5 reasons why you need to patch

Security flaws put your data at risk.

1 Repairing security holes

Hackers love to exploit software vulnerabilities and infect devices with malware. Patching repairs these security holes and reduces the chance of malicious attacks.

2 Latest software

Patch updates add new software features to your devices. Many vendors won't support old versions of software so it's important to keep up to date with patching.

3 Security of your Data and reputation

Not regularly patching puts your business data at risk. Loss of data through malware could leave you unable to operate "business as usual" and result in damage to your reputation.

4 GDPR and sensitive personal data

If you fell victim to a cyber attack and lost personal data, you'd need to prove measures were in place to prevent this. Using a patch management system would help show this.

5 User education on phishing

Patching is used to prevent malware infections but user error makes up the main reason for malware infections. Help secure your business by educating your team on phishing.

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/

cit
Complete I.T.