



**Ministry of Higher Education
and Scientific Research, Iraq**

University of Babylon

Information Technology College

**Information Security
Department**

Study: (morning)



Detecting Phishing Websites With Machine Learning

**A Graduate Project Submitted to the Department of Information Security of
the College of Information Technology, University of Babylon, in Partial
Fulfillment of the Requirements for the Bachelor's degree in Information
Security of Information Technology.**

By

Liqaa Latif jawad Al-Taee

Supervised by

Assistant Lecturer. Israa Saleh Kamil

2023-2024

Abstract

In the contemporary digital landscape, phishing attacks stand out as a pervasive cyber threat, wherein counterfeit websites are meticulously crafted to deceive users. Leveraging a combination of social engineering tactics and malware strategies, these attacks pose a significant menace to both individuals and organizations alike. Given that users rely extensively on web links or URLs to navigate the online realm, there exists a pressing need to cultivate awareness regarding phishing schemes, their detection, and the imperative of adopting preventative measures.

To tackle this issue effectively, our project endeavors to develop a robust methodology for discerning fraudulent (phishing) websites by analyzing extracted features from their URLs. Subsequently, we employ a supervised machine learning approach, specifically the Support Vector Machine algorithm, to construct a predictive model capable of identifying novel instances of deceptive websites. Encouragingly, our experimental findings underscore the efficacy of our chosen methodology, demonstrating an impressive accuracy rate of 90.5 %