SkillNewton

Basic Security Audit Checklist

A practical security audit for small businesses and home offices: accounts, MFA, patching, backups, Wi-Fi, email and incident response.

This checklist helps a small business, shop or home office check its basic cyber security in an afternoon. It covers devices, accounts, passwords, updates, backups, Wi-Fi, email, the website and what to do if something goes wrong. No specialist tools are needed. Work through each section, mark items as done, partly done or missing, then fix the missing items starting with MFA, backups and updates. Repeat the audit every six to twelve months.

How to use it

1. **List what you have.** Start with the asset inventory so you know every device, account and service you need to protect.
2. **Mark each item.** Note whether each item is done, partly done or missing, and who is responsible.
3. **Fix the high-impact gaps first.** MFA on email and banking, working backups and automatic updates prevent the most common losses.
4. **Repeat regularly.** Run the audit again every six to twelve months and whenever staff, devices or services change.

Asset inventory

- [ ] List every device that connects to your network
  Laptops, desktops, phones, printers, routers, CCTV recorders and smart devices.
- [ ] List all online accounts and services
  Email, domain registrar, hosting, banking, GST and accounting software, cloud storage and social media.
- [ ] Record who owns and who can access each one
  Remove access for people who have left.
- [ ] Note where important data is stored
  Customer records, invoices and design files may be on laptops, a NAS and in the cloud.
- [ ] Identify unsupported devices and software
  Systems past their end of support, such as Windows 10 without extended updates, no longer get security fixes.

Accounts, MFA and passwords

- [ ] Turn on multi-factor authentication for email first
  Email controls password resets for everything else. Prefer an authenticator app or passkey over SMS where offered.
- [ ] Enable MFA on banking, domain, hosting, cloud and social accounts
  These are the accounts attackers target for money and control.
- [ ] Use a password manager
  It creates and stores long, unique passwords for every account so nobody reuses one.
- [ ] Give each person their own account
  Shared logins make it impossible to remove one person or see who did what.

- [ ] Use standard user accounts for daily work
  Keep admin rights for installing software and maintenance only.
- [ ] Remove accounts of former staff on their last day
  Also change any shared passwords they knew, such as Wi-Fi.
- [ ] Check whether your email addresses appear in known breaches
  Services such as Have I Been Pwned show breached accounts; change those passwords.

Devices, patching and endpoint protection

- [ ] Turn on automatic updates for operating systems
  Windows Update, macOS Software Update, Android and iOS.
- [ ] Update browsers, office software and other apps
  Remove software nobody uses.
- [ ] Check endpoint protection is on and up to date
  Microsoft Defender is built into Windows; confirm it is active and scanning.
- [ ] Turn on full-disk encryption on laptops
  BitLocker on Windows (Pro and above) or FileVault on Mac protects data if a laptop is lost.
- [ ] Set screen locks with a PIN or password
  Lock after a short idle time on computers and phones.
- [ ] Enable the host firewall
  Windows Defender Firewall and the macOS firewall should be on.

Backups

- [ ] Follow the 3-2-1 rule
  Keep three copies of important data, on two different types of storage, with one copy off-site.
- [ ] Keep at least one backup offline or immutable
  Ransomware encrypts connected drives and synced folders, so disconnect one copy or use versioned cloud backup.
- [ ] Back up automatically on a schedule
  Manual backups are forgotten. Daily is a sensible default for business data.
- [ ] Test a restore at least every quarter
  A backup you have never restored is not proven to work.
- [ ] Include email, cloud and website data
  Cloud services may not keep deleted data for long; check their retention and back up the website and database separately.

Network and Wi-Fi

- [ ] Change the router's default admin password
  Use a long, unique password and turn off remote administration from the internet unless you need it.
- [ ] Update router firmware
  Check for updates in the admin page; replace routers that no longer receive them.
- [ ] Use WPA3, or WPA2 with AES if devices need it
  Avoid WEP, WPA and TKIP. Use a long Wi-Fi passphrase.
- [ ] Turn off WPS
  WPS PIN mode has known weaknesses.

- [ ] Put visitors and smart devices on a guest network
  Keep them separate from computers that hold business data.
- [ ] Check for open ports and port forwards
  Review port forwarding and UPnP in the router; scan your public IP only from a network you own.
- [ ] Change default passwords on CCTV, printers and NAS devices
  These are often exposed and rarely updated.

Email security

- [ ] Publish an SPF record for your domain
  A DNS TXT record listing the servers allowed to send your email, for example `v=spf1 include:_spf.google.com ~all` for Google Workspace.
- [ ] Enable DKIM signing
  Turn it on in your email provider and publish the DKIM key it gives you in DNS.
- [ ] Publish a DMARC record
  Start with `v=DMARC1; p=none; rua=mailto:dmarc@example.com`, review reports, then move to `quarantine` and `reject`.
- [ ] Train staff to spot phishing and payment fraud
  Verify changes to bank details or urgent payment requests by phone using a known number.
- [ ] Turn on the provider's spam and malware filtering
  Check that external emails are clearly labelled.

Website and online services

- [ ] Make sure the website uses HTTPS
  Check the certificate is valid and HTTP redirects to HTTPS.
- [ ] Update the CMS, themes and plugins
  Remove unused plugins and themes, especially on WordPress.
- [ ] Use strong unique passwords and MFA on the site admin and hosting
  Limit the number of admin accounts.
- [ ] Back up the website and database separately from the host
  Keep at least one copy outside the hosting account.
- [ ] Check domain renewal and registrar lock
  Turn on auto-renew and registrar lock so the domain cannot lapse or be transferred.

Logging and incident response

- [ ] Turn on sign-in alerts and audit logs in key services
  Email and cloud providers can alert you to new sign-ins and suspicious activity.
- [ ] Keep router, server and firewall logs where available
  Check how long they are kept and where.
- [ ] Write a one-page incident plan
  Who to call, how to disconnect affected devices and how to restore from backup.
- [ ] Keep an emergency contact list offline
  IT support, ISP, bank, hosting provider and your insurer, if you have cyber cover.

- [ ] **Know how to report incidents in India**
  Report cyber incidents to CERT-In (`incident@cert-in.org.in`); its 2022 directions require covered organisations to report within six hours of noticing.

- [ ] **Know how to report cyber crime and fraud**
  Use the National Cyber Crime Reporting Portal (cybercrime.gov.in) or helpline 1930 for financial fraud.

Online version, with the matching free guide: skillnewton.com/resources/templates/basic-security-audit-checklist/
Learn this hands-on: Networking & Cybersecurity: Foundation & Practical Implementation – skillnewton.com/courses/networking-foundation-course/