

CYBERSECURITY CHECKLIST

FOR SMALL BUSINESSES

- ☐ Educate and train your team
- ☐ Encourage good browsing practices and warn employees not to click suspicious links or download unknown attachments[2].
- ☐ Provide regular security awareness training to help staff recognise phishing emails and social-engineering scams[1].
- ☐ Use strong passwords and multi-factor authentication (MFA)
- ☐ Require employees to create unique, complex passwords and update them periodically[1].
- ☐ Enable MFA wherever possible—this requires users to provide two or more verification factors (e.g., password, token, fingerprint)[3].
- ☐ Secure your network and devices
- ☐ Encrypt your internet connection and install a business-grade firewall[4].
- ☐ Hide and password-protect your Wi-Fi network. For remote workers, require use of a Virtual Private Network (VPN) to securely connect to your systems[4].
- ☐ Use antivirus software on all computers and configure software, operating systems and web browsers to install updates automatically[5].
- ☐ Protect and back up sensitive data

CYBERSECURITY CHECKLIST

FOR SMALL BUSINESSES

- ☐ Work with your bank or payment processor to ensure secure payment processing. Isolate payment systems from less secure programs[6].
- ☐ Control physical access to computers and mobile devices. Provide separate user accounts for each employee and give administrative privileges only to trusted personnel[7].
- ☐ Perform regular data backups—ideally weekly—to cloud storage or other secure media. Include financial, HR and accounting files and important documents[8].
- ☐ Audit cloud storage repositories (e.g., Google Drive, Dropbox) periodically. Limit users' access to only the information they need[9].
- ☐ Monitor vendors and third-party services
- ☐ Check whether your software and service providers offer MFA and other security features[10].
- ☐ Monitor Cloud Service Provider accounts and ensure data is hosted by reputable vendors[11].
- ☐ Assess your risk and plan ahead
- ☐ Conduct a cybersecurity risk assessment to identify vulnerabilities and build a plan to address them[12].
- ☐ Use available planning tools, such as the FCC's Small Biz Cyber Planner 2.0 or the Department of Homeland Security's Cyber Resilience Review[13].