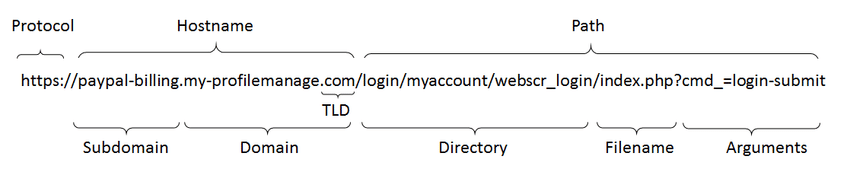
# Detecting Malicious URL

**Problem domain - Phishing, Spamming, Malware, Spoofing**

Malicious URLs are one of the most common cybersecurity threats. They are commonly spread through email, advertisements, web search, social media or links from other websites. There are several methods to identify phishing websites and I would like to focus on the method that uses features of a URL to detect the malicious ones.

A URL is composed of different parts, some mandatory and others optional. The most important parts are as below:



Phishers usually try to make the Internet address (URL) of phishing sites look similar to legitimate sites to deceive online users. They make one or two spelling mistakes in the features of URL such as Domain, SubDomain to make it look similar to a legit website.

In this research paper I would like to identify techniques to detect phishing sites effectively.

**References:**

J. Yuan, G. Chen, S. Tian and X. Pei, "Malicious URL Detection Based on a Parallel Neural Joint Model," in IEEE Access, vol. 9, pp. 9464-9472, 2021, doi: 10.1109/ACCESS.2021.3049625.

URL: <https://ieeexplore-ieee-org.proxy.library.nyu.edu/stamp/stamp.jsp?tp=&arnumber=9316171&isnumber=9312710>

X. Yan, Y. Xu, B. Cui, S. Zhang, T. Guo and C. Li, "Learning URL Embedding for Malicious Website Detection," in IEEE Transactions on Industrial Informatics, vol. 16, no. 10, pp. 6673-6681, Oct. 2020, doi: 10.1109/TII.2020.2977886.

URL: <https://ieeexplore-ieee-org.proxy.library.nyu.edu/stamp/stamp.jsp?tp=&arnumber=9022897&isnumber=9128058>

W. Yang, W. Zuo and B. Cui, "Detecting Malicious URLs via a Keyword-Based Convolutional Gated-Recurrent-Unit Neural Network," in *IEEE Access*, vol. 7, pp. 29891-29900, 2019, doi: 10.1109/ACCESS.2019.2895751.  
URL: <https://ieeexplore-ieee-org.proxy.library.nyu.edu/stamp/stamp.jsp?tp=&arnumber=8629082&isnumber=8600701>