Email Security Awareness

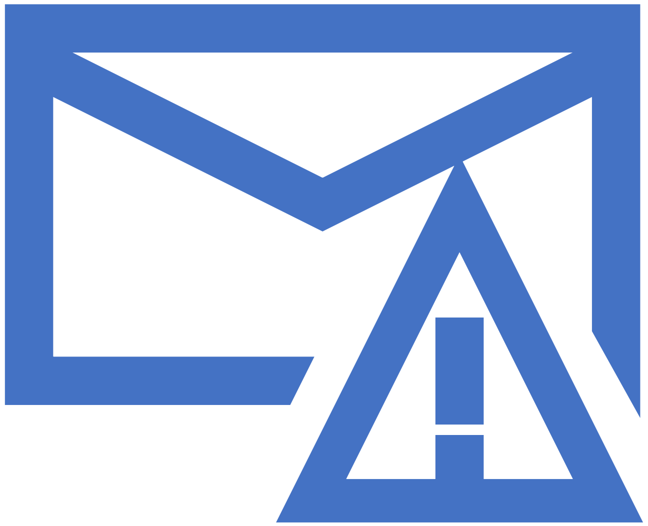
# Module 12

# Learning Objectives

- Recognize phishing and spam emails.
- Understand the risks of malicious attachments and links.
- Learn to use email encryption.
- Follow best practices for secure email communication.

# Why Email Security is Important

- Prevents unauthorized access to sensitive information.
- Protects against phishing, malware, and ransomware.
- Ensures confidentiality in email communication.
- Safeguards organizational reputation and assets.



# Recognizing Phishing Emails

- Generic greetings (e.g., "Dear Customer").
- Urgent requests for personal or financial details.
- Suspicious sender addresses or domains.
- Poor grammar and formatting errors.

# Risks of Malicious Attachments and Links

- **Malicious Attachments**: Can contain malware or ransomware.
- **Links**: May lead to phishing websites or download malicious software.
- Hover over links to verify URLs before clicking.
- Avoid downloading unexpected attachments.

# Email Encryption

- Protects sensitive information from being intercepted.
- Use tools like PGP (Pretty Good Privacy) or S/MIME.
- Verify the recipient's identity before sending encrypted emails.
- Ensure encryption keys are securely stored.

# Best Practices for Email Security

USE STRONG AND UNIQUE PASSWORDS FOR EMAIL ACCOUNTS.

ENABLE MULTI-FACTOR AUTHENTICATION (MFA).

AVOID USING PUBLIC WI-FI FOR ACCESSING EMAIL.

REGULARLY UPDATE AND PATCH YOUR EMAIL CLIENT.

# Avoiding Common Email Scams

LOOK OUT FOR **TOO-GOOD-TO-BE-TRUE OFFERS**.

AVOID CLICKING ON UNEXPECTED OR SHORTENED URLS.

BE WARY OF EMAILS REQUESTING PERSONAL OR FINANCIAL INFORMATION.

REPORT SUSPICIOUS EMAILS TO THE IT SECURITY TEAM.

https://www.cyber.gov.au/protect-yourself/securing-your-email/email-security

# References