DigitalPreventor

Ciberestafas habituales: cómo identificarlas y protegerse

Antes de empezar: qué ofrece esta guía

Internet forma parte de casi todo lo que hacemos: compramos, trabajamos, hablamos con otras personas, gestionamos nuestras cuentas y compartimos información. Esa actividad también es aprovechada por ciberdelincuentes que buscan conseguir dinero, datos personales o acceso a nuestras cuentas.

En España, **la cibercriminalidad se ha convertido en una parte relevante de la delincuencia registrada,** y las estafas informáticas siguen siendo uno de los ciberdelitos más frecuentes. Esto no significa que debamos vivir con miedo, sino aprender a reconocer mejor las situaciones de riesgo.

Sus mensajes pueden parecer reales: un aviso del banco, una empresa de paquetería, una oferta de empleo, una inversión atractiva, una tienda online o **incluso una petición de alguien conocido.** Utilizan la urgencia, la confianza o el miedo para conseguir que actuemos sin comprobar**.**

Esta guía recoge las ciberestafas más habituales y explica cómo suelen funcionar, **qué señales deben hacernos desconfiar, cómo proteger nuestras cuentas, datos y dinero,** qué deben tener en cuenta las empresas y **qué pasos seguir si** creemos que **hemos sido víctimas de un fraude.**

El objetivo es ofrecer **una orientación clara y práctica** para saber cuándo detenerse, cómo comprobar la información y dónde pedir ayuda, reportar o denunciar cuando sea necesario.

ÍNDICE

1. Cómo consiguen engañarnos

Las ciberestafas suelen buscar dos cosas: **parecer creíbles y conseguir que actuemos rápido** antes de comprobar la información.

Para lograrlo, los delincuentes combinan herramientas digitales con técnicas de manipulación, como la urgencia, el miedo, la autoridad, la confianza o la promesa de una recompensa.

Urgencia o miedo
Mensajes como “tu cuenta será bloqueada”, “tu paquete no ha podido entregarse” o “debes verificar tus datos ahora” generan presión y provocar una respuesta inmediata.

Recompensa o necesidad
Premios inesperados, ofertas de empleo, productos muy baratos o inversiones con grandes beneficios.

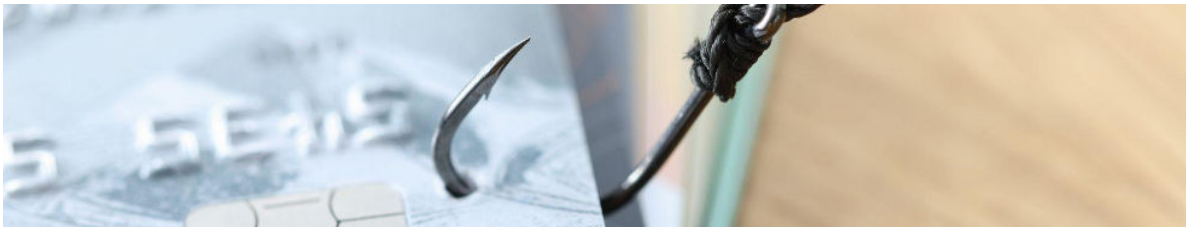
Confianza y autoridad
Logotipos conocidos, nombres de empresas reales, perfiles aparentemente verificados o páginas casi idénticas a las oficiales.

Distracción
La cantidad de mensajes, avisos y notificaciones que recibimos favorece que respondamos de forma automática, especialmente cuando estamos trabajando, con prisa o haciendo varias cosas a la vez.

La mejor defensa es **detenerse unos segundos y verificar por otro canal.**

2. Estafas digitales más habituales

Las ciberestafas cambian de apariencia con frecuencia, pero **muchas siguen un funcionamiento parecido:** alguien suplanta a una persona o entidad de confianza, presenta una situación urgente o atractiva y trata de conseguir que la víctima entregue dinero, datos o acceso a una cuenta. Vamos a ver qué tienen en común las más habituales.



Phishing, *smishing* y llamadas fraudulentas

El *phishing* consiste en el envío de correos electrónicos que aparentan proceder de un banco, una plataforma digital, una empresa de paquetería o una institución pública. Suelen incluir **enlaces a páginas que imitan a las originales o archivos que pueden instalar programas maliciosos.**

Cuando el engaño llega **mediante SMS o aplicaciones de mensajería se conoce como *smishing*.** Aquí son habituales los avisos sobre paquetes retenidos, pagos pendientes, devoluciones de impuestos o supuestos problemas con una cuenta bancaria.

También pueden utilizarse llamadas telefónicas. En estos casos el interlocutor se hace pasar por el banco, una compañía o un organismo oficial y solicita datos, códigos de seguridad o la instalación de una aplicación.

Aunque el canal sea diferente, el objetivo suele ser el mismo: conseguir contraseñas, datos bancarios, códigos de verificación o acceso al dispositivo.

Estafas en redes sociales, tiendas y ofertas laborales

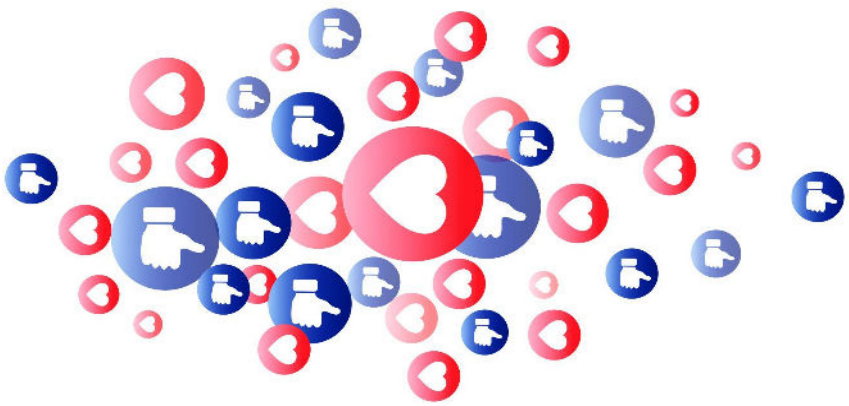
Las **redes sociales** permiten crear perfiles y anuncios con una apariencia muy profesional. Los delincuentes pueden utilizar imágenes robadas, seguidores falsos, opiniones inventadas y logotipos reales para promocionar productos, sorteos, colaboraciones u ofertas de trabajo inexistentes.

Las **tiendas fraudulentas** suelen atraer con precios excepcionalmente bajos o productos difíciles de encontrar. **Después de realizar el pago, el producto no llega,** es distinto al anunciado o la página desaparece.

En las **falsas ofertas laborales** se prometen ingresos rápidos, tareas sencillas o trabajos desde casa. El fraude aparece cuando **se solicitan documentos personales, datos bancarios, pagos por adelantado o transferencias** para poder comenzar.

La estafa de "los likes"

El Banco de España ha advertido sobre **la conocida como estafa de los "me gusta",** en la que **se ofrece dinero por realizar tareas sencillas en redes sociales,** como dar "likes", seguir perfiles o interactuar con publicaciones. Al principio pueden realizar pequeños pagos para generar confianza, pero después solicitan ingresos cada vez mayores con la promesa de obtener comisiones o beneficios.



Robo de cuentas y suplantación de identidad

Una cuenta robada puede utilizarse para engañar a familiares, amistades, clientes o compañeros de trabajo. Un mensaje como "he cambiado de número" o "necesito una transferencia urgente" puede parecer real porque procede de una cuenta conocida o incluye información personal.

Los delincuentes pueden obtener estos datos mediante filtraciones, contraseñas débiles, códigos de verificación compartidos o información publicada en redes sociales. **La Guardia Civil ha alertado,** por ejemplo, de fraudes en los que los datos personales de una víctima pueden utilizarse para registrarla en plataformas de apuestas o actuar en su nombre.

En las empresas, pueden hacerse pasar por un directivo, un trabajador, un proveedor o un cliente. En ocasiones, interceptan una conversación real para solicitar una transferencia, comunicar un supuesto cambio de cuenta bancaria, conseguir documentación confidencial o introducir un programa malicioso.

También se han conocido casos en los que se utilizan identidades profesionales, como la de abogados, para estafar a terceros.

Falsas inversiones y fraudes con criptomonedas

Estas estafas **prometen rentabilidades elevadas, beneficios rápidos o inversiones supuestamente seguras.** Pueden anunciarse mediante perfiles falsos, testimonios manipulados, artículos que imitan a medios de comunicación o imágenes de personas famosas.

La víctima ve en una plataforma que su inversión está aumentando, pero los datos son ficticios. **Cuando intenta recuperar el dinero, le exigen nuevos pagos, en concepto de falsos impuestos, multas o comisiones.**

El fraude puede continuar durante semanas o meses porque **los delincuentes mantienen el contacto,** muestran beneficios aparentes y presionan para que la víctima invierta cada vez más.

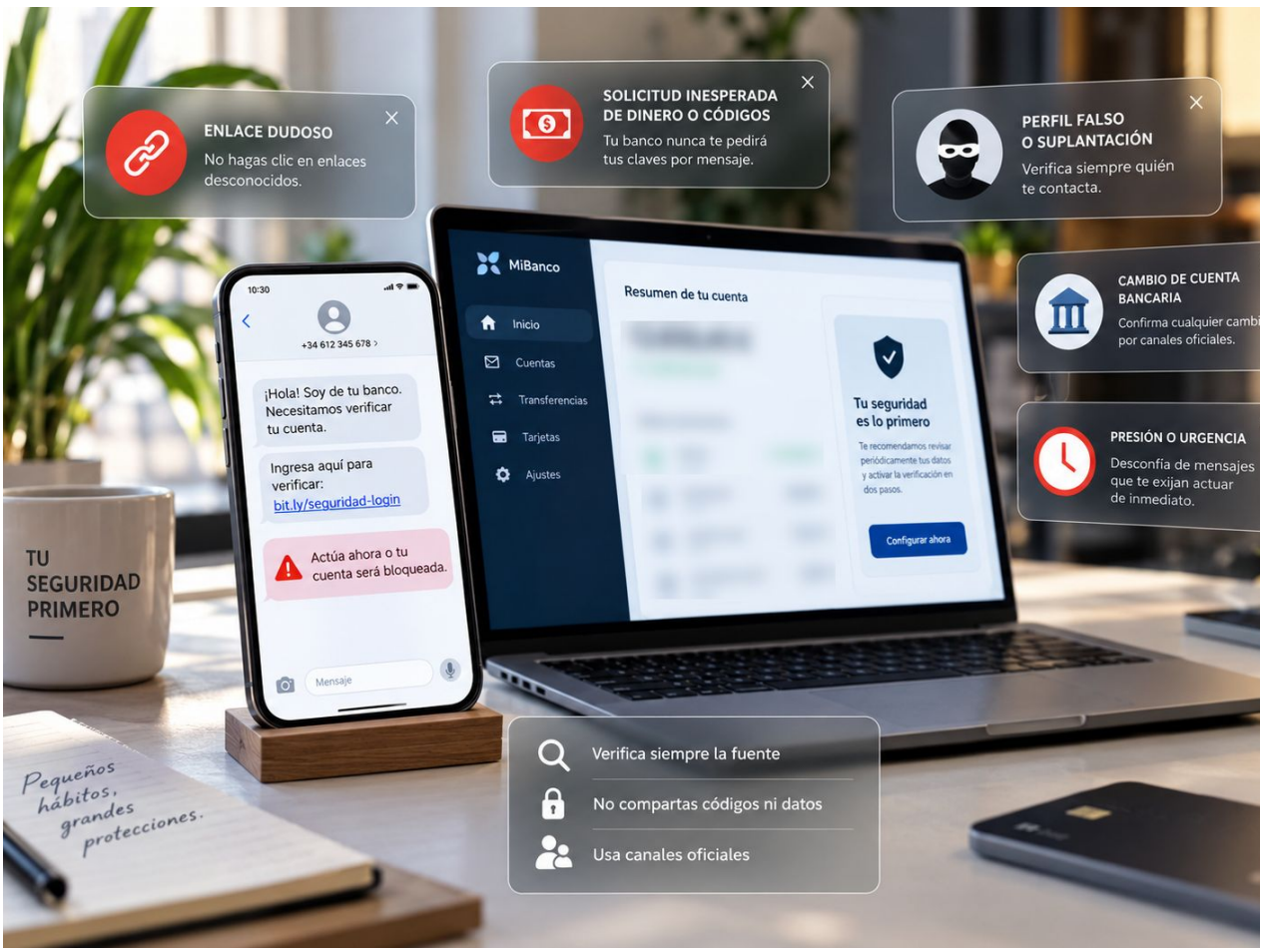
INCIBE ha advertido de fraudes relacionados con falsas plataformas de inversión, intermediarios inexistentes y páginas que imitan servicios legítimos vinculados a inversiones o criptomonedas. Antes de invertir, hay que desconfiar de promesas de beneficios rápidos, operaciones “sin riesgo” o presiones para actuar rápido.

También existen **casos de redes organizadas** que captaban víctimas, utilizaban sus datos y blanqueaban los beneficios obtenidos mediante criptomonedas.

3. Señales para desconfiar

Las ciberestafas no siempre contienen errores evidentes. Algunas utilizan **logotipos reales, páginas muy parecidas a las oficiales, mensajes correctamente escritos y perfiles que aparentan ser auténticos**. Por eso, no debemos confiar únicamente en la apariencia.

Para identificar una posible estafa, es importante fijarse en el conjunto del mensaje: **quién lo envía, qué nos pide, con qué urgencia, por qué canal llega y si la situación tiene sentido.** Muchas veces la señal de alerta no está en un único detalle, sino en la combinación de varios elementos que buscan que actuemos rápido y sin verificar.



Cinco señales para detenerse y comprobar

1. Urgencia, miedo o presión

Desconfía de los mensajes que exigen actuar rápido o presentan consecuencias inmediatas, como el bloqueo de una cuenta, la pérdida de un paquete o la necesidad de verificar datos en ese momento.

2. Promesas demasiado atractivas

Los premios inesperados, los productos con precios muy bajos, los trabajos fáciles desde casa o las inversiones con beneficios elevados y poco riesgo deben revisarse con cautela. Demasiado fácil, rápido o rentable, puede ser una señal de alerta.

3. Solicitudes de datos, dinero o códigos

Desconfía de una petición inesperada de contraseñas, códigos de verificación, datos bancarios, documentos personales, pagos por adelantado o cambios de cuenta, aunque parezca proceder de una persona conocida, un compañero, un directivo o un proveedor.

4. Enlaces, remitentes o páginas sospechosas

En muchos fraudes se utilizan direcciones parecidas a las oficiales, enlaces con pequeñas variaciones, páginas que imitan a las reales o perfiles con apariencia profesional. Desconfía también de tiendas sin datos claros, condiciones poco transparentes o cuentas que pueden haber sido robadas.

5. Cambios de canal o forma de pago

Que una conversación pase a canales menos controlados o que se pidan pagos mediante transferencias, criptomonedas, tarjetas regalo o cuentas bancarias modificadas son señales que han de hacerte sospechar.

4. Proteger cuentas, datos y dinero

Ante un mensaje inesperado, debemos comprobar su autenticidad **por un canal diferente.** Por ejemplo, podemos acceder directamente a la aplicación oficial, llamar al número que ya conocemos o contactar con la empresa sin utilizar los enlaces ni los teléfonos incluidos en el mensaje sospechoso.

Si tienes dudas sobre un mensaje, una web, una llamada o una posible ciberestafa, puedes **contactar con el 017, la Línea de Ayuda en Ciberseguridad del Instituto Nacional de Ciberseguridad (INCIBE)**, un servicio gratuito y confidencial dirigido a ciudadanos, empresas y profesionales.

Tres acciones clave para mantenerse seguro

1. Protege tus cuentas y dispositivos

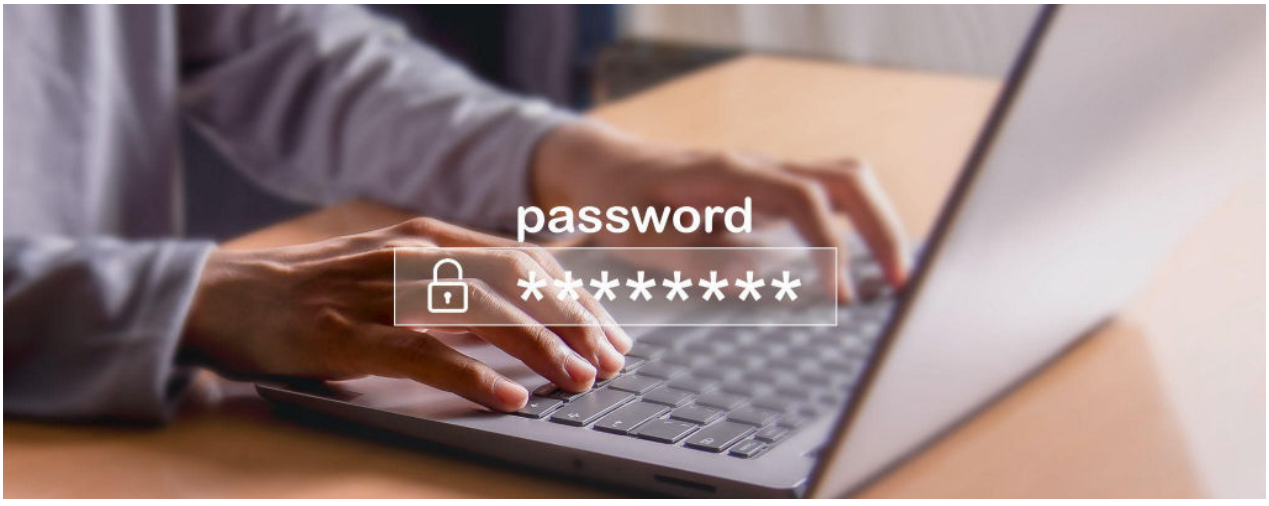
Utiliza **contraseñas diferentes** para cada servicio, largas y difíciles de adivinar. Activa la verificación en dos pasos y no compartas nunca los códigos recibidos por SMS, correo o aplicaciones de autenticación. **Mantén actualizados** dispositivos, aplicaciones y navegadores. Muchas actualizaciones corrigen fallos de seguridad que podrían ser aprovechados por los delincuentes.

2. Comprueba antes de pulsar, descargar o responder

Revisa enlaces, remitentes y archivos adjuntos antes de abrirlos. Si un mensaje genera dudas, **no respondas desde el propio mensaje** ni utilices los enlaces o teléfonos incluidos en él. Accede desde la aplicación oficial o contacta por un canal que ya conozcas.

3. Verificar datos, pagos y cambios sensibles

Confirma por otro medio cualquier solicitud inesperada de dinero, datos personales, documentación, códigos de seguridad o cambios en una cuenta bancaria. Comprobar es **especialmente importante si la petición parece venir de una persona conocida, un proveedor o una entidad de confianza.**



5. Prevención digital en las empresas

En una empresa**, una ciberestafa puede provocar grandes pérdidas** económicas, filtración de datos, interrupción de la actividad, daños reputacionales o impacto en clientes, proveedores y personas trabajadoras.

Un caso real recogido por INCIBE muestra cómo **una empresa recibió un mensaje que aparentaba proceder del CEO del grupo a través de Teams.** En él se solicitaba una operación urgente por valor de 150.000 euros y se facilitaba el contacto de un supuesto abogado para gestionarla.

Este tipo de fraude funciona porque **los delincuentes conocen las dinámicas del entorno laboral:** correos urgentes, facturas pendientes, cambios de cuenta bancaria, solicitudes internas o archivos que parecen venir de proveedores. Aprovechan esas situaciones para suplantar identidades, generar presión y conseguir que alguien actúe sin comprobar.

Por eso, **la prevención digital en las empresas debe combinar tecnología, procedimientos claros y formación.** No basta con tener herramientas de seguridad si las personas no saben qué hacer ante una petición sospechosa.

Medidas básicas para empresas

1. Verificar operaciones sensibles
Establecer una doble verificación para pagos, cambios de cuenta bancaria, facturas inesperadas o solicitudes urgentes de documentación.

2. Definir canales de aviso
Indicar a quién debe comunicarse un mensaje sospechoso, un enlace fraudulento, una descarga dudosa o cualquier posible incidente.

3. Proteger el teletrabajo y los accesos remotos
Usar cuentas corporativas, verificación en dos pasos, conexiones seguras y normas claras para trabajar desde fuera de la oficina.

4. Limitar accesos y revisar permisos
Dar acceso a datos, sistemas de plataformas y herramientas solo a quienes lo necesiten para su trabajo, y revisar esos permisos periódicamente.

5. Formar a los equipos en ciberseguridad
Capacitar a las personas que utilizan correo, dispositivos digitales, redes sociales, o plataformas colaborativas para reconocer fraudes y actuar correctamente.

6. Revisar y actualizar medidas
Mantener actualizados dispositivos, aplicaciones y procedimientos, y revisar de forma periódica si las medidas siguen siendo adecuadas.

6. Qué hacer si sufres una ciberestafa

Los canales oficiales recomiendan actuar con rapidez. Lo importante es cortar el contacto cuanto antes, proteger cuentas, conservar pruebas y pedir ayuda:

1. Corta el contacto

No hagas nuevos pagos, no facilites más datos y no sigas instrucciones de los estafadores, aunque prometan devolver el dinero o solucionar el problema.

2. Protege cuentas y dinero

Si has compartido datos bancarios, hecho un pago o introducido claves en una página sospechosa, contacta con tu banco, revisa movimientos, bloquea tarjetas si es necesario y cambia contraseñas.

3. Revisa dispositivos y accesos

Si has descargado archivos, instalado aplicaciones o permitido acceso remoto, deja de usar ese dispositivo hasta revisarlo. Actualiza contraseñas, cierra sesiones abiertas y solicita ayuda técnica si lo necesitas.

4. Guarda pruebas

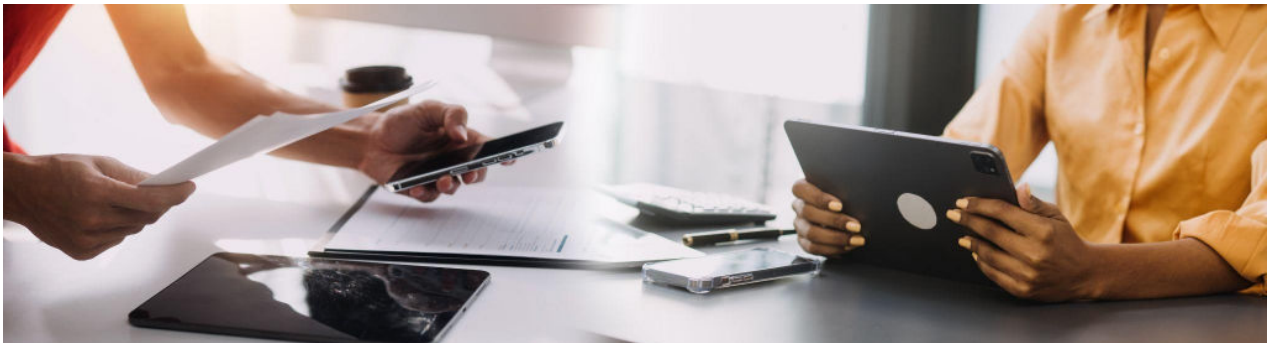
Conserva mensajes, correos, capturas, justificantes de pago, conversaciones y todo lo que pueda servir para reclamar, denunciar o investigar lo ocurrido.

5. Avisa cuanto antes

Informa a tus contactos si pueden estar recibiendo mensajes en tu nombre. Si afecta a un correo, dispositivo o información de empresa, comunícalo internamente cuanto antes.

En el siguiente apartado encontrarás los canales adecuados para pedir ayuda, reportar un fraude o presentar una denuncia.

7. Dónde pedir ayuda, reportar o denunciar



Reportar, pedir ayuda y denunciar no son lo mismo. **INCIBE** puede orientarte y recibir reportes de fraude. Las denuncias por hechos delictivos deben presentarse a las Fuerzas y Cuerpos de Seguridad o al juzgado correspondiente.

Si necesitas orientación

INCIBE, a través de su Línea de Ayuda en Ciberseguridad 017, ofrece asesoramiento ante dudas o incidentes relacionados con ciberseguridad. Es un servicio gratuito y confidencial para ciudadanos, empresas y profesionales. Útil si has recibido un mensaje sospechoso, dudas de una web, o necesitas orientación sobre los pasos a seguir.

Si quieres reportar un fraude digital

INCIBE también permite reportar fraudes como correos de *phishing, smishing,* llamadas fraudulentas, tiendas online falsas, webs maliciosas u otros intentos de engaño.

Este reporte ayuda a analizar la amenaza y puede servir para que se adopten medidas frente a páginas o campañas fraudulentas. Para facilitar la gestión, hay que aportar una descripción del incidente y todas las pruebas posibles (capturas, enlaces, correos, teléfonos o archivos recibidos).

Si has sufrido una estafa o puedes ser víctima de un delito

Si sufres un perjuicio económico, una suplantación de identidad, un acceso no autorizado, una amenaza, un robo de cuentas o cualquier otro hecho que pueda constituir delito, **debes presentar denuncia** ante las Fuerzas y Cuerpos de Seguridad.

La denuncia puede presentarse ante **Policía Nacional, Guardia Civil, policías autonómicas competentes o en el juzgado de guardia correspondiente.** En algunos casos puede iniciarse de forma telemática, pero según el tipo de hecho puede ser necesario acudir presencialmente o ratificar la denuncia. Antes de denunciar, **conserva todas las pruebas disponibles.**

Si afecta a datos personales

Si se han utilizado tus datos personales sin permiso, han creado perfiles falsos, han difundido información personal o se ha producido una suplantación de identidad, también puedes consultar los recursos de la **Agencia Española de Protección de Datos**

Si afecta a banca, tarjetas o transferencias

Si has compartido datos bancarios, detectas cargos no autorizados o has realizado una transferencia fraudulenta, contacta cuanto antes con tu banco. El **Portal del Cliente Bancario del Banco de España** ofrece información sobre fraudes relacionados con banca online, pagos, tarjetas, transferencias y suplantaciones.

Para terminar...

Las ciberestafas cambian constantemente, pero **suelen apoyarse en las mismas estrategias:** generar urgencia, despertar confianza y conseguir que actuemos sin verificar la información.

Conocer cómo funcionan, identificar señales de alerta y mantener hábitos digitales seguros puede ayudarnos a proteger nuestra privacidad, nuestro dinero y nuestras cuentas y también nuestro entorno de trabajo.

Tomarse tan solo unos minutos para comprobar un mensaje, una petición o una operación puede evitar daños difíciles de reparar, como pérdidas económicas, robo de información o acceso a nuestras cuentas. **Y si ya hemos facilitado datos, hecho un pago o perdido el control de una cuenta, actuar rápido** para reducir las consecuencias.

Fuentes consultadas

Ministerio del Interior – Informe sobre la Cibercriminalidad en España 2025

INCIBE – Fraude de email comprometido

INCIBE – Caso real de suplantación del CEO por Teams

INCIBE – Fraude en RR. HH.: cambio de cuenta bancaria

INCIBE – Formación y concienciación en empresas

Banco de España – Estafa de los “me gusta”

Banco de España – Protégete contra el fraude

Banco de España – Qué es el phishing y cómo evitarlo

Guardia Civil - ¿Conocías esta nueva estafa? El business email compromise

Noticias y casos reales

Con el objetivo de ilustrar cómo pueden presentarse estas situaciones en la práctica, se han revisado las siguientes noticias y casos reales de ciberestafas:

El auge del turismo dispara los fraudes en reservas electrónicas de viajes

La Policía Nacional alerta del aumento de estafas por WhatsApp mediante la usurpación de cuentas

Un juzgado obliga a un banco a devolver el dinero estafado a una empresa a la que suplantaron la identidad de su consejero delegado

“No pensé que yo pudiera caer”: el auge de las falsas ofertas laborales que se difunden por WhatsApp y otras redes de mensajería

Detenido por estafar 9.000 euros a un hombre haciéndose pasar por su hijo

Las estafas financieras se multiplican por cinco en una década al cobijo de las redes sociales.

El miedo a las ciberestafas crece en España: seis de cada diez creen que serán víctimas.

Más noticias y casos reales

Estafas online +125% en España: radiografía del ciberfraude.

El fraude digital aumenta un 40% en España: 1.200 estafas al día en 2025.

Casi la mitad de los españoles ha sufrido una estafa o un intento de estafa en el último año, según el CIS.

Nueva estafa de phishing provoca que 5 personas pierdan hasta 71 mil euros.

Alertan de la nueva estafa suplantando a Iberdrola: un falso correo con facturas instala el temido malware Grandoreiro.

Alertan de mensajes de texto falsos que suplantan a la Agencia Tributaria para robar datos bancarios.

Alerta nueva estafa por correo electrónico en España.

Alerta de smishing: el falso SMS de la Agencia Tributaria sobre la Renta que busca robar datos bancarios.

Ciberataques a empresas: estafas tras filtraciones.

GhostPairing: así es el nuevo ciberataque para hacerse con tu cuenta de WhatsApp.

Aviso urgente de la Guardia Civil: así te pueden robar tus datos para usarlos en casas de apuestas.

Mafias digitales roban identidades de abogados para estafar vendiendo residencias permanentes inexistentes.

Desarticulada una red criminal que estafaba a clientes, vendía sus datos y blanqueaba los beneficios con criptomonedas.

Estafa de criptomonedas: Ciberdelincuentes suplantan identidad.

DigitalPreventor