

The 7 deadly sins of Cybersecurity

Is your business protected?



Introduction

No matter how big or small your organisation is, the possibility of a cyber-attack is real. There's never been a more crucial time to make sure your business' IT systems are secure.

Here are the 7 deadly sins of Cybersecurity and what you need to do to ensure your business is protected:





Failing to have a backup system in place

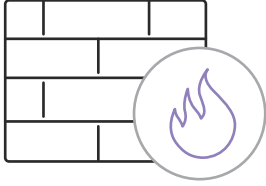
A properly managed backup system is essential and this is arguably the most important step for ensuring your business is protected. Cyber-attacks can strike at any time. A secure backup system ensures the safety of your data and files, meaning you can restore your network easily. Just be sure to perform regular backup checks!



Weak passwords

Having password policies in place will help you and your staff make sure passwords are as secure as possible. From updating passwords regularly to including uppercase letters, there are many ways to strengthen your passwords. These best-practices can be a bit tedious, but they may well save you from a cyber-attack!


3



Not having a firewall installed

Simply put, make sure you have a business-grade firewall and that it is correctly configured. This will make your system more secure from intrusion.

4

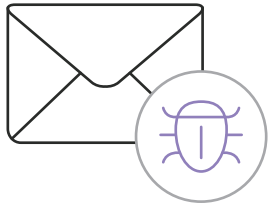


Unclear IT best practices for staff

It's crucial that your staff understand what constitutes acceptable use of your IT systems, from browsing the internet, to the use of their own devices in the office. Don't leave it to chance – make sure you have clear policies in place.



5



Opening emails you aren't 100% sure about

Phishing emails are the number one culprit in the transmission of ransomware, malware and viruses. Train your staff on how to use emails and make sure that everyone treats unusual or unexpected emails with extreme caution. If in doubt - don't open it!



6



A lack of virus and malware protection

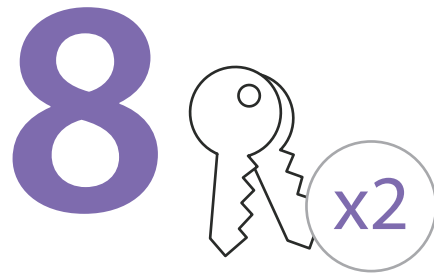
It is vital that your business has a good, business-grade virus and malware protection system that is always on and always up-to-date.



Still using old operating systems

Don't use old and out-of-date operating systems which are no longer supported by their manufacturer. Make sure that your operating systems are kept up-to-date with the latest security patches. Viruses and hackers will take advantage of insecure and unsupported operating systems, such as Windows XP, Windows Server 2003 and Microsoft SBS 2003.

And finally, as a bonus one...



Not using two-Factor Authentication

Two-factor authentication gives your business' IT systems an extra layer of security, minimising the risk of an attacker impersonating a user and gaining access to computers, accounts or other classified information.



Talk to us about Cybersecurity

Don't let it happen to you. If you are not 100% sure that you have fully implemented each of these steps, talk to BTP. It is vitally important to the safe running of your business IT system.



☎ 02380 652 111

✉ info@btpuk.com

🖱 www.btpuk.com