How to protect against malware

vodafone business

Cybercriminals aren't just after big corporations. Small and mid-sized businesses are prime targets too. But being small doesn't mean you have to be an easy target. By taking the right steps, you can protect your business from malware and stay ahead of the threats.

Here's our checklist of 10 essential ways to stay safe.

1. Choose strong passwords

- Ensure every account has a unique, complex password that mixes upper and lowercase letters, numbers, and symbols.
- Use meaningful phrases to create secure passwords, like turning "I love pizza" into "I#l0v3p1zz4."
- Consider a password manager to create and securely store your passwords.

2. Get antivirus software

- Choose antivirus software that offers real-time threat detection and strong malware removal capabilities.
- Keep your software updated and run regular scans to stay protected against new and evolving threats.

3. Train your team

- Carry out regular training sessions to educate your staff on how to spot phishing attempts, avoid suspicious downloads, and stay alert to cyber threats.
- Keep your team up to date on the latest tactics cybercriminals use.

4. Check websites are secure

- Always check for "https" in the URL and look for a padlock symbol before entering any sensitive information.
- Make sure your team know what to look for and report any suspicious sites to IT.

vodafone business

5. Review privacy settings

- Regularly review and adjust privacy settings across every platform you use, from social media to cloud storage.
- Share only the minimum data necessary and limit access to sensitive information wherever possible.

6. Regular software updates

- Keep operating systems, apps, and antivirus software up to date across all devices.
- Don't skip updates, even for a short time, as it leaves you vulnerable to malware that targets outdated software.

7. Use Multi-Factor Authentication (MFA)

- Implement MFA across your business to add an extra layer of security.
- Use methods like a one-time code or fingerprint verification to protect sensitive accounts, even if passwords are compromised.

8. Monitor employee access

- Limit access to sensitive information based on job roles to reduce weak points in your network.
- Set up alerts for suspicious activity and regularly review access permissions to make sure they're still necessary.

9. Be wary of public WI-FI

- Always use a Virtual Private Network (VPN) when accessing public Wi-Fi to encrypt your connection.
- Remind employees to avoid unsecured networks when working remotely to protect sensitive data.

10. Back up regularly

- Regularly back up all critical data – client files, financial records, and more – to a secure offsite location or the cloud.
- Automate your backups to ensure you never forget, and test them to confirm they're working.

vodafone business