



¿CÓMO IDENTIFICAR UN CORREO MALICIOSO?

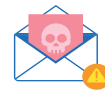
El envío de correos electrónicos falsos, maliciosos o también conocidos como *phishing*, es un método cada día más común. Los atacantes intentan suplantar la identidad de una persona, empresa o entidad con el fin de robar información y hacer uso malintencionado con ella.



Consejos para identificar un correo malicioso:

1. ¿Reconoce el remitente del mensaje?

Compruebe la dirección del mensaje detenidamente. ¡Pueden engañarlo fácilmente!



Si no conoce el remitente, no interactúe con el mensaje, lo mejor es reportarlo como *spam* o *phishing*.

Comúnmente este tipo de mensajes muestran urgencia o alerta.



Verifique la firma, puede compararla con mensajes recibidos anteriormente.



2. Verifique el contenido del mensaje.

Tenga en cuenta los errores de ortografía y gramaticales.

3. No abra enlaces desconocidos o extraños, pase el cursor por encima y verifique antes de dar clic.



4. Si sigue dudando la veracidad del mensaje, no descargue archivos con las siguientes extensiones:

.exe	.pdf
.tar	.doc, xslm o pptm
.vbs	.jpeg

Recomendaciones:

- Lea detenidamente el mensaje, remitente y firma del mensaje.
- No proporcione datos personales ni abra enlaces o archivos si desconfía.
- Reporte el mensaje como no deseado o como suplantación de identidad.
- Mantenga su equipo y antivirus actualizado. Adicionalmente analice el mensaje antes de abrirlo.



Seguir las recomendaciones ayuda a mantener un ambiente informático seguro para usted, y que su información no sea comprometida.

