Cybersecurity Best Practices Checklist

Most small-organization breaches start with a stolen password, a phishing email, or a missed update. These basics close the most common doors. Have your IT provider help with any item you can't check.

ACCOUNTS AND ACCESS

	YES	PARTLY	NO	N/A
Multi-factor authentication is on for email, banking, payroll, and remote access.	☐	☐	☐	☐
Staff use a password manager; no shared or reused passwords.	☐	☐	☐	☐
Each person has their own login; admin rights are limited to those who need them.	☐	☐	☐	☐
Access is removed the day someone leaves.	☐	☐	☐	☐

DEVICES AND SYSTEMS

	YES	PARTLY	NO	N/A
Computers, phones, and network equipment install security updates automatically.	☐	☐	☐	☐
Laptops are encrypted and lock after a few minutes of inactivity.	☐	☐	☐	☐
Antivirus or endpoint protection is installed and monitored.	☐	☐	☐	☐
Guest Wi-Fi is separate from the network used for business systems.	☐	☐	☐	☐

DATA AND BACKUPS

	YES	PARTLY	NO	N/A
Important data is backed up automatically, with one copy offline or off-site.	☐	☐	☐	☐
A restore from backup has been tested in the last six months.	☐	☐	☐	☐
Sensitive data (SSNs, bank details, health information) is stored only where needed.	☐	☐	☐	☐

PEOPLE AND PAYMENTS

	YES	PARTLY	NO	N/A
Staff complete phishing awareness training at least once a year.	☐	☐	☐	☐
Requests to change bank details or send urgent payments are verified by phone using a known number.	☐	☐	☐	☐
There is a written plan for who to call and what to do if a breach happens.	☐	☐	☐	☐

Free guidance for small organizations: CISA Cyber Essentials (cisa.gov).

RED FLAGS TO WATCH

- One shared login for the accounting system
- Updates postponed for months
- Backups that have never been tested
- "Urgent" payment requests that arrive only by email

BEST PRACTICES

- Turn on multi-factor authentication first; it blocks most account takeovers
- Review user accounts every quarter
- Practice your response plan once a year

Need a hand putting this into action?

IAG reviews payment and access controls that protect against cyber-enabled fraud.

Talk with an advisor: integrityadvisorygroup.org/contact

Educational resource, not legal, tax, or accounting advice. IAG provides consulting, investigation, mediation, and training services and is not a CPA firm or law firm.

© 2026 Integrity Advisory Group, LLC