

What is Ransomware?

Ransomware is a cyber attack that locks and encrypts a victim's computer or device data, then demand a ransom to restore access.

There are multiple types of **ransomware**, all equally as dangerous.



Ransomware Attacks

- *Crypto Malware*
- *Screen Lockers*
- *Scareware*
- *Doxware (leakware or extortionware)*



Ransomware spreads across the Internet without set targets. The nature of this file-encrypting malware means that hackers are able to choose their targets.

Preventing the attacks

Ransomware is a profitable market for cybercriminals and can be difficult to stop. Prevention is the most important aspect of protecting your personal data.

- *Protect your data with advanced security software & keep it updated*
- *Update your Operating System and other applications*
- *Be cautious, don't automatically open email attachments or embedded links*
- *Backup data to an external hard drive*
- *Use cloud services to secure your private information*
- *Don't pay the ransom straight away*



With new ransomware variants appearing, it's a good idea to do what you can to minimize your exposure. Stick to these rules and protect your data.

ARE YOU CYBER SAFE?

*Test your defences by booking your free
Cyber Security assessment today.*



Book now:

compexit.co.uk/assessment

Contact us:

hello@compexit.co.uk

0121 296 2500