

Small Business IT & Cybersecurity Readiness Checklist

A practical starting point for protecting your business

Technology problems rarely arrive at a convenient time. Use this checklist to identify common gaps in your computers, accounts, email, backups, and security before they become expensive disruptions.

How to use this checklist

Check each item that is in place. Any unchecked item is worth discussing with your IT provider.

Security and account protection

- ☐ 1. Security updates - All computers, operating systems, browsers, and important applications receive updates regularly.
- ☐ 2. Multi-factor authentication - MFA is enabled for email, Microsoft 365, cloud services, remote access, and administrator accounts.
- ☐ 3. Separate administrator accounts - Employees use standard accounts for daily work, while administrative access is limited and controlled.
- ☐ 4. Endpoint protection - Business computers have active, centrally managed protection against malware, ransomware, and other threats.
- ☐ 5. Email and phishing awareness - Staff know how to recognize suspicious links, attachments, payment requests, and impersonation attempts.

Backup and recovery readiness

- ☐ 6. Important data is identified - You know where documents, financial records, customer information, and other critical files are stored.
- ☐ 7. Backups run automatically - Backups are scheduled, monitored, and protected from accidental deletion or ransomware.
- ☐ 8. Backups are tested - You have successfully restored files - not merely assumed that a backup exists.
- ☐ 9. A recovery plan exists - Your business knows what to do, who to call, and what must be restored first after a serious incident.
- ☐ 10. Former users are removed - Former employees, vendors, and unused accounts no longer have access to business systems or data.

What should you ask your IT provider?

A good IT partner should be able to explain what is being monitored, what is covered, how incidents are handled, and how your business can recover if something goes wrong.

Five questions worth asking

- 1** What is included each month?
Ask whether the service includes monitoring, patching, security tools, backup, remote support, and on-site assistance.
- 2** Who responds when there is a problem?
Know whether you will reach a real person, how support requests are handled, and when after-hours help is available.
- 3** How are backups verified?
A backup should be monitored and periodically tested. A backup that cannot be restored is not a dependable recovery plan.
- 4** What happens after an employee leaves?
Your provider should help disable accounts, remove access, and protect company data during offboarding.
- 5** Can the plan grow with the business?
Your IT service should be able to support new employees, devices, locations, and cloud services as your business changes.

How Shazam! Computers can help

We provide practical managed IT services for small businesses throughout Southeastern Wisconsin. Depending on your needs, services may include proactive monitoring and maintenance, cybersecurity protection, Microsoft 365 and business support, backup and recovery solutions, remote assistance, and on-site support.

Plans are based on your business, your devices, and your actual risk - not a one-size-fits-all package.

Ready to review your business technology?

Schedule a free Business IT Assessment with Eric. We will discuss your current setup, your concerns, and the next practical steps - with no pressure to buy a package online.

Call or text 262-716-7072 | support@shazamcomputers.tech

Serving Burlington, Waterford, Lake Geneva, East Troy, Mukwonago, Muskego, Rochester, and surrounding communities