| | |
|---|---|
| **FECHA** | 25 de mayo de 2026 |
| **ASUNTO** | Documentación técnica – Phishing: Qué es y cómo reconocerlo |
| **AUTOR** | D. Ignacio Valderrama, INFORMATICA LOS LLANOS SL |

# Phishing — Qué es y cómo reconocerlo

El phishing es una técnica de **ingeniería social** mediante la cual un atacante suplanta la identidad de una persona, empresa o servicio de confianza para engañar a la víctima y conseguir que revele información confidencial, haga clic en un enlace malicioso o ejecute una acción que comprometa la seguridad.

El nombre viene del inglés **fishing** (pescar): el atacante lanza un anzuelo y espera a que alguien pique.

Es el vector de ataque más frecuente en el mundo y el punto de entrada de la mayoría de los incidentes graves, incluyendo el ***ransomware***.

## Cómo funciona un ataque de phishing

El mecanismo es siempre el mismo, aunque la forma varía:

Anzuelo → Urgencia → Acción → Compromiso

1. El atacante envía un mensaje que parece legítimo
2. El mensaje genera urgencia o miedo ("su cuenta será bloqueada", "pago pendiente")
3. La víctima hace clic, introduce credenciales o descarga un archivo
4. El atacante obtiene acceso, credenciales o instala malware

## Tipos de phishing

| Tipo | Descripción |
|---|---|
| **Phishing masivo** | Correos genéricos enviados a miles de personas. Bajo esfuerzo, baja personalización |
| **Spear phishing** | Ataque dirigido a una persona concreta, con información personalizada. Mucho más peligroso |
| **Whaling** | Spear phishing dirigido específicamente a directivos o gerentes |
| **Smishing** | Phishing por SMS |
| **Vishing** | Phishing por llamada telefónica |
| **Quishing** | Phishing mediante códigos QR maliciosos |


Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

## Ejemplos reales adaptados a micropymes

### Ejemplo 1 — Phishing masivo bancario

*De: seguridad@bbva-alertas.com Asunto: ⚠️ Acceso sospechoso detectado en su cuenta*

*Estimado cliente, hemos detectado un acceso no autorizado a su cuenta. Para proteger sus fondos, debe verificar su identidad en las próximas 2 horas o su cuenta quedará suspendida.*

*[Verificar mi cuenta ahora]*

**Señales de alerta:**

- Dominio falso: *bbva-alertas.com* en lugar de *bbva.es*
- Urgencia artificial con plazo concreto
- El enlace lleva a una web que imita al banco pero captura las credenciales

### Ejemplo 2 — Suplantación de proveedor cloud

*De: noreply@microsoft-365-support.com Asunto: Tu suscripción de Microsoft 365 ha caducado*

*Tu licencia de Microsoft 365 Business ha expirado. Para evitar la pérdida de acceso a tu correo y archivos, renueva tu suscripción antes de las 24h.*

*[Renovar ahora]*

**Señales de alerta:**

- El dominio no es *microsoft.com*
- Una micropyme que usa M365 tiene alta probabilidad de picar porque el servicio es real y crítico
- El enlace pide número de tarjeta en una web clonada

### Ejemplo 3 — Spear phishing dirigido al gerente

*De: carlos.lopez@proveedor-habitual.es* (dominio ligeramente modificado) *Asunto: Factura pendiente de pago — URGENTE*

*Hola María, te adjunto la factura del mes pasado que quedó pendiente. El número de cuenta ha cambiado recientemente, los nuevos datos están en el PDF adjunto. Cualquier duda me llamas.*

*Un saludo, Carlos*

**Señales de alerta:**

- El dominio es casi idéntico al real pero con una letra cambiada (*proveedor-habitual.es* vs *proveedor-habituai.es*)
- Usa nombres reales obtenidos de LinkedIn o la web de la empresa


Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

- El PDF contiene malware o datos bancarios falsos para desviar el pago
- Este tipo de ataque se llama también **fraude del CEO** o **BEC** (*Business Email Compromise*)

### Ejemplo 4 — Smishing (SMS)

*SMS de: CORREOS Su paquete no ha podido ser entregado. Pague 1,99€ de gastos de gestión para reprogramar la entrega: [enlace acortado]*

**Señales de alerta:**

- Enlace acortado que oculta el destino real
- El importe pequeño reduce la desconfianza
- La web destino solicita datos de tarjeta

### Ejemplo 5 — Quishing (código QR)

Un cliente recibe por correo postal o email un documento con un código QR que supuestamente lleva a una encuesta de satisfacción o a descargar una factura. El QR dirige a una web maliciosa que solicita credenciales o instala malware en el móvil.

**Por qué es especialmente peligroso:** el usuario no puede ver la URL antes de escanear, y los móviles tienen menos protecciones que los ordenadores.


Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

## Cómo detectar un phishing — Checklist práctico

Ante cualquier mensaje que pida una acción urgente, revisar:

| Pregunta | Qué buscar |
|---|---|
| **¿El remitente es legítimo?** | Revisar el dominio completo, no solo el nombre visible |
| **¿Esperaba este mensaje?** | Si no esperabas una factura, un paquete o una alerta, desconfía |
| **¿Hay urgencia artificial?** | "Tienes 2 horas", "tu cuenta será bloqueada" son señales de alarma |
| **¿El enlace va donde dice?** | Pasar el cursor por encima sin hacer clic para ver la URL real |
| **¿El adjunto es esperado?** | Nunca abrir adjuntos no solicitados, especialmente .exe, .zip o .pdf de origen dudoso |
| **¿Pide credenciales o datos de pago?** | Ningún servicio legítimo los pide por correo |
| **¿La web tiene HTTPS?** | Necesario pero no suficiente: los sitios de phishing también pueden tenerlo |

### Qué hacer si se sospecha o se ha caído en un phishing

**Si sospechas, pero no has hecho clic:**

- No interactuar con el mensaje
- Notificarlo al responsable de seguridad
- Eliminarlo

**Si has hecho clic, pero no has introducido datos:**

- Notificarlo al responsable de seguridad
- Escanear el equipo con el antivirus
- Vigilar comportamientos anómalos en el sistema

**Si has introducido credenciales:**

- Cambiar la contraseña de inmediato desde otro dispositivo
- Revocar sesiones activas
- Activar MFA si no estaba activo
- Notificar al responsable de seguridad
- Activar el procedimiento de gestión de incidentes

**Si has realizado una transferencia:**

- Contactar de inmediato con el banco para intentar detenerla


Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com

- Denunciar ante las Fuerzas y Cuerpos de Seguridad
- Notificar a la AEPD si hay datos personales afectados

## Integración en el plan director de ciberseguidad

Esta información se integra en los siguientes entregables ya desarrollados:

- **Registro de riesgos:** R-001 y R-002 cubren el phishing como amenaza principal
- **Plan de tratamiento:** T-001 (formación) y T-002 (MFA) son las contramedidas directas
- **Procedimiento de incidentes:** la sección de phishing con clic ya está contemplada
- **Política de uso aceptable:** sección 4 (correo electrónico) cubre el comportamiento esperado
- **Formación del personal:** este contenido es la base del módulo de concienciación


Ignacio Valderrama
***Colegiado 3120021W CPITINA***

Estella, a 25 de mayo de 2026


Informática Los Llanos, S.L. C/Carlos II el Malo 1 bajo – 31200 Estella (Navarra)
Tfno.: 948555339
administración@informáticalosllanos.com