

# HOW TO RECOGNIZE A MALICIOUS ATTACHMENT

You received an email with an attachment. Do you download it?  
Follow these steps to make a safe decision.

## READ WARNINGS

- » If your email service or antivirus software warned the attachment is dangerous, **DO NOT DOWNLOAD!**
- » Some hackers will "warn" you that you should ignore such alerts. This is a trick!  
**NEVER IGNORE MALWARE ALERTS**

## EXAMINE MESSAGE

- » Did it come from a legitimate source?
- » Does the content of the email look normal?
- » Would you expect an attachment from this sender?
- » If you answered **NO** to any of these, the attachment is likely **MALICIOUS**

## INSPECT FILE EXTENSION

Take a look at the file extension (the part that follows the dot). Be suspicious of the following extensions:

### .EXE

- » **DO NOT DOWNLOAD!** This is an executable file
- » Most email clients block .EXE attachments

### .ZIP, .7z, .RAR and other archived files

- » Archiving is a common way to hide malware from antivirus
- » Be extra suspicious of password-protected archives

### DOCX, XLSM, PPTM

- » These documents contain MACROS, or scripts hackers often use to run malicious code

### UNKNOWN or MISSING EXTENSIONS

- » If you don't recognize the extension **DO NOT TRY OPENING THE FILE!**

## USE CAUTION

- » Even if a file is a simple DOC or PDF document, think twice before opening it
- » If you can, **contact the sender** using an alternative channel (email or IM) to verify
- » Use your email client **Preview** feature before downloading
- » Make sure that all software you use for viewing documents has the latest **security patches** installed