Email Attachments: When Is Opening Them Safe?

Software / Articles

by
Jessica Drew

The internet today can be risky for the safety of the expensive laptop or desktop you invested in because hackers are continually coming up with new ways to infect users computers. However, the majority of users' computers by far become infected with the worst forms of malware, including viruses, Trojans and worms, from downloading malicious **email attachments**. It s crucial to become savvy in this area and know when it s safe to open email attachments and when you should simply delete the email because it definitely looks suspicious. Sometimes, educating yourself on a few key parameters can provide better protection than the best antivirus software available. Here is the gist of what you need to know about email attachments and guarding the safety of your computers:

How Malware is Spread Through Email Attach

Before viruses that spread through email attachments can infect your computer, you must first download an infected attachment. It would seem that most users would simply not download email attachments from senders they do not trust, but it s not that simple. Scammers often hack into users' email accounts to send malicious attachments to their contacts.

Today's hackers have advanced software for guessing common, name- and birthday-based passwords that allows them to access hundreds or even thousands of email accounts. What this means is that you can actually receive an email from a good friend or family member with a dangerous email attachment. While the malicious email attachment was sent from your friend s account, your friend did not send the email the person who hacked into his or her account did. However, users are inclined to trust the contents of emails from friends and family.

Second, many email attachments scams come from senders who pose as banks or other authoritative entities emailing you about an issue with your account. These messages say something to the tune of There is a problem with your account at XYZ (which is a real bank or organization in which you do have membership). Please open the attached file to view your balance or statement, credits or monies owed and so forth."

The email appears professional but vague, and then curious, and average users become slightly concerned and tend to open the attachment to try to figure out what is wrong with their accounts. However, the attachment is bogus, and accessing it will actually download a virus or malware and install it on your computer. Unfortunately, many antivirus software suites will not detect that an infection has occurred until after the fact, once you have already downloaded it.

How Can You Tell When Email Attachments Are Safe?

With all these sophisticated methods that hackers hold up their sleeve, it may seem impossible to distinguish between suspicious emails and legitimate messages. However, there is actually an easy way to tell if email attachments are safe that works the vast majority of the time. You can tell if an email attachment is safe by assessing the file extension.

A file extension is the three letters that follow the period at the end of the file name. Microsoft has classified several types of dangerous extensions; however, only a few are considered safe. These are GIF, JPG or JPEG, TIF or TIFF, MPG or MPEG, MP3 and WAV. These extensions represent different file types and are the formats that the majority of internet users tend to send as email attachments.

If you receive an email even if it is from a friend or a bank that does not have one of the file extensions listed above after the file name and subsequent period, you should never open the attachment unless you know for certain that it is legitimate. Other file extensions that are commonly sent as email attachments such as DOC, XLS and TXT, which represent text documents and Excel files, can be infected. However, many users send these types of documents for work-related reasons, and if you know the sender and you are expecting the file or know what it s about, these attachments should be safe to open as well.

Finally, you should be exceptionally wary of files with double extensions, such as image.gif.exe. The only extension that matters is the last one. In the example above, EXE represents an executable file that will automatically run software upon download. Files with double extensions are almost always deceptive and malicious in intent.