

Reconocer un correo de phishing

Las 5 señales que delatan un mensaje fraudulento — y la regla de los 60 segundos.

LAS 5 SEÑALES

1

La dirección real no coincide

Mira la dirección completa del remitente, no el nombre mostrado: paypal.com no es paypal.com.

2

Urgencia artificial

«En 24 h», «acción inmediata»: la presión es en sí misma la señal de alarma.

3

El enlace no lleva adonde muestra

Pasa el cursor sin hacer clic: el destino real aparece abajo. Pulsación larga en el móvil.

4

Adjunto inesperado

Principal vector de los ransomware. Confirma por otro canal antes de abrir — y haz copias de seguridad.

5

Petición de información sensible

Ningún organismo legítimo pide contraseñas o números de tarjeta por correo.

La regla de los 60 segundos

1. Cierra el correo — sin responder, sin hacer clic.
2. Abre una pestaña nueva y entra tú mismo en el sitio oficial.
3. Comprueba si el problema existe de verdad. Casi siempre: no.

La urgencia es su arma. El tiempo es la tuya.

Denunciar y reaccionar

Ante cualquier intento de fraude: llama gratis al 017 (INCIBE), todos los días.

Adjunto abierto por error: análisis antivirus + cambia tus contraseñas.

Ayuda oficial y gratuita: línea 017 · incibe.es