



5 tips to stop ransomware

Be alert, backup and patch!

1

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!

2

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.

3

Backup

Backing up your data with a Disaster Recovery Solution allows you to get back what's gone in a worst case scenario, limiting business downtime and reduces damage to reputation.

4

USB free zone

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

5

Don't pay the ransom!

If you install the latest patches and updates, educate your team and use a Cyber Security and Disaster Recovery Solution, paying a ransom shouldn't ever be on your to-do list!

We always recommend a multi-layered approach, which is why a combination of cyber security and disaster recovery solutions as well as educating your team is important.

For more advice and tips visit
WWW.COMPLETE-IT.CO.UK/BLOG/

