DEFEAT RANSOMWARE: BACKUP YOUR DATA

*Posted on **May 07,2017** by **IT Communications***

The destructive Petya ransomworm caused destruction and major interruptions of services around the world last week. Unfortunately, it's becoming progressively more difficult to avoid these attacks as cybercriminals become more clever and inventive in their methods. While there are ways to prevent that you fall prey to such an attack, there's one thing you can do which will ensure that you are safe. And it's not technical or difficult to do.

Once a week, backup all your data. Yes, this is a menial, boring administrative task - and we all hate those, but by ensuring that your data is safe and sound elsewhere, it won't matter if your PC is infected by ransomware or any other malware. If you do lose your data, you will have another version available.

Here are a few quick tips to help you:

1. Choose one day a week which suits you and make an appointment in your diary to do a **weekly backup**.
2. Try not to overwrite your previous backup. Rather make **consecutive copies** in various folders on your external hard drive or on your network space and name each with the particular day's date. If any of the documents become corrupt for some reason, you can always fall back on a previous version.
3. **Regularly check** that **the medium** on which you made your backup is still in working order and you're able to access your documents.
4. Use **more than one backup medium**, for example, your network space AND an external hard drive.

Where should you backup data?

1. Each staff member has access to his/her own **network space** (usually the h-drive) where you can save an allocated amount of data for free. You have 1GB at your disposal to backup your most critical documents. At an extra cost of R10-00 per 1GB this space can also be increased. This network space is also available via the web at storage.sun.ac.za if you find yourself away from the SU network.
2. On your **departmental network space** (usually the g-drive). The departmental drive can be used for files used by more than one person and 15GB is allocated to each department. SharePoint can also be used by groups for sharing documents.
3. **OneDrive** allows each staff member 5TB of storage space. This is available via the Office365 suite. https://portal.office.com/
4. If you choose to have your data close at hand, get yourself an **external hard drive**. Never save important data on a flash drive – its sole function is for transporting data from one device to another and is not a dependable medium for backup. Just ensure that these devices are stored somewhere else (not also in your office) or in a safe. If confidential, SU documents are kept on an external hard drive, files have to be protected with a password or encrypted. Keep in mind that if you lose the password, not even IT can salvage your data.
5. Alternatively, you can save data in the cloud. We've already mentioned OneDrive, but **GoogleDrive or Dropbox** are also examples of this. It is extremely important that cloud storage is only for personal use, not for any academic information or sensitive data. Also keep in mind that if you use more than one device, you have to sync data across devices and this will incur costs.

More tips on backups, as well as activating Windows' automatic backup function on www.backblaze.com.

Posted in:E-mail,Security,Tips | Tagged:Data Backup,Ransomware | With 0 comments