EMAIL ATTACHMENTS

Because email use has become so common, many computer users don’t fully appreciate the risks associated with it. The fact is that email attachments are the primary source of computer virus and malware attacks. Email attachments can conceal malicious programs and software masquerading as harmless files, but that can infect a computer if opened.

An email attachment that contains malware is meant to trick the recipient into clicking on it. They are often disguised as evites, cute pictures or stories, job postings or other interesting information. Even if an attachment appears to come from a trusted source, unless you are expecting it—don’t open it. If there is any doubt, contact the sender directly to verify.

WHAT TO WATCH OUT FOR:

□ Email messages that seem overly urgent and ask you to click on an attachment to fix a problem are almost always bogus. Verify the claim before taking any action.
□ Email attachments sent from a helpdesk, support center or other IT groups should be questioned and verified. It is extremely unlikely that a support team will ask you to open an attachment without first contacting you.
□ Email messages from friends or colleagues asking you to click on the attachment may or may not be legitimate. If you weren’t expecting the email or attachment, verify before you open it.
□ If an email message containing an attachment purports to be from a professional source, but contains improper wording or other grammatical errors, question its authenticity.

HOW TO PROTECT YOURSELF:

□ The best way to prevent a bogus email attachment from doing harm is to make sure your computer’s anti-virus software and security patches are up-to-date.
□ Learn to scan attachments with your anti-virus or anti-malware software prior to opening them.
□ Learn to carefully scrutinize email messages, even if they appear to come from a trusted source. If you are at all suspicious, don’t open the attachment.
□ Don’t be fooled by urgent messages that ask you to immediately open an attachment—this is a common tactic employed by cyber-criminals to catch you off guard.
□ Report any suspected malicious software attachment or suspected incident immediately to the proper support team or IT group.

Key Points

- Email attachments can contain malware.
- Don’t open attachments from unknown senders.
- Carefully scrutinize any message containing an attachment.
- Verify the authenticity of unexpected attachments.