What could happen if I download and open a malware attachment?

Opening a malware attachment is like letting a spy into your computer.
The spy can then:

- steal your documents and private information
- use your computer's camera to watch you
- use your computer's microphone to listen to you
- record every keystroke to steal your passwords

… and much more.

How can I share or receive a file then?
Do not send attachments to anyone. Make it a point with your contacts to discourage them from sending one to you.
If you receive an email attachment and you don't recognize the sender or the email address, don't open it and don't reply. Ignore it. If you are expecting an email with an attachment from someone, take a minute to confirm via text message or a phone call that they actually sent it before downloading.
Even if you have confirmed the sender, stay safer by following these steps:

1. Use an email service that lets you view attachments online without downloading them (for example, Gmail lets you preview attachments in Google Drive). This allows you to see what's in a document without actually having to download or open it.
2. Upload files to platforms like Google Drive, Dropbox, or other file-sharing services instead of emailing them.

Remember:

The best thing to do when you receive an email attachment is to ignore it. Start getting used to not only not opening attachments, but also not sending them.
Be smarter than the attackers. Start Detaching yourself from Attachments!