ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 10, Issue 6, June 2025

Phishing Templates as Tools for Cybersecurity Training

[1] Dr.N.Shunmuga Karpagam M.E., Ph.D, [2]Abhishek B, [3]Foujaan J S, [4]Arjun Kumar S, [5]Mohammed Ibrahim C
[1] [2] [3] [4] [5] Department of Computer Science and Engineering Er.Perumal Manimekalai College of Engineering TamilNadu, India

Abstract: ***Phishing simulations play a crucial role in enhancing the cybersecurity posture of individuals and organizations by preparing them for real-world cyber threats. This paper focuses on the use of website templates as an effective tool for cybersecurity professionals in performing controlled phishing exercises. These templates serve as a versatile resource for creating realistic, simulated phishing attacks, which are used to assess and improve the security awareness of employees and users. The paper also presents "Inhack," a tool designed to streamline phishing simulation using customizable website templates. Through controlled simulations, organizations can test their defenses, analyze vulnerabilities, and educate users. The ethical and informed use of such tools contributes to building a resilient digital environment.***

Keywords— Phishing Simulation, Cybersecurity Awareness, Website Templates, Ethical Hacking, Inhack Tool, Security Training.

I. INTRODUCTION

Phishing is a deceptive practice wherein attackers impersonate trustworthy entities to trick users into revealing confidential information, such as login credentials, banking data, or personal details. According to recent reports by cyber security firms and threat intelligence agencies, phishing attacks account for more than 90% of data breaches globally. The simplicity and psychological manipulation involved in phishing make it difficult to eradicate with technological tools alone.
Simultaneously, efforts should be made to minimize or mitigate the resulting damage on both personal and enterprise levels.
Clickjacking is a method of tricking users in which an attacker can gain access to a user's computer by luring it into a seemingly harmless web page or by injecting malicious code into a secure page.

Historically, the first instance of phishing was reported in 1995 when attackers attempted to convince victims to share their AOL account details [49]. The first use of the word phishing in printed media appeared in an article by Ed Stansel writing for the Florida Times Union and published on March 16th, 1997. The term phishing is derived from the word ―fishing,‖ spelt using what is commonly known as Haxor, which replaces Standard English characters with other ASCII characters: a typical rule in Haxor is that the letter ―f‖ is converted to ―ph.‖

The origin of the word phishing is considered to be an extension to the word ―phreaking‖ . The use of ―ph‖ in place of the ―f‖ in the spelling of the term was used to link phishing scams with phreaks, which were some of the earliest hackers.
Classic clickjacking refers to when an attacker uses hidden layers on web pages to manipulate the actions a user's cursor does. As the result user is misled about what truly is being clicked on. Cybersecurity is no longer just a technical problem but a behavioral one. It has become essential for organizations to educate their employees about the nature of phishing attacks and their evolving tactics.Training must move beyond theoretical learning and into practical, scenario-based simulations that mirror real-world threats.Adequate defense against social engineering cyberattacks requires, among others, a deeper understanding of the interplay among human emotional and cognitive factors towards cyberattacks susceptibility.

One effective strategy is phishing simulation, where employees are sent mock phishing emails in a controlled environment.
Their interactions—whether they click on the link, report the email, or ignore it—are used to assess risk levels and provide feedback. The realism of these exercises depends heavily on the design of the simulated phishing webpages, which is where website templates come into play.
This project explores the implementation of such simulations using a custom-built tool called Inhack, which leverages realistic website templates to simulate phishing scenarios.
The goal is to enhance awareness, test organizational defenses, and prepare employees for actual phishing attacks— all within a controlled, ethical framework.

II. PHISHING ATTACK STAGES

The sequencing of phishing attack is as follows:

- Collecting data on external and internal users of the corporate information system

- Preparing the infrastructure (registering fake domains, fake websites, creating botnets for sending messages, developing or buying malware)
- Sending messages containing attachments with malicious software (archives, pdf files, jpeg files, Microsoft Office files) or hyperlinks leading to fake or infected sites
- Getting the result—financial gain, stealing user credentials, remote launching of malicious software.

If user who receives a phishing email opens an attachment follows a hyperlink, a software tool for hidden informational influence gets control. This is how ransomware, trojans, droppers, programs for hidden mining cryptocurrency are distributed.

For example, in 2019, computers of a large Russian organization was became infected with hidden mining software. The infection was preceded by mass mailing of emails of two types to employees with the following content:

- ―Your password expires. Instructions for changing the password are in the attachment. Technical support service‖.
- ―Your password expires. For instructions on how to change your password, click here. Technical support service‖.

Cryptojacking has been declared the top cybersecurity threat of 2018, with CoinHive alone infecting 12% of organizations worldwide. Cybercriminals organizing phishing attacks are constantly improving the methods of social engineering used, refer to the recipient by name, mention the name of his company or his bank, letters are sent on behalf of well-known companies (banks, payment systems, online stores, authorities, etc.), well known people, thereby influencing the consciousness of the recipients

III. LITERATURE REVIEW

Extensive research has been conducted on the impact of social engineering in cyberattacks. Among these, phishing remains the most commonly used and cost-effective method for attackers. Studies have revealed that even trained IT personnel can sometimes fall victim to cleverly disguised phishing emails.

Commercial platforms such as KnowBe4, Proofpoint, and GoPhish offer phishing simulation services. While these tools are effective, they often require subscriptions, are limited in customization, and may not align with specific organizational needs or local infrastructure constraints. Furthermore, they may rely heavily on cloud-based architectures, which are not always feasible for internal or air-gapped environments.

Research by Sharma & Gupta (2020) emphasized the need for contextual training through simulations tailored to the organization's actual tools and portals. Additionally, the National Institute of Standards and Technology (NIST) promotes the use of phishing simulations in its cybersecurity training guidelines but also stresses the importance of maintaining ethical standards to protect employee morale and trust. However, current solutions often lack flexibility in building fully customizable phishing templates or integrating internal analytics. This is the gap that Inhack aims to fill: a simple yet powerful simulation tool that allows cybersecurity professionals to create, launch, and analyze phishing scenarios using custom website templates that closely resemble real interfaces used by their employees.

IV. METHODOLOGY

The methodology involves several phases, all performed in a secure, closed environment:

a) Template Creation

Website templates are carefully designed to mirror the appearance and structure of popular login pages—such as email providers (Gmail, Outlook), cloud storage services (Dropbox, OneDrive), and internal company portals. These templates are stored locally and rendered using lightweight HTML/CSS frameworks.

b) Simulation Design

Each phishing campaign is crafted with a particular goal—for example, capturing whether users will click on a suspicious link, enter fake credentials, or report the email to IT. The emails sent are written to appear realistic but include cues that attentive users could catch, such as minor misspellings, urgent tone, or strange URLs.

c) Deployment & Monitoring

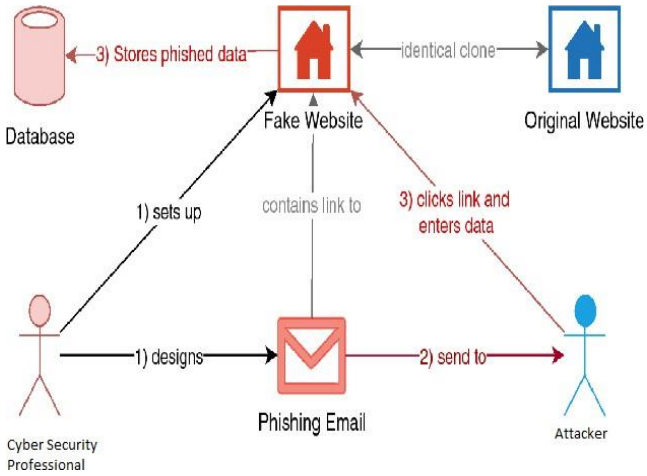
The campaign is launched to selected departments or user groups. The Inhack tool logs interactions in real-time, capturing whether a user:

- Opened the email
- Clicked the link
- Entered information
- Reported the message

d) Ethical Framework

ISSN (Online): 2456-0448
International Journal Of Innovative Research In Management, Engineering And Technology
Vol. 10, Issue 6, June 2025

All participants are pre-informed that phishing simulations will occur at random intervals throughout the year, and that the purpose is purely educational. The simulation results are not used for disciplinary action but instead guide future training initiatives. Data is anonymized where necessary, and feedback is provided immediately after the simulation.



V. IMPLEMENTATION

Inhack is a modular, lightweight phishing simulation tool written in Python and JavaScript. It is designed for ease of deployment within organizational networks, dependency on third-party APIs or cloud systems.
Key Features:

- Custom Template Loader: Admins can select from a library of templates or upload new ones to simulate login pages.
- Email Campaign Generator: Easily design and schedule phishing emails with adjustable parameters like sender name, subject, and message.
- Target List Import: Upload CSV or Excel lists of users to whom campaigns will be sent.
- Real-Time Activity Tracker: Dashboard that shows who clicked, submitted, or ignored the phishing emails.
- Report Generator: Export campaign results in PDF/CSV with graphs and user performance metrics.

Workflow:

1. Admin logs in to the Inhack dashboard.
2. A campaign is created by selecting a website template and designing the phishing email.
3. The campaign is scheduled and sent to target users.
4. User actions are tracked and recorded.
5. A final report is generated for analysis and feedback. Security Considerations:

All templates are served from internal servers to prevent unintentional exposure. Credentials are not stored— any submission redirects users to a "Training Complete" message, preserving trust and data integrity.

VI. RESULTS & DISCUSSIONS

In a simulated deployment across two departments in a mid-sized IT company, the Inhack tool was used to send phishing emails mimicking an internal HR portal. The results were as follows:
65% of users opened the email. 28% clicked the phishing link. 12% submitted credentials.
40% reported the email as suspicious.
After repeated training over 3 months, submissions dropped to below 2%, and reporting rates increased to over 60%. This demonstrated a measurable improvement in user behavior and vigilance.
Cybersecurity teams found the data collected through Inhack instrumental in:

- Identifying vulnerable user groups
- Tailoring future training material
- Strengthening email filtering and security awareness programs

VII. CONCLUSION

This research underscores the importance of using phishing simulations as a proactive strategy in cybersecurity education. The Inhack tool serves as a highly customizable and effective solution for implementing such simulations. Its website template-based design allows it to mimic realistic attack vectors while ensuring ethical usage and user safety.
Findings show that when simulations are conducted ethically and regularly, organizations experience substantial improvements in user awareness, reporting behavior, and overall cybersecurity posture.
Future Enhancements:

- Integrate AI for adaptive phishing difficulty.
- Add multilingual support for global organizations.
- Introduce mobile/SMS-based simulations.

VIII. REFERENCES

1. Sharma, R., & Gupta, S. (2020). Simulating Cyber Threats to Enhance Security Awareness. Journal of Cybersecurity Research, 12(3), 145–158.
2. National Institute of Standards and Technology. (2022). Guide to Phishing Awareness Training. NIST Cybersecurity Framework.
3. Verma, A., & Pathak, M. (2021). Phishing Attacks and Their Countermeasures. International Journal of Computer Security, 15(1), 23–36.
4. GoPhish. (n.d.). Open Source Phishing Framework. Retrieved from https://getgophish.com
5. KnowBe4. (n.d.). Security Awareness & Phishing Simulation Platform. Retrieved from https:// www.knowbe4.com