Analyzing a URL

In This Module

- What are the different parts of a URL?
- How can we analyze a URL?
- What are some signs of a malicious or risky URL?

What Risks Can Malicious URLs Pose?

Malicious URLs:

- Can be used in phishing schemes to gain access to your information
- Can expose you to malware and viruses

What Are the Parts of a URL?

https://www.examplewebsite.org/en

Protocol. The first part of a URL is the protocol, or the way a browser should access the information. HTTPS is considered secure protocol. If you see a URL with “http” instead, be wary since this is not secured protocol.

What Are the Parts of a URL?

https://www.examplewebsite.org/en

Domain. The domain is the heart of the URL and indicates where the URL is going. The final part (.org) is the top-level domain and says what kind of site it is. For example, .com is a commerce site and .gov is a government one.

What Are the Parts of a URL?

https://www.examplewebsite.org/en

Path. This final part specifies the specific page or resource you're visiting. In this case, "en" refers to an English language version of a site.

Signs of a Malicious URL

- Issues in the domain such as:
  - Spelling errors
  - Excessive hyphens
  - Odd symbols
- Suspicious top-level domains
- Shortened URLs that are hiding the full URL

Activity

What warning signs do you see in this URL?

Hudsonuniversity.edulogin.com

Activity

What warning signs do you see in this URL?

http://hudsoununiversity.edu.student-login%.ie

Analyzing Malicious URLs

In the example **Hudsonuniversity.edulogin.com**:

- The actual top-level domain is ".com." 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

Analyzing Malicious URLs

In the example **http://hudsoununiversity.edu.student-login%.ie**:

- The domain name here is actually “student_login%.ie” and not “hudsonuniversity.edu”
- There’s a spelling error (hudsoun instead of hudson)
- The domain contains odd symbols

Tactics Used by Scammers

Cybersquatting: Scammers will take legitimate URLs and use bogus top-level domains as a way to fool people. An example of this could be microsoft.co (instead of .com) or facebookcom.xyz/login (an xyz domain instead of the actual .com)

Typosquatting: With this approach, scammers will include a small spelling error as a way to trick people. An example of this would be Microsft (instead of Microsoft) or Appple (instead of Apple)

Tactics Used by Scammers

Trusted terms: Phishing schemes often include words like “login,” “bank,” “account,” etc. in their phony URLs to get people to click.

Shortened URLs: Scammers often shorten or hide the URL so that you can’t fully see what you are actually clicking on and visiting.

Avoiding Malicious URLs

- **Pay attention to the context:** Is this URL part of a suspicious email or an overly urgent text message? If you are seeing signs of a scam, do not click!
- **Pay attention to the URL:** Look for spelling errors, symbols, or other issues with the top-level domain or protocol

Avoiding Malicious URLs

- **Use a tool to help**: Tools like URL extenders can help you see what exactly a shortened URL is concealing
- **Hover over links**: You can also hover over links to see what they are, but some scammers have found ways to avoid this sort of detection. If you are still unsure, use a tool to check

Takeaways

- Remember that scammers often use malicious URLs to obtain access to your data and expose you to malware and other risks
- The best defense against malicious URLs is to not click on them!
- Pay attention to what you are seeing with the URL and be on the alert for errors, strange details, and overall signs of a scam
- Use tools and resources to check on URLs before you click them

Resources

Reputation Checkers

Check the reputation of a URL or IP address

URL Void (link)

Virus Total (link)

Resources

URL Extenders and IP Lookups

Investigate shortened URLs or IP addresses

CheckShortURL (link)

Expand URL (link)

Resources

Sandboxes

Scan and analyze a URL before you commit to clicking it

URL Scan (link)

Questions?

NYC Digital Safety

Privacy & Security