



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.**

Esto sucede cuando logran pasar las barreras como el antispam del correo oficial.

Depende de nosotros saber como identificar un correo electrónico malicioso.



1. ¿Esperabas un email de esta persona/identidad?

Comprueba que el email coincida con al persona o entidad remitente que dice ser o si esta suplantado a alguien.



2. Asunto

¿Capta tu atención el asunto del correo?

La mayoría de los correos fraudulentos utilizan asuntos llamativos e impactantes para captar tu atención.

Ten en cuenta esta consideración. Premios, espacio de almacenamiento extra para Gmail, celulares, etc.



3. Objetivo del mensaje

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



4. Redacción

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

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 dirige.

Si no coincide o es una web no segura, sin certificado de seguridad (https://), no hagas clic.



6. Adjuntos

Analiza los adjuntos antes de abrirlos, puede tratarse de un malware.

Los **ANTIVIRUS** y analizadores de ficheros te ayudarán a identificar si están infectados. a la que dirige.

Si no coincide o es una web no segura, sin certificado de seguridad (https://), no hagas clic.

Departamento Redes y Conectividades
(int. 1174-1273)

redes@hcdiputados-ba.gov.ar