



SEPTIEMBRE 2026

Enfoka-Trends

Estafas digitales: cómo reconocerlas, protegerse y actuar a tiempo

Estafas digitales: cómo reconocerlas, protegerse y actuar a tiempo

Una llamada del "banco", un SMS de mensajería o un cobro de una supuesta obligación legal, las y los estafadores no distinguen entre una multinacional y un pequeño comercio.

¿Por qué su negocio es un objetivo atractivo?

Si usted lleva su comercio prácticamente solo o sola, la decisión, la firma y el pago pasan por la misma persona. No hay un departamento de administración que dude, ni personal de informática que revise el correo. Además, atiende llamadas mientras despacha, revisa el móvil entre visitas de su clientela y paga facturas con prisa. Los y las delincuentes lo saben y lanzan campañas masivas y automatizadas a la espera de que alguien, en algún momento, tenga un despiste.

El fraude online funciona como una pesca de arrastre. Se envían miles de mensajes casi idénticos y basta con que algunos prosperen. Esto golpea especialmente a personas bajo el Régimen Especial de Trabajadores Autónomos (RETA) y pymes, porque tienen menos medidas de seguridad y un solo clic puede paralizar su actividad o desviar sus pagos.

¿Cómo prevenirlas?

La prevención es un hábito. Dedique diez minutos al mes a revisar los movimientos de la cuenta, los avisos de su banco y los perfiles con su nombre. Consulte los avisos de INCIBE (Instituto Nacional de Ciberseguridad), porque las estafas cambian de disfraz cada pocos meses. Y acuerde con quien le ayude en el negocio, sea una persona empleada o un familiar, que ningún pago ni código se da por teléfono sin comprobación.

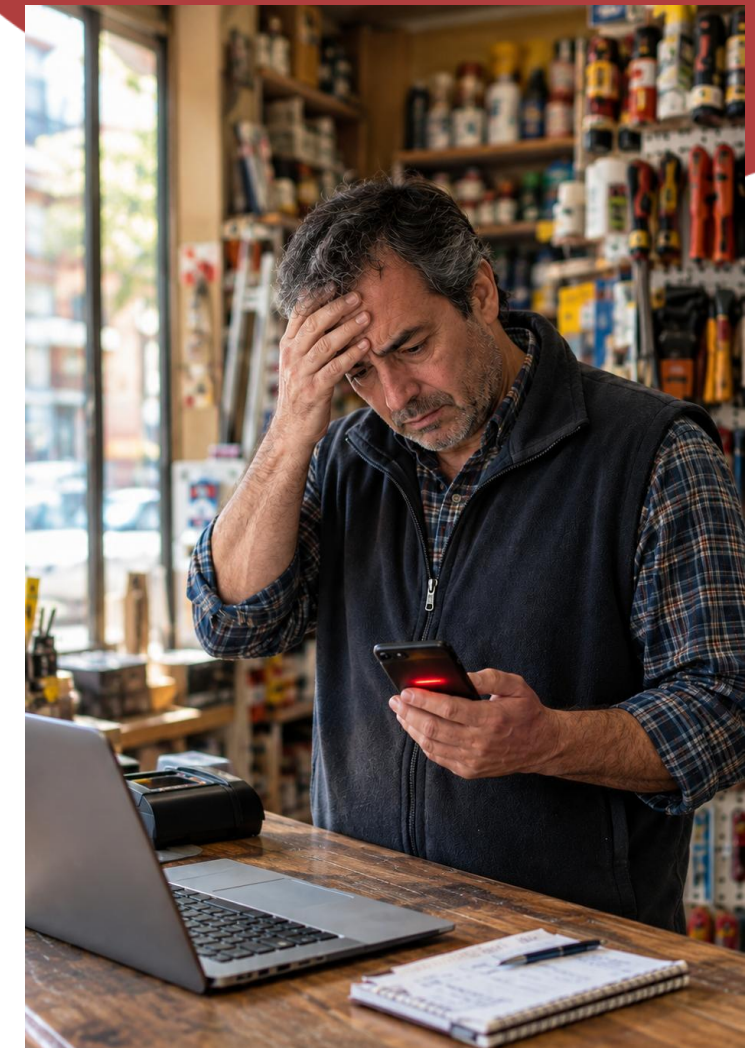


Imagen generada con Inteligencia Artificial

Estafas digitales: cómo reconocerlas, protegerse y actuar a tiempo

ENFOKA-TRENDS SEPTIEMBRE 2026

Las cinco estafas que debe conocer

1. «Soy del banco»: suplantación telefónica

Cómo funciona. Alguien le llama diciendo que es de su banco y que hay un movimiento sospechoso que hay que «cancelar». El *spoofing* es la técnica que altera el número que aparece en su pantalla, de modo que parece el del banco. Incluso pueden pedirle que compruebe que el número coincide con el de la web oficial.

Ejemplo. Una peluquería recibe una llamada «del departamento de seguridad» que le pide confirmar un código recibido por SMS «para bloquear una transferencia». Ese código es, en realidad, la autorización para vaciar su cuenta.

Señales de alerta. Los y las delincuentes se hacen pasar por personal empleado del banco para pedir contraseñas, códigos de acceso o números de cuenta. También aplican urgencia para que no tenga tiempo de pensar.

Consecuencias. Pérdida de dinero de la cuenta del negocio y, a veces, de la personal.

2. Phishing por correo, SMS y WhatsApp

Cómo funciona. El *phishing* es un mensaje falso que imita a un banco, a la Administración o a otra empresa para que pulse un enlace o entregue claves. Por SMS se llama *smishing*.

Ejemplo. La Tesorería General de la Seguridad Social alertó de un SMS falso dirigido a personas bajo el Régimen Especial de Trabajadores Autónomos que prometía una devolución de impuestos. Una señal de fraude era que las devoluciones corresponden a la Agencia Tributaria, no a la Tesorería. Una variante muy dañina para negocios es el cambio de cuenta en una factura. El o la atacante modifica el número de cuenta de una factura de una empresa proveedora para desviar el pago.

Señales de alerta. Enlaces que no coinciden con la web oficial, saludos genéricos, peticiones de claves o códigos, y pagos inmediatos o poco habituales.

Consecuencias. Robo de credenciales, pagos desviados y acceso a su correo o su banca.



Imagen generada con Inteligencia Artificial

Estafas digitales: cómo reconocerlas, protegerse y actuar a tiempo

ENFOKA-TRENDS SEPTIEMBRE 2026

3. Falsas webs y falsas tiendas en redes sociales

Cómo funciona. Hay dos caras del problema. La primera es la de tiendas falsas que se anuncian en redes. La segunda es la suplantación de su propio negocio. En las redes sociales, los o las delincuentes crean un perfil casi idéntico al de la empresa, con variaciones mínimas en el nombre, para hacerse pasar por ella. Con ese perfil pueden engañar a las personas que les siguen para que caigan en un fraude que parece hecho bajo su nombre. Se han denunciado tiendas falsas que se presentan como pequeños comercios locales.

Ejemplo. Una floristería descubre que un perfil clon con su logo anuncia un sorteo y pide «gastos de envío» a su clientela.

Señales de alerta. La clientela le pregunta por acciones de marketing que usted no ha iniciado, o aparecen cuentas a su nombre en redes sociales con pocas publicaciones.

Consecuencias. Daño a su reputación, clientela estafada que le reclaman a usted y pérdida de confianza.

4. Falsos técnicos de soporte

Cómo funciona. Le llaman o le aparece un aviso en pantalla diciendo que su ordenador está infectado. Se ofrecen a arreglarlo y le piden claves o que instale una herramienta de control remoto. Con ella pueden secuestrar el equipo, robar datos o hacer transacciones.

Ejemplo. A un comercio le aparece un aviso de bloqueo en la pantalla de su TPV por infección de virus y se le comunica que recibirá una llamada «del soporte informático» de su software de gestión de ventas, le piden instalar un programa de acceso remoto y, minutos después, el cursor se mueve solo por su perfil de banca online.

Señales de alerta. Una llamada que usted no ha pedido, el aviso de virus con teléfono de contacto y la insistencia en instalar algo.

Consecuencias. Pérdida de dinero, datos de la clientela expuestos y equipos bloqueados.



Imagen generada con Inteligencia Artificial

Estafas digitales: cómo reconocerlas, protegerse y actuar a tiempo

5. Falsas obligaciones legales o cuotas

Cómo funciona. Se hacen pasar por organismos oficiales, como Hacienda, Seguridad Social o registros, y le reclaman un pago o un trámite «obligatorio».

Ejemplo. Con la tienda abierta, le llega un SMS que habla de una actualización pendiente y le invita a pulsar un enlace. El dominio del enlace incluye palabras como «portal», «seg» o «social» para parecer oficial, y la página reproduce la imagen del portal de la Tesorería. Allí aparece una supuesta referencia de expediente y un concepto de «regularización de cuotas», y se le reclaman 38,74 euros. Según Autónomos y Emprendedor, una cantidad tan pequeña resulta creíble como ajuste de cotizaciones y no invita a comprobarla. El enlace lleva a una pasarela de pago falsa, que imita la aplicación Importass, donde le piden los datos de su tarjeta.

Señales de alerta. Los avisos falsos suelen tener faltas de ortografía, frases mal construidas y plazos muy cortos para que actúe de prisa. La Seguridad Social no pide pagar deudas ni actualizar datos personales mediante enlaces enviados por SMS.

Consecuencias. Si introduce los datos de su tarjeta, puede sufrir cargos que usted no ha autorizado y quedar expuesto a otros intentos de fraude con esos datos. Si ya facilitó su tarjeta, no espere a que aparezca un cargo. Bloquéela de inmediato, avise a su banco y guarde las pruebas para denunciar. También puede pedir ayuda al teléfono 017 de INCIBE.

Las situaciones que puede tener que afrontar si se ve afectado son diversas. Puede perder dinero directamente o por una factura falsa. Además, hay que dedicar tiempo a reclamar y denunciar, lo que también cuesta. Si se accede a su ordenador, correo o agenda, puede haberse producido una brecha de datos personales. La normativa establece un plazo de 72 horas para notificarla a la AEPD desde que se tiene constancia. Su clientela puede ser estafada en su nombre, y sus llamadas pueden llegar a ser marcadas como spam.

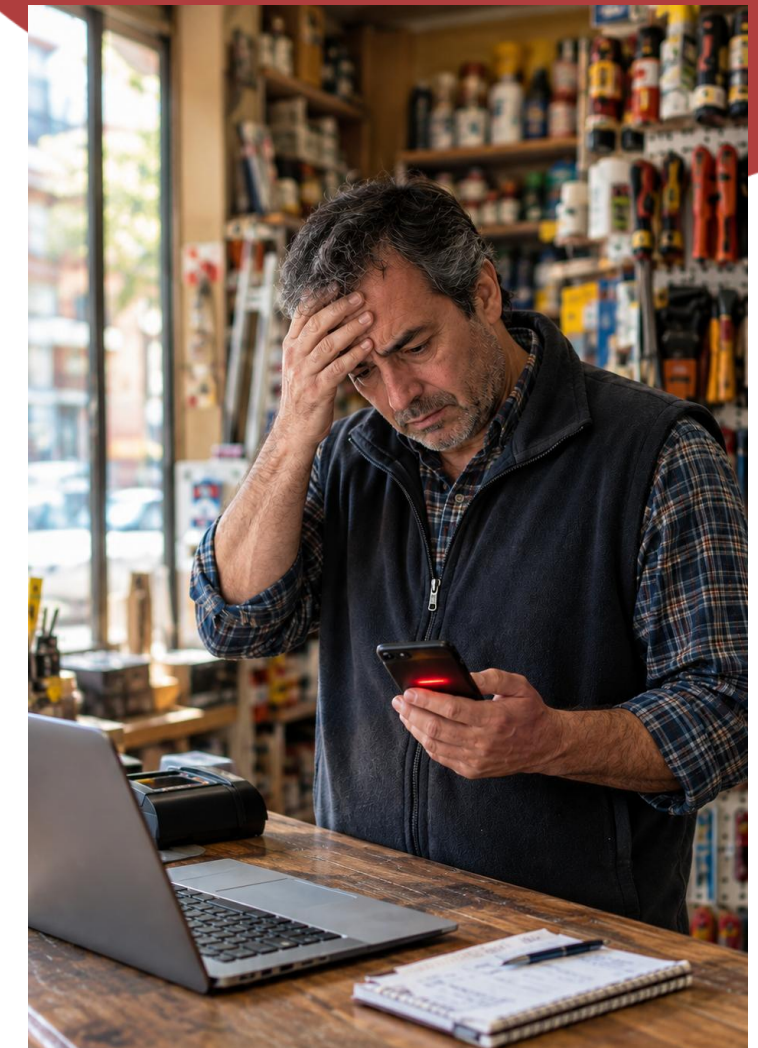


Imagen generada con Inteligencia Artificial

Estafas digitales: cómo reconocerlas, protegerse y actuar a tiempo

¿Qué dicen los datos?

- **Incidentes de ciberseguridad (INCIBE, 2025).** El CERT de INCIBE gestionó 122.223 incidentes en 2025, un 26 % más que en 2024. El fraude online sumó 45.445 casos, un 19 % más que el año anterior, y el *phishing* fue la técnica más frecuente, con 25.133.
- **Empresas afectadas.** El último desglose oficial que hemos localizado es el de 2024: se atribuyeron a empresas 31.540 incidentes, el 32,4 % del total. Esa categoría incluye pymes y personas bajo el Régimen Especial de Trabajadores Autónomos.
- **Delitos denunciados (Ministerio del Interior, 2025).** Se registraron 488.426 ciberdelitos, un 5,1 % más que en 2024, lo que supone el 19,8 % de toda la criminalidad. Casi nueve de cada diez fueron fraudes informáticos (429.677), que aumentaron un 4 %. Estas cifras incluyen a particulares y empresas.
- **Personas propietarias de pymes españolas (Mastercard, encuesta de 2024-2025).** El 23 % afirmó haber sido víctima de una estafa en su negocio, el 13 % perdió dinero y el 7 % perdió clientela. Además, el 29 % cree que tendría que cerrar si sufriera un ciberataque.
- **Ciberataques a pymes (Hiscox, 2025).** Según este informe, casi el 60 % de las pymes españolas sufrió al menos un ciberataque en los doce meses anteriores.
- **Comercio minorista.** Check Point Software cifra en un 178 % el aumento de incidentes de *ransomware* y filtraciones de datos en el comercio minorista español en 2024. Es un tipo de ataque distinto a las estafas de este informe, pero indica hacia dónde se dirige la presión.

Los números oficiales solo reflejan lo que se denuncia o se comunica. Es razonable pensar que la realidad será aún mayor.

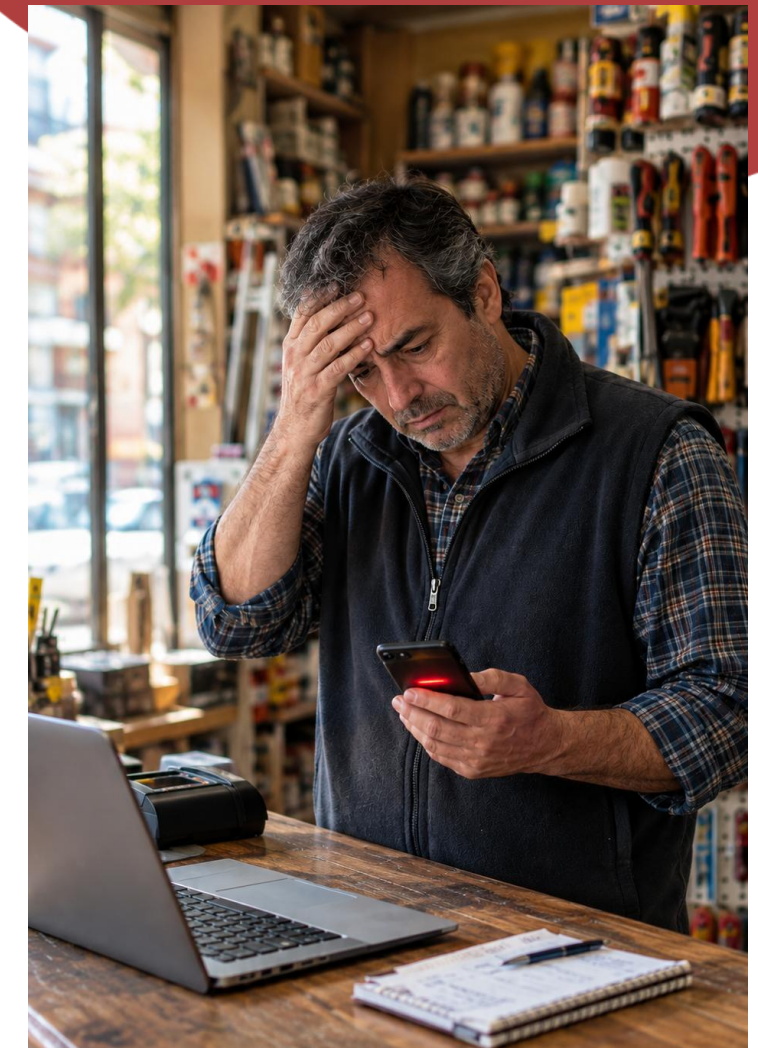


Imagen generada con Inteligencia Artificial

Estafas digitales: cómo reconocerlas, protegerse y actuar a tiempo

Cómo protegerse: medidas sencillas y baratas

1. **Regla de oro del «cuelgue y llame».** Ante una llamada de su banco o de personal técnico, cuelgue y llame usted al teléfono oficial de su tarjeta o de la web. INCIBE recomienda contrastar por otra vía cualquier llamada que le parezca sospechosa.
2. **Nunca dicte códigos ni claves,** ni por teléfono ni por mensaje. Su banco no se los pedirá.
3. **Verificación en dos pasos** en el correo, la banca, las redes y la web. Es una de las defensas más eficaces.
4. **Contraseñas distintas** para cada servicio, con un gestor de contraseñas si le resulta cómodo.
5. **No instale programas de acceso remoto** a petición de personas desconocidas.
6. **Verifique los cambios de cuenta** de empresas proveedoras llamando a un teléfono que ya tuviera, no al de la factura.
7. **Alertas y límites en el banco,** y una cuenta separada para el negocio.
8. **Copias de seguridad** de sus archivos, guardadas fuera del ordenador.
9. **Vigile su marca,** busque su nombre en redes de vez en cuando y avise a su clientela de cuáles son sus perfiles oficiales.

Nadie está a salvo de un despiste, pero casi todas estas estafas comparten un patrón: urgencia, un código o una clave que le piden, y una llamada o mensaje que usted no esperaba. Si aprende a parar, colgar y comprobar por otro canal, habrá frenado la mayoría.

Dedique esta semana media hora a activar la verificación en dos pasos, revisar las alertas de su banco y guardar el teléfono 017 en su móvil, es una línea gratuita y confidencial, atienden a empresas y profesionales todos los días de 8:00 a 23:00.

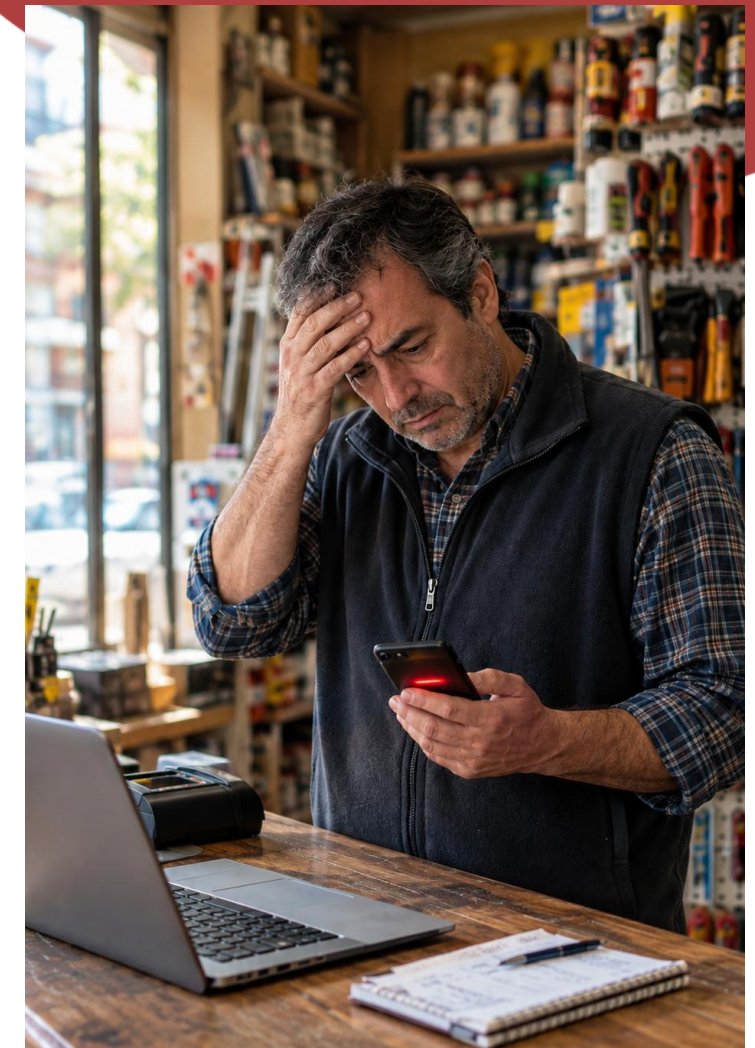


Imagen generada con Inteligencia Artificial

Bibliografía

- **Carlos Olivera (LinkedIn, 2026)** *Las estafas digitales más comunes de este año.* Recuperado el 28 de septiembre de 2026 de <https://www.linkedin.com/pulse/las-estafas-digitales-m%C3%A1s-comunes-de-este-a%C3%B1o-olivera-villanueva-cybre/>
- **INCIBE (2026)** *INCIBE detectó más de 122.000 incidentes de ciberseguridad en 2025.* Recuperado el 28 de septiembre de 2026 de <https://www.incibe.es/incibe/sala-de-prensa/incibe-detecto-mas-de-122000-incidentes-de-ciberseguridad-en-2025>
- **itUser (2026)** *Los ciberataques en serie golpean a autónomos y pymes.* Recuperado el 28 de septiembre de 2026 de <https://tecnologiaparatuempresa.ituser.es/seguridad/2026/03/los-ciberataques-en-serie-golpean-a-autonomos-y-pymes>
- **Lucía Fernandez (Libre Mercado, 2026)** *Las tiendas falsas se disparan: así operan las estafas que engañan a miles de usuarios en TikTok, Instagram y Facebook.* Recuperado el 28 de septiembre de 2026 de <https://www.libertaddigital.com/libremercado/2026-04-14/las-tiendas-falsas-se-disparan-asi-operan-las-estafas-que-enganan-a-miles-de-usuarios-en-tiktok-instagram-y-facebook-7387416>
- **Guijarro Pique Asociados (2026)** *¿Qué puedo hacer si he sido víctima de phishing o una estafa bancaria?* Recuperado el 28 de septiembre de 2026 de <https://www.guijarropique.com/phising-estafa-banco>
- **Sol Galindo (Autónomos y emprendedores 2025)** *Los ciberataques contra los pequeños comercios se triplicaron en 2024: el 28% accedió a pagar un rescate.* Recuperado el 28 de septiembre de 2026 de <https://www.autonomosyemprendedor.es/articulo/todo-digital/ciberataques-pequenos-comercios-triplicaron-2024-28-accedio-pagar-rescate/20250220132209041096.html>