

Don't make it easy for them

The small office security checklist. Built on CISA's four core steps and the National Cybersecurity Alliance's 2026 theme. Tick it off, file it, and check again in six months.



Office	Checked by	Date	Next check
--------	------------	------	------------

01 Passwords

- ☐ **Every account has its own long password**
A passphrase of four or more random words. Never reused between sites.
- ☐ **The office uses a password manager**
Shared logins live in a shared vault, not a spreadsheet or a sticky note.
- ☐ **Default passwords are changed**
Router, printer, cameras, backup box: anything that came with admin/admin.

02 Multifactor authentication

- ☐ **MFA is on for everyone's email**
Microsoft 365 or Google Workspace, every user, including the owner.
- ☐ **MFA is on for banking, payroll and your domain**
The accounts that move money or control your website and email.
- ☐ **An authenticator app or passkey, not text codes**
Use the stronger option wherever the service offers one.

03 Scams and phishing

- ☐ **Everyone knows how to report a suspicious email**
One address or one button, and no blame for asking.
- ☐ **Payment and bank-detail changes are confirmed by phone**
Call a number you already have, never the one in the email.
- ☐ **Surprise "IT support" calls get a call back**
Hang up and call your IT on a number you know.

04 Updates

- ☐ **Windows and Mac install updates on their own**
Automatic updates on, and computers restart at least weekly.
- ☐ **Browsers, PDF readers and Zoom are current**
Third-party apps are where attackers look first.
- ☐ **The router or firewall is up to date**
Check the admin page, or ask whoever installed it.
- ☐ **Devices past end of support have a replacement date**
CISA's "replace" step: no more security fixes means it has to go.

05 Backups and records

CISA's next step for organizations.

- ☐ **Backups run on their own, one copy off-site**
A cloud copy or a drive that is not plugged in all the time.
- ☐ **A restore was tested this year**
Pick one file from last month and get it back.
- ☐ **Sign-in and computer logs are kept**
So there is a record to look at if something happens.

06 If something goes wrong

CISA: have an incident response plan and use it.

- ☐ **One page says who to call**
Your IT, your bank, your insurer. Taped inside a cupboard, not only on a computer.
- ☐ **Staff know how to unplug a computer from the network**
Pull the cable or switch Wi-Fi off. Don't turn it off or wipe it.
- ☐ **You know where to report it**
Cyber incidents: cisa.gov/report. Online fraud: ic3.gov.

Want a second set of eyes?

Our free 30-minute assessment goes through this list with you, remotely or on-site, and tells you what to fix first. rainier-it.com/contact