Phishing Resilience: Enhancing Awareness Through Simulation Engagements

Presented by:

Adnan Alsaadawi

Introduction

Phishing is a major cyber threat

University students are vulnerable targets

This project focuses on raising awareness

Simulations used to assess and improve resilience

The project is educational, practical, and measurable

Problem Statement & Motivation

🚨 Problem Statement

- Many students are unable to identify realistic phishing emails
- Traditional awareness methods (e.g., posters, generic emails) have limited impact
- There is a lack of hands-on, engaging phishing training in universities
- Students often do not report suspicious emails when they encounter them

💡 Motivation

- To create a safe and realistic phishing simulation for students
- To measure how students respond to real-life phishing tactics
- To raise awareness through practical experience instead of passive materials
- To help reduce human error — the most common cause of cyber incidents

Aim and Objectives

🎯 **Aim:**
Enhance phishing awareness and behavioural response among university students through a simulated phishing campaign.

✅ **Objectives:**

- Design a realistic and convincing phishing scenario
- Deploy the campaign to university students
- Track user interactions
- Assess awareness levels before and after the simulation
- Analyse behavioural trends and reporting habits
- Provide recommendations for improving phishing awareness

Methodology

GoPhish used to design and deploy the phishing campaign

Mailgun provided secure email delivery via authenticated domain

Landing and redirect pages were built using **HTML/CSS**

Hosted the simulation on **a DigitalOcean** VPS

Pre- and post-simulation **surveys** were created in Google Forms

Target Audience: University **Students**

Data was **anonymised**; no real credentials stored

Challenges and Solutions

Challenge	Solution
Gmail SMTP blocked	Replaced with Mailgun for secure and reliable email delivery
Emails going to spam	Implemented SPF, DKIM, and DMARC authentication on custom domain
Designing realistic phishing content	Used HTML/CSS for landing and redirect page styling
Handling real participant data	Ensured anonymity and avoided credential storage
Server setup and deployment	Deployed GoPhish on DigitalOcean VPS via PuTTY for secure remote access

Results & Analysis

📈 Campaign Performance

- Total Emails Sent**:** 50
- Open Rate: 66%
- Click Rate: 22%
- Form Submissions: 16%
- Reports Submitted: 0

🔍 Key Observations

- The email subject line and format successfully encouraged opens
- A noticeable number of students clicked without verifying authenticity
- 16% of users submitted data on the fake login page
- No participant reported the phishing attempt, indicating a lack of reporting awareness
- The results confirmed students are vulnerable to realistic phishing emails

Simulation Feedback

📊 Post-Simulation Survey Highlights

- 96% of participants reported increased phishing awareness
- Most rated the phishing email as believable and professional
- Many admitted they would have clicked the link in a real scenario

🔑 Key Lessons Learnt By Students

- Always verify the sender’s email address
- Hover over links before clicking
- Be cautious of urgency or emotionally persuasive

Project Demonstration

What I Will Demonstrate:

- GoPhish campaign setup with target group and sending profile
- Phishing email design using a scholarship theme
- Landing page that mimics a university login portal
- Redirect page hosted on GitHub explaining the simulation
- GoPhish tracking dashboard showing opens, clicks, and submissions
- Key survey responses from participants (before and after simulation)

Recommendations for Future Improvement

- Conduct regular phishing simulations for both students and staff
- Introduce simple reporting tools in university email systems
- Use interactive training methods to improve engagement and retention
- Provide instant feedback after each simulated attack
- Expand simulations to include SMS and social media phishing scenarios
- Collaborate with IT teams to build a culture of cyber awareness

Conclusion

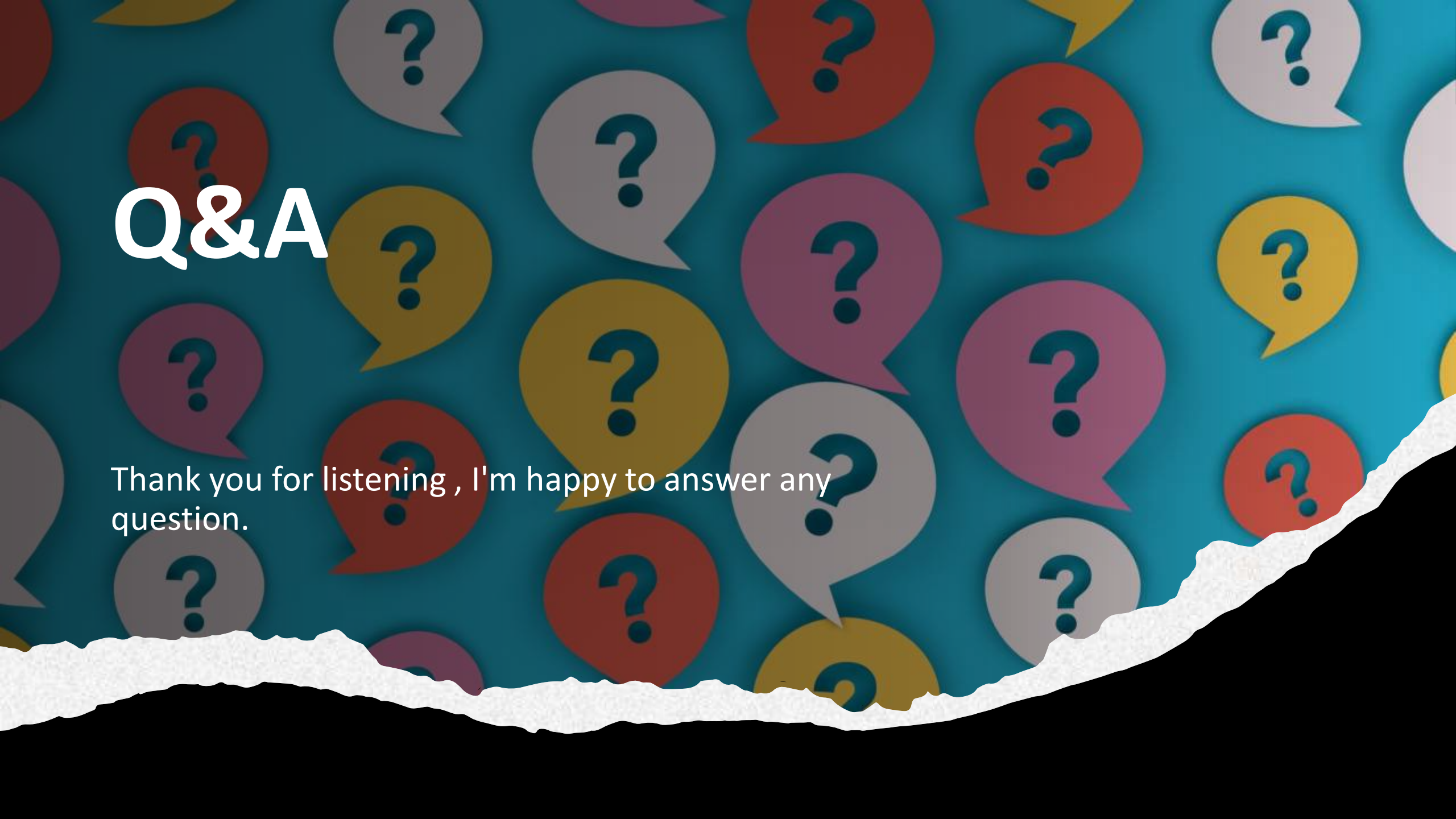
The phishing simulation successfully revealed real behavioural vulnerabilities

Many participants engaged with the phishing email, but none reported it

Students showed significant improvement in awareness after the simulation

Simulation-based learning proved more effective than traditional awareness methods

The project achieved its aim of enhancing phishing resilience through practical exposure


Q&A
Thank you for listening , I'm happy to answer any question.