Phishing Simulation Assessment for Tech Crush

Organization: Tech Crush

Project Type: Security Awareness Phishing Simulation

Date: Jan 15th, 2026

Prepared by: Group 4

1. Executive Summary

Tech Crush conducted an authorized phishing simulation to assess employee awareness and susceptibility to phishing attacks. The exercise involved sending a simulated phishing email to selected staff members and monitoring how recipients interacted with the message.

The purpose of the simulation was to evaluate human-related security risks and identify gaps in security awareness. The campaign was conducted ethically, with no malware involved and no real credentials collected or stored.

The results show that a portion of staff interacted with the phishing email, confirming that phishing remains a significant cybersecurity risk. These findings emphasize the need for continuous security awareness initiatives and regular testing to strengthen the organization's security posture.

2. What Was Done

- A controlled phishing simulation was designed and executed with management authorization.
- A simulated phishing email was sent to staff members within a defined scope.
- User actions such as email opens, link clicks, and simulated credential submissions were tracked.
- The campaign ran for a limited period and collected only interaction metrics for analysis.

3. Key Findings

The following results were recorded during the phishing simulation:

- **Total emails sent:** 10
- **Emails opened:** 7
- **Phishing links clicked:** 7
- **Credentials submitted (simulated):** 4

These metrics provide a clear indication of staff interaction with phishing-style emails.

4. Risk Assessment

The findings indicate a **high level of phishing risk** within Tech Crush. Users who clicked phishing links or submitted credentials demonstrate vulnerability to social engineering attacks. In a real-world scenario, such actions could allow attackers to gain unauthorized access to systems or sensitive information.

Human behavior remains a critical factor in cybersecurity, and phishing attacks continue to exploit trust and lack of awareness.

5. Business Impact

A successful phishing attack could result in:

- Compromise of employee accounts
- Exposure of confidential company data
- Operational disruption
- Financial and reputational damage

Addressing phishing risks is therefore essential to protecting the organization's assets and maintaining trust.

6. Recommendations

To reduce phishing-related risks, the following actions are recommended:

1. Implement mandatory cybersecurity awareness training for all staff.
2. Conduct regular phishing simulations to reinforce awareness.
3. Establish a clear and simple process for reporting suspicious emails.
4. Strengthen email security policies and user verification procedures.

7. Conclusion

The phishing simulation provided valuable insight into Tech Crush's current cybersecurity awareness level. Although no real harm occurred, the results demonstrate that phishing remains a credible threat.

Compromised credentials could lead to internal systems, resulting in downtime and data exposure.

By adopting continuous training, routine testing, and clear security policies, Tech Crush can significantly reduce its exposure to phishing attacks and improve its overall security resilience.