

5 Tips To Stop Ransomware



Be alert, backup and patch!



Get clued up on phishing

Clicking on malicious links in fake emails is the most common way to get infected with ransomware. Watch out for links and attachments, the send from address and spelling!



Patches and updates

Ensure you are installing the latest patches and software updates on your devices to help secure your data. These security updates are there to stop the criminals getting in.



Backup your data

Backing up your data with a disaster recovery solution allows you to get back what's gone in a worst case scenario. It helps to limit business downtime and reduces damage to reputation.



Create a USB free zone

Ban the use of personal USB drives within your organisation and if using a USB is necessary, ensure you are providing a protected USB drive.



Don't pay the ransom!

If you install the latest patches, educate your team and have cyber security and disaster recovery solutions in place - paying a ransom shouldn't ever be on your to-do list!

We always recommend a multi-layered approach including multi-layered cyber security support, disaster recovery solutions and user education.

**For more advice on
cyber security visit:**

www.complete-it.co.uk/cyber-security/

