To: All Employees

From: IT / Security Department

Date: [Insert Date]

Subject: Urgent: Cybersecurity Awareness and Phishing Prevention

Dear Team,

To ensure the safety of our company data, we are launching a mandatory cybersecurity awareness initiative focused on anti-phishing measures. Phishing remains the most common method used by attackers to gain unauthorized access to our internal systems.

Key Red Flags to Watch For:

- Emails creating a false sense of urgency or threats.
- Requests for sensitive information (passwords, social security numbers, or financial data).
- Generic greetings like "Dear Customer" or "Valued Employee."
- Suspicious links or unexpected attachments.
- Mismatched sender email addresses (e.g., @microsoft-support.net instead of @microsoft.com).

Best Practices:

- Never click on links or download files from unknown sources.
- Hover your mouse over any link to see the actual destination URL before clicking.
- Use Multi-Factor Authentication (MFA) on all available accounts.
- If you receive a suspicious email, do not reply or forward it to colleagues.

Reporting Protocol:

If you suspect you have received a phishing email or have accidentally clicked a suspicious link, please report it immediately to [Insert Email Address/Phone Number]. Early reporting is the best way to prevent a security breach.

Thank you for your cooperation in keeping our organization secure.

Best regards,

[Your Name/Department]
[Your Title]