BROTHERLY TECHNOLOGY

CYBERSECURITY CHECKLIST

Small Business Cybersecurity Checklist

A plain-English audit you can run without a technical background. Covers the controls that actually stop the attacks small businesses get hit with.

01	**Password, MFA and access rules worth enforcing today**
02	**How to spot the phishing patterns aimed at small teams**
03	**What your backup must do to survive ransomware**

Use this guide to assess where you are, identify the evidence you need, and turn the biggest gaps into a practical action plan.

Prepared by Brotherly Technology
Owner-led IT, security, and compliance support.

BROTHERLY TECHNOLOGY

15-MINUTE ASSESSMENT

Start with the current state

Mark each item Yes, Partial, or No. A written policy only counts as Yes when the process is operating and you can show evidence.

[ ] MFA protects email, remote access, admin accounts, finance, and other critical cloud apps.	[ ] Yes [ ] Partial [ ] No
[ ] Staff use unique passwords stored in an approved password manager.	[ ] Yes [ ] Partial [ ] No
[ ] Daily work is performed without local or cloud administrator rights.	[ ] Yes [ ] Partial [ ] No
[ ] Departures disable accounts, sessions, forwarding rules, tokens, and shared access immediately.	[ ] Yes [ ] Partial [ ] No
[ ] Supported operating systems and applications receive timely security updates.	[ ] Yes [ ] Partial [ ] No
[ ] Endpoint protection, firewall, email filtering, and monitoring generate owned alerts.	[ ] Yes [ ] Partial [ ] No
[ ] Sensitive files are stored in approved systems with role-based access.	[ ] Yes [ ] Partial [ ] No
[ ] Payment and banking changes require verification through a known, separate channel.	[ ] Yes [ ] Partial [ ] No
[ ] Staff know how to report suspicious messages without forwarding dangerous content.	[ ] Yes [ ] Partial [ ] No
[ ] Backups include critical cloud and onsite data, with an isolated or immutable copy.	[ ] Yes [ ] Partial [ ] No
[ ] Restore tests prove the business can resume within agreed RTO and RPO targets.	[ ] Yes [ ] Partial [ ] No
[ ] An incident plan lists decision-makers, insurer, legal counsel, IT, and alternate communications.	[ ] Yes [ ] Partial [ ] No

Quick score: Yes = 2, Partial = 1, No = 0. Start with any No that could stop work, expose sensitive data, or create an avoidable contract cost.

ACCESS BASELINE

Enforce the rules that stop account takeover

Strong access control combines a unique identity, resistant authentication, least privilege, and a fast offboarding process.

Control	Practical rule	Evidence
MFA	Require for all users; prefer phishing-resistant methods where practical	Coverage report and exception list
Passwords	Unique, long, manager-generated; no shared spreadsheets	Password manager adoption and policy
Admin rights	Separate admin identities; no routine admin use	Admin group report and review record
New users	Manager-approved role template and least privilege	Request, approval, and provision log
Departures	Immediate disable, token revoke, data transfer, device return	Completed offboarding checklist
Reviews	Recurring review of privileged, shared, vendor, and stale access	Signed review and corrective actions

For finance and executives, add independent verification of bank, payroll, gift-card, invoice, and password-reset changes.

PHISHING AND RECOVERY

Recognize the pattern, then make one click survivable

Phishing succeeds through urgency, authority, curiosity, and a plausible request. Pair awareness with controls that limit impact.

1	Teach staff to slow down on unexpected sign-ins, payment changes, QR codes, file shares, and urgent executive requests.
2	Verify sensitive requests using a known phone number or existing thread - never contact details inside the suspicious message.
3	Use email authentication, filtering, safe links/attachments, and conditional access to reduce exposure.
4	Design backups so compromised production credentials cannot alter every copy; monitor every job.
5	Run a restore test and a tabletop incident exercise that includes alternate communications and insurer notification.

What to watch for

WATCH: MFA is enabled for admins but not the wider workforce.

WATCH: A shared mailbox or vendor account has no named owner.

WATCH: Employees can install software and browser extensions without review.

WATCH: Backups are reachable with the same administrator account as production.

WATCH: The incident contact list exists only in email.

MAKE IT ACTIONABLE

Turn the worksheet into a 30-day plan

Do not try to solve everything at once. Assign one owner, one next action, and one date for each priority.

NOW	Name the owner and confirm the current state.	_____
NEXT 7 DAYS	Fix the highest-risk gap or gather the missing evidence.	_____
NEXT 30 DAYS	Complete the remaining quick wins and set review dates.	_____
NEXT QUARTER	Test the process, document results, and assign improvements.	_____

Notes / decisions / questions for your provider

_____

_____

_____

_____

_____

Want a second set of eyes? Book a free consultation at brotherlytechnology.com/contact/ or call 404-907-1005.

Reference points: CISA Secure Our World: cisa.gov/secure-our-world | NIST Cybersecurity Framework 2.0: nist.gov/cyberframework

This guide is educational and is not legal, regulatory, tax, or insurance advice. Confirm requirements and pricing for your organization with qualified advisors and vendors.