Microsoft

¡Piénsatelo antes de hacer clic!

Los hackers disfrazan los enlaces de phishing y los anuncios fraudulentos para que parezcan fuentes creíbles y engañarte para que hagas clic en ellos.

Los hackers usan enlaces dañinos para encontrar una manera de entrar en tus dispositivos, como tu...

- Tablet
- Teléfono
- PC

Cuando entran, pueden...

- Espiarte
- Acceder a tu cámara
- Bloquear tu dispositivo
- Robar tu información
- ...y más

Los enlaces dañinos pueden aparecer en...

- Sitios web
- Buscadores
- Mensajes de texto
- Mensajes de correo electrónico
- Publicaciones en las redes sociales
- Mensajes directos (DM)

Protégete con una buena higiene cibernética

Busca estas banderas rojas comunes del phishing

¿Qué es el phishing? El acto de usar mensajes falsos o enlaces peligrosos para intentar robar tu información.

#1 Faltas de ortografía o errores en el texto del mensaje

#2 Información de contacto incorrecta o sospechosa

#3 El enlace (o el correo electrónico del remitente) no te lleva a donde se supone que debería

#4 El mensaje transmite amenazas y urgencia

#5 Te pide que proporciones información privada

#6 Descuentos y ofertas de recompensas poco realistas

No todos los enlaces desconocidos son intentos de phishing...
También podrían ser anuncios fraudulentos.

¿Cómo se puede identificar un anuncio fraudulento?

- Los anuncios fraudulentos pueden parecerse a anuncios reales, así que no des por sentado que son legítimos solo porque llevan la etiqueta «**Anuncio**» o «**Patrocinado**»
- Puede haber señales de alerta similares a un mensaje de phishing, como solicitar datos personales y ofrecer una recompensa a cambio

Los enlaces de phishing se te envían directamente a ti, mientras que los **anuncios fraudulentos** son enlaces peligrosos con los que te encuentras.

Si recibes o abres un enlace extraño, esto es lo que puedes hacer:

¡No intentes arreglarlo tú mismo!

Cuéntaselo inmediatamente a un padre, tutor o maestro.