Project Title

Detecting brand squatting domains used for phishing attacks

Project Description:

This project is designed to protect prominent brands, such as qatarairways.com, from malicious squatting domains (e.g., combosquatting, bitsquatting). It encompasses frontend development, API integration, and backend model implementation. It will provide granular solutions with different performances, including registration time, passive DNS time, and certificate creation time solutions. For a given brand, registration records will be analyzed to identify malicious squatting domains.

Project Type: Research or Engineering

Internship Batch:

- **Batch 1:** May 11 to July 10, suitable for Education City students, i.e., CMUQ, TAMUQ and HBKU students

Duties/Activities:

- Implement and optimize backend models for domain squatting detection.
- Conduct data analysis on domain registration records to detect malicious activity.
- Collaborate with the team to refine detection models and improve system performance.
- Develop and enhance the frontend using React.
- Integrate APIs to facilitate real-time data processing.

Required Skills: React, Phyton

Preferred Intern Academic Level: Undergraduate (Senior) or Graduate students in Computer Science, Cybersecurity, Data Science, or a related field.

Learning Opportunities:

- Gain hands-on experience in cybersecurity and domain protection.
- Work with real-world datasets to identify phishing threats.
- Learn about Graph Neural Networks, contrastive learning and their application in security.
- Improve skills in React development, API integration, and Python-based security analysis.

Expected Team Size: A team of 2 members

Mentors

Name: Dr. Fatih Deniz Email: fdeniz@hbku.edu.qa