Email Security Best Practices

Phishing Awareness

Phishing emails attempt to steal credentials or install malware. Be suspicious of unexpected emails, especially with urgent requests or attachments.

Verify sender email address carefully - attackers often use similar-looking domains. Hover over links to see actual destination before clicking.

Identifying Suspicious Emails

Red flags: Urgent requests for credentials or money, poor grammar/spelling, generic greetings, mismatched sender/reply-to addresses.

Suspicious attachments: Unexpected files, unusual extensions (.exe, .zip, .scr), files from unknown senders.

Reporting Phishing

Forward suspicious emails to phishing@company.com. Don't click links or open attachments. IT will investigate and notify you of findings.

Reporting helps protect others. Even if you're unsure, report it - better safe than sorry.

Email Attachments

Scan attachments with antivirus before opening. Be especially cautious with executable files, macros, and compressed archives.

Don't open attachments from unknown senders. Verify unexpected attachments with sender through separate communication channel.

Link Safety

Hover over links to preview destination URL. Be wary of shortened URLs or links with misspellings. Don't click links in suspicious emails.

Type URLs directly into browser for sensitive sites like banking or company portals. Bookmark frequently used sites.

Email Encryption

Use email encryption for confidential or restricted data. Encryption option available in email client for sensitive messages.

Encrypted emails require recipient to authenticate before viewing. Use for financial data, personal information, or trade secrets.

Email Retention

Follow company retention policy - don't delete emails that may be needed for legal or business purposes. Auto-deletion applies after retention period.

Archive important emails for future reference. Don't use email as primary file storage - use approved document management systems.

External Email Warnings

Emails from external senders are tagged with warning banner. Exercise extra caution with external emails requesting action or information.

Verify requests through known contact information, not information in the email itself.

Business Email Compromise

CEO fraud and vendor impersonation are common. Verify unusual requests for wire transfers or sensitive data through phone call to known number.

Don't rely solely on email for financial transactions. Follow approval workflows and dual authorization requirements.

Email Forwarding

Don't auto-forward company email to personal accounts. This violates data protection policies and creates security risks.

Use email client's mobile app or webmail for remote access. Contact IT if you need email access on personal devices.

Spam and Unwanted Email

Mark spam using email client's spam button. Don't unsubscribe from suspicious emails - this confirms your address is active.

IT maintains spam filters but some may get through. Report persistent spam to IT for filter updates.