Phishing Simulation and User Awareness Training

Prepared by: Leo D. Dorsey

Objective

To test user resilience to phishing attacks, identify common behaviors leading to compromise, and strengthen awareness through targeted training and education.

Tools & Methods

Tools Used: Gophish, Mailtrap, HTML email templates, Google Forms

Metrics Tracked: Email open rate, link click rate, credential submission attempts

Training Delivery: Internal slide deck, phishing awareness checklist, follow-up quiz

Implementation Steps

1. Designed realistic phishing email templates mimicking common attack vectors.
2. Launched phishing campaigns and tracked response metrics.
3. Analyzed engagement and identified user behaviors.
4. Delivered awareness training with best practices and red flag indicators.
5. Conducted follow-up quiz to assess knowledge retention.

Results / Findings

- 40% email open rate, 15% click-through, 5% submitted credentials
- Training improved reporting and reduced risky behavior
- Users demonstrated stronger awareness in subsequent tests

Conclusion

This project enhanced user awareness of phishing tactics and reduced the likelihood of successful social engineering. Ongoing simulations and education foster a security-first culture.


Gophish Campaign Dashboard
Campaigns
Users
Templates
Landing Pages
Campaign: Q1 Awareness Test
Emails Sent: 100
Opened: 40
Clicked: 15
Submitted Data: 5
Recent Activity
09:02 AM - alice@company.com clicked link
09:04 AM - bob@company.com submitted credentials
09:10 AM - carol@company.com opened email
09:15 AM - dave@company.com clicked link
09:20 AM - eve@company.com submitted credentials

Recognizing Phishing Emails

- Watch for urgent or threatening language
- Verify the sender's email address carefully
- Avoid clicking on suspicious links or attachments
- Look for misspellings or grammar errors
- When in doubt, report the email to IT