Identifying a Fake URL

What is a Fake URL?

A URL (Uniform Resource Locator) is the address for a website. A fake URL is a URL that looks like it leads to one website but actually leads to a different website. Some hackers use fake URLs to trick unsuspecting users into downloading malware or sharing personal information. To stay safe, we must learn how to identify a real URL from a fake URL.

What to Look For

- Source - Many fake URLs come from questionable sources like spam emails and fake social media accounts.
- Misspellings - Typosquatting describes URLs with a website name misspelled or with different punctuation (e.g., amzon.com instead of amazon.com).
- Domain Name - Comobsquatting describes URLs with second-level domains that include more than just the brand name (e.g., amazonTVs.com instead of amazon.com).
- Shortened - Shortened URLs are long URLs that were compressed. Hackers use them to pass filters and confuse users about where the URL leads to.

How to Stay Safe

- Use URL scanners like urlscan.io or virustotal.com to scan for malware or phishing before clicking on a URL.
- Use URL unshorteners like checkshorturl.com to expand a short URL.
- Do not always assume that a URL with https:// is safe.
- Do not quickly click URLs out of habit. Take some extra time to examine a URL for safety first.