Files Blocked by Exchange Online Protection

Files stripped by the State of Montana email Gateway.

Currently the State of Montana uses ProofPoint (PPT) as our mail gateway. There are two scenarios in which you will not receive a file that is attached to an email sent to you: if the file contains a virus, or if the file type matches one of the following file types. Please note, while we list the common extensions it's not the file extension that is checked it is the actual file type itself that matters.

If PPT scans the attached file and detects a virus, it will strip the attached file and discard it. PPT will send you a notification that the file is infected. In this situation, the sender will need to clean the file (and likely his/her computer) and resend the cleaned file.

If PPT detects a match between the file and the list of blocked files, it will also discard the file and send notification to you. In this scenario, it is recommended to use a file transfer service such as the States (https://transfer.mt.gov) or One Drive or another approved file transfer service.

In both of these scenarios, we **do not** keep copies of the blocked/infected files and are unable to retrieve the discarded files.

The current list of file extensions blocked for e-mail is;

386,3gr,add,ade,asp,bas,bat,chm,cmd,com,cpl,crt,dbx,dll,exe,fon,hlp,hta,inf,ins,isp,js,jse,lnk,mdb,mde,msc,msi,msp,mst,ocx,pcd,pif,reg,scr,sct,shs,shb,url,vb,vbe,
vbs,vxd,wsc,wsf,wsh,ws,ps1,ps1xml,ps2,ps2xml,psc1,psc2,msh,msh1,msh2,mshxml,msh1xml,msh2xml,scf,class,jar,jnlp,pyw,pyz,pyzw,psdm1,appcontent-
ms,hpj,
settingcontent-ms,website,mcf,printerexport,theme,vbp,xbap,xll,xnk,msu,grp,py,psd1,cer,pyc,der,pyo,pl,diagcab,cnt,zace,ani,app,csh,der,fxp,gadget,ht,htt,its,
ksh,mad,maf,mag,mam,maq,mar,mas,mat,mau,mav,maw,mda,mdt,mdw,mdz,mid,ops,pi,plg,prf,prg,pst,tmp,vsmacros,vsw,wmf,wmv,xnk,

This is not an all inclusive list, additional file types such as any form of executable file and commonly used malicous file types are also stripped.

As of October 2019 Encrypted or Password Protected files (including PDF's) are now stripped. While the state has removed encrypted files since 2012, please see below, PDF's were allowed due to limitations in previous gateway solutions. With the current solution if a PDF or any other file type can be scanned and is non-malicious it will be delivered, however, if the file is encrypted or password protected and it cannot be scanned by the gateway it will be stripped. Users will still receive the original e-mail and any other attachments than can be scanned, they will also be notified what attachments were stripped and why.

Finally, we block macro enabled files sent from external senders.
Macros can allow for the injection of malware into a computer system without the end-user's awareness.
This attack vector has increased in popularity with threat-actors over the past three years and is often used to introduce ransomware into networks.
These extensions include: *.docm, *.dotm, *.potm, *.ppam, *.ppsm, *.pptm, *.xlam, *.xlsb, *.xlsm, *.xltm

SITSD apologizes for the inconvenience that this may cause, and recommends the use of the State's secure file transfer service that has built-in antivirus features that scan any and all files that traverse through it.
This can be found at https://transfer.mt.gov.

Note: As of July 2012 encrypted compressed file attachments are now blocked.
All of those file extensions either have, or have had, security exploits embedded in them which pose significant risks to the State's network and computer resources.