

Hidden File Extensions: Safe Demo & Protection Guide

Windows + macOS | Simple, practical, and fact-checked

First understand this: Hiding an extension only changes what the filename looks like in Finder/File Explorer. It does **not** convert the file into another format. For example, renaming or hiding part of a filename does not turn an executable into an image.

1. Safe demo: see how extension hiding works

Use **only your own harmless test files**. You do not need malware or a real executable for this demo.

Windows 11

To hide extensions for the demo	To show them again (recommended)
Open File Explorer.	Open File Explorer.
Open the three-dot menu > Options.	Select View > Show.
Open the View tab.	Turn ON File name extensions.
Check "Hide extensions for known file types", then OK.	You should now see extensions such as .jpg, .pdf, .exe, etc.

Note: On Windows 10, the wording/layout can differ. The key setting is **Hide extensions for known file types**; Microsoft also documents turning extensions on from File Explorer.

macOS

Hide extension for one test file	Show extensions for protection
Select your harmless file in Finder.	Open Finder > Settings > Advanced.
Press Command-I (Get Info).	Turn ON "Show all filename extensions".
Expand Name & Extension.	This overrides the per-file "Hide extension" setting and shows extensions.
Check "Hide extension".	For one file, Command-I > Name & Extension > uncheck "Hide extension".

2. What is the double-extension trick?

A filename can contain more than one dot. What matters is the file's real type and the extension being used by the operating system/application - not the part of the name that merely looks familiar.

Filename	What it suggests at a glance	What to notice
photo.jpg	Image	Ends in .jpg

photo.jpg.exe	May look image-related because “.jpg” appears in the name	Ends in .exe; on Windows this is an executable file type
invoice.pdf.exe	May look PDF-related	Ends in .exe, not .pdf

Important: An .exe file is not automatically malware. Legitimate Windows software also uses .exe. The red flag is an unexpected executable, especially when it is presented as a photo/document or comes from an untrusted source.

3. How to identify a suspicious file

- 1. Show filename extensions.** This removes one easy source of confusion.
- 2. Read the ending carefully.** A name such as photo.jpg.exe ends in .exe.
- 3. Do not trust the icon alone.** File icons can vary; use the extension and file information as clues.
- 4. Check where it came from.** Be cautious with unexpected email, DM, cloud-share, or download files.
- 5. Pay attention to OS warnings.** Do not bypass security prompts just to open an unknown file.
- 6. When unsure, do not run it.** Verify with the sender or scan/check the file using your normal security tools.

4. Quick protection settings

Windows	macOS
File Explorer > View > Show > File name extensions = ON	Finder > Settings > Advanced > Show all filename extensions = ON
Keep Windows security warnings/protectations enabled.	Keep macOS security warnings/protectations enabled.
Treat unexpected executable/script files cautiously.	Do not assume a familiar-looking filename or icon proves the file is safe.

5. If you already opened something suspicious

Do not keep reopening it. Run your operating system's security scan, remove/quarantine anything it flags, and update the OS/security software. If you entered a password after opening the suspicious file or believe an account may be affected, change that password from a trusted device and review active sessions/sign-ins.

One-line takeaway

Do not decide whether a file is safe from its name or icon alone. Show extensions, check the real file type, and be cautious with unexpected files.

Fact-check sources: Microsoft Support - File Explorer / common filename extensions; Apple Support - Show or hide filename extensions on Mac.

Microsoft Support | Apple Support