¿Cómo identificar un *enlace malicioso?*

¡Cuidado con los enlaces de phishing! Pueden llevarte a sitios fraudulentos que buscan obtener tus datos.
Antes de hacer clic, sigue estos consejos:

1

Revisa la ortografía

Los enlaces maliciosos a menudo tienen errores ortográficos o variaciones sutiles en los nombres de dominio, por ejemplo:

"http://microsft.com" en lugar de
"http://microsoft.com"

2

Examina enlaces abreviados

Cuidado con los enlaces cortos, verifica la URL antes de hacer clic y usa un expansor si es necesario. Puede que Microsoft mande algo así:

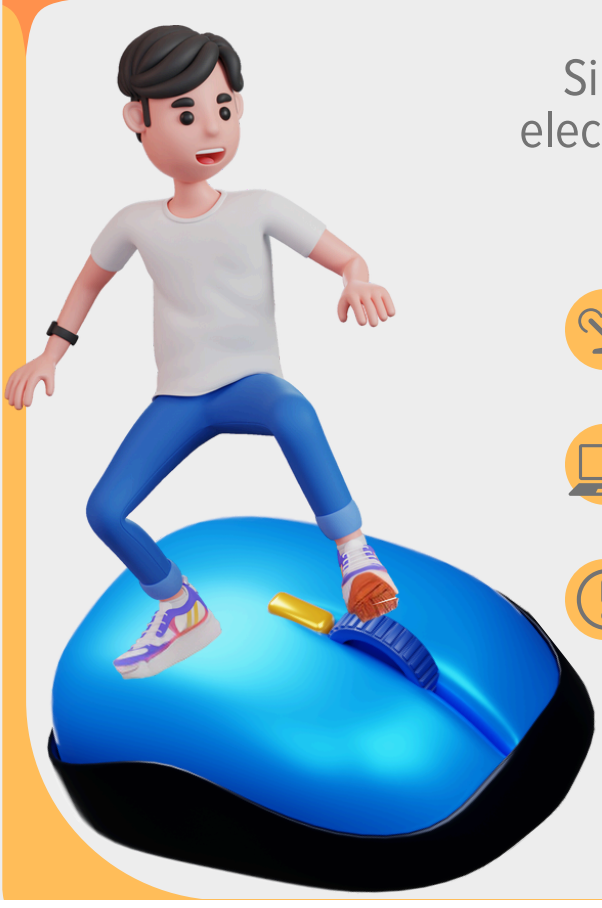
“https://shorturl.at/H46q7” y no
"http://microsoft.com"

3

Busca números y guiones

Los enlaces con muchos números o guiones pueden ser sospechosos. Los sitios legítimos rara vez usan excesivamente estos caracteres en sus URLs. No es lo mismo:

"http://microsoft-secre1-online.com" que
"http://microsoft/secureonline.com"



Si recibes un enlace en un correo electrónico del que sospechas, debes hacer esto:

- Pasa el ratón por encima del enlace para comprobar el destino real.
- Escribe la dirección manualmente (no interactúes con el enlace que enviaron).
- Denuncia inmediatamente el correo electrónico.

TU LOGO AQUÍ