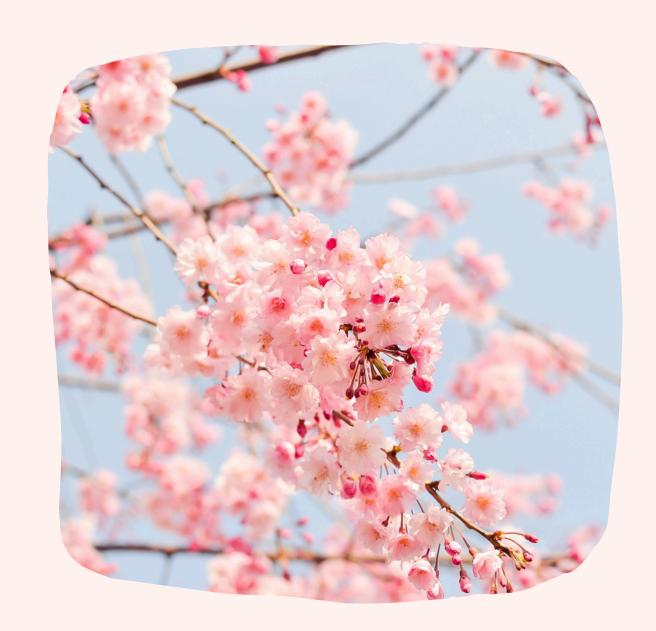


INTRODUCTION

- Definition: Phishing is a cyber attack that uses disguised email as a weapon. The goal is to trick the email recipient into believing that the message is something they want or need.
- Common Targets: Employees, customers, and anyone with access to sensitive information.
- Consequences: Data breaches, financial loss, and reputational damage.





HOW TO IDENTIFY A PHISHING EMAIL

- Suspicious Sender: Check the sender's email address for slight misspellings or unfamiliar domains.
- Generic Greeting: Be cautious of emails that do not address you by name.
- Urgent Language: Phishing emails often create a sense of urgency or fear.
- Unexpected Attachments/Links: Do not open attachments or click on links from unknown sources.

PROTECTING YOURSELF FROM PHISHING ATTACKS

- Verify Requests: Always verify email requests for sensitive information or action, especially if unexpected.
- Use Strong Passwords:
 Ensure your passwords are strong and unique across different accounts.

- Hover Over Links: Hover your mouse over links to see the actual URL before clicking.
- Report Suspicious Emails:
 Immediately report any
 suspicious emails to your IT
 department

CASE STUDIES OF PHISHING ATTACKS

Example 1: Company A lost \$1.5 million due to a successful phishing attack targeting their finance department.

2. Example 2:
Organization B
experienced a data
breach affecting
thousands of customers
due to a phishing email.

RESPONDING TO PHISHING ATTEMPTS

- Do Not Interact: Do not reply, click links, or open attachments in the suspected email.
- Report Immediately: Report the email to your IT department or use the designated reporting tool.
- Stay Informed: Keep up to date with the latest phishing techniques and prevention methods.

