# Cómo identificar un correo electrónico malicioso

**Cientos de emails fraudulentos llegan a nuestras bandejas de correo y, aunque muchos son eliminados, otros consiguen su objetivo, ser leídos. Depende de nosotros saber cómo identificar un correo electrónico malicioso:**

## 1 REMITENTE

**¿Esperabas un email de esta persona/entidad?**

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

## 2 ASUNTO

**¿Capta tu atención el asunto del correo?**

La mayoría de los correos electrónicos fraudulentos utilizan asuntos llamativos o impactantes para captar tu atención. Ten en cuenta está consideración.

## 3 OBJETIVO DEL MENSAJE

**¿Cuál es el objetivo del correo?**

Una entidad de servicios como el banco, suministros del hogar (agua, gas) u otros nunca te pedirán datos personales por correo. Además, si es de carácter urgente, amenazante o con ofertas o promociones demasiado buenas para ser verdad, es muy posible que sea un fraude.

## 4 REDACCIÓN

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

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

## 5 ENLACES

**¿Los enlaces llevan a una página legítima?**

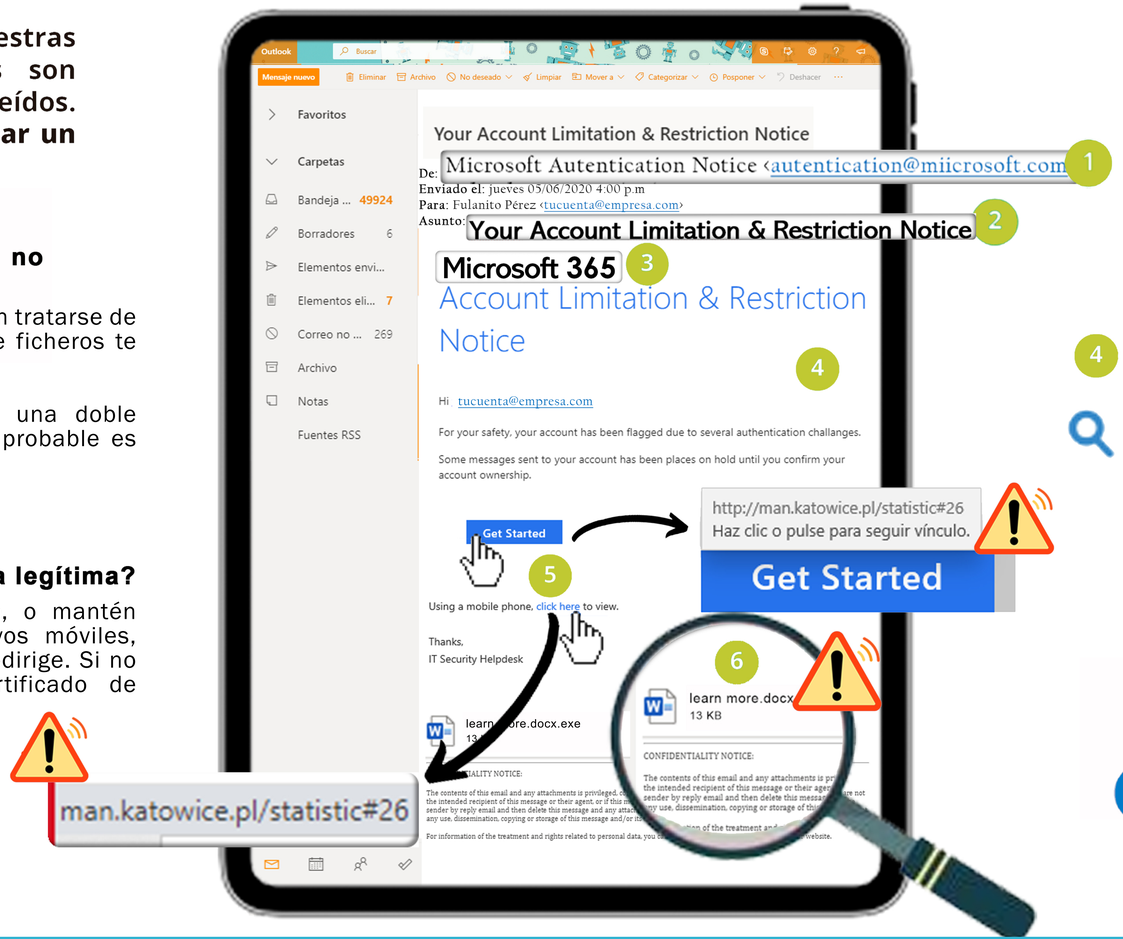
Sitúa el cursor encima del enlace, o mantén presionado el enlace en dispositivos móviles, podrás ver la URL real a la que te redirige. Si no coincide o es una web sin certificado de seguridad (https://) no hagas clic.

## 6 ADJUNTOS

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

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

También revisa que el adjunto no tenga una doble extensión (.docx.exe) si es el caso, lo más probable es que sea malware.




Finalmente, **no olvides utilizar el sentido común y aplicar todos los consejos sobre ciberseguridad e higiene de datos que te estaremos compartiendo** para convertirte en un usuario ciberseguro.

¡Sigue estos consejos y mantén tu correo libre de riesgos!

PARA MÁS INFORMACIÓN ENTRA A:

www.smartekh.com

Grupo Smartekh