Assignment- Anti Phishing Prediction

Anti-phishing refers to efforts to block phishing attacks. Phishing is a kind of cybercrime where attackers pose as known or trusted entities and contact individuals through email, text or telephone and ask them to share sensitive information. Typically, in a phishing email attack, and the message will suggest that there is a problem with an invoice, that there has been suspicious activity on an account, or that the user must login to verify an account or password. Users may also be prompted to enter credit card information or bank account details as well as other sensitive data. Once this information is collected, attackers may use it to access accounts, steal data and identities, and download malware onto the user's computer.

Content

This dataset contains 48 features extracted from 5000 phishing webpages and 5000 legitimate webpages, which were downloaded from January to May 2015 and from May to June 2017. An improved feature extraction technique is employed by leveraging the browser automation framework (i.e., Selenium WebDriver), which is more precise and robust compared to the parsing approach based on regular expressions.

Anti-phishing researchers and experts may find this dataset useful for phishing features analysis, conducting rapid proof of concept experiments or benchmarking phishing classification models.

Submission : 20th Feb, 2022

Please send the assignment to "projects.tcrinnovation@gmail.com"