FILE TYPES THAT CAN HACK YOU

Ask Grammy™

USUALLY SAFE TO OPEN

(Only if you trust the sender)

.pdf – Documents
.jpg / .jpeg / .png – Photos & images
.txt – Simple text files
.mp3 / .mp4 – Audio & video

Think of these as: "View-only" files

BE CAREFUL

(These can hide dangerous files inside)

.zip / .rar – Compressed folders
.iso / .img – Disk image files
.docm / .xlsm / .pptm – Documents with macros

You may not see the danger until you open or extract them

Think of these as: "Sealed boxes"

HIGH RISK

DO NOT OPEN from email or messages

.exe – Programs (can install malware)
.bat / .cmd – Command scripts
.vbs / .js / .ps1 – Script files
.scr – Screensavers (actually programs)
.lnk – Shortcuts (can be disguised)
.hta / .cpl / .jar – Less common, still risky

These don't just open... they run

COMMON SCAM TRICKS

Double endings (for example: invoice.pdf.exe (not a PDF!)

Hidden endings
Looks like a safe file... but isn't

Fake icons
Looks like a document, acts like a program

Password-protected ZIP files
Prevents security scanning

THE 5-SECOND SAFETY RULE

Did I go get this file... or did it come to me?

- You went to a trusted website → usually OK
- It showed up unexpectedly → don't open it

IMPORTANT REMINDER

Companies like PayPal, Amazon, Microsoft, and the IRS: Do NOT send random attachments for you to open. If you get one, it's a red flag

WHAT TO DO INSTEAD

- Don't open the file
- Go directly to the company's official website
- Log into your account there
- Check for messages or alerts

GRAMMY'S BOTTOM LINE

If you weren't expecting it, don't open it
If you don't recognize the ending, don't trust it