Security Alert: Reported Phishing Attempt

2025-10-02 - Shanelle McPherson - Comments (0) - Cybersecurity Awareness

Security Alert: Reported Phishing Attempt

Dear Team,

It has come to our attention that a **phishing attempt** was recently reported within our company. The suspicious email (see screenshot above) was designed to appear legitimate, requesting direct contact regarding a “task” while attempting to bypass normal communication channels.

This is a reminder that cybercriminals often use urgent or vague language to trick employees into revealing sensitive information or engaging in unsafe communication practices.

Employee Best Practices to Stay Protected:

1. **Verify the sender** – Always check the sender’s email address carefully. Look out for misspellings or unusual domains.
2. **Do not click links or open attachments** from unknown or suspicious senders.
3. **Be cautious of urgent or vague requests** – Phishing emails often pressure you into acting quickly without full details.
4. **Never share sensitive information** (passwords, credentials, company data) over email or text unless verified through official channels.
5. **Report suspicious emails immediately** by forwarding them to the IT/Security team. Do not delete them until confirmed safe.
6. **Use company-approved communication tools** for official discussions instead of responding directly to questionable emails.

Next Steps:

- The IT Security Team is actively monitoring for similar attempts.
- Please remain vigilant and report any suspicious emails right away.

Your awareness and quick action are key to protecting both yourself and the company.

Attachments

- Phishing Attempt.webp [36.21 KB]