Analyzing a URL

Learn strategies for analyzing URLs and avoiding unsafe or risky URLs.

1. What are the parts of a URL?

To analyze a Universal Resource Locator (URL), it helps to know what the different parts of a URL are and what you should expect to see. Let's look at a sample URL: https://www.microsoft.com/en-us/

Example	Part of URL	Explanation and Definition	Risk Factors
https	Protocol	The protocol describes how a web browser should retrieve the information from the URL.	The key here is to look for "https" or secure protocol. URLs with "http" aren't secured and are considered risky.
www.microsoft.com	Domain	The domain is the name of the website and the type of website this is. Domains consist of a second-level and a top-level domain. In this case, the second-level domain is "www.microsoft" and the top level domain is ".com," which indicates it is a commercial site.	Domains are where scammers can hide things or trick people. For instance, scammers might use a risky top-level domain and pair it with a trusted second-level domain to fool people. An example of this could be "www.microsoft.xyz"
/en-us/	Path	The path indicates the specific page or resource you'll be accessing from the website. In this case, the path indicates we are visiting the English language US version of the Microsoft website.	Scammers might include trackers or strange symbols in the file path. Note that a scammer might use a shortened URL, like a bit.ly, to hide the suspicious nature of their URL paths.

2. How can you analyze a URL and determine if it is safe?

Here are some things to look for when analyzing a URL.

Protocol

- **Pay attention to the protocol:** Remember to check for "https" or secure protocol. If you aren't seeing a https protocol, look up what you are seeing to determine if it is secure, and don't click the link until you are sure it is secure.

Domain and Path

- **Pay attention to the details in the domain and the path:** Look for things like small spelling errors, a strange top-level domain, or odd symbols. These can often be a sign of a risky or unsafe URL.
- **Pay attention to the whole domain:** Scammers will often add on extra, suspicious elements to a domain that otherwise looks trustworthy. Don't be fooled by a trusted element in a domain; instead, pay attention to the entire thing and make sure the whole domain is legitimate.
- **Remember that the top-level domain comes last:** Domains go from second to top-level domains, meaning that the top-level domain is the last thing you see before the path. Scammers will often use a legitimate looking second-level domain to trick people. Pay attention to everything between the protocol "https" and the "/" sign.
- **Investigate shortened or customized URLs:** It is very easy to shorten a URL or to make a customized link for an email. Use a tool (see below) to check these types of URLs before clicking on them. Shortened URLs can be a good way for a scammer to hide malicious links!

Here are some examples of risky URLs using the famous fictional school, Hudson University:

Hudsonuniversity.edulogin.com

In this example, the actual top-level domain is ".com" and the scammer merged in the path with the domain to fool people. A legitimate version of this would look more like the following: hudsonuniversity.edu/login

Hudsoununiversity.edu

In this example, the word Hudson is misspelled as "Hudsoun." This technique is often used by scammers to get people to click on bogus links that, at first glance, look fine.

http://hudsonuniversity.edu.student_login%.ie

This example contains many issues! First, this link used the insecure http protocol. Second, the domain name here is actually "student_login%.ie" and not "hudsonuniversity.edu." Remember, the top-level domain comes last! Finally, this domain contains odd symbols, which can be the sign of an unsafe URL.

3. How can you investigate URLs?

There are many tools and resources that you can use to investigate URLs.

Reputation checkers: These types of sites can check the reputation of a URL or IP address and warn you if it is suspicious or malicious.

https://www.urlvoid.com/
https://www.virustotal.com/gui/home/url

URL extenders and IP lookups: These tools can be used to investigate shortened URLs or IP addresses. Remember, shortened URLs are often used to hide malicious URLs.

https://checkshorturl.com/
https://www.expandurl.net/
https://www.ipvoid.com/

Sandboxes. These sites let you scan and analyze a URL before you commit to clicking it

https://urlscan.io/

Finally, most web browsers have security features that warn you if a URL is malicious. Pay attention to these warnings in case you accidentally click something you shouldn't!

For some bonus URL analysis practice, explore the links listed above and see if you can determine how and why they are legitimate!