SMALL BUSINESS IT SECURITY CHECKLIST

18 checks to find the gaps before a hacker does.

Most break-ins at small businesses start with something simple: a reused password, a fake invoice email, or a backup nobody tested. Work through this list with whoever handles your IT. It takes about 15 minutes.

1. Check the box
if it's true for your business today.

2. Not sure?
Leave it blank. Unknown usually means "no."

3. Count your checks
and see your score on page 2.

PASSWORDS & ACCOUNTS

- [ ] 01 **Multi-factor authentication (MFA) is on for email and Microsoft 365 or Google.**
The code from your phone stops most account takeovers, even when a password leaks.

- [ ] 02 **Every person has their own login. No shared accounts.**
Shared logins make it impossible to remove one person's access or see who did what.

- [ ] 03 **Passwords live in a password manager, not a spreadsheet or sticky note.**
A password manager makes long, unique passwords easy for everyone.

- [ ] 04 **Access is turned off the same day someone leaves.**
Email, files, apps and Wi-Fi: former employees shouldn't be able to get back in.

COMPUTERS & PHONES

- [ ] 05 **Windows and Mac updates install automatically on every computer.**
Updates close the holes attackers use. "Remind me later" is how they stay open.

- [ ] 06 **Every computer has active antivirus or endpoint protection.**
Check that it's turned on, up to date and actually being watched.

- [ ] 07 **Laptops are encrypted (BitLocker on Windows, FileVault on Mac).**
A lost or stolen laptop is an inconvenience instead of a data breach.

- [ ] 08 **Screens lock automatically after a few minutes.**
Walk-up access is the easiest kind there is.

EMAIL

- [ ] 09 **Your team knows how to spot a phishing email and who to report it to.**
  Urgent requests, odd links and "new bank details" are the classic signs.
- [ ] 10 **Payment or bank-detail changes are confirmed by phone, using a number you already have.**
  Never use the phone number in the email asking for the change.
- [ ] 11 **Your email domain has SPF, DKIM and DMARC records set up.**
  These make it much harder for scammers to send email that looks like it came from you.

BACKUPS

- [ ] 12 **Important files back up automatically, including Microsoft 365 or Google data.**
  Cloud apps keep your files running, but they aren't a full backup on their own.
- [ ] 13 **At least one backup copy is kept separate from your network.**
  Ransomware tries to encrypt your backups too. A separate copy is your way back.
- [ ] 14 **You've test-restored a file in the last 90 days.**
  A backup you've never restored from is only a hope.

WI-FI & NETWORK

- [ ] 15 **Guest Wi-Fi is separate from the network your business computers use.**
  Customers and visitors shouldn't share a network with your files or card reader.
- [ ] 16 **The router or firewall password isn't the default, and its software is up to date.**
  Default passwords are published online for every model.

YOUR PLAN

- [ ] 17 **You know exactly who to call and what to do if you're hacked.**
  Write it down now: who to call, how to reach your bank, your insurer and your IT help.
- [ ] 18 **You have a list of your key systems, vendors and who has admin access.**
  You can't protect, or recover, what you can't see.

Your score: _____ **/ 18**

16–18 checks
Strong foundation. Review this list every quarter to keep it that way.

11–15 checks
Solid start with a few real gaps. Fix MFA, backups and updates first.

10 or fewer
Your business is an easy target. Get help closing the gaps soon.

Want a second set of eyes on your results?

Request a free, no-obligation consultation. Tell us which boxes you couldn't check, and CompuTek will help you decide what to fix first, in plain English.

REQUEST ONLINE
computek.info

© 2026 COMPUTEK · CRISTIAN@COMPUTEK.INFO