



Small Business Cybersecurity Checklist

A practical checklist for reducing risk, protecting accounts, and improving everyday security.

Your IT Department. Your Cybersecurity Team. Your Technology Partner.

Network Solutionist, LLC

Serving Wilmington, Newark, Middletown, Dover, Rehoboth Beach, and businesses across Delaware.



How to Use This Checklist

Review each item with leadership, IT, or your managed service provider. Mark what is complete, prioritize what is missing, and revisit the list every quarter.

Best practice mindset: cybersecurity is not a one-time project. It is an ongoing business discipline involving people, process, and technology.

Core Security Checklist

Done	Security Item	Why It Matters
☐	Enable multi-factor authentication for email, Microsoft 365, banking, payroll, and remote access.	MFA helps reduce the risk of account takeover when a password is stolen.
☐	Use unique passwords stored in a business-approved password manager.	Password reuse turns one breach into many breaches.
☐	Keep operating systems, browsers, firewalls, and business applications updated.	Updates often include security patches for known vulnerabilities.
☐	Protect all endpoints with managed antivirus or endpoint detection.	Centralized visibility helps detect threats before they spread.
☐	Back up critical data and test restores regularly.	A backup is only useful if the business can restore from it.
☐	Secure Wi-Fi with strong encryption and separate guest access.	Guest devices should not have direct access to business systems.
☐	Limit administrator rights to only those who need them.	Least privilege reduces the blast radius of mistakes or malicious activity.
☐	Require security awareness training for employees.	Many incidents begin with a phishing email or unsafe user action.
☐	Maintain an incident response contact list and decision plan.	A written plan reduces confusion during an urgent event.
☐	Review vendor and third-party access.	Outside access should be tracked, approved, and removed when no longer needed.

Helpful Reference Points

- CISA emphasizes small business action plans, MFA, patching, backups, and incident response planning.



-
- FTC guidance highlights protecting data, updating software, backing up files, requiring strong passwords, encryption, and MFA.
 - SBA guidance recommends employee training, secure networks, updated antivirus/software, and MFA.

Disclaimer

This guide is for general educational purposes and does not replace a formal cybersecurity assessment, compliance review, or incident response engagement.

Need help turning this into an action plan?

Network Solutionist, LLC can help assess, secure, monitor, and support your business technology environment. (302) 485-9850 | info@nsolutionist.com | nsolutionist.com

