How to identify a *malicious link?*

Beware of phishing links! They can take you to fraudulent sites that seek to obtain your data. Before clicking, follow these tips:

1

Check spelling

Malicious links often have misspellings or subtle variations in domain names, for example:

“http://microsft.com” instead of **”http://microsoft.com”**

2

Browse abbreviated links

Beware of short links, check the URL before clicking and use an expander if necessary. Microsoft may send something like this:

“https://shorturl.at/H46q7” and not **”http://microsoft.com”**

3

Search for numbers and dashes

Links with lots of numbers or hyphens can be suspicious. Legitimate sites rarely overuse these characters in their URLs. It is not the same:

“http://microsoft-secre1-online.com” than **”http://microsoft/secureonline.com”**

If you receive a link in an email that you suspect, you should do this:

- Hover your mouse over the link to check the actual destination.
- Type the address manually (do not interact with the link they sent).
- Immediately report the e-mail.

TU LOGO AQUÍ

Grupo Smartekh | Security Culture Management

La creación de este material petenece a Grupo Smartekh