

¿QUÉ ES EL PHISHING ?



<https://www.incibe.es/ciudadania>

- 1 La dirección del remitente no coincide con el nombre de la empresa o entidad que dice ser.
- 2 El mensaje contiene errores gramaticales o de ortografía.



3 Apela a tus emociones para que accedas a las peticiones de manera urgente.

4 Facilita un enlace para realizar la gestión en cuestión.

5 Lleva adjunto un archivo que supuestamente es un documento oficial.

Fraude que consiste en enviar correos electrónicos que suplantán a entidades y empresas conocidas para engañar a los usuarios bajo cualquier excusa y robar así sus datos personales, bancarios, contraseñas, etc.

¿Has caído en el engaño? Sigue estos consejos:

- 1 Cambia tu contraseña lo antes posible si la has facilitado. Y actualiza la de otros servicios online en los que utilizaras la misma.
- 2 Contacta con tu entidad bancaria si has proporcionado datos bancarios.
- 3 Realiza búsquedas en Internet de tus datos personales para comprobar que no se estén usando.
- 4 Reenvía el correo fraudulento a INCIBE (incidencias@incibe-cert.es)
- 5 Denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado proporcionando las evidencias.
- 6 Y si aún tienes dudas, contacta con 'Tu Ayuda en Ciberseguridad' de INCIBE, llamando al 017, o a través de WhatsApp (900 116 117) o Telegram (@017INCIBE).



¿Cómo actuar ante él?
¡No respondas al email sospechoso! En caso de duda, contrasta la información con la empresa que supuestamente te está contactando a través de sus canales oficiales.

