estafas a través de correo electrónico, publicidad engañosa en Internet, delitos contra la propiedad industrial e intelectual, interceptación de comunicaciones electrónicas, revelación de secretos, uso no autorizado de terminales y falsedades documentales

Retos o consejos peligrosos

Un fenómeno muy extendido en Internet, y que puede resultar muy peligroso, son los denominados ***challenges***, que pueden traducirse por desafíos o retos. Los jóvenes son muy propensos a aceptar estos desafíos, ya que se asocian a valentía, popularidad y superación de las reglas establecidas. Tanto retos como consejos peligrosos tienen gran repercusión a través de las redes sociales, por **famosos**, ***youtubers*** e ***influencers***, por lo que un reto puede dar la vuelta al mundo en pocos días, y las recomendaciones poco rigurosas de algunos ***influencers*** pueden impulsar a los adolescentes a realizar diferentes prácticas de riesgo para la salud. También se corre el peligro de contactar con personas desconocidas y revelarles información personal. Las **Fuerzas y Cuerpos de Seguridad del Estado** y la **Dirección General de Tráfico** alertan a menudo sobre estos peligros. Por eso, los **padres o adultos deben conocer estas prácticas** para poder prevenirlos y minimizar su impacto perjudicial, que puede llegar a ser mortal, **desarrollando la capacidad crítica de los menores e informando** de contenidos peligrosos en la web .

Criptomonedas

Desde 2009 en Internet han aparecido las **criptomonedas**, de las cuales la más conocida es el ***bitcoin***, aunque todavía no son de uso generalizado. Son **virtuales**, algoritmos matemáticos sin soporte físico, que se caracterizan por ser **convertibles** - tienen un valor real, aunque aleatorio -, **descentralizadas**, porque no las emite ninguna autoridad ni banco central nacional, **encriptadas** - de ahí su nombre - y **anónimas**. Se usan a través de una **billetera o monedero virtual** donde se almacenan y transfieren. Su mayor problema para el usuario deriva precisamente de **carecer de respaldo, regulación ni supervisión oficiales y de ser muy volátiles**, por lo que hay que **tener mucho cuidado para evitar riesgos**, grandes pérdidas de valor e incluso fraudes y actos delictivos, y **no utilizarlas nunca sin información suficiente**.

PARA MÁS INFORMACIÓN:

Agencia Española de Protección de Datos (AEGPD): **https://www.aepd.es - Tlfs: 901.100.099 y 912.663.517.**

Oficina de Seguridad del Internauta (OSI): **https://www.osi.es/es**

Instituto Nacional de Ciberseguridad (INCIBE): **https://www.incibe.es - Tlfs: 912.127.626 y 987.877.189.**

Agencia Española de Consumo, Seguridad Alimentaria y Nutrición (AECOSAN): **https://www.aecosan.msssi.gob.es**

Centro Europeo del Consumidor: **https://www.cec-msssi.es - Tlf: 918.224.555.**

Grupo de Delitos Telemáticos de la Guardia Civil: **https://www.incibe.es**

Confianza online: **https://www.confianzaonline.es - Tlf: 913.091.347.**

SUBVENCIONADO:

GENERALITAT VALENCIANA
Conselleria d'Economia Sostenible, Sectors Productius, Comerç i Treball

G.V. Germanías 31, entlo. 1º B, 46006, Valencia

Telf.963514177

unae.info@gmail.com

UNAE