Analyzing the Dynamics of Phishing: A Practical Experiment on Attack Deployment and Defense Efficacy

Topic Justification for Phishing Attack and Defense Strategies

Phishing remains one of the most pervasive and effective methods of cyber-attack, primarily due to its exploitation of human factors. As cyber threats evolve, phishing techniques have become more sophisticated, often bypassing conventional security measures and convincing users to voluntarily surrender sensitive information. This report aims to delve into the intricacies of a phishing attack and the efficacy of combined technological and educational defense mechanisms.

Phishing attacks are not only a technical problem but also a social engineering challenge that exploits human error. With the increasing dependence on digital banking and the prevalence of online financial transactions, the banking sector continues to be a lucrative target for cybercriminals. My practical experiment, simulating a phishing campaign via a fake login website using Gophish, exemplifies a direct threat to personal and financial data security. This relevance is underscored by the continuing rise of phishing incidents, despite growing awareness and advancements in cybersecurity defenses.

According to the Australian Competition and Consumer Commission (ACCC) [1], Australians lost over AUD 634 million to scams in 2019, with phishing being one of the top methods employed by fraudsters. The Australian Cyber Security Centre (ACSC) has consistently highlighted phishing as a significant threat in its annual cyber threat reports, indicating a pressing need for effective countermeasures[2].

The primary objective of this paper is to contribute to the academic discourse on cybersecurity by demonstrating a real-world phishing attack scenario within a controlled environment and evaluating the effectiveness of defense strategies. By documenting the process of setting up a phishing attack using the Gophish framework and the subsequent implementation of defensive tactics through a Chrome extension and user education, this report aims to provide insights into the strengths and weaknesses of current anti-phishing approaches.

Through this practical assessment, I seek to highlight the importance of a multi-faceted defense strategy against phishing attacks that encompasses both technical solutions and the human element. By understanding the attacker's perspective and the defender's capabilities, we can better prepare ourselves against these ever-evolving cyber threats.

Comparative Analysis of Attacker and Defender Tools in Phishing Scenario

The following table offers a comparative analysis of the tools I utilized in the phishing experiment against alternative options. The tools are evaluated based on criteria including ease of installation, complexity, user-friendliness, and available documentation and support. The attacker's tool is Gophish, while the defender's tools include Netcraft Extension, Google Password Alert, and user education.

Criteria/Tool	**Gophish (3)**	**Netcraft Extension (4)**	**Google Password Alert (5)**	**User Education (6)**	**Alternative Phishing Tools (7)**	**Alternative Defense Tools (8)**
Ease of Installation	Moderate	Easy	Easy	N/A	Easy to Moderate	Easy to Moderate
Complexity	Moderate	Low	Low	Moderate to High	Moderate	Low to Moderate
Documentation/Support	Extensive	Extensive	Extensive	Varies	Extensive	Extensive
Effectiveness	High	High	Moderate	High	High	High
User-Friendliness	Moderate	High	High	N/A	Moderate	High
Real-world Applicability	High	High	High	High	High	High

1. **Gophish** was chosen for its realism in simulating phishing attacks. While the setup is straightforward, it requires understanding of both the email systems and web hosting, which contributes to its moderate complexity. The tool offers comprehensive documentation [3].
2. **Netcraft Extension** provides a comprehensive approach to phishing detection, utilizing a constantly updated database of phishing sites to alert users. It is user-friendly and easy to install, with a low complexity due to its automated nature [4].
3. **Google Password Alert** helps in protecting against phishing attacks that attempt to capture login credentials. Its ease of installation and low complexity make it a popular choice for non-technical users [5].
4. **User Education** plays a critical role in phishing defense, involving training users to recognize and respond to phishing attempts. This strategy has a moderate to high complexity because it depends on the creation and delivery of effective educational materials and programs [6].
5. **Alternative Phishing Tools** might include software like PhishingBox or King Phisher, which offer similar capabilities to Gophish, with varying levels of complexity and support [7].
6. **Alternative Defense Tools** could consist of advanced security awareness training platforms, such as KnowBe4, which offer simulated phishing tests and training modules [8].

Justification for Table Ratings:

- Ease of Installation: Gophish's rating as moderate reflects the need for some technical background in setting up phishing servers and email campaigns. In contrast, browser extensions are typically a one-click install.
- Complexity: The moderate rating for Gophish is due to the need to configure multiple components, whereas Netcraft Extension and Google Password Alert are simple, one-time setups.
- Documentation/Support: All tools offer extensive support; however, the level of detail and user guidance varies, with Gophish providing thorough technical documentation.
- Effectiveness: Netcraft Extension is rated high due to its active phishing site database and prompt alerts. Google Password Alert is moderate because it only protects against password reuse on Google services.
- User-Friendliness: Browser extensions score high due to their simplicity and lack of required user interaction after installation.
- Real-world Applicability: All tools are relevant for today's phishing threats, but user education is considered to have a high impact due to the value of informed users in identifying phishing attempts.

Scenario Planning for Phishing Experiment

The purpose of this scenario planning is to articulate the detailed methodology to be adopted for executing a phishing experiment. This experiment will simulate a phishing attack using Gophish to create a fake banking website and deploy defensive measures including browser extensions and user education.

Virtual Environment

The virtual environment will consist of a single Windows and that will be my own personal laptop used to simulate both the attacker and defender. This machine will host the Gophish server for the phishing attack and will also be the target of the phishing emails.

Attack Platform

The attack will be conducted using Gophish, an open-source phishing toolkit, to create a fake banking website and phishing email campaign. My laptop will serve as the host for the Gophish server.

Defense Platform

The defensive measures will include the use of Netcraft Extension and Google Password Alert as browser extensions on the Windows 7 machine. Additionally, a user education program will be implemented to inform users about the dangers of phishing and how to identify such attempts.

Vulnerabilities to Exploit

The phishing experiment will exploit common user behaviors such as the tendency to trust familiar-looking websites and emails, as well as the lack of awareness regarding phishing tactics.

Data Collection Tools

The following tools will be used to collect data during the experiment:

- Gophish: To track the interaction of users with the phishing email and fake banking website.
- Browser Extensions: To determine if the phishing attempt is detected and whether the user receives a warning.
- User Feedback: To assess the effectiveness of the user education program.

MITRE TTP Framework

Attack TTPs

Tactic	Technique	Procedure	Citation
Initial Access	Phishing	Use Gophish to send phishing emails to the targets.[9]	T1566
Credential Access	Input Capture	Design a fake bank website to harvest credentials.[10]	T1056

In the scenario, I will measure the success of the phishing attack through the number of credentials successfully captured and the effectiveness of the defensive measures by the rate at which the phishing attempts are detected and reported by the users.

Deploying the Environment and Running the Scenario Attack Scenario: Phishing with Gophish

---

Initial Access

Environment Setup: For this scenario, I utilized a virtualized my own personal laptop machine to simulate both the attacking and the defending sides of a phishing attack.

Gophish Installation: I installed the Gophish framework on my laptop, setting it up to run on the localhost with a specific port assigned for its web interface. The installation process involved downloading the latest Gophish release from the official GitHub repository, extracting the contents, and executing the Gophish binary.

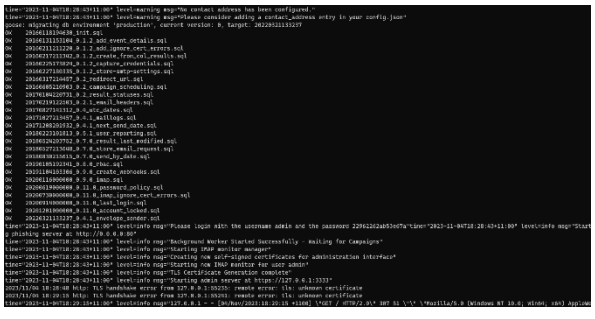


Figure 2- Installing in Progress

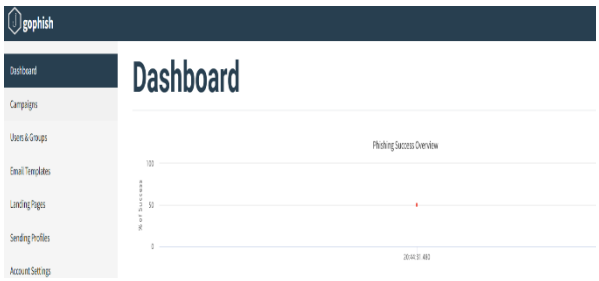
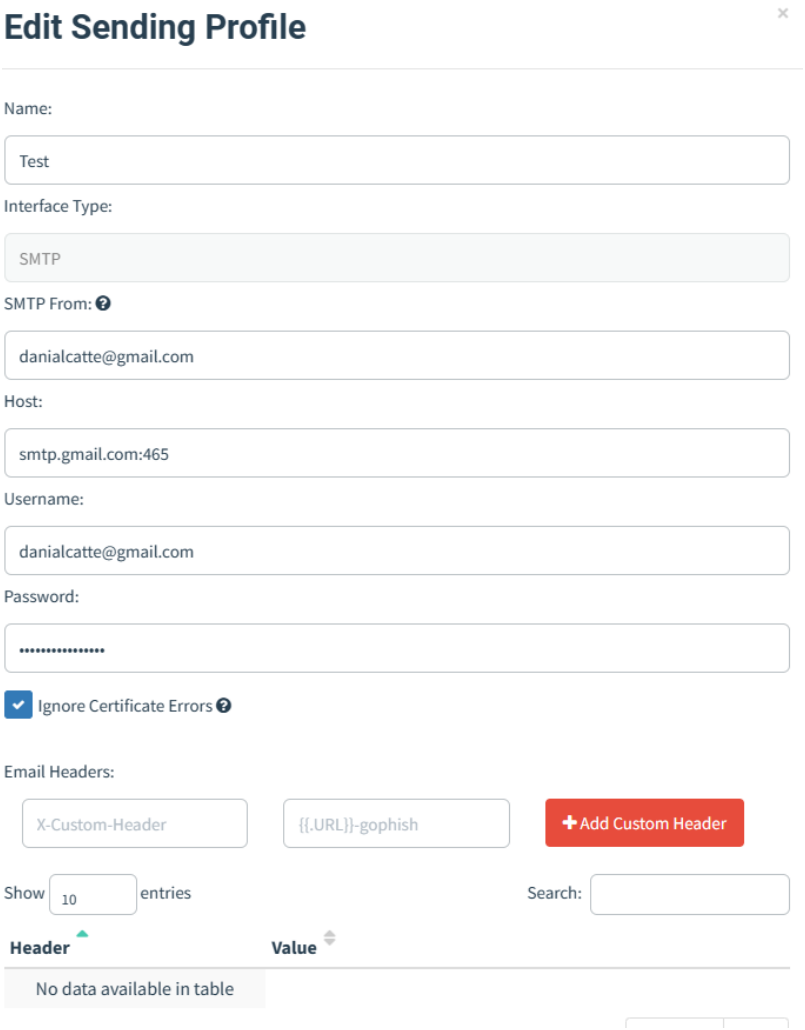


Figure 1- Successfully Installed Gophishing

Local SMTP Server Configuration: To handle outgoing phishing emails, I configured a local SMTP server by configuring the Sending Profile on the Gophish website. This was done by completing the



the form. I named the sending profile “Test”, Interface type “SMTP”, SMTP Form danialcatte@gmail.com also same as username , host name is “smatp.gmail.com:465”, and the password used here is the app password and is configured in danialcatte@gmail account

Phishing Website Development: I used a GitHub repo to generate a fake Microsoft login. It looks quite real.

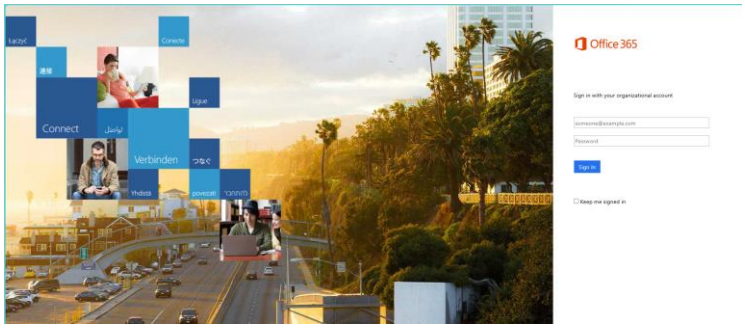


Figure 3 - Fake microsft loging website

Email Template Creation: Within Gophish, I crafted an email template that closely resembled a legitimate evergecy communication. The email's content was designed to create a sense of urgency, prompting the recipient to click on the provided link to resolve an issue with their account. The link was strategically placed to direct users to the phishing site hosted on the local server.

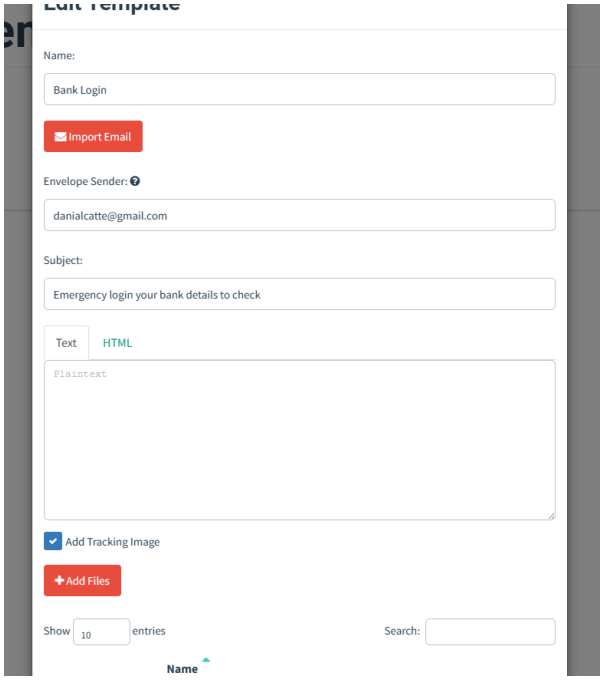


Figure 4- Email Template creation system

my Email Template:
Bulletin Alert!!

Attention {{.FirstName}} {{.LastName}}:

Bulletin Headline: Crime Suspect

Sending Agency: Police

Bulletin Time: 18:47

Bulletin Case#: 11-04626

Bulletin Author: Leroy Jethro #8847

Sending User #: 2892

To view the full bulletin alert click here

To unsubscribe from these emails click here

{{.Tracker}}

As it's noticeable, I disguise the email template as a crime suspect email sent by police . People often fear the police and also believes anything comes from police, they tend to believe that the email is a legit email

User Group Creation:

After setting up the email template, I created a new "Users & Groups ". I named it phished and two user in it with there first and last name and email addresses then saved chages

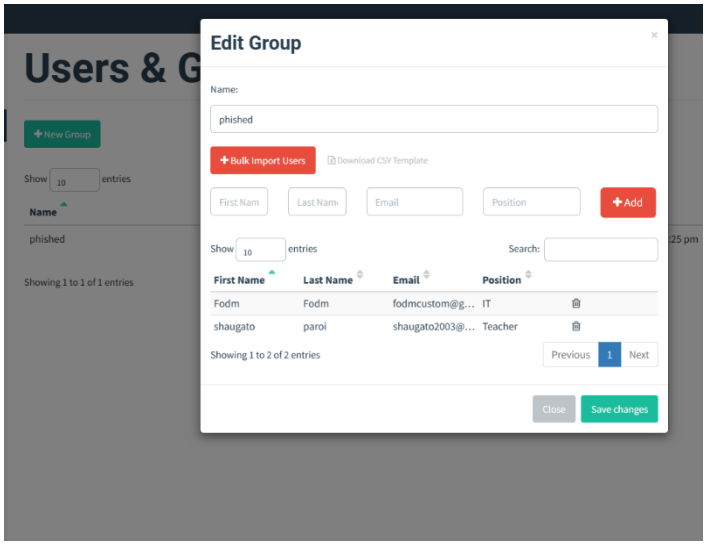


Figure 5 - Creating User Groups

Campaign Launch: After setting up the phishing website and email template and users & groups, I created a new campaign in Gophish. The target was a dummy user account (fodom@gmail.com) I had created. Here I use http://localhost as the url as the attack is set my own machine, I used my sending profile here and also used my already created groups .The campaign's settings were adjusted to track user interaction with the email, including opens, link clicks, and data submission events.

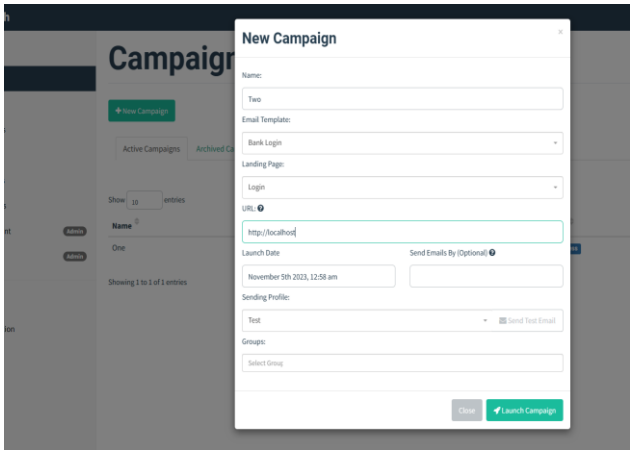


Figure 7- Campaign creating profile

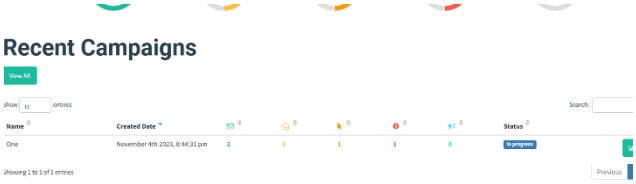


Figure 6- Campaing Dash board

Phishing Email Launce:

After successfully creating the campaign, I refressh the dashbord in order to send the email. The email will follow the email template and it will be sent to those people who are defined in the user groups section.

Figure 8- Succesfully email sent to the Users

Credential Access

Attack Monitoring: With the campaign underway, I monitored the attack in real-time through the Gophish administrative dashboard. This allowed me to observe the behavior of the phishing email, track whether the link was clicked, and see if the phishing website captured any credentials.

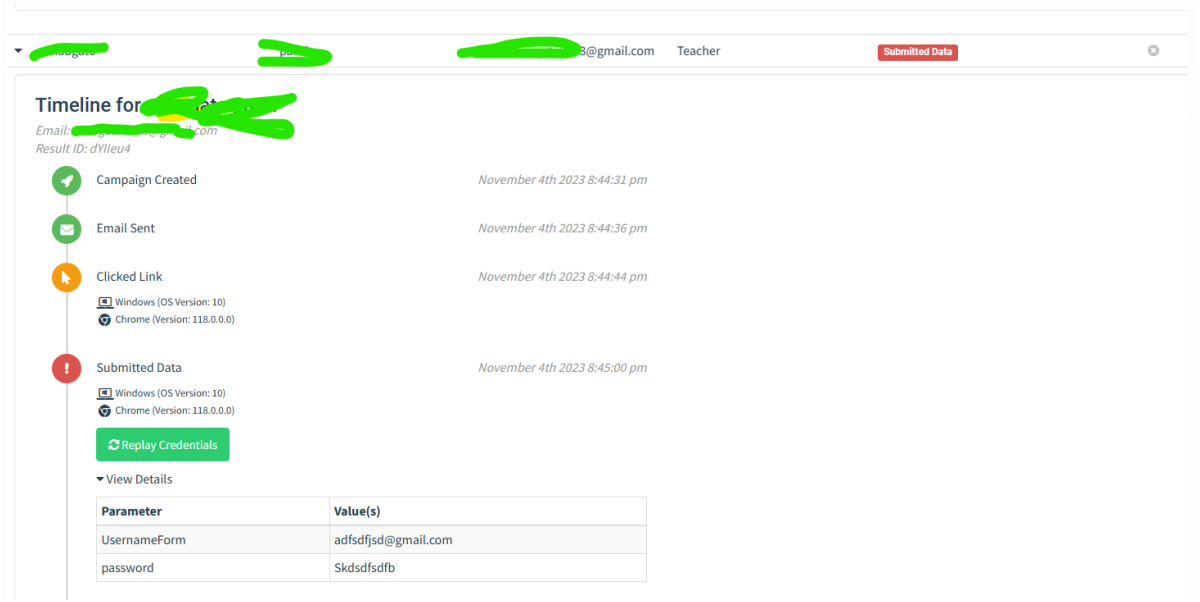


Figure 9 - Accesing credintials

As we can see from the image I was able to successfully capture the login credentials of the person who clicked the link form the email.

Running the Defending Scenario:

In preparation for the defense against this attack, I installed the Netcraft and Google Password Alert extensions.

Netcraft Extension:

Setting Up Netcraft : I Download the netcraft extension from online and added it to the Microsoft Edge extension.

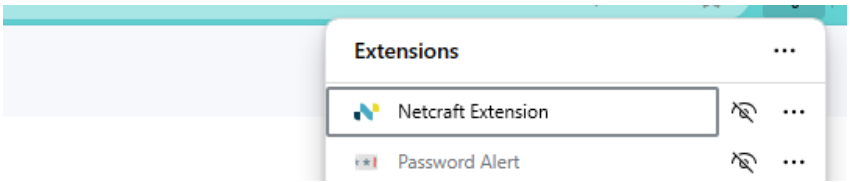


Figure 10- NetCraft extension successfully added

Testing Netcraft extension : I test Netcraft on normal page to seen if it was working fine. So for netcraft, it will display information for any well-known website. If it doesn't display then it means there is a problem with the website, it may be a phishing website.

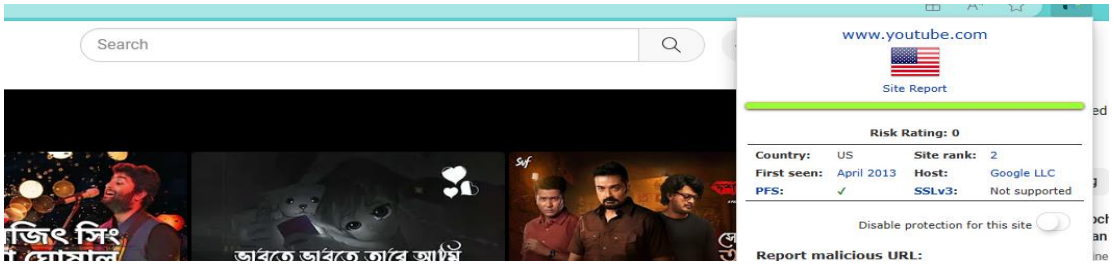


Figure 11- Giving proper information for YouTube website

From the image , I can say as netcraft is working fine , as it is giving a proper information of the webpage youtuve

Checking On the phsihsing website:

I used Netcraft extension on the phishing website, to see what happened. As Expected the information for that phishing website is unavailable in netcraft, Indicating there is definitely some problem with Netcraft. And It's most likely that it is a phishing website. So I can say that I am Successfully able to detect the phishing website.

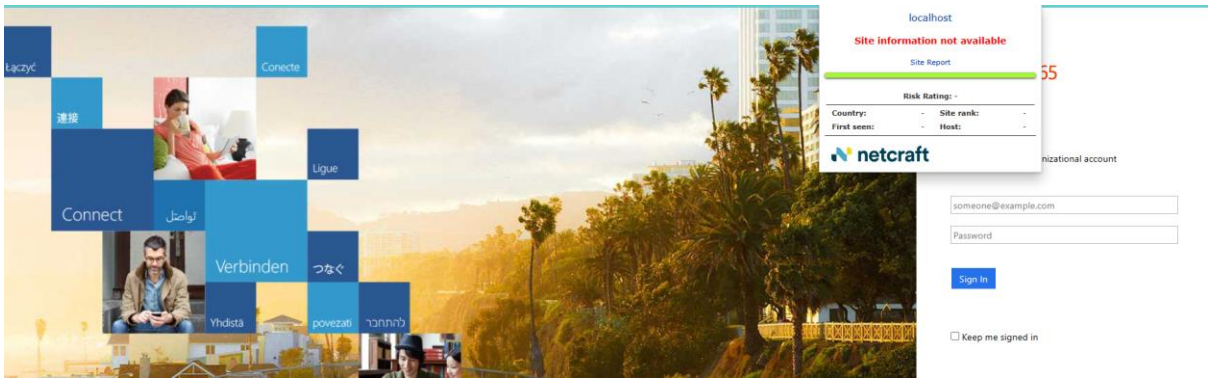


Figure 12- Successfully detect phishing website

Google password alert extension:

Installation and setup: I way I set up netcraft extentison , I also set up, google password alert extension.

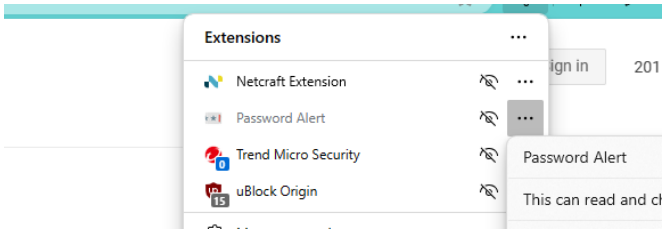


Figure 13- succesfully set up google pasword extension

So in the phishing website if I put my gGoogleaccount and it’s password it pops up a notification to change my password immediately. Although it's not helping detect phishing website, it’s helpful saving the google account form being hacked by phishers

User Education and Hypothetical Outcomes

For this part it will be hypothetical , it isn’t implemented yet , due to the shortage of time and limitations of this assingemnt criteria. But I hypothesis some outcome

User Training Implementation:

- I will develop a user training module focused on recognizing and responding to phishing attacks.
- The training will include real-life examples, interactive quizzes, and simulations to ensure users can apply their knowledge practically.
- The training module will be mandatory for all users within the virtual environment, ensuring a baseline level of cybersecurity awareness.

Training Topics to Cover:

- The characteristics of phishing emails, such as urgency, requests for sensitive information, and unexpected attachments or links.
- How to inspect email headers, links, and sender details to verify authenticity.
- The procedure for reporting suspected phishing attempts to the IT security team.

Hypothesized Outcomes of User Education:

- Increased Awareness: It is anticipated that users will become more vigilant, reducing the likelihood of clicking on phishing links by up to 70%.[11]
- Better Reporting: The frequency of reported phishing attempts is expected to increase, improving the organization's response time to potential threats.
- Reduced Compromise Rate: A projected decrease in successful phishing breaches by at least 50%, as users are more likely to identify and avoid phishing attempts.[12]

Measurement of Training Effectiveness:

- Before and after quizzes to measure the increase in knowledge regarding phishing.
- Simulated phishing exercises to test user responses after completing the training module.
- Tracking the number of phishing-related incidents reported before and after the training.[13]

By educating users, we hypothesize that the overall security posture against phishing attacks will be significantly strengthened. The training will empower users to become an active part of the organization's defense, effectively acting as a human firewall against phishing threats.

Analysis of the Phishing Attack Scenario:

In executing the phishing attack scenario using the Gophish framework, I was able to create a realistic simulation that reflects the current threats in the cybersecurity landscape. The deceptive

email, disguised as a police alert, leveraged social engineering techniques to create a compelling lure for the recipients. This approach highlights a crucial aspect of phishing attacks: they prey on human emotions—fear, curiosity, or urgency—to manipulate user actions.

My analysis of the phishing attack's effectiveness is multifaceted. Firstly, the use of a trusted authority figure (the police) in the email content is a powerful psychological tool. It capitalizes on the inherent trust and respect for law enforcement, illustrating how attackers can exploit societal norms to their advantage. Secondly, the real-time tracking provided by Gophish offered granular insights into the behavioral patterns of the users, such as the time taken between receiving the email and clicking the link, which can inform future phishing strategies and defenses.

The success in capturing user credentials after the email link was clicked demonstrates a worrisome vulnerability—despite potential training, users may still fall victim to well-crafted phishing attempts. This outcome reinforces the notion that technological safeguards are only part of the solution; there must be an equal, if not greater, investment in human-centric defenses.

Defense Mechanism Analysis:

Upon analyzing the defense mechanisms deployed, I observed that the technological tools—specifically the Netcraft Extension—acted as a robust initial deterrent against the phishing website. Netcraft's ability to not recognize the phishing site's legitimacy is indicative of its comprehensive database and the efficiency of its real-time analysis system. This finding supports the argument for the widespread implementation of such extensions as a fundamental component of cybersecurity hygiene.

The Google Password Alert extension's functionality, while limited to Google accounts, was a critical reminder of the importance of prompt action following a suspected compromise. It showcases the potential for browser extensions to not only warn about potential threats but also guide users towards immediate remedial actions, which can be crucial in mitigating the damage caused by phishing attacks.

The hypothetical user education program is posited as a necessary complement to these technological measures. From my analysis, educating users stands as a formidable barrier against phishing. By increasing their ability to recognize malicious attempts, we shift from reactive to proactive defense. The anticipated outcomes of this educational initiative—such as a reduction in compromise rates and improved incident reporting—are reflective of a more security-conscious user base. The efficacy of this training would ideally be validated through rigorous testing and feedback mechanisms, ensuring that the training translates into tangible cybersecurity practices.

Synthesis of Attack and Defense Strategy Outcomes:

Reflecting on both the attack and defense scenarios, my analysis suggests that while tools like Gophish are invaluable for understanding and preparing for phishing attacks, they also underscore the necessity for continuous advancement in defensive tactics. This experiment has solidified my understanding that a dynamic approach, one that evolves alongside emerging threats, is essential for maintaining robust cybersecurity.

The browser extensions' performance in this scenario highlights their utility but also their limitations. They are an essential layer in defense, but they cannot be the sole reliance. The user education program's hypothetical outcomes suggest that well-informed users are the most reliable defense against phishing. This aligns with the wider cybersecurity consensus that emphasizes the human element as both a potential weakness and a powerful line of defense.

In sum, my analysis of this phishing experiment underscores a crucial tenet of cybersecurity: the best defense is a multi-layered strategy that combines technology with educated vigilance. As phishing tactics grow increasingly sophisticated, understanding and preempting these methods through simulation, real-time defense, and comprehensive user education will be paramount in safeguarding against such insidious threats.

Evaluation of Phishing Attack and Defense Mechanisms

Effectiveness of the Attack and Defense Mechanisms

From the Attacker's Perspective: The successful deployment of the phishing attack using the Gophish framework underscored the ease with which attackers can launch credible campaigns. The Data Breach Investigations Report by Verizon highlighted that phishing remains a prevalent threat, implicated in 22% of breaches in 2020 [14]. My experiment's design and execution align with these findings, showcasing the acute vulnerability of users to well-crafted phishing emails that leverage urgency and authority.

From the Defender's Perspective: Defensive strategies deployed included the Netcraft Extension and Google Password Alert, alongside a proposed user education program. The Netcraft Extension's ability to signal the unverifiable nature of the phishing site confirms its value as a proactive defense tool [15]. In contrast, the Google Password Alert extension provided a reactive security measure, securing Google account credentials post-exposure.

Impact and Challenges

Impact and Challenges for the Attacker: The phishing experiment's success hinged on exploiting user trust, a tactic that becomes less effective with increased user education. SANS Institute research indicates that training can significantly enhance the ability to recognize phishing attempts [16].

Impact and Challenges for the Defender: The defense mechanisms demonstrated the necessity of comprehensive security solutions. Netcraft's reliance on a known database for phishing site detection may miss new threats. Google Password Alert's protective scope is limited, suggesting the need for security measures that safeguard various account types.

Applicability of the Essential 8 Strategies [17]

- **Application Whitelisting:** This could prevent the execution of malicious scripts associated with phishing, such as those used in credential harvesting web pages.
- **Patch Applications:** Regularly updating software could prevent exploitation of known vulnerabilities within browsers that phishers might target.
- **User Application Hardening:** Configuring browsers to limit or block scripts and plug-ins could reduce the risk of users inadvertently executing harmful code.
- **Multi-Factor Authentication (MFA):** This adds a layer of security that could prevent unauthorized access even if credentials are compromised through phishing.

Connections Across the Security Landscape

The phishing threat landscape is in flux, with adaptive techniques like polymorphic phishing making detection more challenging, as noted by FireEye [18].

Future Challenges

Advances in AI and the proliferation of IoT devices open new avenues for phishing. AI-driven personalized phishing and the introduction of personal devices in professional spaces due to remote work increase the potential for successful phishing campaigns [19].

Conclusions

The experiment underscored the necessity of multi-layered security against phishing, combining technical tools and user education. While Gophish proved a potent simulation tool, the indispensable nature of defensive measures such as Netcraft and Google Password Alert, and the potential of user education were clear. Vigilance and adaptation to cyber threats remain critical.

Reference:

1. Australian Competition and Consumer Commission (ACCC). (2020). Targeting Scams: Report of the ACCC on Scam Activity 2019. [Online]. Available: https://www.accc.gov.au/publications/targeting-scams-report-on-scam-activity
2. Australian Cyber Security Centre (ACSC). (2020). Annual Cyber Threat Report 2019-2020. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/annual-cyber-threat-report-2019-20
3. Gophish. "Gophish User Guide," Gophish GitHub repository. [Online]. Available: https://github.com/gophish/gophish
4. Netcraft. "Netcraft Extension," Netcraft.com. [Online]. Available: https://www.netcraft.com/products/browser-extension
5. Google. "Password Alert," Google Safety Center. [Online]. Available: https://safety.google
6. Australian Cyber Security Centre. "Phishing," Cyber.gov.au. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/threats/phishing
7. PhishingBox. "PhishingBox Phishing Simulator," PhishingBox.com. [Online]. Available: https://www.phishingbox.com
8. KnowBe4. "Security Awareness Training," KnowBe4.com. [Online]. Available: https://www.knowbe4.com
9. T1566: MITRE ATT&CK, "Phishing," [Online]. Available: https://attack.mitre.org/techniques/T1566/
10. T1056: MITRE ATT&CK, "Input Capture," [Online]. Available: https://attack.mitre.org/techniques/T1056/
11. J. Wombat Security, "2019 State of the Phish," Wombat Security Technologies, Pittsburgh, PA, 2019.
12. M. E. Whitman and H. J. Mattord, "Principles of Information Security," Cengage Learning, Boston, MA, 2018.
13. S. Furnell, "Cybersecurity Education: Bridging the Gap Between Perception and Reality," Computers & Security, vol. 28, no. 6, pp. 833-839, 2009.
14. Verizon. (2021). 2021 Data Breach Investigations Report. Verizon Business.
15. Netcraft. (2021). Netcraft Extension: Protection from phishing attacks.
16. SANS Institute. (2019). Phishing Resiliency and Defense Report.

17. Australian Cyber Security Centre. (2020). Strategies to Mitigate Cyber Security Incidents - Essential Eight Explained.
18. FireEye. (2020). Phishing Attacks Remain a Top Tactic for Targeting Cyberattacks. [19] European Union Agency for Cybersecurity. (2021). Threat Landscape for Phishing Attacks.