Comprehensive IT User Support Guide: Phishing Detection & Response

1. Introduction

This guide provides employees with essential information for identifying phishing attempts, responding correctly to suspicious emails or messages, and preventing security incidents in a 1,000-employee organization. Awareness and quick action help protect company data and systems.

2. What is Phishing?

Phishing is a cyberattack in which attackers impersonate trusted entities to steal sensitive information such as passwords, financial details, or confidential company data.

Phishing attempts can appear through:
- Email
- Text messages (SMS phishing or 'smishing')
- Phone calls ('vishing')
- Fake websites designed to capture login credentials

3. Common Signs of a Phishing Attempt

Be alert for the following indicators:

- Unexpected requests for personal or company information
- Suspicious links or attachments
- Emails with spelling or grammar errors
- Sender address slightly altered to appear legitimate
- Urgent or threatening language
- Messages claiming account suspension or password expiration
- Offers that seem too good to be true

4. How to Inspect an Email Safely

Before interacting with any link or attachment, complete these checks:

- Hover over links to view their real destination.
- Verify sender email address for misspellings.
- Check for unexpected file attachment types (ZIP, EXE, HTML).
- Review the tone and urgency of the message.
- Compare suspicious messages with previous legitimate communications.

5. If You Suspect a Phishing Email

If something seems suspicious, do NOT:

- Click any links
- Download or open attachments
- Respond to the sender

Instead, follow these steps:

1. Use the company’s built■in “Report Phishing” button (if available).
2. Forward the suspicious message to IT Security.
3. Wait for confirmation before deleting the message.
4. If you already clicked a link or entered credentials, contact IT immediately.

6. After Reporting a Phishing Attempt

After IT receives your report, they may:

- Analyze the email and block similar messages
- Temporarily lock your account if compromise is suspected
- Require a password reset
- Run a malware scan on your workstation
- Notify affected teams or the entire organization if needed

7. Best Practices to Prevent Phishing Attacks

Adopt these habits to reduce risk:

- Never share passwords or MFA codes
- Use company-approved password managers
- Keep devices and software updated
- Avoid connecting to unknown WiFi networks
- Attend mandatory cybersecurity training sessions
- Double-check requests involving money, system access, or personal data

8. When to Contact IT Support

Contact IT immediately if:

- You clicked a suspicious link
- You entered your credentials into a suspicious webpage
- You downloaded an unknown attachment
- Your device begins acting unusually
- You believe your account has been compromised

9. IT Support Contact Information

IT Security & Helpdesk
Phone: (555) 123-4567
Email: security@company.com
Ticket Portal: https://helpdesk.company.com
Hours: Monday–Friday, 8:00 AM – 6:00 PM
Emergency Support: On-call security engineer available after hours

10. Conclusion

Phishing remains one of the most common security threats to organizations. By staying aware, following best practices, and reporting suspicious content quickly, employees help maintain a secure and resilient environment for all 1,000 team members.