Know Your Network, Know Your Risk

A fillable security map for your home or small business.

COMPANION TO

Cybersecurity for Everyone

Secure by Design, Safe by Habits

Terence Sadler

SECRETS-FREE BY DESIGN

Write where it's kept, never what it is. No passwords, PINs, Wi-Fi keys or recovery codes belong on these pages — only a pointer to where each one lives (password manager, safe, sealed envelope). If this document is ever lost, copied or stolen, it hands an attacker no keys. Even so, treat it like a spare house key: keep the file in your password manager or an encrypted folder, and store any printed copy somewhere safe.

HOW IT WORKS

1. **The Map** — Sketch how the internet reaches you: modem, router and the networks behind it. p. 2
2. **Devices** — List everything that connects, then flag the risky ones green, yellow or red. pp. 3–4
3. **Accounts** — The 12–15 accounts that would hurt most if lost, and how each is protected. p. 5
4. **Hygiene Checks** — Twelve quick checks you can finish in an afternoon. p. 6
5. **If It Goes Wrong** — A one-page plan to tape inside a cabinet door. p. 7

SMALL BUSINESS ADD-ON (pp. 8–10) B1 People & Access · B2 Vendors, Cloud & Data Map · B3 Recovery, Remote Access & Compliance

ABOUT THIS DOCUMENT

Household or business name

Document owner

Backup person who knows where this is kept

Date created

Last reviewed

Next review due

Using this for

☐ Home ☐ Small business (also complete B1–B3)

Review rhythm: home — twice a year; small business — every quarter; everyone — whenever you add a router or device, someone leaves, or a breach notice arrives.

1 · The Map

CORE · EVERYONE

Sketch how the internet reaches your home or office. Work left to right. Record models and locations — and for every secret, only *where it is kept*.



WHAT ELSE IS PLUGGED IN?

Old ISP boxes, range extenders, a second router, a ‘temporary’ switch. **Attackers love what you forgot about** — if a box with blinking lights isn’t on this page, find out whose it is and why it’s there.

NOTES & ANYTHING UNUSUAL

2 · Devices (1 of 2): People Devices

CORE · EVERYONE

List every computer, phone, tablet and console that connects. Compare against your router's connected-device list — if you can't match a name, find out why before moving on.

	Device (make & model)	Owner	Room / location	Name in router list (or last 4 of MAC)	Network *pick one*	Still gets security updates? *pick one*	Auto-update on *tick if yes*	Sensitive data *tick if yes*	Internet-facing *tick if yes*	Risk flag *pick one*
1							☐	☐	☐	
2							☐	☐	☐	
3							☐	☐	☐	
4							☐	☐	☐	
5							☐	☐	☐	
6							☐	☐	☐	
7							☐	☐	☐	
8							☐	☐	☐	
9							☐	☐	☐	
10							☐	☐	☐	
11							☐	☐	☐	
12							☐	☐	☐	
13							☐	☐	☐	
14							☐	☐	☐	
15							☐	☐	☐	

HOW TO FLAG RISK (pick Green, Yellow or Red in the last column)

RED — fix first

No longer gets security updates (or you can't tell) **and** it is internet-facing or on your Main network. Replace it, move it to Guest/IoT, or retire it.

YELLOW — schedule a fix

Gets updates but auto-update is off — or it is unsupported yet safely isolated on Guest/IoT and not internet-facing.

GREEN — keep an eye on it

Gets updates, auto-update is on, and it sits on the right network for what it is.

Internet-facing = reachable from outside your home: cameras and doorbells you watch remotely, anything with port forwarding or remote access switched on, home servers and NAS drives.

2 · Devices (2 of 2): Smart Home & Everything Else

CORE · EVERYONE

Now the things people forget: smart TV · doorbell and cameras · baby monitor · thermostat · voice speaker · printer · smart plugs and bulbs · robot vacuum · garage door · smart lock · EV charger · watch or fitness tracker · NAS · e-reader · ‘smart’ appliances.

	Device (make & model)	Owner	Room / location	Name in router list (or last 4 of MAC)	Network *pick one*	Still gets security updates? *pick one*	Auto-update on *tick if yes*	Sensitive data *tick if yes*	Internet-facing *tick if yes*	Risk flag *pick one*
1							☐	☐	☐	
2							☐	☐	☐	
3							☐	☐	☐	
4							☐	☐	☐	
5							☐	☐	☐	
6							☐	☐	☐	
7							☐	☐	☐	
8							☐	☐	☐	
9							☐	☐	☐	
10							☐	☐	☐	
11							☐	☐	☐	
12							☐	☐	☐	
13							☐	☐	☐	
14							☐	☐	☐	
15							☐	☐	☐	

HOW TO FLAG RISK (pick Green, Yellow or Red in the last column)

RED — fix first

No longer gets security updates (or you can’t tell) **and** it is internet-facing or on your Main network. Replace it, move it to Guest/IoT, or retire it.

YELLOW — schedule a fix

Gets updates but auto-update is off — or it is unsupported yet safely isolated on Guest/IoT and not internet-facing.

GREEN — keep an eye on it

Gets updates, auto-update is on, and it sits on the right network for what it is.

Internet-facing = reachable from outside your home: cameras and doorbells you watch remotely, anything with port forwarding or remote access switched on, home servers and NAS drives.

3 · Accounts & Crown Jewels

CORE · EVERYONE

List the 12–15 accounts that would hurt most if someone took them over. Record how each is protected and where its password lives — never the password itself. Tick **Needs fixing** for any gap: no MFA, text-message codes only, or an out-of-date recovery email or phone.

Start with: primary email · phone carrier · Apple / Google account · bank and credit cards · password manager · cloud photos and files · shopping (Amazon) · tax and government sites · social media · school or work portals · domain and website host (business).

Your phone number is a master key. Anyone who controls it can reset many of your other accounts. Ask your carrier for a port-out / SIM-lock PIN, and prefer an authenticator app or passkey over text-message codes.

	Account / provider	Login / email used (never the password)	Sign-in protection (MFA) *pick one*	Recovery email / phone attached	Credential kept in *pick one*	Last reviewed *MM/DD/YYYY*	Needs fixing *tick if yes*
1							☐
2							☐
3							☐
4							☐
5							☐
6							☐
7							☐
8							☐
9							☐
10							☐
11							☐
12							☐
13							☐
14							☐

Review rhythm: twice a year at home, quarterly in a business — and right after any breach notice. Passkeys and authenticator apps beat text-message codes; hardware keys beat both.

Last full review of this page

4 · Network Hygiene Checks

CORE · EVERYONE

Twelve quick checks, most under five minutes each. Tick the box and enter the date when you check, then repeat on your review date. Stuck? Search your router's model number plus the setting name, or ask a trusted tech-savvy friend.

- ☐ **Router firmware is current**
  Log in to the router (or its app) and look for updates. Turn on automatic updates if offered.
  Last checked: _____

- ☐ **Router admin login is not the default**
  This is the *admin* login, not the Wi-Fi password. Make it unique and keep it in your password manager.
  Last checked: _____

- ☐ **WPS is turned off**
  The push-button / PIN setup shortcut is convenient — and has long-known weaknesses.
  Last checked: _____

- ☐ **Remote management is off**
  The router's admin page should open only from inside your network, never from the internet.
  Last checked: _____

- ☐ **Wi-Fi uses WPA3 (or WPA2-AES)**
  Avoid WEP, WPA/TKIP and open Wi-Fi. Keep your name and address out of the network name.
  Last checked: _____

- ☐ **Visitors use a guest network**
  Guests, kids' friends and contractors stay off your Main network.
  Last checked: _____

- ☐ **Smart-home gear has its own network**
  Cameras, TVs and plugs live on IoT or Guest, so one hacked gadget can't reach your laptop.
  Last checked: _____

- ☐ **Old, unsupported devices are retired or isolated**
  Everything flagged Red on the Devices pages has a plan and a date.
  Last checked: _____

- ☐ **DNS filtering is on**
  Use a security or family DNS service (for example Quad9 or OpenDNS) on the router to block known bad sites.
  Last checked: _____

- ☐ **Automatic updates are on everywhere**
  Phones, computers, tablets, consoles and apps — set it once, then spot-check quarterly.
  Last checked: _____

- ☐ **Backups exist — and a restore was tested**
  Aim for 3 copies, 2 kinds of storage, 1 offsite. Restore one file to prove it works.
  Last checked: _____

- ☐ **Router's device list matches your inventory**
  Open the connected-devices list. Investigate every name you don't recognize.
  Last checked: _____

Score yourself. Anything unchecked goes on your to-do list — start with the items that protect the front door (1–5).

Checks complete (of 12): _____ Next hygiene review due: _____ Reviewed by: _____

5 · If It Goes Wrong

CORE · EVERYONE

FIRST THREE MOVES

1 Contain it

Take the affected device off the network: switch off Wi-Fi or unplug the cable. Don't wipe it or throw it away yet — you may need it to see what happened. If the router itself looks tampered with, unplug it and call your ISP.

2 Secure the keys

From a different, clean device, change your primary email password first, then your bank and the rest of page 5. Turn on MFA and choose "sign out of all other sessions." Change Wi-Fi and router admin passwords last.

3 Call the people who can stop the damage

Your bank or card fraud line, your cell carrier (ask for a port-out lock) and your ISP. Freeze your credit — it's free. Small business: also your IT provider, insurer and attorney.

COMPROMISE OR JUST A GLITCH?

- Password-reset or MFA prompts you didn't ask for
- Friends say they got odd messages or invitations from you
- An unfamiliar device in the router's connected list
- Router settings changed (admin password, DNS servers, port forwards)
- Charges, logins or alerts you don't recognize
- A device that is suddenly slow, hot or full of pop-ups
- Browser redirects, new extensions, or a lock screen demanding payment

Two or more? Treat it as a compromise and start with move 1.

REPORT & FREEZE

Freeze your credit (free): equifax.com · experian.com · transunion.com
Report identity theft: IdentityTheft.gov
Report internet crime (FBI): ic3.gov

WHO TO CALL

Internet provider (ISP) support

Bank / card fraud line

Cell carrier

Trusted tech helper (name & phone)

Router maker support

Other (name & phone)

WHERE MY BACKUPS LIVE

Backup 1 — where & how often

Backup 2 — where & how often

Last restore test (date)

IF I'M UNAVAILABLE

Person who knows where this document and the emergency access info are kept

Print this page. Tape it inside a cabinet door or keep it next to the router. In a crisis, nobody reads manuals — and nobody remembers phone numbers.

B1 · People & Access

ADD-ON · SMALL BUSINESS

Who can get into what? List everyone with access — employees, contractors, family helpers, your IT provider. Review access every quarter and whenever a role changes.

Business name

	Person & role	Systems & data they can reach	Admin rights *tick if yes*	MFA on *tick if yes*	Device *pick one*	Access reviewed *MM/DD/YYYY*	Security training *MM/DD/YYYY*	Offboarded (date) *MM/DD/YYYY*
1			☐	☐				
2			☐	☐				
3			☐	☐				
4			☐	☐				
5			☐	☐				
6			☐	☐				
7			☐	☐				
8			☐	☐				
9			☐	☐				

OFFBOARDING CHECKLIST (do it the same day — every time)

- ☐ Disable email, single sign-on and VPN the same day
- ☐ Remove from shared password vaults; rotate any shared passwords they knew
- ☐ Revoke access to cloud tools, vendor portals and payment systems
- ☐ Change admin logins (router, domain registrar, social accounts) if they knew them
- ☐ Collect or remotely wipe company devices; remove work email from personal phones
- ☐ Revoke API keys, tokens and app passwords; remove from MFA and admin roles
- ☐ Collect keys, badges and any VPN or token hardware
- ☐ Record the date in the table above and note who verified it

NEW HIRE, DAY ONE

MFA on before the first login · only the access the job needs · security basics within 30 days · acceptable-use policy signed · dates recorded in the table above

B2 · Vendors, Cloud & Data Map

ADD-ON · SMALL BUSINESS

Your business runs on other people's computers. List every cloud service and vendor that holds your data or can touch your systems. If one is breached, what do you lose?

Business name

	Service / vendor	Used for	Who administers it	MFA on *tick if yes*	Data it holds *pick one*	Credential kept in *pick one*	Renewal / contract date *MM/YYYY*
1				☐			
2				☐			
3				☐			
4				☐			
5				☐			
6				☐			
7				☐			
8				☐			

DATA MAP — WHAT WE HOLD, WHERE, AND WHO CAN SEE IT

Data type	Where it lives	Who can access it	Backed up *tick if yes*	Encrypted *tick if yes*	How long we keep it
Customer information			☐	☐	
Payment & financial			☐	☐	
Employee records			☐	☐	
Contracts & key files			☐	☐	
Other crown jewel			☐	☐	

Data you can't name is data you can't protect. If a row is empty, that's your first homework: find out where it really lives.

B3 · Recovery, Remote Access & Compliance

ADD-ON · SMALL BUSINESS

NETWORK SEGMENTATION CHECK

- ☐ Guest Wi-Fi is separate from staff Wi-Fi
- ☐ Card terminals / POS are isolated from office computers
- ☐ Cameras, printers and smart devices sit on their own network
- ☐ Router and firewall admin pages reachable only from one management computer

REMOTE ACCESS

☐ VPN ☐ Remote-desktop / support tool ☐ Cloud-only (none needed)

Tool(s) used

Who has remote access

☐ MFA required for all remote access

CRITICAL-SYSTEM RECOVERY — IF IT WERE GONE TOMORROW

	Critical system	Longest we can be down *pick one*	What's backed up & where	Last restore test *MM/DD/YYYY*	Who decides & leads recovery
1					
2					
3					
4					
5					
6					

COMPLIANCE & CONTRACT FLAGS

- ☐ We accept credit or debit cards (PCI DSS)
- ☐ We handle patient or health information (HIPAA)
- ☐ Government or prime-contractor security clauses (CMMC, NIST SP 800-171)
- ☐ We hold customer financial data (GLBA / FTC Safeguards Rule)
- ☐ State breach-notification or privacy laws apply to our customers' data
- ☐ Our insurer, bank or biggest client requires specific controls (MFA, backups, training)

KEY CONTACTS

IT provider (name & phone)

Cyber-insurance carrier & claims line

Policy number kept in

Attorney (name & phone)

Who decides during an incident (and backup)