

Using Caution with Email Attachments

Original release date: September 10, 2009 | Last revised: May 31, 2017

Why can email attachments be dangerous?

Some of the characteristics that make email attachments convenient and popular are also the ones that make them a common tool for attackers:

- Email is easily circulated – Forwarding email is so simple that viruses can quickly infect many machines. Most viruses don't even require users to forward the email—they scan a users' computer for email addresses and automatically send the infected message to all of the addresses they find. Attackers take advantage of the reality that most users will automatically trust and open any message that comes from someone they know.
- Email programs try to address all users' needs – Almost any type of file can be attached to an email message, so attackers have more freedom with the types of viruses they can send.
- Email programs offer many "user-friendly" features – Some email programs have the option to automatically download email attachments, which immediately exposes your computer to any viruses within the attachments.

What steps can you take to protect yourself and others in your address book?

- **Be wary of unsolicited attachments, even from people you know** – Just because an email message looks like it came from your mom, grandma, or boss doesn't mean that it did. Many viruses can "spoof" the return address, making it look like the message came from someone else. If you can, check with the person who supposedly sent the message to make sure it's legitimate before opening any attachments. This includes email messages that appear to be from your ISP or software vendor and claim to include patches or anti-virus software. ISPs and software vendors do not send patches or software in email.
- **Keep software up to date** – Install software patches so that attackers can't take advantage of known problems or vulnerabilities (see [Understanding Patches](#) for more information). Many operating systems offer automatic updates. If this option is available, you should enable it.
- **Trust your instincts** – If an email or email attachment seems suspicious, don't open it, even if your anti-virus software indicates that the message is clean. Attackers are constantly releasing new viruses, and the anti-virus software might not have the signature. At the very least, contact the person who supposedly sent the message to make sure it's legitimate before you open the attachment. However, especially in the case of forwards, even messages sent by a legitimate sender might contain a virus. If something about the email or the attachment makes you uncomfortable, there may be a good reason. Don't let your curiosity put your computer at risk.
- **Save and scan any attachments before opening them** – If you have to open an attachment before you can verify the source, take the following steps:
 1. Be sure the signatures in your anti-virus software are up to date (see [Understanding Anti-Virus Software](#) for more information).
 2. Save the file to your computer or a disk.
 3. Manually scan the file using your anti-virus software.
 4. If the file is clean and doesn't seem suspicious, go ahead and open it.

- **Turn off the option to automatically download attachments** – To simplify the process of reading email, many email programs offer the feature to automatically download attachments. Check your settings to see if your software offers the option, and make sure to disable it.
- **Consider creating separate accounts on your computer** – Most operating systems give you the option of creating multiple user accounts with different privileges. Consider reading your email on an account with restricted privileges. Some viruses need "administrator" privileges to infect a computer.
- **Apply additional security practices** – You may be able to filter certain types of attachments through your email software (see [Reducing Spam](#)) or a firewall (see [Understanding Firewalls](#)).

Both the National Cyber Security Alliance and US-CERT have identified this topic as one of the top tips for home users.

Author

US-CERT Publications