Phishing Awareness and Detection – Project Report

Executive Summary

This project simulates the full lifecycle of a phishing attack and defense strategy. Our team launched phishing campaigns using GoPhish and SendGrid to assess user susceptibility, then developed a Bash-based detection script to identify suspicious emails. By combining offensive (red team) and defensive (blue team) tactics, we replicated a realistic SOC workflow to strengthen our understanding of phishing threats and detection techniques.

Tools & Technologies

- GoPhish – Phishing simulation platform
- SendGrid – SMTP email delivery service
- Carrd.co – Hosted phishing landing pages
- DigitalOcean VM – Hardened cloud server for hosting GoPhish and script
- Bash & Fetchmail – Email ingestion and analysis scripting
- OSINT Tools – Used to collect publicly available email addresses
- Email Platforms Tested – Gmail, Outlook, Yahoo
- Custom Domains – azure-support.info, support-staff.info (authenticated sender identities)

Campaign Execution

Two email templates were created: one themed as a Cybersecurity Summit invitation and the other mimicking a Splunk event. Each campaign was sent to 31 classmates via SendGrid using authenticated sender domains. Interaction was tracked via GoPhish and custom landing pages.

Results:

- Splunk Campaign: 31 sent / 21 opened / 6 clicked (29%)
- Cybersecurity Summit Campaign: 31 sent / 20 opened / 6 clicked (30%)

These results highlight that even cybersecurity-aware users can fall for well-crafted, timely phishing emails.

Phishing Detection Script

To emulate a blue team response, we developed a Bash script that detects potential phishing indicators in emails retrieved using Fetchmail. It performs rule-based checks using standard Unix tools (grep, sed, awk), and flags:

- Untrusted Senders – e.g., gmail.com, yahoo.com
- Generic Greetings – e.g., “Dear Customer”
- Urgency Triggers – e.g., “Your account has been suspended”
- Suspicious Links – e.g., URLs with terms like login, verify, secure
- Harmful Attachments – e.g., .exe, .bat, .zip

Each result is displayed with color-coded terminal output, mimicking SOC alert visibility. Emails are processed from /var/mail/sysadmin.

Challenges Encountered

- Deliverability issues across Outlook and Yahoo due to domain reputation
- Initial domain blocked by registrar; required re-registration and new records
- GoPhish server shutdowns fixed via systemd service configuration
- Fetchmail skipped older messages, requiring script tuning
- Detection script had limited scalability and was not integrated into any real-time mail platform

Skills Gained

- Configuring SPF/DKIM for email authentication
- Using GoPhish for campaign simulation and tracking
- Ethical OSINT for target list generation
- Bash scripting for SOC-style email detection
- Collaborating across red and blue roles to mimic real-world threat workflows

Conclusion

This project reinforced our understanding of both phishing attack techniques and defense mechanisms. By working through setup, delivery, user behavior tracking, and script-based detection, we developed hands-on experience that aligns with the investigative and analytical responsibilities of a SOC analyst.

Our approach demonstrated that with realistic phishing themes, even trained users can be vulnerable. It also highlighted the value of basic detection automation to support incident response and awareness programs in enterprise environments.