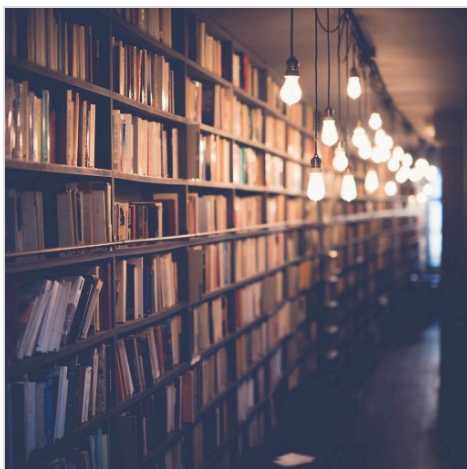


L U M B R E



# Reconocer un correo o enlace peligroso

**Materia:** Conocimientos para la Vida · Seguridad Digital

03/10/2026

## Antes de empezar

La inspección de 5 segundos que evita el 90% de los ataques: lee el correo antes de tocar.

### QUÉ APRENDERÁS

- Inspeccionar la dirección real de un enlace, verificar el dominio del remitente y reconocer las señales típicas de un correo de phishing (urgencia, adjuntos, ortografía).

## El correo: la puerta que los atacantes más intentan

### Lo que vas a saber hacer

El 90% de los ataques empiezan con un correo. Saber distinguir un remitente legítimo de un falso, y un enlace seguro de una trampa, te protege antes de que hagas clic.



*Imagen libre de Wikimedia Commons (CC BY 3.0, autor: Armando Marquez Lopez)*

VIDEO

## ¿Cómo identificar correo de estafa, fraude o phishing? #tips #tecnologia #phishing #mail #yorko

Video: identificar correos fraudulentos enlaces.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=SsnTQ-ieDEk>

## Leer un enlace antes de abrirlo

ACTIVIDAD INTERACTIVA DISPONIBLE EN  
LUMBRE

### 1. Inspeccionar antes de hacer clic



## Señales de un correo sospechoso

- Saludo genérico ("Estimado cliente") cuando te conocen por nombre.
- Errores de ortografía o traducción rara.
- Dominio que imita pero no es el oficial.
- Adjuntos inesperados (factura, "multa") o que piden "activar contenido".
- Solicitud de datos, contraseñas o pago por gift card.

## El "From" que engaña

Pueden mostrar un nombre conocido pero el correo real detrás es otro. En Gmail y otros, despliega la cabecera completa y verifica el texto entre los signos de "remitente". Ante duda, no respondas: contacta a la supuesta empresa por su canal oficial que tú escribas.

ACTIVIDAD  
INTERACTIVA  
DISPONIBLE EN  
LUMBRE

**2. Recibe un correo de "tu banco":  
"confirmación de datos urgente, haga clic  
aquí". El enlace va a banco-verificacion-  
mx.com. ¿Qué es lo correcto?**



**3. Un enlace puede mostrar un texto amable pero llevar a otra dirección.**

- ☐ Verdadero
- ☐ Falso

**4. El ataque que usa un correo falso para que reveles datos se llama**

\_\_\_\_\_.

**5. La forma MÁS segura de entrar a tu banco desde un correo que llega:**

- ☐ Usar el botón del correo
- ☐ No usar el link; abre la app o escribe tú la dirección oficial
- ☐ Responder con tus datos
- ☐ Reenviarlo para que lo revise tu familia

**6. Une cada señal con su lectura**

|    |                              |       |
|----|------------------------------|-------|
| 6. | ortografía y traducción rara | _____ |
| 6. | asunto con urgencia hoy      | _____ |
| 6. | adjunto inesperado           | _____ |
| 6. | dominio parecido pero falso  | _____ |

**Opciones:** posible fraude · presión para que no pienses · no abrir sin confirmar · suplantación

ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

**7. Palabras clave**



## Comprueba lo aprendido

**8. La próxima vez que te llegue un correo con un enlace "urgente", inspecciona la dirección real antes de abrir y verifica el dominio. Escribe un ejemplo que detectes esta semana.**

Pasa el cursor o mantén presionado.

---

---

---

---

---

## Referencia curricular

|                 |                                                |
|-----------------|------------------------------------------------|
| <b>Materia:</b> | Conocimientos para la Vida · Seguridad Digital |
|-----------------|------------------------------------------------|

Versión interactiva completa (con actividades, videos y autoevaluación):



<https://lumbre.lat/object/cvl-dig-1-004-correo-seguro>

Material educativo generado desde Lumbre · [lumbre.lat](https://lumbre.lat)