Phishing Email Analysis Report

Sample Phishing Email

From: microsoftsupport@accountupdate365.com

To: user@example.com

Subject: Action Needed: Confirm Your Microsoft Account

Date: Tue, 21 May 2025 09:45:01 +0000

Dear User,

We've noticed unusual login attempts on your Microsoft account.

To ensure your security, we require you to confirm your details immediately.

Please click the link below to verify your account:

http://accountupdate365.com/verify-now

Failure to verify will result in access restrictions.

Sincerely,

Microsoft Account Team

Phishing Indicators Identified

1. Impersonated Sender:
   - Email claims to be from Microsoft but uses a suspicious domain (accountupdate365.com).

2. Suspicious URL:
   - Link leads to a non-Microsoft domain which is likely designed to steal login credentials.

3. Unusual Urgency:
   - The message pressures the user to act quickly by threatening account restrictions.

Phishing Email Analysis Report

4. Generic Salutation:

- No personal name is used, only 'Dear User'.

5. Authentication Failures:

- SPF/DKIM/DMARC checks likely fail when analyzed.

6. Domain Spoofing:

- 'microsoftsupport@accountupdate365.com' is not a valid Microsoft support address.

7. Origin IP Location:

- Header reveals sending server is from an unrelated IP range (non-Microsoft).

Conclusion

Conclusion:

This email demonstrates clear signs of phishing such as impersonation of Microsoft, use of misleading URLs, and urgency tactics.

The sending domain does not match official Microsoft domains, and header analysis would confirm failed authentication.

Users should avoid clicking on links and report such emails.