HOW TO RECOGNIZE A MALICIOUS ATTACHMENT

WARNING !

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

1 READ WARNING

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

2 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**

3 INSPECT FILE EXTENSION

Please take a look at the file (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

DOCM, 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!**

4 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

Source : www.infosecinstitute.com

FIS Financial Information Services

Make LIFE Easier