

## Anti-Virus Dangerous File Attachments

The following is a list of file attachments that may be **blocked** by the service (the attachments are removed from emails before delivery to you and placed in a quarantine area for 30 days should you wish to receive them): [If you wish to receive these files from someone you know, ask them to zip the files first. John Draper]

# These are known to be dangerous in almost all cases.

- .reg Possible Windows registry attack
- .chm Possible compiled Help file-based virus
- .cnf Possible SpeedDial attack
- .hta Possible Microsoft HTML archive attack
- .ins Possible Microsoft Internet Comm. Settings attack
- .jse\_ Possible Microsoft JScript attack
- .lnk Possible Eudora \*.lnk security hole attack
- .ma\_ Possible Microsoft Access Shortcut attack
- .pif Possible MS-Dos program shortcut attack
- .scf Possible Windows Explorer Command attack
- .sct Possible Microsoft Windows Script Component attack
- .shb Possible document shortcut attack
- .shs Possible Shell Scrap Object attack
- .vbe or .vbs Possible Microsoft Visual Basic script attack
- .wsc .wsf .wsh Possible Microsoft Windows Script Host attack
- .xnk Possible Microsoft Exchange Shortcut attack

# These 2 added by popular demand - Very often used by viruses

- .com Windows/DOS Executable
- .exe Windows/DOS Executable

# These are very dangerous and have been used to hide viruses

- .scr Possible virus hidden in a screensaver
- .bat Possible malicious batch file script
- .cmd Possible malicious batch file script
- .cpl Possible malicious control panel item
- .mhtml Possible Eudora meta-refresh attack

# Deny filenames ending with CLSID's

{[a-hA-H0-9-]{25,}\}

Examples:

A977FF0C-8757-4E76-8533-482F91946233

000209FF-0000-0000-C000-000000000046

# Deny filenames with lots of contiguous white space in them.

Filename contains lots of white space

# Deny all other double file extensions. This catches any hidden filenames.

Found possible filename hiding

Examples:

.txt.pif

.doc.pif

.doc.com

.txt.exe