



MINIMISE THE RISK OF THE CRYPTOLOCKER VIRUS

Ransomware is malicious software that cyber criminals use to hold your computer or files for ransom, demanding payment from you to get back your data. We have created a list of 10 things you can do to minimise the risk of your business being affected.

IS YOUR OPERATING SYSTEM & SECURITY SOFTWARE REGULARLY UPDATED?

Updating your operating system with the latest security patches, updates, and drivers ensures that your computer is up-to-date and will help keep your computer free from viruses and other security threats.



ARE YOUR EMAILS FROM A LEGITIMATE SOURCE?

Opening attachments now is always a little bit iffy, so only open attachments that you are expecting. Even emails that appear to be from a legitimate source are suspicious.



CONSIDER MOVING MORE DATA TO THE CLOUD

Data stored in online document libraries (i.e. SharePoint, DropBox, Google Drive) are access by web URL instead of a drive letter. These documents are inaccessible by CryptoLocker.

A great thing about SharePoint document libraries is that they can be used in Windows Explorer just like a folder in a network share. Not only is the data more accessible, but you escape update and maintenance of another server.



SHOW HIDDEN FILE EXTENSIONS

One way that Cryptolocker frequently arrives is in a file that is named with the extension ".PDF.EXE", counting on Window's default behavior of hiding known file-extensions. If you re-enable the ability to see the full file-extension, it can be easier to spot suspicious files.

If you are unsure about this step, ask your IT Manager or provider.



THINK YOU'VE BEEN COMPROMISED?

If you believe you have been compromised, disconnect your computer from networks immediately i.e. turn it off, and seek professional advice.

If you run a file that you suspect may be ransomware, but you have not yet seen the characteristic ransomware screen, if you act very quickly you might be able to stop communication with the C&C server before it finish encrypting your files.

Acting quickly could save your business precious time and effort.



USE REPUTABLE ANTIVIRUS

It is always a good idea to have both anti-malware software and a software firewall to help you identify threats or suspicious behavior.

Malware authors frequently send out new variants, to try to avoid detection, so this is why it is important to have both layers of protection.



REGULARLY BACKUP

The single biggest thing that will defeat ransomware is having a regularly updated backup.

If you are attacked with ransomware you may lose that document you started earlier this morning, but if you can restore your system to an earlier snapshot or clean up your machine and restore your other lost documents from backup, you can rest easy.



EDUCATE STAFF

Make sure your staff are educated in good computing practices and know how to spot threats, even minor ones.



BLOCK .EXE FILES OVER EMAIL, INCLUDING WITHIN ZIP FILES

If your gateway mail scanner has the ability to filter files by extension, you may wish to deny mails sent with ".EXE" files, or to deny mails sent with files that have two file extensions, the last one being executable ("*.*.EXE" files, in filter-speak).

These are a lot of techy words that don't mean a lot to many people, so ask your IT Manager or provider.



USE SYSTEM RESTORE

You might be able to take your system back to a known-clean state. However, newer versions of Cryptolocker can delete "Shadow" files from System Restore, which means those files will not be there when you try to to replace your malware-damaged versions.



It is always best practice to protect yourself against data loss with regular backups. That way, no matter what happens, you will be able to restart your digital life quickly.

Want to learn more or get more details? Great!

info@focus.net.nz



www.focus.net.nz