TECHCRUSH PHISHING SIMULATION POLICY

Prepared by: Group 4

Date: Jan 15th, 2025

1. Purpose

This policy defines the rules and guidelines for conducting phishing simulation exercises within Tech Crush. The purpose of these simulations is to assess employee awareness of phishing threats and improve the organization's security posture through controlled and ethical testing.

2. Scope

This policy applies to all phishing simulation activities carried out for training, assessment, or academic evaluation purposes involving Tech Crush staff, systems, or communication channels.

3. Authorization

All phishing simulation activities must receive prior approval from authorized management. Simulations shall be conducted within a clearly defined scope, timeframe, and target group. Unauthorized phishing activities are strictly prohibited.

4. Ethical Guidelines

The following ethical principles shall govern all phishing simulations:
- No real malware shall be distributed.
- No real credentials shall be stolen or misused.
- All credential submissions are simulated and used strictly for awareness measurement.
- Simulation results shall not be used for disciplinary action.

5. Data Handling and Privacy

- Only interaction metrics such as email opens, link clicks, and simulated submissions shall be collected.
- All collected data shall be securely stored and accessed only by authorized personnel.
- Data shall not be shared outside the scope of this project.
- All data shall be deleted after reporting and evaluation are completed.

6. Reporting and Use of Results

The results of phishing simulations shall be used to:

- Identify weaknesses in staff phishing awareness
- Improve cybersecurity training programs
- Support risk assessment and security policy development

7. Policy Review and Compliance

    This policy shall be reviewed periodically to ensure compliance with organizational, legal, and academic requirements. Any violation of this policy may result in termination of simulation activities.