Microsoft

¡Piensa antes de hacer clic!

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

Los hackers usan enlaces malos para encontrar una manera de ingresar a tus dispositivos, como tu...

- Tablet
- Teléfono
- Computador

Cuando entran, pueden...

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

Los malos enlaces pueden estar en...

- Sitios web
- Buscadores
- Mensajes de texto
- Correos electrónicos
- Publicaciones en redes sociales
- Mensajes directos (DM)

¡Protégete con cuidados cibernéticos!

Busca estas banderas rojas comunes de phishing

¿Qué es el phishing? ¡El acto de usar mensajes falsos o enlaces peligrosos para tratar de robar tu información!

#1 Errores ortográficos o errores en el texto del mensaje

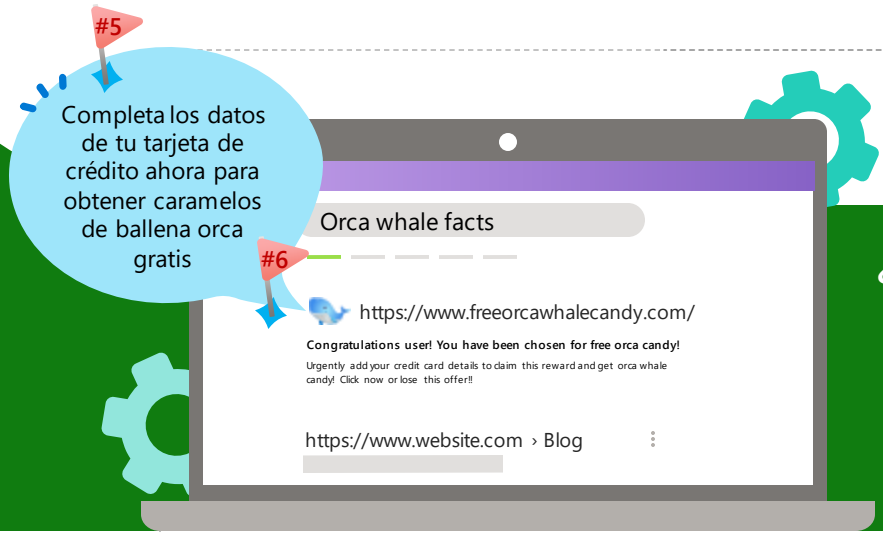
#2 Información de contacto incorrecta o sospechosa

#3 El enlace (o el correo electrónico del remitente) no va a donde esperarías

#4 El mensaje transmite amenaza y urgencia

#5 Te pide que proporciones información privada

#6 Ofertas y gangas



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

¿Cómo se puede identificar un anuncio fraudulento?

- Los anuncios fraudulentos se pueden hacer parecer anuncios reales, así que no asuma que son legítimos solo porque tienen una etiqueta de "Anuncio" o "Patrocinado"
- Puede tener señales de alerta similares a un mensaje de phishing, como solicitar datos personales y ofrecerte recompensas a cambio.

Enlaces de phishing son enviados, 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!

Díle inmediatamente a un padre, tutor o maestro.