Important Ways to Prevent Data Loss

337 TDO KB October 24, 2023 Setup 8.13K

Overview

This article will go over how to protect your data in TDO.

Detailed Instructions

Protect your data

In order to prevent massive data loss due to malware or ransomware (commonly seen as the Cryptolocker), please ensure that you are backing up your data using the TDO Backup Utility and that your IT has a strong Antivirus solution installed that has the proper Exclusions created in order for TDO to run.

In the event that ransomware reaches your TDO directory, unless there is a backup of your data there is no way that your data can be recovered.

We have had several offices lose months and sometimes years' worth of data due to not following our Best Practices.

BACKUPS ARE NOT OPTIONAL

It is the Doctor and IT's responsibility to ensure that backups are run at your office. TDO Tech Support is happy to help set up the Backup Utility, but someone at your office MUST take responsibility in ensuring the backups are running without errors.

Ideally, there should be a backup running on an admin machine in the event there is a problem on your server, as well as a backup running to an external hard drive.

It is also strongly recommended that there is a cloud backup run which is something that comes with TDO Cloud Services.

For more information on setting up a backup using the TDO Backup utility, please read the following article:

Configuring a TDO Backup

Note: If your IT would like to use a different utility to back up data on the server, it must be **in addition** to the TDO Backup, not in place of it.

Antivirus Solutions

It is strongly recommended that your IT have an antivirus solution in place.

Please view our article on Antivirus article to see which antivirus programs are not recommended, as well as proper exclusions that need to be created.

Antivirus Exclusions

There may be additional programs recommended by your IT to help prevent against threats on your workstations (such as Malwarebytes, Adblock, etc) and it is completely fine to use those but it will be up to your IT to ensure that none of those programs conflict with TDO.

What to Do if Infected by Ransomware

Your absolute first step will be to contact your IT who will need to do a thorough analysis of the files affected and locked for use. Also, your IT will find the computer which initially contracted it and fix that computer.

At this point, the files that are locked will need to be replaced with files from a backup.

If files encrypted by cryptolocker or other ransomware have not been backed up, they will be unrecoverable.

Online URL: https://kb.tdo4endo.com/article.php?id=337