**Social Engineering & Phishing Simulation Report**  
**Submitted by:** Shravani Joshi  
**Internship Program:** Future Interns – Cybersecurity Track  
**Project Title:** The Art & Impact of Phishing: A Hands-On Simulation  
**Date:** 15-05-25

**1. Objective**

The primary objective of this experiment was to simulate a phishing attack in a controlled environment to assess user behavior, understand the psychological triggers behind phishing success, and highlight the importance of security awareness training. This task was conducted ethically and intended strictly for educational and awareness purposes.

**2. Scope of the Simulation**

* Design and deploy a realistic phishing campaign
* Monitor and analyze user engagement (email opens, link clicks, credential submissions)
* Evaluate the effectiveness of the attack vector
* Generate recommendations for awareness and defense improvements

**3. Tools & Resources Used**

* **Gophish:** Open-source phishing framework for campaign management and tracking
* **OWASP Juice Shop:** Vulnerable web application used to replicate a realistic login page
* **Custom Email Template:** Designed to resemble standard corporate communication

**4. Methodology**

**4.1 Campaign Setup**

* A phishing campaign was configured using Gophish.
* A professional-looking email lure was crafted to prompt users to "verify" their credentials.
* The login page of OWASP Juice Shop was cloned and hosted to collect simulated submissions.

**4.2 Target Simulation**

* Simulated users were "targeted" with the phishing email.
* No real user data or credentials were collected; all interactions were anonymized.

**4.3 Data Tracking**

Gophish tracked:

* Email open rates
* Link click-through rates
* Fake credential input attempts

**5. Key Observations**

* **High Click Rate:** A significant percentage of simulated users clicked the link, indicating a strong trust in the legitimacy of the email.
* **Credential Submission:** Multiple simulated entries were captured, showing a potential failure to recognize a fake login interface.
* **Response Time:** Most interactions occurred within the first 30 minutes of email delivery, emphasizing the urgency-effectiveness of the lure.

**6. Insights & Analysis**

* **Psychological Triggers Worked:** Use of urgency and familiar branding increased effectiveness.
* **Human Factor Remains Vulnerable:** Even with basic security knowledge, users can be deceived by well-crafted emails.
* **Need for Awareness Training:** Users were unaware of basic signs of phishing such as suspicious URLs, generic greetings, and login page inconsistencies.

**7. Impact & Learning Outcomes**

* Understood how social engineering bypasses technical defenses by targeting human psychology.
* Gained experience in ethical simulation of phishing attacks within a controlled framework.
* Recognized the critical role of user education alongside firewalls, antivirus, and network monitoring tools.

**8. Recommendations**

1. **Conduct Regular Phishing Simulations** to reinforce awareness.
2. **Implement Interactive Training Modules** focusing on real-life phishing scenarios.
3. **Introduce Multi-Factor Authentication (MFA)** to mitigate risk even if credentials are compromised.
4. **Promote a "Think Before You Click" Culture** through internal communication campaigns.

**9. Conclusion**

This simulation emphasized that phishing is not just a technical issue but a **behavioral vulnerability**. Through hands-on experience, I’ve gained a deeper appreciation for the complexities of social engineering and its real-world impact. Going forward, these insights will inform how I approach cybersecurity—focusing on both systems and the people who use them.