INSTITUTO NACIONAL DE CIBERSEGURIDAD

# GESTIÓN DE LA PRIVACIDAD, IDENTIDAD DIGITAL Y REPUTACIÓN ONLINE EN INTERNET

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

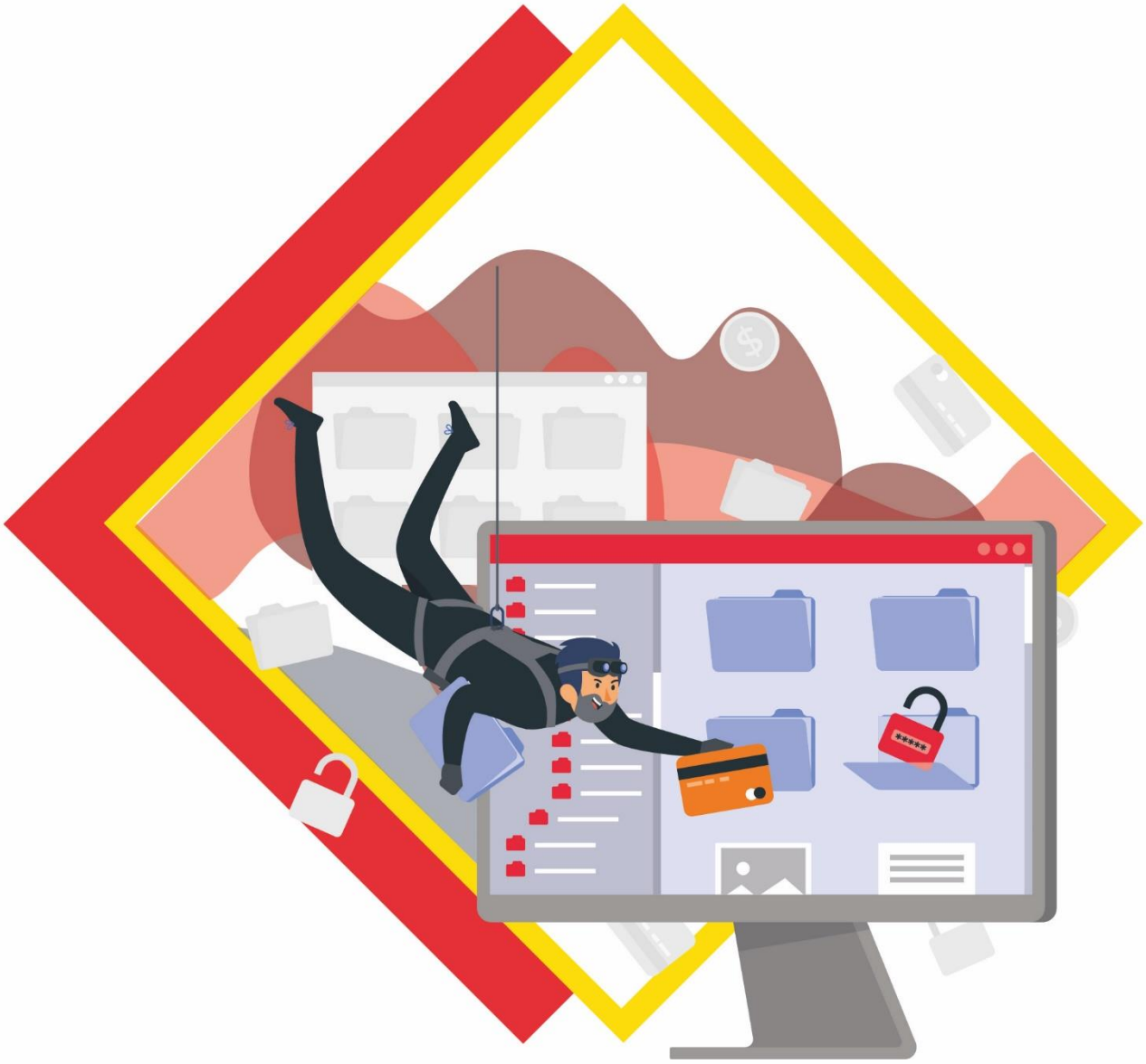
INSTITUTO NACIONAL DE CIBERSEGURIDAD

017

GOBIERNO DE ESPAÑA
MINISTERIO PARA LA TRANSFORMACIÓN DIGITAL Y DE LA FUNCIÓN PÚBLICA
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL
incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD
017

# MÓDULO 5

## Estafas económicas, robo de información personal y publicidad no deseada



# ÍNDICE

# 1. *Phishing*, *Smishing*, *Vishing* y estafas económicas

Sin duda alguna, el siglo XXI es el periodo de la historia de la humanidad en el que mayores cambios se han producido en lo que respecta a los procesos de comunicación entre nosotros y con nuestro entorno.

## SABÍAS QUÉ

España es uno de los países de la Unión Europea que más ha crecido en conexiones a Internet de uso no profesional (hogares), alcanzando un 95% de cobertura en viviendas en 2020?

Datos extraídos de: Ver enlace

Además, la llegada del COVID-19 ha reducido, en cierta forma, nuestro miedo al uso de Internet en operaciones que anteriormente se realizaban, exclusivamente, de forma presencial. En definitiva, el consumo digital se ha incrementado exponencialmente, dando paso a la normalización de aspectos como el teletrabajo; se han mejorado los procesos *online*, y se ha incrementado la fiabilidad de las aplicaciones. Todo ello se ha traducido en que los avances tecnológicos han agilizado nuestras vidas y somos más prácticos, precisos y eficientes, pero, por otro lado, más vulnerables.

Igualmente, los ciberdelincuentes se han adaptado a los tiempos, utilizan medios tecnológicos para acceder a nuestro entorno digital, robar nuestros datos personales, suplantar nuestra identidad o infectar nuestros dispositivos. Durante 2021, el servicio Tu Ayuda en Ciberseguridad de INCIBE gestionó más de 69.000 consultas, siendo las más frecuentes las relacionadas con fraudes *online* de tipo *phishing*, suplantación de identidad y falso servicio técnico.

Los ataques producidos en entornos digitales son conocidos como **ciberataques**. Existen muchos tipos, pero nos vamos a centrar en aquellos más frecuentes, conocidos como **ataques de ingeniería social**, que son aquellos en los que los ciberdelincuentes usan técnicas para ganarse nuestra confianza y que hagamos algo o le facilitemos algún tipo de información bajo su manipulación y engaño, como, por ejemplo, instalar un *software* malicioso, facilitar nuestras contraseñas o hacer compras en sitios web fraudulentos.

Los tipos de ataques por ingeniería social más comunes son el ***phishing***, ***smishing*** y ***vishing***:

- ***PHISHING***: Se produce a través del correo electrónico. Los ciberdelincuentes envían un correo electrónico a sus víctimas haciéndose pasar por una fuente fiable para ellos, como su banco, una red social, una empresa reconocida, etc.

  El correo electrónico generalmente contiene algún archivo adjunto o enlace a páginas web fraudulentas, con el objetivo de obtener información personal o bancaria de la víctima, realizar algún cargo económico o infectar el dispositivo.

  Para identificar si un correo electrónico constituye un ***phishing*** debemos seguir los siguientes pasos:

  - **Remitente**: el dominio del *e-mail* debe coincidir con el de la supuesta entidad.
  - **Asunto**: si es demasiado llamativo e intenta captar nuestra atención, debemos mantenernos alerta.
  - **Objetivo**: si nos piden realizar una acción con premura a través de una excusa con carácter urgente, promociones u ofertas, puede tratarse de un fraude.
  - **Redacción**: otro factor es si tiene fallos ortográficos o parece una mala traducción de otro idioma.
  - **Enlaces**: siempre debemos revisar los enlaces previamente antes de acceder, para comprobar que nos redirigirán a la web original.
  - **Adjuntos**: antes de descargar un adjunto debemos analizarlo con un antivirus o analizador de ficheros, ya que puede contener *malware*.

- ***SMISHING***: se distribuye a través de SMS. Al igual que en el *phishing*, los ciberdelincuentes suplantan la identidad de empresas de confianza para engañarnos con algún pretexto, para que facilitemos nuestra información personal o bancaria a través de un enlace que incluirán en el mensaje.

  Recomendaciones para evitar el ***smishing*:**

  - Desconfiar de remitentes y números de teléfonos desconocidos.
  - No fiarse de mensajes de entidades que no se hayan solicitado.
  - No hacer clic en enlaces sospechosos.

- ***VISHING***: este método de ataque se realiza mediante llamadas telefónicas. El ciberdelincuente simulará tratarse de un empleado de una empresa, organización o incluso de una persona de confianza para nosotros, con el objetivo de obtener información personal o incluso infectar nuestros dispositivos.

  El caso más frecuente de *vishing* es aquel en el que el ciberdelincuente se hace pasar por el soporte técnico de una compañía informática para comunicarnos que nuestro dispositivo móvil o portátil ha sido infectado, por lo que necesitan acceder en remoto. Para ello, debemos instalar una aplicación bajo sus instrucciones para así, supuestamente, solucionar el problema. Instalando esta aplicación lo que realmente haremos será infectar nuestro dispositivo, facilitándole el control al ciberdelincuente.

  En la actualidad, también es muy frecuente que los ciberdelincuentes se hagan pasar por agentes de una entidad bancaria que quieren ayudarnos a resolver algún problema que se ha detectado en relación a nuestras cuentas bancarias, tarjetas, aplicación móvil, etc.

  Recomendaciones para evitar el ***vishing*:**

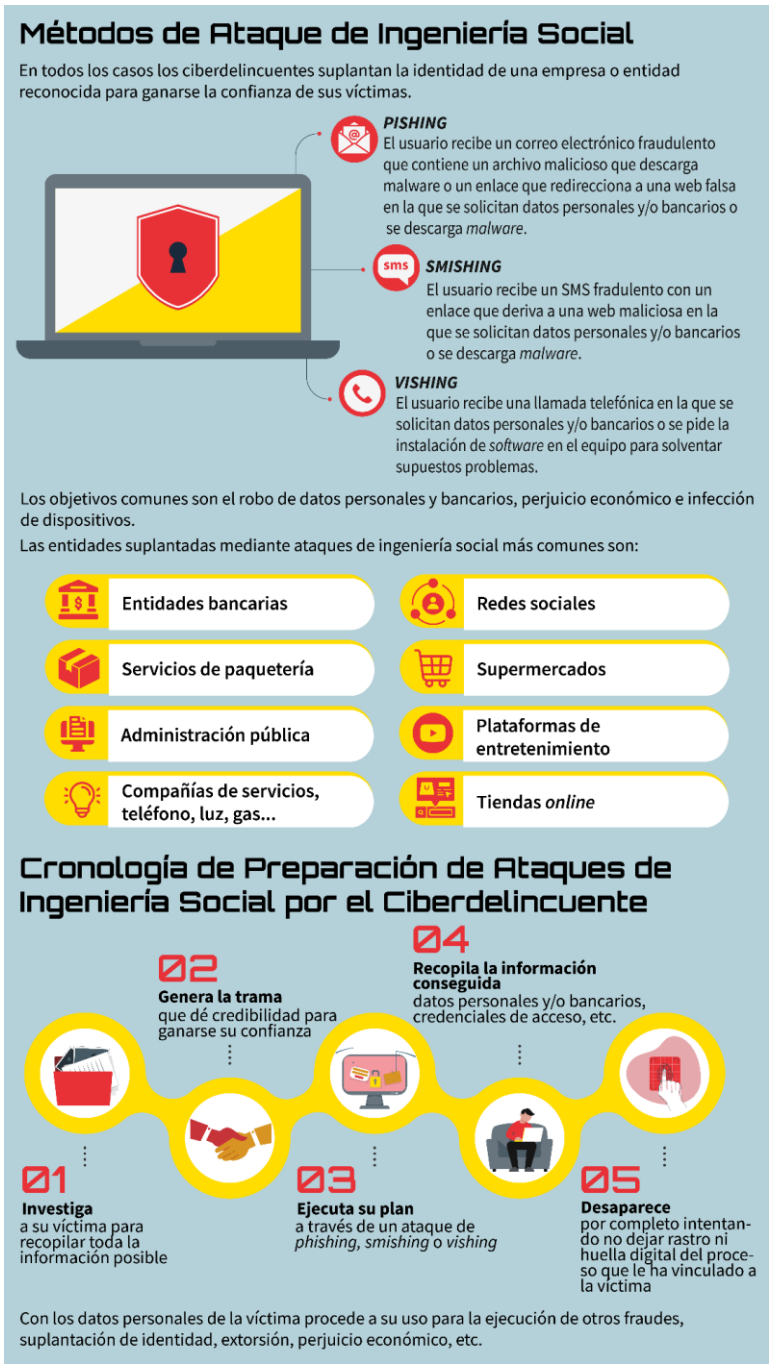
  - No proporcionar información personal por teléfono. Si nos contacta nuestro proveedor, ya debe tener todos nuestros datos identificativos.
  - Realizar comprobaciones con la persona que nos está llamando.
  - Sospechar de las llamadas con números desconocidos o con numeración fuera de lo común.
  - Atentos ante llamadas que no esperábamos.
  - En caso de duda, colgar la llamada y ponernos nosotros en contacto directamente a través de los canales oficiales de la entidad.

Además, de forma general debemos tener siempre en cuenta:

- Las sucursales bancarias nunca piden confirmar datos confidenciales por Internet ni a través de enlaces.
- Utilizar un buen antivirus que mejore la seguridad de los dispositivos.
- Mantener el sistema operativo, *software* y aplicaciones siempre actualizados.
- Evita abrir correos electrónicos de fuentes desconocidas.
- Nunca contestar o reenviar correos electrónicos o mensajes sospechosos.

- Escribir directamente la URL en el navegador, en vez de acceder mediante un enlace.
- Nunca facilitar datos personales y bancarios en cualquier web.
- No utilizar redes wifi públicas para acceder a servicios *online* en los que se intercambie información privada o se realicen trámites bancarios.

A continuación, explicamos de forma visual estos tres ataques de ingeniería social:



## 2. Medidas para combatir la publicidad no deseada

La publicidad en Internet es todo aquel proceso que utiliza plataformas *online* para la comercialización de bienes y servicios. Los métodos por los que nos puede llegar o aparecer publicidad maliciosa en Internet son varios:

**1**

La tendencia más extendida se basa en la emisión de correos electrónicos, por ejemplo, de una tienda *online* ofreciéndonos sus servicios, una promoción o descuentos.

Por otro lado, también existen correos publicitarios que esconden enlaces a sitios web maliciosos o a la descarga de algún programa infectado con algún tipo de virus o *malware*.

**2**

Se diseña un vídeo o imagen sobre productos y servicios y se posiciona en webs, foros o blogs de interés.

Aunque las webs filtran y eliminan los enlaces a sitios web maliciosos, algunos *banners* pueden "colarse", por ejemplo, si tenemos nuestro navegador desactualizado.

**3**

**POP-UPS (VENTANAS EMERGENTES)**

Publicidad que se presenta mediante ventanas emergentes cuando entramos en un sitio web. Además de ser molestos, suelen ser utilizados por los ciberdelincuentes para redirigirnos a páginas web falsas, que suplantan la identidad de webs o servicios legítimos.

También pueden ser utilizadas por los ciberdelincuentes para redireccionar a webs maliciosas.

**4**

**NOTIFICACIONES**

Similares a los *pop-ups*, pero dentro del propio navegador. Suelen incluir mensajes relacionados con permisos solicitados por la página web o cambios en las políticas de *cookies* y permiten informar a los usuarios sobre actualizaciones o novedades en las webs.

Las empresas crean perfiles con los que publicar este tipo de anuncios publicitarios, aunque también son los propios usuarios los que reenvían y comparten sus publicaciones para así llegar a más gente.

El principal peligro reside en aquellos anuncios fraudulentos que terminan por viralizarse. Muchos usuarios no son conscientes de que están haciendo clic o compartiendo una publicación maliciosa hasta que es demasiado tarde.

## 5 PUBLICACIONES EN REDES SOCIALES

Según lo recogido en la memoria anual de la Agencia de Protección de Datos correspondiente al año 2022, de las más de 15.000 reclamaciones recibidas por la Agencia, el 13% corresponde a publicidad no deseada y suponen el 2º lugar en cuanto a la cuantía de las sanciones impuestas.

Dentro de la publicidad no deseada debemos hacer mención a la **publicidad maliciosa** (*malvertising*), técnica para intentar, principalmente, infectar nuestros dispositivos o hacernos caer en otro tipo de fraudes, como el robo de datos personales y bancarios, a través de la manipulación de la publicidad *online*, **escondiendo *malware* que nos infectará en caso de acceder a la publicidad sin ser conscientes de ello o redirigiendo a webs fraudulentas**. La publicidad maliciosa se puede presentar en espacios web seguros, por lo que debemos mantenernos siempre en alerta.

Algunos ejemplos de técnicas utilizadas por los ciberdelincuentes son:

- **Anuncios fraudulentos.** Aunque se pueden encontrar en webs legítimas, es común encontrarlos en webs de dudosa fiabilidad. Suelen ser llamativos, ocupar un gran porcentaje de la pantalla y esconder el botón de cierre. Nos redirigirán a webs fraudulentas.
- **Sorteos y concursos falsos y maliciosos.** Aparecen en publicaciones de redes sociales o *pop-ups* en páginas web. Suelen hacernos creer que hemos sido ganadores de un sorteo, concurso o promoción como excusa para redirigirnos a una web fraudulenta.

- ***Pop-ups* que dificultan la navegación y redirigen a webs fraudulentas.** Comunes en webs de descargas ilegales, al utilizar un navegador desactualizado o en dispositivos infectados por *adware*. Son comunes los mensajes en los que se indica que el ordenador está infectado y que necesitamos instalar una actualización nueva del antivirus, aunque también pueden ofrecernos ofertas o descuentos para que hagamos clic sobre ellos. Con esta acción descargaremos *malware* o accederemos a una web fraudulenta.
- **Notificaciones maliciosas que aparecen en el navegador.** Nos comunican que debemos realizar una actualización de la web o navegador o solicitan permisos al sitio web. Suelen abusar de estos permisos para suscribirnos a sitios de publicidad no deseada o descargar *malware*.

Como usuarios de Internet podemos realizar ciertas **prácticas y configuraciones** para combatir la publicidad no deseada y minimizar el riesgo:

a) ***Configuración del navegador:*** para evitar la visualización de anuncio malicioso podemos deshabilitar las notificaciones y ventanas emergentes o *pop-ups* y redirecciones a otras webs.

1. Cómo configurarlo en el navegador Chrome.
2. Cómo configurarlo en el navegador Firefox.

b) ***Bloqueadores de anuncios mediante instalación de extensiones:*** otra opción sencilla es la de utilizar extensiones o *plugins* de navegador con la funcionalidad de bloqueadores de anuncios. Así, eliminaremos la gran mayoría de los anuncios que nos encontramos al navegar sin que tengamos que hacer nada extra.

***Enlace: Consultar bloqueadores de publicidad***

c) ***Configuración de filtros antispam:*** podemos configurar nuestro servicio de correo electrónico con el fin de no recibir mensajes que cumplan con ciertas pautas que indiquemos. Por ejemplo, podemos bloquear por dominio, palabra o grupos de palabras y remitente del correo; si adjunta archivos excesivamente grandes; si el usuario no se encuentra dentro de la lista de remitentes seguros, etc. Así, conseguiremos minimizar la recepción de correo no deseado, ordenar de manera eficiente el buzón de entrada y reducir el riesgo de apertura de correos electrónicos maliciosos.

d) ***Configuración en redes sociales:*** si vemos publicidad no deseada en alguna de nuestras redes sociales, haciendo clic directamente en el menú de opciones del anuncio podremos ocultarlo o denunciarlo. En el primer caso, debemos elegir entre varias opciones añadidas para personalizar la visualización, o no, de ese tipo de anuncios; en el segundo caso, lo que hacemos al denunciar es indicar que probablemente sea publicidad no deseada.

Si no queremos hacer esta configuración anuncio por anuncio, tenemos opciones dentro de la configuración para limitar la cantidad de anuncios que podemos ver al navegar por la red social. Ejemplo en Facebook.

Además, para minimizar el riesgo debemos tener en cuenta:

1. **NO DAR CONSENTIMIENTO A TODO**: debemos ser cautos a la hora de aceptar las *check boxes* (casillas de selección) de consentimiento que aparecen en las webs. Es muy importante leer las condiciones generales de uso para verificar que la finalidad del uso de nuestros datos es realmente la perseguida.

2. **EJERCE DERECHOS**: los usuarios somos propietarios de nuestros datos personales, tenemos la opción de ejercer los derechos recogidos en el Reglamento General de Protección de Datos Europeo (RGPD) y en la Ley española, tal como estudiamos en el Módulo 1 de este curso. Además, encontraremos información sobre ellos en la web de la Agencia Española de Protección de Datos. Por ejemplo, el derecho de oposición permite evitar que se usen los datos de alguien de forma ilícita o, por ejemplo, para la creación de perfiles de consumidor para el envío de publicidad. El derecho al olvido permite el borrado y, por tanto, no uso, de los datos personales, siempre y cuando se den las condiciones fijadas en el Reglamento y la Ley. El ejercicio de los derechos siempre será gratuito y se debe tener en cuenta que existen plazos legales de conservación de los mismos. Pasado el tiempo legal, las entidades tendrán que borrar nuestros datos personales de sus servidores.

3. **DESVINCULAR DATOS:** en muchas ocasiones son las propias entidades las que ofrecen sistemas sencillos para desvincular nuestro correo electrónico o teléfono de la recepción de publicidad. Por ejemplo, enviando un *e-mail* a una dirección indicada, mandando un SMS, pinchando en una URL o llamando a un teléfono gratuito.

4. **INSCRIBIRSE EN LA LISTA ROBINSON:** dentro de la normativa citada existe la figura de los **sistemas de exclusión publicitaria**. En España disponemos de la **Lista Robinson,** que es gestionada por la Asociación Española de Economía Digital (**ADIGITAL**). Si una empresa va a realizar una campaña publicitaria, previamente debe consultar la Lista Robinson para eliminar de la comunicación a aquellos usuarios inscritos en el canal que utilizará. Así, podremos restringir la publicidad no deseada inscribiéndonos de forma gratuita y voluntaria.

   Al inscribirnos, podremos elegir el medio o canal de comunicación a través del cual no deseamos recibir publicidad (correo postal, llamadas telefónicas, correo electrónico, etc.). El registro se hace eficaz a partir del segundo mes, por lo que es posible seguir recibiendo publicidad en el plazo del trámite.

5. **USAR LOS SISTEMAS DE MEDIACIÓN:** si seguimos recibiendo publicidad no deseada, podemos solicitar una mediación:

   - Utilizando el canal de mediación ofrecido por la **Asociación para la Autorregulación de la Comunicación Comercial**, también conocida como AUTOCONTROL, en lo que respecta a las comunicaciones comerciales de los principales operadores de telefonía adheridos.

     El objetivo de este sistema es interponer una reclamación rellenando un formulario que aparece en la dirección indicada. Se abrirá entonces un proceso de mediación durante un plazo máximo de 30 días y, a continuación, se emite un acuerdo de mediación para ambas partes.

6. **USAR LOS SISTEMAS DE RECLAMACIÓN**: si aun habiendo seguido los pasos anteriores seguimos recibiendo publicidad no deseada, podemos presentar una reclamación:

   - Reclamar mediante la sede electrónica de la Agencia de Española de Protección de Datos (AEPD), en caso de haber ejercido los derechos de oposición y/o supresión y/o bien no haber sido atendidos o no resueltos satisfactoriamente. Desde la sede electrónica de la AEPD se puede iniciar el proceso de reclamación pertinente.

# 3. Tiendas *online* fraudulentas

La llegada de Internet ha traído cambios sustanciales a nuestros estilos de vida, pero, si debemos resaltar uno de ellos, es el relacionado con el comercio electrónico, ya que nos ha dado la oportunidad de gestionar nuestras compras de forma cómoda, con precios más competitivos, con mayor disponibilidad de producto y mayor información sobre los mismos. Desde el punto de vista empresarial, se ha garantizado la supervivencia de muchas entidades que han visto en el negocio *online* una nueva ventana para la sostenibilidad de sus ingresos y equilibrios económicos.

Ahora tenemos acceso a comprar por Internet bienes que hace unos años nos hubiese resultado imposible. Sin duda, el comercio electrónico ha venido para quedarse, ya que es algo que favorece tanto a compradores como a vendedores, que ven aumentar su rango de clientes de forma nacional o incluso mundial.

Según el Informe "Compras online en España" de 2023 (con datos del año 2022) el volumen total del comercio electrónico superó los 85.000 millones de euros. El 83,1% de las personas usuarias de Internet ha hecho alguna compra online en 2022, lo que se traduce en 27,9 millones de compradores, casi cuatro puntos porcentuales más que el año 2021. Entre ellos, el 7,4% eran nuevos compradores.

*Fuente de los datos: Ver enlace

La pandemia producida por el COVID-19 en el año 2020 ayudó a que las ventas *online* se afianzaran, aumentando el porcentaje de personas que dan al salto a las compras por Internet.

Las compras en tiendas físicas se encuentran debidamente reglamentadas en lo que respecta a la información que se le debe proporcionar al cliente sobre un bien o servicio, los plazos de devolución, el etiquetado, las formas de pago, las quejas y reclamaciones, etc. En la tienda *online* suelen surgirnos dudas sobre estas cuestiones: ¿quién está detrás de ella?, ¿cómo se devuelve un producto?, ¿de qué plazos se disponen?, etc.

Las tiendas *online* y sus transacciones están igualmente reguladas y existen unas garantías, no solo las referidas al bien o servicio contratado, sino también todo lo relacionado con el proceso y la confidencialidad y seguridad de nuestros datos, es decir, al no realizarse físicamente, el proceso de compra requiere de una serie de garantías de seguridad, transparencia e integridad adicionales al modelo tradicional.

En los procesos de compra *online* debemos tener especial cautela a la hora de saber detectar aquellas plataformas y tiendas electrónicas fraudulentas. Se deben revisar

los avisos legales y políticas de privacidad para saber quién está detrás de las mismas; verificar las conexiones seguras mediante HTTPS y si disponen de certificados de confianza, precios estables y equiparables al precio real de mercado; no dejarse llevar por ofertas vertiginosas; evitar enlaces que llevan a descargas de *software* o donde los procesos de pago se realizan en otros apartados que no son pasarelas de pago bancarias (tipo PayPal), etc. Si caemos en una tienda fraudulenta podremos ser víctimas de robo de datos personales y perjuicio económico.

A continuación, te explicamos qué pasos debes dar para comprobar si estás ante una posible tienda fraudulenta o por el contrario es legítima:

1. **CERTIFICADOS DE SEGURIDAD Y CONEXIÓN SEGURA:**

Es muy importante que verifiquemos estos dos campos antes de llevar a cabo cualquier compra *online*. Esta necesidad es indispensable cuando vamos a facilitar datos de carácter personal y bancarios.

- Verifica que la web tiene en su URL el protocolo de cifrado HTTPS. Esto nos va a garantizar que el flujo de datos e información es cifrado protegiendo la confidencialidad y la integridad del proceso.
- Verifica que la zona de compra *online* dispone de un candado de color verde. Si clicamos sobre él, podemos verificar la titularidad del mismo, el tipo de certificado de seguridad, si la conexión es segura, etc.
- NOTA: algunas tiendas *online* fraudulentas cumplen con estos requisitos, por lo que no son decisivos y se debe analizar también el resto de factores.

2. **VERIFICACIÓN DEL DOMINIO Y COINCIDENCIA DE LA URL:**

Hoy en día disponemos de herramientas que nos permiten verificar la autenticidad e identidad de un dominio. Para ello, podemos utilizar servicios web, como, por ejemplo:

Ver enlace dominio  Ver enlace who.is

Si insertamos en las webs indicadas la dirección URL de la plataforma de comercio electrónico, nos arrojará un pequeño informe en el que se nos indica la titularidad de la misma, fecha de alta y caducidad, etc. Si la entidad es de prestigio y está consolidada en el mercado, probablemente lleve varios años de alta. Desconfía de las plataformas que tienen poco recorrido, ya que los ciberestafadores dan altas y bajas constantemente para no ser pillados.

Además, debemos verificar que la URL coincide con el nombre de la empresa o entidad que supuestamente es y no se ha modificado ligeramente a través de alguna letra y/o carácter.

### 3. POLÍTICAS Y LOS TEXTOS LEGALES:

Todas las plataformas de comercio electrónico deben facilitar la política de privacidad y protección de datos, condiciones generales de uso, aviso legal, política de devoluciones, etc. Si no incluyen esta información, lo más probable es que sea una tienda *online* fraudulenta.

Cabe recordar que en las transacciones electrónicas deben cumplirse una serie de normas legales que atienden a la ordenación del comercio minorista, los servicios de la sociedad de la información, protección de datos personales y garantía de los derechos digitales o garantías a los consumidores y al propio comercio electrónico, entre otras relacionadas con temas fiscales y tributarios.

Es interesante detenerse y leer los siguientes campos dentro de la plataforma de comercio electrónico:

- **AVISO LEGAL**: deben aparecer perfectamente identificados los datos de la entidad que está detrás de la operación de compra/venta *online* de bienes y servicios; esto es, razón social (o autónomo), CIF/NIF, dirección a efecto de notificación, teléfono, dirección de correo, etc. En este espacio se suele hacer referencia a la propiedad industrial e intelectual de los contenidos de la propia web.
- **POLÍTICA DE PROTECCIÓN DE DATOS (PRIVACIDAD):** en este espacio se define con claridad y transparencia la finalidad para la que se recaban los datos, plazos de conservación, a quién dirigirse en caso de ejercer los derechos de acceso, rectificación, supresión, oposición y portabilidad, etc.
- **CONDICIONES GENERALES DE USO (COMPRA):** en este apartado suelen detallar todo lo referente al proceso de la compra, condiciones de devolución (desistimiento), plazos de entrega, factura, formas de pago, disponibilidad del bien o del servicio, etc. Al respecto de las formas de pago, verificar que se ofrecen varias alternativas, siempre realizadas por pasarelas de pago bancarias y nunca aceptar la modalidad de pago en efectivo.
- **POLÍTICA DE COOKIES:** verifica la existencia de un faldón inicial de *cookies* en el que se informa adecuadamente de aquellas que son necesarias estrictamente para garantizar la estabilidad de la compra y aquellas que requieren de un consentimiento específico para su uso (marketing y publicidad, por ejemplo).

### 4. CERTIFICADOS DE CONFIANZA *ONLINE*:

Son unos sellos emitidos por entidades de prestigio que garantizan códigos de conducta adecuados y métodos transparentes, responsables y seguros en el comercio electrónico.

### 5. OFERTAS:

Debemos desconfiar de las gangas y de los descuentos de vértigo. Es muy probable que sea para incitarnos a la compra inmediata. Verifica el bien o el servicio con otros proveedores, compara precios, características similares, etc.

### 6. ASPECTO DE LA WEB:

Aunque es cierto que en los últimos años los ciberdelincuentes han mejorado la apariencia de las plataformas de comercio electrónico, si nos fijamos bien, podemos observar errores en la tipografía, tamaño, falta de agilidad y usabilidad de la plataforma, programación defectuosa, etc.

Es importante comprobar la homogeneidad en el diseño, que todo sea coherente. La tipografía de letra debe coincidir en todo el proceso. Las imágenes pueden someterse a búsqueda en el navegador para comprobar que son de la tienda que dicen ser o bien verificar si es otra que ya esté en la Red. La calidad de la imagen también es muy importante.

Debemos comprobar la transparencia en el lenguaje, que sea entendible. Muchas veces, las webs fraudulentas provienen de traducciones automáticas de otros idiomas y no se entiende lo que dicen.

### 7. OPINIONES:

Es importante buscar en foros la opinión de otros clientes. Los navegadores permiten buscar de manera sencilla la experiencia de otros clientes con la tienda, y podrá ayudarnos a tomar una determinación sobre si comprar o localizar el producto en otra web.

Sin olvidar que no debemos dar una alta credibilidad a las opiniones que aparezcan en la propia web, ya que pueden ser introducidas por los propios ciberdelincuentes. Siempre es mejor rastrear por la Red los comentarios de otros usuarios.

### 8. MÉTODOS DE PAGOS:

Las tiendas fraudulentas no suelen disponer de varias formas de pago y aunque las ofrezcan en inicio con muchas posibilidades a elegir, al final solo será posible, de

forma general, pagar a través de MoneyGram, Western Union o transferencia bancaria. De ser así, lo mejor será no realizar la compra. Si nos ofrecen otros tipos de pago, como PayPal, Bizum, Google Pay, Apple Pay o tarjetas de crédito, debemos asegurarnos de que nos redirigen a una pasarela de pago segura, que disponga de HTTPS.

En la siguiente infografía se detallan los métodos de pago para comprar *online* de forma segura: