Avoiding Dangerous Attachments

Prevent an attachment from infecting your computer or network with malicious software.

Know Your Attachment Types

While any attachment can be dangerous, these types can be especially harmful:

Executable files
(.exe, .msi, .js extensions)
Avoid these attachments. They install and run applications.

Compressed files
(.zip, .jar, .rar, .7z extensions)
These are a favorite hiding place for malware.

Microsoft® Office® files
(.doc, .docx, .xls, .xlsx, .ppt, .pptx extensions)
Office macros can contain malicious code. Use extra caution and don't enable macros.

Treat Attachments Carefully

Follow these steps to stay safe:

1 Seek Confirmation from Sender
Whenever possible, verify the attachment is legitimate. Use a new message or phone call. Don't reply to the original email.

2 Examine the Details
Does the attachment type seem appropriate? Do the language and content seem correct?

Still not sure if an attachment is safe?
Check with your IT or security team for help.