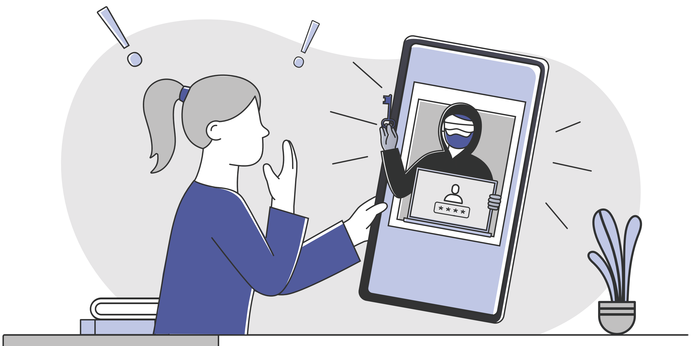
CLASICOS DEL PHISHING

A través del **phishing**, los **ciberdelincuentes** nos envían correos electrónicos en los que suplantan la identidad de diferentes entidades. En ellos nos requieren de alguna acción de manera urgente, como pinchar un link o enviar cierta información. El objetivo es **generar alarma** para obtener nuestra información personal y bancaria.



¿TE SUENAN?

Esa persona que va a bloquear tu cuenta en 48h si no la verificas.

Ese regalito que te dan a cambio de nada.

Las fotos y vídeos que van a eliminarte si no introduces el código.

El sorteo del que formas parte sin haber participado.

Esa cuenta expirada que nunca te has hecho.

La entrega reprogramada de un paquete que nunca has pedido.

¡QUE NO TE LA CUELEN!

Todos estos emails tan urgentes siempre tienen algo en común, por eso es importante que antes de caer, sigas estas recomendaciones:

Verifica la URL: asegúrate de que sea legítima y no pinches. En su defecto, accede al sitio web introduciendo manualmente la dirección directamente en el navegador o buscador.

Inspecciona la ortografía y gramática: estos correos a menudo contienen errores.

Comprueba que se **dirigen a la persona correcta** y que no se hace uso de estructuras genéricas.

Cuidado con las urgencias: a menudo incluyen amenazas o urgencias para que actúes rápidamente.

Fíjate en el remitente: si el email proviene de una dirección que parece extraña, ten precaución.

Confirma la identidad por otros medios: contacta a la empresa o entidad por teléfono, para verificar que el email sea legítimo.

Cautela con los archivos adjuntos y enlaces: estos archivos o enlaces pueden contener malware y suelen usarse acortadores de URL para enmascarar las redirecciones.

Si detectas un intento de phishing, comunícanoslo enviando un email a **incidencias@cyberzaintza.eus**