Como detectar un correo electronico fraudulento

Guia practica para identificar correos electronicos sospechosos mediante el analisis de cabeceras y el uso de herramientas especializadas.

Obtener las cabeceras completas del email

Las cabeceras de un correo electronico contienen informacion tecnica sobre el remitente real, los servidores intermedios y los mecanismos de autenticacion. Esta informacion es fundamental para detectar suplantaciones de identidad (email spoofing).

Gmail

1. Abrir el correo sospechoso
2. Hacer clic en los tres puntos verticales (menu)
3. Seleccionar "Mostrar original" o "Ver origen del mensaje"
4. Se abrira una nueva ventana con las cabeceras completas

Microsoft Outlook (escritorio)

1. Abrir el correo con doble clic
2. Ir a Archivo > Propiedades
3. En la seccion "Encabezados de Internet" aparecen las cabeceras completas

Outlook Web (OWA)

1. Abrir el correo sospechoso
2. Hacer clic en los tres puntos junto a "Reenviar"
3. Seleccionar "Ver origen del mensaje"

Mozilla Thunderbird

1. Abrir el correo sospechoso

2. Hacer clic en "Mas" en la esquina superior derecha
3. Seleccionar "Ver codigo fuente"

Apple Mail (Mac)

1. Abrir el correo sospechoso
2. Ir a Vista > Mensaje > Todas las cabeceras
3. O usar el atajo Cmd + Shift + H

Yahoo Mail

1. Abrir el correo sospechoso
2. Hacer clic en los tres puntos del menu
3. Seleccionar "Ver mensaje sin formato"

Obtener el texto plano del email

El texto plano permite ver el contenido real sin formato HTML, revelando enlaces ocultos o contenido enmascarado.

Gmail

1. En "Mostrar original", buscar la seccion "text/plain"
2. Alternativamente, copiar el contenido y pegarlo en un editor de texto

Outlook

1. Abrir el correo
2. Ir a Archivo > Guardar como
3. Seleccionar formato "Solo texto (*.txt)"

Thunderbird

1. Ir a Ver > Cuerpo del mensaje como
2. Seleccionar "Texto sin formato"

Metodo universal

Seleccionar todo el contenido del correo (Ctrl+A o Cmd+A), copiar y pegar en un editor de texto plano como Notepad o TextEdit en modo texto.

Que buscar en las cabeceras

Al analizar las cabeceras, hay que prestar atencion a estos elementos clave:

Campos principales

- **From:** Direccion del remitente mostrada (puede estar falsificada)
- **Return-Path:** Direccion real de retorno
- **Received:** Cadena de servidores por los que paso el correo
- **Message-ID:** Identificador unico del mensaje
- **Date:** Fecha y hora de envio

Registros de autenticacion

- **SPF (Sender Policy Framework):** Verifica si el servidor que envio el correo esta autorizado por el dominio
- **DKIM (DomainKeys Identified Mail):** Firma digital que verifica la integridad del mensaje
- **DMARC (Domain-based Message Authentication):** Politica que combina SPF y DKIM

Senales de alerta

- Discrepancia entre el dominio en "From:" y "Return-Path:"
- Registros SPF, DKIM o DMARC con resultado "fail" o "softfail"
- Retrasos excesivos entre servidores (horas en lugar de segundos)
- Servidores de origen en paises inesperados
- Multiples saltos por servidores desconocidos

Herramientas online para analizar cabeceras

Estas herramientas gratuitas facilitan la interpretacion de las cabeceras:

MessageHeader de Google (Recomendada)

- **URL:** https://toolbox.googleapps.com/apps/messageheader/?lang=es
- Herramienta oficial de Google, disponible en espanol
- Identifica retrasos de entrega y posibles anomalias
- Muestra resultados de SPF y DKIM de forma clara

Microsoft Message Header Analyzer

- **URL:** https://mha.azurewebsites.net/
- Analisis detallado de cabeceras
- Interfaz clara y profesional

MXToolbox Email Headers

- **URL:** https://mxtoolbox.com/EmailHeaders.aspx
- Analisis completo con informacion de reputacion
- Incluye verificacion de listas negras

Mail Header Analyzer

- **URL:** https://mailheader.org/
- Interfaz sencilla
- Muestra geolocalizacion de servidores

PowerDMARC Header Analyzer

- **URL:** https://powerdmarc.com/email-header-analyzer/
- Especializado en autenticacion DMARC
- Informes detallados de SPF y DKIM

Recursos oficiales INCIBE

El Instituto Nacional de Ciberseguridad de Espana (INCIBE) proporciona guias y recursos gratuitos:

Guias de referencia

- Dudas sobre la legitimidad de un correo - Aprende a identificarlos - Guia para empresas sobre identificacion de correos fraudulentos
- Email Spoofing - Comprueba quien te envia un correo sospechoso - Guia ciudadana sobre suplantacion de identidad en correos

Contacto INCIBE

- **Linea de ayuda:** 017 (gratuito y confidencial)
- **Horario:** Todos los dias de 8:00 a 23:00
- **Web:** https://www.incibe.es

Verificadores de direcciones de correo

Para comprobar si una direccion de correo existe o es valida:

- **Captain Verify:** https://captainverify.com/mail-tester.html
- **VerifyEmailAddress:** https://www.verifyemailaddress.org/es/

Recomendaciones finales

1. **Nunca hacer clic** en enlaces de correos sospechosos
2. **No descargar adjuntos** sin verificar el remitente
3. **Contactar directamente** con la organizacion supuestamente remitente
4. **Reportar** correos fraudulentos a la entidad suplantada y a INCIBE
5. **Mantener actualizado** el software de correo y antivirus

---

Ultima actualizacion: Enero 2026

Fuentes:

- INCIBE - Instituto Nacional de Ciberseguridad
- Google Admin Toolbox
- MXToolbox

Revision #1
Created 2026-01-14 12:45:31 UTC by Abkrim
Updated 2026-01-14 12:45:31 UTC by Abkrim