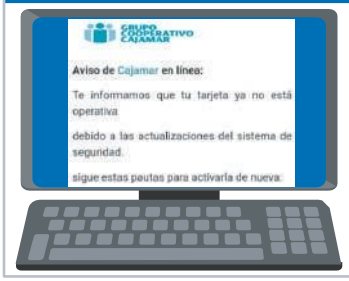
¿Cómo **identificar** un correo electrónico malicioso?

01 REMITENTE

¿Esperabas un email de esa persona/entidad?

Comprueba que el correo coincida con la persona o entidad remitente que dice ser o si está suplantando a alguien.

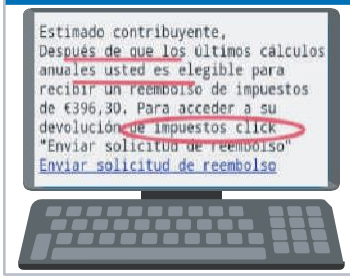
02 ASUNTO Y OBJETIVO DEL CORREO



¿Capta tu atención el asunto del correo?
La mayoría de correos fraudulentos utilizan asuntos llamativos e impactantes para captar tu atención.

¿Cuál es el objetivo del correo?
Ninguna entidad te pedirá tus datos personales por correo. Además si es de carácter de urgente, amenazante o con ofertas y promociones muy atractivas, es muy posible que sea un fraude.

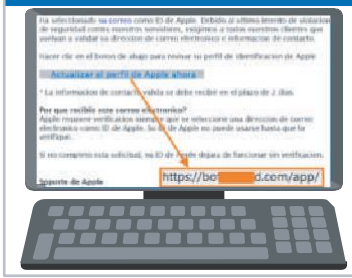
03 REDACCIÓN



¿Tiene errores ortográficos o parece una mala traducción de otros idioma?

Revisa la redacción en busca de errores de ortografía o gramaticales. Además, si no está personalizado o parece una traducción automática, sospecha.

04 ENLACES



¿Los enlaces llevan a una página legítima?

Sitúa el cursor encima del enlace, o mantén presionado el enlace en dispositivos móviles, podrás ver la URL real a la que se dirige. Si no coincide o es una web sin certificado de seguridad (https://), no hagas clic.

05 ADJUNTOS

¿Contiene un archivo adjunto que no estabas esperando o es sospechoso?

Analiza los adjuntos antes de abrirlos, puede tratarse de un *malware*. Los antivirus y analizadores de ficheros te ayudarán a identificar si están infectados.

Si tienes dudas o consultas: serviciost2d@up.edu.pe