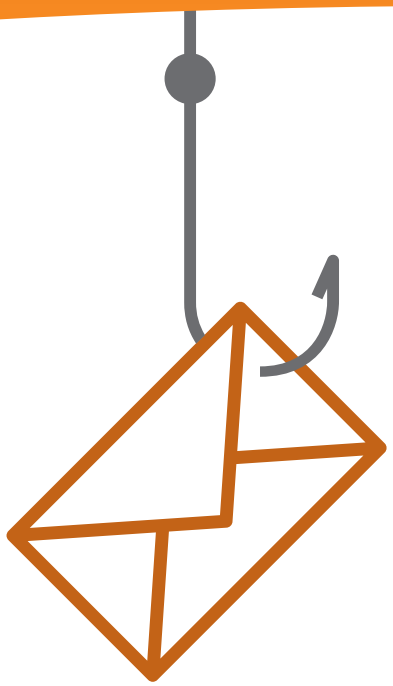
CÓMO IDENTIFICAR UN MAIL DE PHISHING

El **phishing** es el intento de engaño a través de una comunicación electrónica que simula proceder de alguien de confianza.

El ataque parte del envío de un mail o mensaje que parece provenir de una empresa, organización o persona que conocemos, con la intención de que llevemos a cabo algún tipo de acción:



- Descargar un archivo
- Pinchar sobre un enlace
- Facilitar información
- Realizar un pago

Aunque el objetivo principal de este tipo de ataques suele ser la **obtención de información confidencial** (números de tarjetas de crédito, contraseñas), en la actualidad esta técnica también se usa para **infectar equipos o para convertirnos en víctimas de algún tipo de estafa**.

El **91%** de los incidentes de seguridad empiezan con un ataque de phishing

Los mensajes suelen apelar a la necesidad de actuar con urgencia, alertarnos de algún tipo de problema, amenazarnos con posibles sanciones o seducirnos con alguna atractiva oferta.

Conoce nuestros **6 consejos** para identificar un posible mail de phishing

akcent cybersecurity

Una característica común de esta clase de mensajes es el uso de algún tipo de anzuelo para hacernos picar:

De: MusicStore <franz01@mail.com>
Para: Anna Rovira
Fecha: 17/01/18
Asunto: Tu compra en MusicStore
Adjunto: Recibo de compra.doc

Apreciado cliente,
Gracias por tu compra en MusicStore el 17/01 10:39.
Nombre del producto: 80's Greatest Hits
Número de pedido: 8EK1734-01
Total pedido: 39.56€

Si no has autorizado esta compra, por favor: **Clica aquí para tramitar una devolución**

http://mail2chef.com/senderip.php

1. **Fíjate en la dirección del remitente**. Si parece proceder de una entidad legítima pero la dirección corresponde a una cuenta personal (tipo gmail o hotmail), lo más probable es que se trate de un engaño.

2. **Desconfía siempre de los adjuntos**, especialmente si son ejecutables o contienen macros. Descarga solo aquellos que estés esperando.

3. Sospecha de mails que requieran realizar alguna **acción**, sobretodo aquellos que crean **sensación de urgencia**.

4. Desconfía de mails que contengan **saludos genéricos** ("apreciado cliente, estimado titular de la cuenta"). Pregúntate si la organización que te contacta debería conocer tu nombre.

5. No te dejes engañar por la **aparente profesionalidad** del redactado y la utilización de logos oficiales. En la actualidad ya no siempre encontramos traducciones forzadas o faltas ortográficas en los mails fraudulentos.

6. Antes de pinchar sobre un enlace **utiliza el puntero del mouse** para ver dónde te dirige. Sitúate encima (¡sin hacer click!) y no accedas si la dirección que aparece no se corresponde con el dominio de esa entidad.

Una organización con un equipo preparado para detectar mails fraudulentos es menos vulnerable a los ataques de phishing.