



# 2014

## How Should I protect my computer files from ransom hackers?

# How should I protect my computer files from ransom hackers?

## Articles report files encrypted by hackers for financial gains:

<http://news.techworld.com/security/3415635/ransom-hackers-encrypt-medical-centres-entire-database/>

<http://www.christianpost.com/news/crypto-locker-virus-hackers-give-users-100-hours-to-pay-ransom-for-malware-removal-or-lose-all-files-107519/>

## Discussion:

Ransomware attacks your data by encrypting important files and demanding a ransom in return for decrypting them. Securing your important files behind a firewall, may not be sufficient. The best way to protect against ransomware is to make frequent backups of your important files, and keep the backups on a different system. But more copies increases the chances of your important files being stolen.

## Protect your files and backups with Chameleon:

LucidPort's Chameleon encrypts files and drives, internal and external, with secure AES encryption. **One device for all your data**

1. Create encrypted internal or external drives to store your sensitive files.
2. Encrypt individual files and folders.
3. Without the Chameleon, the drives and files are not readable, but they can still be copied and backed up just like normal files. Use automatic backup software to copy Chameleon encrypted drives and files. For ultimate safety, send the backups to a remote site or cloud storage. Since they're encrypted, it's safe to store them anywhere.
4. Encrypted files can still be hijacked by ransomware, but because you have a recent backup, you can discard the hijacked files and restore from the (encrypted) backups.

For details, please visit these LucidPort websites

Chameleon FAQ : <http://www.lucidport.com/faq.html>  
Back up your data: [http://www.lucidport.com/tutorial\\_backup.html](http://www.lucidport.com/tutorial_backup.html)