A logo with a star

Description automatically generated

# **Phishing Link Detector Script Documentation**

## ITSC-203 – Scripting for Tool Construction

## Name: Yousuf Azhar Abdul Quddus

## Student ID: 000871519

## Instructor: Andrew Campbell

##### Reconnaissance:

###### Classifications of phishing links through mentors and online research (citations):

* **Static Analysis:** VirusTotals’ Indicators of Compromise (IOCs)
  + Unusual email domain: Awkward URL patterns / Misspelling within the URL.
  + Domain age: ensure the domain is not new and has been open for a decent amount of time.
  + URL length: length is unnecessarily long or unusual.
  + Spelling mistakes within the domains/sub-domains.
  + Ensure website is using https rather than http: not always the case but can be one check that can be considered.
  + Check against websites whether the link is compromised.
* **Dynamic Analysis / Sandboxing:** Hybrid Analysis:
  + Check header to see if any file is being executed upon opening link.
  + Check and open link in a sandbox environment.
  + Places the computer in an isolated environment from the rest of the networks, ensuring host machines or other devices on the network do not get affected in the process.
  + Analyzing Webpage Content: checking visual appearance to see mimicking of an existing site alongside checking embedded JavaScript execution
* **Dynamic Analysis Traffic Monitoring:** 
  + Capturing select packets that may indicate phishing attempts and put into a file for further analysis.

The most efficient approaches include **dynamic analysis**, **behavioral monitoring**, and **sandboxing**.

##### Requirements:

* **#pip install requests**
  + *Used for VirusTotal’s API.*
* **#pip install python-dotenv**
  + Used for .env file to use API key

##### Citations:

* Personal Mentor:

Hassan Saffar: Cybersecurity Specialist & Analyst @ IBM | SOC Analyst | Team Lead

* <https://www.virustotal.com/gui/home/upload>