Dangerous-Files

Note: For a better browsing experience we give the "answer" here at the beginning. See below for a more detailed explanation of this threat.

What file types can be dangerous

Although none of the listed file types are malicious per se, they are often used by attackers to "hide" malware. Most commonly:

- LibreOffice:
  - `.odt`: Text documents (Writer)
  - `.ods`: Spreadsheets (Calc)
  - `.odp`: Presentations (Impress)
  - `.odg`: Drawings (Draw)
  - `.odb`: Databases (Base)
- Microsoft Office:
  - `.docx`: Word documents
  - `.xlsx`: Excel spreadsheets
  - `.pptx`: PowerPoint presentations
- `.pdf`: PDF's
- even image formats like `.gif` have reportedly been exploited, also on mobile devices.

> [!tip]
>
> It is recommended to avoid the above "complex" file types if they are not necessary. If you still have to open such a file from an untrusted source, we recommend using Dangerzone.
>
> Use text files and markup languages like markdown if possible instead.

Why this matters

> [!note] It is a matter of security culture to reconsider if it's really necessary to send an invitation text as a PDF or a draft of a press release as Word document. If it is enough to use the possibilities, that safe markup languages like markdown give you, them use just them.

Markdown is even compatible to collaborative tools like e.g. Nextcloud.

In many contexts we see that people are kind of ashamed of sending plain text invitations for example. They feel that they owe their friends some more effort than just text. While this shows a pretty nice property of friendship, we also have to talk about the problems that this brings along and that it might be worth it to break this behavior down towards a more conscious approach.

What is a file type

Different programs expect their files to have a specific format. They expect the files to follow a pattern that the program recognizes to function correctly.

Each file type is typically identified by a specific extension (such as `.odf`, `.pdf`, `.jpg`), which signals to the operating system what program should open it and how it should behave. For example, if you click on a file that ends with `.pdf`, the operating system knows that is has to open the file with a PDF reader and not with you music player.

How can files be dangerous

Consider a simple text file (not a word document, but a simple plain text file!). A normal text file contains, no surprise, text, which is nothing else than characters, like "A", "a", ";", "/" and so on. Those text file can be read and displayed from simple programs like Gnome's "gedit", Windows notepad, and so on. They are not capable of advanced features, such as calculating tables, like Excel, or LibreCalc.

More advanced programs like Excel, PowerPoint, or modern PDF viewers are capable of much more advanced features. PDF viewers for example can display interactive forms, that you can fill out right inside the PDF viewer. They can have drop-down menus and more.

> [!caution] This means, that your PDF viewer, PowerPoint, Excel etc. are able to **execute additional code**, that is delivered inside the file they are processing.

While this is necessary to use the full feature set of the program, the capability to execute additional code can expose severe security risks.

You probably all heard about viruses being distributed through PDFs. This is exactly what is exploited here:

> [!note] An attacker can smuggle some malicious code inside the PDF. You open the PDF with your PDF viewer. The PDF viewer detects some code and thinks: "Ah, I have to execute this, so that the user has the full functionality of this file" and executes the code, which can then perform malicious actions such as stealing your data and sending it to the attacker.

Version #3
Erstellt: 2026-05-20 17:43:09 UTC von ESC-IT Migration Bot
Zuletzt aktualisiert: 2026-05-23 14:49:00 UTC von ESC-IT Migration Bot