

The risks of receiving email attachments

Not only does email allow us to communicate with people all over the world, but it also lets us share documents via email attachments. Email attachments are files sent along with an email message. An attachment can be any kind of file at all, including formatted word-processed documents, spreadsheets, databases, graphics, and even software.

Warning: Attachments can spread viruses. Unfortunately, sending and receiving email attachments is not without risk -- attachments can contain computer viruses. Do not open or save attachments that you weren't expecting or which seem suspicious. If you receive an email message that contains an attachment from someone you know, you can protect yourself from the possibility of infecting your system by not opening it until you've saved it to your hard drive and scanned with an anti-virus program.

If you receive an e-mail attachment, even if it is coming from a name or email address you recognize, do not open under any circumstances. If you think it may be legitimate, simply e-mail the person and ask "did you just send me an email attachment?" or create a system with that person where they can notify you if they have sent an attachment. It is much easier to take the time to ask than it is to try to undo the damage after you've opened it.

Be suspicious of any attachment or link. Many self-propagating viruses will mail themselves to you before the sender has discovered that his/her machine is infected. Many viruses and Trojans spread as "worms" and modern worms often appear to have been sent by someone you know. Smart worms scan your address book, especially if you use Microsoft Outlook or Outlook Express, and replicate by masquerading as legitimate attachments from legitimate contacts.