COMPUTER it SOLUTIONS, INC.

Email Security Best Practices

Protecting Your Business from Phishing, Malware, and Fraud



Recognize the warning signs

Fraudulent messages often look authentic. A familiar logo, recognizable name, or polished writing is not proof that a message is safe.

01 PAUSE
Unexpected or urgent?

02 VERIFY
Use a known contact method

03 REPORT
Tell your IT team

01 Verify the actual sender

- Inspect the complete email address, not just the displayed name.
- Watch for changed letters, unfamiliar domains, and unexpected messages from known contacts.
- Confirm unusual requests using a telephone number or contact method you already trust.

02 Check links before clicking

- On a desktop, hover over a link to inspect its destination without opening it.
- Do not follow unexpected links to sign in to Microsoft 365, banking, or other important accounts.
- Use a known bookmark or type the official website address directly.

03 Treat attachments carefully

- Do not open unexpected ZIP files, programs, scripts, invoices, or Office documents.
- Never enable macros or bypass an antivirus warning because an email asks you to.
- Confirm unexpected attachments with the sender through a separate trusted channel.

COMMON PHISHING HOOKS “Your mailbox is full.” “Your password expires today.” “Open the attached invoice.” “We changed our bank account.”

Protect accounts and payments

04 Recognize emotional manipulation

- Be suspicious of urgent demands, threats, secrecy, or requests to act immediately.
- Look closely at unexpected document-sharing invitations and security alerts.
- Good grammar and professional branding do not guarantee legitimacy.

05 Protect passwords and sign-in codes

- Use strong, unique passwords and a reputable password manager.
- Enable multifactor authentication (MFA) wherever it is available.
- Never share passwords, one-time codes, or approve sign-in prompts you did not initiate.

06 Independently confirm payment changes

- Call a vendor using a previously verified number before changing ACH, wire, or banking details.
- Question unexpected gift-card requests, urgent transfers, and confidential financial requests.
- Do not rely solely on an email conversation to authorize significant payments.

07 Keep devices and programs updated

- Install Windows, Outlook, browser, PDF reader, and other security updates.
- Keep endpoint protection enabled; never turn it off just to open a file.
- Report recurring updates failures or security warnings to IT.

IMPORTANT A message may come from a genuinely compromised account. Verification matters even when the sender looks familiar.

Use email and cloud tools safely

08 Reject unsolicited tech support

- Do not call numbers in unexpected “computer infected” notices.
- Never grant remote access or install software at an unverified sender’s request.
- Contact your regular IT provider directly for help.

09 Verify shared documents

- Question unexpected OneDrive, SharePoint, Dropbox, or Google Drive invitations.
- Never enter your password or authentication code into a suspicious document-access page.
- Confirm unexpected shared files through a trusted channel.

10 Protect sensitive information

- Check recipient addresses carefully before sending confidential information.
- Use approved secure-sharing methods for sensitive financial or personal records.
- Avoid forwarding business mail into personal accounts without company approval.

11 Report suspicious messages

- Do not reply, click, open, or call contact details provided in a suspicious message.
- Report it to IT; use Outlook’s “Report Phishing” feature if available.
- Keep the message available if IT requests evidence; otherwise delete it after reporting.

12 If you clicked something suspicious

- Stop interacting with the email, website, or file and contact IT immediately.
- Tell IT whether you opened a file, entered credentials, approved a prompt, or made a payment.
- Follow IT instructions for password resets, session revocation, scanning, or network isolation.
- Do not conceal the mistake or erase logs and files before IT reviews them.

Before you click: quick checklist

Take 10 seconds to review these questions. If you cannot answer confidently, pause and verify first.

- ☐ Was I expecting this email?
- ☐ Have I checked the sender's actual email address?
- ☐ Does the request fit normal business activity?
- ☐ Have I independently confirmed unusual links, files, login requests, or payment changes?
- ☐ Would I be comfortable calling the sender directly to verify?

IF SOMETHING SEEMS WRONG Do not click or respond. Contact your organization's IT administrator or Computer IT Solutions immediately. Fast reporting can greatly reduce the damage from a cyber incident.

STOP. THINK. VERIFY.

Your first line of defense is a moment of caution.

COMPUTER IT SOLUTIONS, INC.

15315 NW 60th Avenue, Suite 100 • Miami Lakes, FL 33014

Office: 305-442-0136 | www.compits.net

dan@computeritsolutions.net