EPiC Series in Computing

Volume 106, 2025, Pages 114–121

Proceedings of the 20th Asia Joint Conference on Information Security

Phishing Attack Simulation and Detection Strategies: A Case Study on NTNU Moodle Platform

Yao Yu Lee[1] and Albert Guan[2]

[1] Department of Computer Science and Information Engineering, National Taiwan Normal University
e0900115866@gmail.com

[2] Department of Computer Science and Information Engineering, National Taiwan Normal University
albert.zj.guan@gmail.com

Abstract

With the development of the digital society, phishing attacks have become an increasingly serious cybersecurity threat, posing risks not only to general users but also serving as a common initial intrusion method in Advanced Persistent Threat (APT) attacks. In this study, we simulated a phishing attack targeting the Moodle system of National Taiwan Normal University and collected 104 valid survey responses to investigate phishing website recognition behaviors. The results indicate that checking the URL is one of the most effective methods for users to identify phishing websites. In the future, we plan to develop a browser extension integrated with Large Language Models (LLMs) to automatically detect high-risk phishing websites and provide real-time warnings to users, thereby enhancing overall protection capabilities.

Keywords Phishing, URL, Social Engineering, Phishing Attack Simulation, Phishing Detection.

1 Introduction

In recent years, the number and frequency of phishing attacks have continued to rise, posing a significant challenge for information security protection. According to the Anti-Phishing Working Group (APWG) 2023 Q4 report, a total of 4,987,809 phishing attack incidents were observed globally in 2023, setting a new historical record [1]. This highlights that phishing attacks have become a major threat that cannot be ignored in the modern cybersecurity landscape.

1.1 Phishing Techniques

Phishing is an attack method that combines social engineering and fraud. Attackers typically impersonate legitimate websites and use channels such as emails, text messages, messaging apps, or social media platforms to lure victims into voluntarily disclosing sensitive personal information, such as account credentials, passwords, or credit card numbers [2]. With the widespread adoption and simplification of website-building technologies, the technical barrier

to setting up phishing websites has been significantly lowered. Modern counterfeit websites also exhibit a high degree of visual similarity to legitimate sites, further enhancing the stealthiness of such attacks. Users often find it difficult to distinguish between real and fake websites based solely on UI (user interface) differences, a finding that is also supported by the experimental results of this study.

According to the APWG report, in the fourth quarter of 2016, fewer than 10% of phishing websites used the HTTPS protocol. By the second quarter of 2020, more than 70% of phishing websites had adopted HTTPS [3]. This shift is mainly attributed to modern browsers displaying "Not Secure" warnings on HTTP pages, making unencrypted phishing websites easier to detect. Moreover, the widespread availability of free and automated SSL/TLS certificate services (such as Let's Encrypt) has enabled attackers to easily obtain valid certificates and apply HTTPS to phishing sites, thereby deceiving users' intuitive judgments about security. This phenomenon has seriously challenged traditional user behavior that relied on the presence of HTTPS as a safety indicator.

1.2 APT and Phishing

Advanced Persistent Threats (APTs) are sophisticated cyberattacks targeting specific high-value entities, characterized by high levels of stealth and long-term infiltration. Typical targets include government agencies, military units, large enterprises, and critical infrastructure. APT attackers often employ a combination of social engineering, vulnerability exploitation, malware deployment, and other techniques to infiltrate target systems in stages and operate covertly over extended periods to achieve strategic objectives.

Phishing attacks are commonly used as an effective initial penetration method in APT campaigns. Attackers craft phishing emails or social messages to lure victims into voluntarily providing credentials or executing malicious programs. Studies have shown that in cases involving Iranian APT groups, over 50% of the initial intrusions were carried out through phishing methods. For example, attackers would forge Google Drive sharing links to trick victims into visiting a fake Google login page and stealing their credentials [4]. Such attacks often feature highly realistic webpage designs and valid SSL certificates, making it difficult even for security-aware users to recognize anomalies immediately.

After successfully using phishing to gain initial access, APT attackers often move laterally within networks, escalate privileges, and ultimately achieve goals such as data theft, infrastructure disruption, or intelligence gathering. Therefore, phishing attacks are not isolated incidents but are critical first steps in the broader infiltration chain, significantly reducing overall penetration costs and increasing attack success rates.

1.3 Real-World Cases of Phishing

In the real world, one of the most common phishing techniques involves attackers impersonating websites frequently used by the public, such as Facebook (as shown in Figure 1). Victims are lured to these fake websites via social media or other channels and are tricked into entering their account credentials. Once attackers obtain these credentials, they can directly hijack the victims' accounts and may further launch credential stuffing attacks, increasing the risk of compromising accounts on other platforms.

Additionally, phishing attacks are often seen in financial fraud scenarios. Attackers impersonate payment platforms or banking websites to lure victims into entering credit card information on fake payment pages, leading to theft of funds or fraudulent transactions, and resulting in significant financial losses for the victims.

Figure 1: Fake Facebook UI

2 Research Objectives

Based on the aforementioned background, this study simulates phishing attacks targeting the Moodle system of National Taiwan Normal University. We built a realistic phishing website to explore the implementation process of phishing attacks and corresponding defense strategies. To further quantify user recognition behavior under different scenarios, we designed a questionnaire and successfully collected 104 valid samples. The survey focused on the impact of URL display and device type (desktop vs. mobile) on users' ability to identify phishing websites.

Through this study, we aim to gain a deeper understanding of the key factors that affect users' phishing site recognition accuracy, and to propose specific and practical defense recommendations, thereby enhancing public awareness and cybersecurity resilience against phishing attacks.

3 Research Methodology

This study is divided into two major parts: phishing website simulation and questionnaire design. The following sections detail each step of the process:

3.1 Phishing Website Simulation

- **Web Interface Simulation**: A Python script was used to crawl resources from the National Taiwan Normal University (NTNU) Moodle login page, including HTML, CSS, and JavaScript files, along with necessary icon assets from Font Awesome. After obtaining an initial local copy, the HTML structure and resource links were manually corrected to ensure that the webpage appearance and interactive functionality closely matched the official site.

- **Backend Phishing System Development**: Flask was used as the backend framework to implement server-side functionalities for the phishing website. When users entered their account credentials on the page, the information was submitted via forms and securely stored in a database or file system for subsequent analysis. To lower users' suspicion, after collecting credentials, the system automatically redirected victims to the official Moodle login page to simulate a real login experience.
- **Phishing Domain Registration and Deployment**: To increase the credibility of the phishing website, a domain name highly similar to the official site (`moodle3.ntnu.edu.tw`) was registered, namely `ntnu.work.gd`, with a subdomain `moodle3.ntnu.work.gd` created. A valid SSL certificate was applied for and installed to avoid browser security warnings. The phishing site also mimicked multiple common paths from the official system, such as `/`, `/login/`, and `/login/index.php`, to further enhance realism and deception.

3.2 Questionnaire Survey Design

To quantitatively analyze users' ability to recognize phishing websites under different scenarios, a questionnaire survey was designed and conducted with the following process:

- A total of 104 valid responses were collected.
- Respondents were divided into four scenario groups: desktop with URL hidden, mobile with URL hidden, desktop with URL visible, and mobile with URL visible.
- Each respondent was required to complete two tasks:
  - Subjectively rate the similarity (on a scale of 1 to 5) between the presented webpage and the official site.
  - Select the version they believed to be the official website from given options.

Examples of the webpage interfaces shown in the questionnaire are illustrated from Figure 2 to Figure 5, namely the real desktop website (Figure 2), the fake desktop website (Figure 3), the real mobile website (Figure 4), and the fake mobile website (Figure 5).

Through the dual experimental design of phishing website simulation and questionnaire survey, this study explores the factors affecting users' phishing site recognition behavior and provides a foundation for subsequent defense strategies.

Figure 2: Real desktop UI

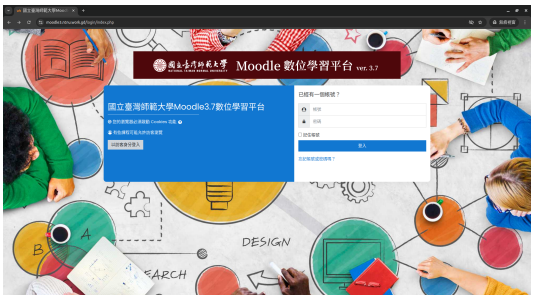

Figure 3: Fake desktop UI

Figure 4: Real mobile UI

4 Experimental Results

4.1 Basic Survey of Participants

According to the survey results, as many as 80.2% of respondents reported having encountered phishing attacks. However, only 32.7% stated that they proactively check URL authenticity more than half of the time during daily browsing. Furthermore, only 29.8% indicated that they would immediately change their account passwords upon encountering a webpage redirection to prevent account compromise.

These findings suggest that although most users have experience with phishing attacks, their overall vigilance and preventive behaviors against phishing threats remain insufficient. This also validates the effectiveness and deceptive nature of the "redirection strategy" commonly employed in phishing attacks.

Figure 5: Fake mobile UI

4.2 Results of the NTNU Moodle Phishing Experiment

In the simulated phishing attack targeting the National Taiwan Normal University Moodle system, the survey results showed that participants in the groups where URL information was visible exhibited significantly higher phishing site recognition accuracy compared to those in the URL-hidden groups. This further confirms the critical role of URL information in distinguishing between real and fake websites.

The experimental data for each group are summarized as follows:

Table 1: Statistics of Similarity Scores and Recognition Accuracy Across Groups

Group	Average Similarity Score	Recognition Accuracy
Desktop (URL Hidden)	4.25/5.0	7.7%
Mobile (URL Hidden)	4.61/5.0	10.6%
Desktop (URL Visible)	3.89/5.0	39.4%
Mobile (URL Visible)	3.72/5.0	67.3%

As observed from Table 1, participants in the URL-hidden groups (unable to directly view complete URL information), whether on desktop or mobile devices, rated the counterfeit websites as more visually similar to the real ones, and their recognition accuracy was significantly lower compared to the URL-visible groups.

Further analysis shows that, regardless of URL visibility, participants using desktop devices had lower overall recognition accuracy than those using mobile devices. A possible reason is that, on desktop devices, the URL bar occupies a relatively smaller portion of the screen, making users less likely to pay attention to the URL while browsing, thereby increasing the difficulty of detecting phishing websites.

5 Discussion

The high fidelity achieved by the phishing website in this study is primarily attributed to the use of web scraping techniques to download the official National Taiwan Normal University (NTNU) Moodle login page resources, including HTML, CSS, and JavaScript files, followed by high-accuracy reproduction. Since web scraping allows for rapid and low-cost duplication of website appearances and functionalities, attackers can easily build phishing websites that are almost indistinguishable from official ones, significantly increasing the success rate of phishing attacks.

Based on the experimental results, several key observations can be summarized:

- **Importance of URL Information**: In scenarios where users are unable to access URL information, they rely solely on the website's appearance for judgment, making them more susceptible to counterfeit UIs and resulting in a significant drop in recognition accuracy. This highlights the critical role of URL inspection education in phishing prevention.
- **Increased Risk on Desktop Devices**: Due to the relatively smaller size of the URL bar on desktops compared to mobile devices, users are less sensitive to URL anomalies during browsing, making desktop environments particularly attractive targets for phishing attacks.
- **Threat of Simulation Technologies**: By utilizing web scraping and static resource reconstruction, attackers can rapidly create highly realistic phishing websites, greatly confusing average users. Pure visual inspection is no longer sufficient for effective phishing prevention.

To mitigate the risks of phishing attacks, organizations and enterprises should adopt the following countermeasures:

- **Enhance Website Protection Mechanisms**: During the construction and maintenance of official websites, deploy anti-scraping techniques such as bot detection, resource encryption and obfuscation, and dynamic rendering, to prevent large-scale automated scraping and reduce the likelihood of phishing site generation.
- **Strengthen Internal Cybersecurity Training**: Regularly conduct cybersecurity training for organizational members and employees to raise awareness of phishing threats, particularly emphasizing URL inspection practices and conducting drills to identify common phishing tactics such as redirection and counterfeit websites.
- **Develop Automated Detection and Protection Tools**: Implement phishing prevention systems based on large language models (LLMs) or machine learning techniques, such as browser extensions capable of analyzing URLs and website behaviors in real-time, identifying potential phishing threats, and actively warning users to reduce victimization risks.

6 Future Work

Recently, Takashi Koide and colleagues proposed the ChatPhishDetector system, which demonstrated the outstanding performance of large language models in the field of phishing site detection. The system directly utilizes existing LLMs such as GPT-4V for website analysis,

eliminating the need for data collection and model training, while enabling rapid and effective detection of multilingual and diverse phishing websites. In their experiments, ChatPhishDetector achieved a precision of 98.7%, recall of 99.6%, and an F1-score of 99.2% on their custom dataset, significantly outperforming other well-known phishing detection methods such as Phishpedia and PhishStorm [5]. These results show that integrating existing LLM APIs can not only reduce the costs of model development and maintenance but also rapidly adapt to evolving phishing tactics while maintaining high detection accuracy.

Based on these insights, the future direction of this study is to develop a phishing prevention browser extension powered by large language models (LLMs). This extension will connect to existing LLM APIs and submit URLs that users are about to visit for real-time risk evaluation. If a URL is deemed high-risk, the system will immediately trigger a warning popup to alert the user, thereby reducing the risk of phishing attacks.

In addition, future work will expand the questionnaire sample size to further explore behavioral differences in phishing prevention across different user demographics (e.g., age groups, professional backgrounds). Through broader and deeper behavioral analysis, the system's user interface and alert strategies can be optimized, and more effective cybersecurity training programs can be designed for various user groups, ultimately enhancing overall information security protection.

7 Conclusion

Through phishing attack simulation and questionnaire surveys, this study confirmed that relying solely on website UI appearance or HTTPS security indicators is insufficient for effectively preventing phishing attacks. The results indicate that checking the correctness of the URL remains the most effective and reliable method for identifying phishing websites.

Additionally, this study recommends that website developers strengthen anti-scraping mechanisms during the design of login interfaces to prevent hackers from easily duplicating frontend resources, which could be exploited to create highly realistic phishing websites. In the future, we will continue to promote the development of AI-powered anti-phishing browser extensions, combined with user education initiatives, to enhance the overall cybersecurity resilience of society.

References

[1] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report: 4th Quarter 2023," 2023.

[2] J. James, S. L., and C. Thomas, "Detection of Phishing URLs Using Machine Learning Techniques," in *Proc. 2013 International Conference on Control Communication and Computing (ICCC)*, Trivandrum, India, Dec. 2013.

[3] Anti-Phishing Working Group (APWG), "Phishing Activity Trends Report: 2nd Quarter 2020," 2023.

[4] R. Simons, "Investigating Initial Access Strategies and Malware Deployment Tactics Used by Iranian Advanced Persistent Threat Groups," 2023 IEEE International Conference on Big Data (BigData), 2023.

[5] T. Koide, H. Nakano, and D. Chiba, "ChatPhishDetector: Detecting Phishing Sites Using Large Language Models," *IEEE Access*, vol. 12, pp. 1–12, 2024, doi: 10.1109/ACCESS.2024.3483905.