How-To-Document Resource:
How to recognize typosquatting

What is typosquatting and how to recognize it.

Typosquatting, also called ***URL hijacking***, a sting site, or a fake URL, is a form of cybersquatting, and possibly brandjacking which relies on mistakes such as typos made by Internet users when inputting a website address into a web browser.

The typosquatter's URL will usually be one of five kinds, all similar to the victim site address:
A common misspelling, or foreign language spelling, of the intended site
A misspelling based on a typographical error
A plural of a singular domain name
A different top-level domain: (i.e. .com instead of .org)
An abuse of the Country Code Top-Level Domain (ccTLD) (.cm, .co, or .om instead of .com)

Examples

'Goggle.com'
Google called 'Goggle.com' has existed which was considered a phishing/fraud site. A 2018 check revealed it to redirect users to adware pages, and a 2020 attempt to access the site through a private DNS resolver hosted by AdGuard resulted in the page being identified as malware and blocked for the user's security.

‘yuube.com’
yuube.com, targeting YouTube users by having it programmed to redirect to a malicious website or page, that asks users to add a security check extension that is really malware

‘microaoft.com’
microaoft.com was set up to show what looked like the Microsoft main site, but would show false malware warnings urging users to call them, which likely led to cases of tech support scam.