Guía integral anti-phishing (2025)

Esta guía está escrita para ti, no para el equipo técnico. Queremos que te resulte fácil, rápida de leer y útil en tu día a día. No hace falta saber de informática: bastan unos hábitos simples y un poco de calma antes de hacer clic.

Índice

Antes de empezar

Todos podemos picar alguna vez. Los engaños funcionan porque nos pillan con prisas, con miedo o con la cabeza en otra cosa. El objetivo realista no es “no caer nunca”, sino **reducir mucho las probabilidades** y **reaccionar bien** si algo ocurre.

Qué es el phishing

El phishing es cuando alguien se hace pasar por tu banco, una mensajería, Hacienda o incluso por un compañero para que le des **contraseñas, códigos**, o para que **pagues** algo que no corresponde. A veces te empujan a instalar una aplicación o a entrar en una web falsa que se parece muchísimo a la auténtica.

Señales que notarás en la vida real

Suelen aparecer juntas:

- **Prisa** o **amenaza**: “en 24 h cerramos tu cuenta”, “último aviso”.
- **Solicitud rara**: te piden contraseña, un **código SMS**, o cambiar el **IBAN** por email.
- **Enlaces sospechosos**: el texto dice una cosa pero la dirección es otra, larguísima o extraña.
- **Tono que no encaja**: saludos raros, faltas, o un “jefe” pidiéndote tarjetas regalo.
- **Adjuntos que no esperabas**: una “factura” o un “albarán” que no te cuadra.

Si notas una o dos de estas, **para un momento**. Esa pausa de segundos suele ahorrarte problemas.

Método S.T.O.P. (tu mini-protocolo personal)

S – Suelta el ratón. No pulses aún.
T – Toma aire. Date 20 segundos. La prisa es su mejor arma.
O – Observa la dirección. Mira la web completa o el remitente real; ¿es exactamente el de siempre?
P – Prueba otra vía. Entra escribiendo tú la web o llama al contacto de siempre. No uses el enlace del mensaje.

Funciona con emails, SMS, WhatsApp, llamadas y códigos QR.

Cómo comprobar sin liarte

- Abre una pestaña nueva y **escribe tú la dirección** del banco, mensajería, Hacienda o la herramienta de trabajo.
- **Llama** al número que ya tienes guardado (no al que viene en el mensaje).
- Pide a una segunda persona que lo mire contigo. Dos miradas calman mucho las dudas.

Cosas que nunca deberías hacer

- Enviar **contraseñas**, **códigos de verificación** o fotos del **DNI** por correo o chat.
- Instalar programas o extensiones porque te lo pide alguien por teléfono.
- **Aprobar pagos** o cambios de **IBAN** sin confirmar por teléfono con el contacto habitual.
- Usar la **misma contraseña** en todas partes.

Si sospechas en el momento

No hace falta montar un drama:

1. No pulses.
2. Haz un pantallazo.
3. Reenvía la sospecha a quien corresponda en tu empresa.
4. Borra el mensaje para no caer después.

Si es una llamada, cuelga con educación (“ahora no puedo”), y luego **llama tú** al número oficial.

Si ya hiciste clic o diste datos

Pasa página, actúa y listo.

Solo hice clic: cierra la pestaña y entra a la web correcta escribiéndola tú.

Escribí usuario y contraseña: cambia la contraseña desde la web auténtica, cierra sesiones abiertas y activa el doble paso (si no lo tenías). Revisa reglas raras en tu correo (reenvíos automáticos).

Di el código de verificación (2FA): entra a tu cuenta real, cierra todas las sesiones, cambia contraseña y vuelve a activar el doble paso.

Di tarjeta o pagué algo: llama al banco para bloquear y revisar cargos.

Instalé algo: desinstálalo y evita meter contraseñas hasta que revisen el dispositivo.

Envié foto del DNI o datos personales: avisa; puede que haya que tomar más medidas.

Hábitos que te blindan sin complicarte la vida

- **Marcadores**: guarda los accesos importantes (banco, correo, herramientas) y entra siempre desde ahí.
- **Contraseñas únicas** con un **gestor de contraseñas**. Te quita dolores de cabeza.
- **Doble paso** (código en app) en todo lo importante.
- Mantén **móvil y navegador** al día.
- Separa lo **personal** y el **trabajo** (perfiles o navegadores distintos).

Pagos y facturas: el punto más delicado

Los timos más caros suelen venir por aquí. Una regla sencilla te evita la mayoría: **ningún cambio de IBAN se aprueba solo por email**. Se confirma **por teléfono** con el contacto de siempre y, si podéis, que lo revisen **dos personas** (quien pide y quien autoriza). Además, comprueba importe, concepto y fechas.

Texto útil para responder un cambio de IBAN

“Hola, para poder tramitar el cambio necesitamos confirmarlo por teléfono con el contacto habitual. ¿Podéis indicarnos con quién hablar? Gracias.”

Trabajo híbrido o desde casa, sin paranoias

- Usa Wi-Fi con contraseña. Evita redes públicas para cosas sensibles.
- Bloquea el equipo cuando te levantes.

- En videollamadas, revisa qué compartes y quién está en la sala.
- No mezcles cuentas personales y de trabajo en el mismo perfil del navegador.

Dudas típicas (rápidas de leer)

¿El candado significa que es seguro? No necesariamente. Solo indica conexión cifrada. Lo importante es la **dirección exacta**.

¿El doble paso me salva siempre? Ayuda muchísimo, pero si metes el código en una web falsa, no. Entra desde tus marcadores.

¿Y si el mensaje viene de alguien conocido? Puede que le hayan robado la cuenta. Si pide algo raro o urgente, confirma por otra vía.

¿Puedo denunciar? Si hay dinero de por medio, habla con tu banco y valora denuncia (Policía Nacional/Guardia Civil). Para orientación general existe el 017.

Ejemplos comentados (lo verás clarísimo)

Paquete retenido por 1,79 €
Engaña porque es una cantidad pequeña y mete prisa. La web no es la oficial y el enlace suele estar acortado. Lo correcto: entrar tú a la web de la mensajería desde tus marcadores o escribiéndola.

Hacienda: notificación urgente
Engaña por el miedo. Suelen adjuntar un .html o .zip. Lo correcto: entrar a la sede electrónica escribiendo la dirección oficial.

Banco: "verificación de dos pasos"
Te piden el código fuera de la app. Lo correcto: abrir la app del banco y comprobar allí las alertas.

Proveedor: "hemos cambiado de cuenta"
Parece real porque copia hilos antiguos. Lo correcto: llamar al teléfono de siempre y pedir doble revisión interna.

Herramienta de trabajo: restablece tu contraseña
Coincide con tu rutina y por eso cuela. Lo correcto: entrar desde tu marcador guardado, no desde el correo.

WhatsApp del "jefe" pidiendo tarjetas regalo
Autoridad + urgencia. Lo correcto: llamar al jefe al número de siempre. Ningún proceso serio pide tarjetas regalo.

QR en una mesa
Puede ser una pegatina encima. Lo correcto: pedir el QR del local o escribir su web.

Mini-entrenamientos (para practicar cinco minutos)

- Señala tres señales rojas en un SMS que te pide un pago pequeño por un paquete.
- Escribe cómo rechazarías con educación un cambio de IBAN hasta verificar por teléfono.
- Practica cortar una llamada de "soporte" inesperada y volver a llamar tú al número oficial.

Plantillas rápidas

Reportar sospecha
"Asunto: Posible phishing — No abrir. He recibido este mensaje sospechoso. No he hecho clic ni abierto adjuntos. Adjunto pantallazo. ¿Podéis revisarlo?"

Aviso general a clientes si detectáis suplantación
"Hemos detectado intentos de suplantación. Nunca pedimos contraseñas ni códigos por email. Para operar, entra escribiendo nuestra web o desde tus marcadores."

Versión de bolsillo (resumen para tener a mano)

- Si hay **prisa** o piden **datos** → **S.T.O.P.**
- Escribe tú la **dirección** o usa **marcadores**.
- **No des códigos** ni contraseñas por mensaje o llamada.
- Cambios de **IBAN**, solo tras **llamar** al contacto habitual y con **doble revisión**.
- Si caes, **cambia contraseñas**, **cierra sesiones** y **avisa**. Fin del susto.

Cualquier duda, háznosla llegar. Mejor preguntar una vez de más que una de menos.