Small Business Cybersecurity Checklist

Passwords • MFA • Backups • Email Security • Devices • Incident Response

This checklist is educational and does not replace professional cybersecurity advice. Adapt it to your business risk and compliance needs.

Account Security

Prompt 1

List all business-critical accounts, including email, hosting, domain registrar, bank, payment processor, CRM, and admin dashboards.

Prompt 2

Enable multi-factor authentication on every account that controls money, customer data, website access, or admin privileges.

Prompt 3

Move shared passwords from spreadsheets, chats, browsers, or notes into a password manager.

Prompt 4

Remove access for former employees, contractors, agencies, and unused admin accounts.

Prompt 5

Review password reuse across business accounts and replace reused passwords with unique credentials.

Email and Phishing

Prompt 6

Train staff to verify unexpected attachments, invoices, password reset messages, and urgent payment requests.

Prompt 7

Create a simple rule: payment detail changes must be confirmed through a second channel.

Prompt 8

Check email forwarding rules monthly for suspicious forwarding addresses.

Prompt 9

Use a suspicious link scanner before opening unknown URLs from emails or chat messages.

Prompt 10

Create a process for employees to report phishing attempts without fear or delay.

Devices and Updates

Prompt 11

Turn on automatic updates for laptops, phones, browsers, and major business software.

Prompt 12

Require screen locks and device passwords on all business laptops and phones.

Prompt 13

Install reputable endpoint security on employee devices used for work.

Prompt 14

Disable unused software, browser extensions, and old apps that no one maintains.

Prompt 15

Create a monthly device review for lost, old, or unused hardware.

Backups and Recovery

Prompt 16

Identify critical business data: website files, customer records, invoices, contracts, product data, and financial records.

Prompt 17

Create at least one cloud backup and one separate backup for critical files.

Prompt 18

Test restoring one file from backup every month.

Prompt 19

Document who is responsible for backups and where recovery instructions are stored.

Prompt 20

Protect backup accounts with MFA and unique passwords.

Website and Domain Security

Prompt 21

Enable MFA for domain registrar, DNS provider, hosting provider, Cloudflare, CMS, and admin accounts.

Prompt 22

Check that domain registration email is active, secure, and monitored.

Prompt 23

Update CMS, themes, plugins, and integrations regularly.

Prompt 24

Remove unused plugins, abandoned tools, and old admin accounts.

Prompt 25

Keep a written record of DNS settings, hosting provider, and emergency contacts.

Cloud and SaaS Access

Prompt 26

List every SaaS tool your business uses and identify the admin owner for each.

Prompt 27

Review user permissions quarterly and remove unnecessary admin rights.

Prompt 28

Enable login alerts where available for critical SaaS tools.

Prompt 29

Export or back up important SaaS data when possible.

Prompt 30

Cancel unused SaaS tools to reduce attack surface and cost.

Payments and Finance Protection

Prompt 31

Require approval from two people before changing vendor bank details.

Prompt 32

Use separate accounts for banking, bookkeeping, ecommerce, and payroll access.

Prompt 33

Review payment processor users and API keys monthly.

Prompt 34

Limit refund, payout, and payment settings access to trusted admins only.

Prompt 35

Create a fraud response checklist for suspicious transactions.

Employee and Contractor Access

Prompt 36

Create an onboarding checklist for tool access and security expectations.

Prompt 37

Create an offboarding checklist to remove access on the final working day.

Prompt 38

Use role-based access instead of giving everyone admin permissions.

Prompt 39

Review contractor access every 30 days.

Prompt 40

Document who owns each shared account and why it exists.

Monitoring and Free Tools

Prompt 41

Check business email addresses in Have I Been Pwned for breach exposure.

Prompt 42

Use VirusTotal to check suspicious URLs or files that are not confidential.

Prompt 43

Use CISA free resources to review current small-business cybersecurity guidance.

Prompt 44

Use Shodan carefully only for assets you own or are authorized to review.

Prompt 45

Document findings and assign owners for every issue discovered.

Incident Response

Prompt 46

```
Write down who to contact if an account is hacked, ransomware appears, or customer data is exposed.
```

Prompt 47

```
Create a short incident checklist: disconnect, preserve evidence, reset credentials, notify owners,
restore backups.
```

Prompt 48

```
Store emergency contacts offline or in a secure password manager note.
```

Prompt 49

```
Prepare template messages for internal alerts and customer notification if needed.
```

Prompt 50

```
Run a 30-minute tabletop exercise once per quarter.
```

Final note

Review and adapt every item before using it in real business, classroom, legal, hiring, or analytics workflows.