Phishing Email Analysis Report

Introduction

This report analyses a suspicious email to identify phishing characteristics and improve awareness of social engineering tactics.

Email Content Analysis

Sender Name & Address: no-reply@access-accsecurity.com (note the lookalike domain)

Subject Line: Urgent: Microsoft account unusual signin activity

Message Body:

- Uses urgent language (“Immediate action required”)
- Requests unusual login attempt
- Report the user
- Contains a suspicious link: [Click Here to Verify](
  http://thebandalisty.com/track/o41372VMxcF18708448jvob1821750ugT33736NSbF176)

Observed Red Flags:

- The sender address is a lookalike, not the real Microsoft domain.
- Report the user.
- Unusual urgency and threats.
- Spelling and grammar errors.

Email Header Analysis

Header Accessed By: “Show Original” option in Gmail.

Header Findings:

- From: no-reply@access-accsecurity.com
- Reply-To: solutionteamrecognizd03@gmail.com
- Return-Path: bounce@nonkfrgr.co.uk
- SPF/DKIM/DMARC: SPF fails (unauthorized sender)

Conclusion: Addresses and technical fields do not match official sources, and sender authentication fails—strong indicators of spoofing.

Phishing Indicators List

- Sender address is not from official domain.
- Return-Path and Reply-To differ from From field.
- Message requests confidential information and uses urgency.
- Hyperlink leads to a non-official, suspicious site.
- Email fails SPF authentication.

Answers to Interview Questions

1. What is phishing?

Phishing is a cybercrime where attackers pose as trusted organizations to steal sensitive information via scam emails.

2. What signs did you spot?

Suspicious sender, urgent tone, request for credentials, generic greeting, fake link, header inconsistencies.

3. What did the header reveal?

The sender and return-path don’t match, use of bad domains, and sender fails authentication.

4. How can you tell an email is suspicious?

Unfamiliar sender, urgency, odd links, grammar mistakes, mismatched domains.

5. What should you do if you get a phishing email?

Don’t click links; don’t reply; report it to IT/security and delete it.

6. What is social engineering?

Tricking people into giving up confidential information by psychological manipulation.

7. Why is social engineering dangerous in phishing?

It exploits human trust and can bypass technical defenses.

8. How do attackers succeed?

By copying styles of real organizations and creating a sense of urgency or fear.

Conclusion

Reviewing sender information, content, and headers is crucial for identifying phishing attacks and protecting sensitive information.