Chapter 3
A Novel Phishing Attack Prediction Model With Crowdsouring in Wireless Networks

Senthilkumar Subramanian
University College of Engineering, BIT Campus, Anna University, Tiruchirappalli, India

Nithya Venkatachalam
University College of Engineering, Villupuram, Anna University, India

Regan Rajendran
University College of Engineering, Villupuram, Anna University, India

ABSTRACT

As the web and applications for knowledge technology developed, many attacks and security problems started to emerge. The last couple of years have seen a significant development in 6G wireless networking. It is challenging to create a secure wireless network. In phishing attacks on wireless networks, attackers create phishing websites that allow users to enter personal information such as usernames, passwords, security numbers, and credit card details. Phishing emails that contain links to websites that are used to spread malware. This project suggests a real time phishing detection plug-in for the web browser which uses a random forest classifier to identify and notify users. As a result, the consumer can get an alert right away. The suggested systems specify wireless phishing attack detection in the current context and produce superior results. The authors proposed 18 traits in order to cover every aspect of phish behavior. With the help of an accepted dataset, the suggested phishing detection system was trained.

DOI: 10.4018/978-1-6684-8306-0.ch003

INTRODUCTION

Network users gain from developing and using the Internet in various ways. Security is becoming crucial due to the widespread use of networks, yet, Wireless devices, computers, networks, data, applications, etc., are all strongly tied to wireless security. Wireless networks can easily access, modify, and disrupt those systems because there are more and more web connection in schools, e-markets, hospitals, banks, and the armed forces. Smartphone have become the go-to electronic devices for most people because of their low cost, ease of use, small size, and battery life. As the use of mobile phone has grown, so too have the security risks associated with them. Attackers now frequently target wireless gadgets. Attackers solicit the user's private information by sending SMS links to phishing Web Pages. The privacy of user data on networks has emerged as one of the most important research concerns because wireless networks make a vast amount of data readily available. The usage of mobile phishing assaults results in numerous incidences of privacy infringement. It is challenging to protect wireless networks from phishing and other assaults since they provide open access. When using a Wi-Fi to Wi-Fi connection, regular consumers must be aware of security precautions and are more susceptible to phishing scams(Goel, D., & Jain, A. K. 2018). In this phishing attack, the "No Internet Connection" web page is displayed in the victim's browser to trick him into thinking he does not have an internet connection. The victim may notice Google Chrome with the message "Unable to Connect to the Internet" if they use that particular browser. The victim is operating Windows; therefore, the same header allows us to display a web-based mimic of Windows network manager.

In the review "Phishing Insights 2021" by Sophos, researcher insecurity claims that phishing attempts against enterprises increased significantly during the pandemic as millions of employees working from home became a primary target for hackers. According to 60% of IT teams, the number of phishing emails aimed at employees grew in 2020. It was possible to identify which phishing URLs were related to each issue by analyzing them globally between January 2020 and February 2021, COVID-related topics, keywords created and applying to match. We discovered that between December 2020 and February 2021, phishing attempts about and targeting pharmacies and hospitals increased by 189%, while vaccine-related phishing assaults increased by 530%. Software as a Service (Saas), webmail, and phishing attacks reached 22.2% in a quarter, according to Comparitech Security Company's study on attack data for 2019–2021. As a result, financial institutions now represent the majority of targets (22.5%). As shown in figure 1 below, assaults against payment and e-commerce platforms have increased by a small percentage.

Figure 1. Most targeted industries 2020