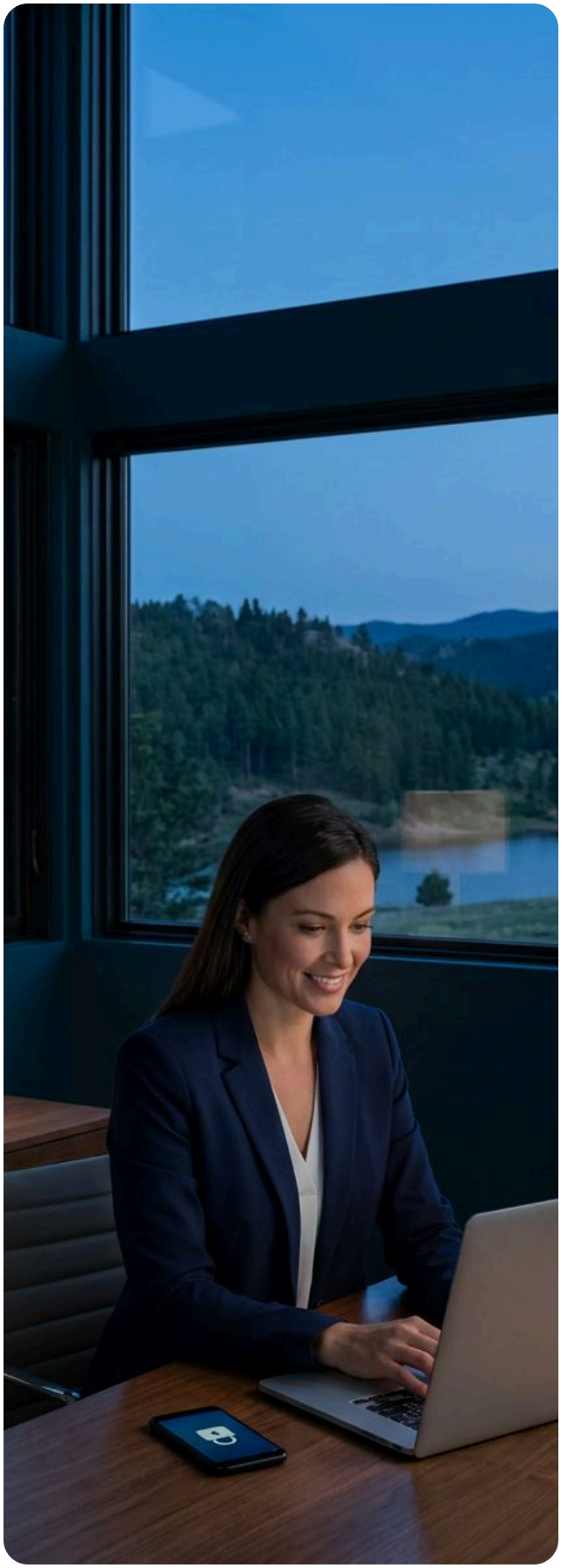
TECHNICAL FRAMEWORK GUIDE

# Personal Digital Security

A practical cybersecurity guide for individuals and solo professionals — without the jargon.

## INSIDE THIS GUIDE

- Home network, router & WiFi security
- Strong passwords & passkeys
- Two-factor authentication
- Public WiFi, VPNs & safe browsing
- Backups, encryption & identity theft
- AI-era scams & smart habits



TECHNICAL FRAMEWORK
IT SOLUTIONS FOR BUSINESS

techframework.com
Fort Collins, CO · Edition 2026

CONTENTS

# What's Inside



### WHO SHOULD READ THIS

Anyone who wants practical, plain-language guidance on personal and home cybersecurity — no technical background required. It's written for individuals — and for professionals who may hold client data. It covers best practices; it is not a step-by-step manual, and technology changes quickly. When something is beyond your comfort level, engage a professional.

START HERE

# Why Personal Cybersecurity Matters

A single compromise can cost you money, time, and trust — often long after the incident, and not always recoverable even when you're insured.

## Financial loss

You can lose a considerable amount of money if you are hacked, and some of those losses may be irreversible. The damage isn't always immediate — fraudulent activity can unfold slowly, over months.

## Liability

If you hold information on other people — as medical, financial, real estate, and insurance practitioners do — you carry the risk of civil action and government fines. Every state has breach-reporting laws and penalties tied to personally identifiable information (PII).

## Reputation

For a business professional, suffering a breach through a lack of due diligence — and having to notify clients, vendors, and partners — can affect your bottom line, if not sideline you entirely.

> **THE THEME OF THIS GUIDE**
>
> Most breaches trace back to a single human moment: acting in a rush instead of pausing to evaluate. The tools in this guide reduce your risk; the habit of slowing down is what ties them together.

YOUR FIRST LINE OF DEFENSE

# Home Router Security

First, the difference between two devices people often confuse.

Your **internet modem** is supplied by your internet provider and links your home to the internet — much like a landline connects a phone to the phone company. Your **home router** then securely connects all your wired and wireless devices — computers, phones, TVs — to that modem. Your router should be set up and maintained by someone who knows what they're doing; it is a common point of attack when it isn't.

## Change the default password

The first step after connecting a new router is to change its default administrator password. Default credentials are published online and are the first thing an attacker tries.

## Keep firmware updated

Routers receive firmware (software) updates throughout their life that fix security vulnerabilities and bugs. Enable automatic updates if your router supports it, and replace hardware that no longer receives them.

## Don't bypass your router

Anything that lets a device reach the internet without passing through your router sidesteps its protection — joining your modem's own WiFi, a neighbor's network, or wiring a device straight into the modem. Route everything through the router. If your provider gave you a combined modem-and-router, ask them or a professional to confirm its built-in protections are on, or to run it behind your own router.

### GUEST VS. TRUSTED WIFI

A capable router lets you enable a separate **guest** network. Devices on guest WiFi can't reach devices on your main network unless you allow it. Put visitors — and smart-home gadgets like TVs and voice assistants — on guest WiFi, and keep your computers and phones on the trusted network.

BARRIERS AGAINST ATTACK

# Firewalls

There are two kinds, and both act as a barrier against intrusion. A **hardware firewall** is built into an appliance like your home router. A **software firewall** comes standard on PCs and Macs and is on by default. You rarely need to change the defaults, and doing so is a job for a professional. Your hardware firewall is the guard at the outer gate; your software firewall is a second barrier — for when the first is bypassed, and whenever you use your device away from home.

**FIREWALLS ARE NOT BULLETPROOF**

They can be bypassed the moment you download malware or click a phishing link. A firewall protects the perimeter; it can't undo an invitation you send yourself.

LOCK DOWN THE AIRWAVES

# WiFi Security

## 1 Use strong encryption

Encryption scrambles the data between your device and your router so no one can eavesdrop. Use **WPA3** where your devices support it — it's the most secure option. **WPA2** remains acceptable for home use if you use a strong password and keep firmware current. Avoid the older WEP and WPA entirely.

## 2 Set a long WiFi password

For WiFi, length matters more than complexity. Make it at least **15 characters** — it doesn't need to be impossible to type. Mix in upper and lower case, a number, and a symbol.

**OPTIONAL EXTRAS — LIMITED VALUE**

You may see **MAC address filtering** and **hidden network names (SSID)** recommended as security steps. (A **MAC address** — "Media Access Control" — is a unique hardware ID built into every network device; it has nothing to do with a Mac computer.) Both offer little real protection — MAC addresses can be copied and hidden names can still be discovered — and they often cause connection headaches. Strong encryption and a long password matter far more; treat these as optional, not essential.

DETECT & REMOVE THREATS

# Malware Protection

Malware protection matters most on **Windows and Mac** computers — keep it installed and current on every machine. Phones and tablets are more locked down; protect them by keeping the operating system updated and installing apps only from the official app stores.

For most people, **Microsoft Defender** (included with Windows) is a genuinely strong baseline, and **Bitdefender** often scores well in independent lab tests if you want a paid option. Both are solid **traditional antivirus**.

## Antivirus vs. EDR

Traditional antivirus mostly recognizes *known* threats — it matches files against a list of malware it already knows. **EDR** (Endpoint Detection and Response) goes further: it watches how programs *behave*, so it catches brand-new "zero-day" attacks no list has seen yet, can automatically isolate a threat, and in some cases can undo damage — such as reversing the file changes made by ransomware. It's the enterprise-grade protection large companies rely on.

### EDR FOR THE HOME

Enterprise EDR is now available to individuals, too. As one example, **EDR for Home** (edrforhome.com) is a managed service built on the **SentinelOne** platform — it adds behavior-based detection, ransomware rollback, and cross-platform coverage (Windows, Mac, Linux) beyond traditional antivirus. It's worth knowing this category exists if you handle sensitive data; compare current options before you buy.

### ONE NAME TO AVOID

Kaspersky products can no longer be legally sold to U.S. customers, and no longer receive U.S. security updates, following a 2024 federal determination. If Kaspersky is still installed, replace it.

SHRINK YOUR FOOTPRINT

# Online Accounts

Most of us have created countless accounts we no longer use. Each forgotten one is another door into your digital life — and should be closed.

## Find the ones you forgot

- **“Sign in with Google/Apple”:** review connected apps in your Google or Apple account security settings and revoke what you don’t use.
- **Social logins:** each platform (Facebook, etc.) has a privacy area listing the apps and sites you’ve logged into — prune them.
- **Inbox clues:** search your email for “welcome,” “confirm,” “verify,” and “thank you for signing up” to surface nearly every account tied to your address.
- **Browser-saved logins:** your browser’s saved passwords reveal old accounts you’ve forgotten. Review and clean them out.

### A SHORTCUT FOR DELETIONS

**JustDeleteMe** (justdeleteme.xyz) is a free directory of direct links to the account-deletion page of hundreds of services, color-coded by how hard each one makes it. It turns “how do I even close this?” into one click.

Going forward: use a password manager (page 12) so new accounts are tracked automatically and never become the ones you forget.

RECLAIM YOUR PRIVACY

# Protecting Your Personal Information

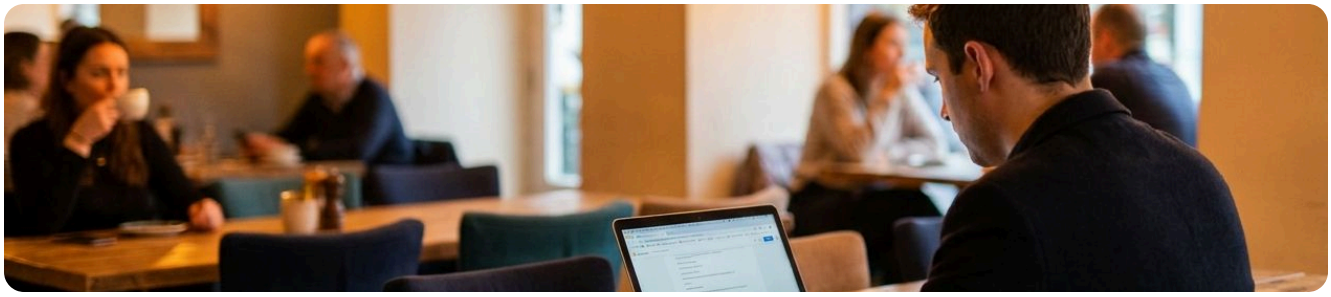
Online privacy can feel lost — advertisers and big companies seem to know everything about you. It's not ESP; it's **data brokers**. These legal businesses scrape and buy personal data, package it into profiles, and sell it.

In many states you can ask brokers to delete your data, and those covered by the law must comply — but the rules vary by state and broker, and there are hundreds of them. Removal services do the finding, requesting, and re-checking for you. Reputable options include **Optery**, **DeleteMe**, and **Incogni**; each offers a paid service and free DIY opt-out guidance.

> **SET IT AND RE-CHECK IT**
> Brokers re-list data over time, so removal is ongoing, not one-and-done. The better services re-scan every couple of months — which is exactly why a service beats a single manual pass.

OUT IN THE WILD

# The Risks of Public WiFi



The biggest risk on public WiFi is someone positioning themselves between you and the connection — so you're handing data to an attacker instead of the venue. Anyone can stand up a WiFi network with any name for very little money. That "Airport_Free_WiFi" may not be the airport's.

## Protect yourself

- **Use your phone instead.** Turn off WiFi and use your phone's hotspot for your laptop or tablet — the simplest, safest option.
- **If you must use public WiFi, use a VPN** (next page) to shield your traffic.
- **Avoid sensitive transactions** — banking, shopping — while on it.

### A NOTE OF REASSURANCE

Nearly all websites now use HTTPS (the padlock), which encrypts your connection to that specific site — the vast majority of web traffic is encrypted today. That's real protection, but it doesn't cover everything you do, so the habits above still matter.

PRIVATE TUNNELS

# VPNs

A VPN (Virtual Private Network) adds privacy and security to your connection — most useful on WiFi you don't control.

A VPN routes your traffic through an encrypted tunnel, hiding it from others on the same network and masking your location. Reputable providers include **Proton VPN**, **Mullvad**, **NordVPN**, and **IVPN**. Paid subscriptions are worth it, especially if you travel; be cautious of "free" VPNs, which often monetize your data. After subscribing, install the app on your PC, Mac, and phone.

### TWO DIFFERENT KINDS OF VPN

A **work (corporate) VPN** connects you back to your employer's network so you can reach work systems from home or the road — it's set up by your IT team for access, not personal privacy. A **personal (privacy) VPN**, the kind described here, protects your own traffic on networks you don't control. They're different tools for different jobs — one is not a substitute for the other.

### GOOD TO KNOW

You may occasionally need to turn a VPN off — some banking sites block logins from VPN connections. That's a minor inconvenience, not a reason to skip using one.

### PERSPECTIVE

A VPN shifts your trust to the VPN provider — they can see the traffic your network or ISP no longer can, so choose a reputable provider with recent, credible independent audits and a clear privacy policy. And because most sites already use HTTPS, a VPN is less essential than it once was for everyday browsing — but it stays valuable on public or untrusted networks.

ACCOUNTS & ACCESS

# Strong Passwords & Passkeys

Passwords are no longer the whole story. The strongest accounts pair a good password manager with **passkeys** — a phishing-resistant sign-in that replaces the password entirely.

## Do the basics well

- Use a **unique** password for every account — aim for **15+ characters**. Length beats complexity.
- Let a **password manager** generate and remember them (page 12).
- Stop rotating passwords on a schedule — change them **when a breach is reported**, not by the calendar.

## Then move to passkeys

A passkey uses your device's face or fingerprint unlock to sign you in — nothing to type, steal, or phish. It's tied to the real website, so it can't be handed to a fake login page. Turn passkeys on for your **most important accounts first** (email, banking, your password manager); they sync across your devices through your platform or password manager. Keep a backup sign-in method enabled so you're never locked out if you lose a device.

**BOTTOM LINE**

Keep strong, unique passwords where passkeys aren't offered yet — and adopt passkeys everywhere they are. Passkeys are now in widespread use, with the largest platforms making them the default for new accounts.

YOUR DIGITAL VAULT

# Password Managers

A password manager stores, protects, and remembers your passwords — so you only remember one. You sign in with a single **master password**, and it fills your credentials into sites and apps automatically. Good managers also store card numbers, licenses, and secure notes. Reputable choices include **1Password** and **Bitwarden** (Bitwarden has a strong free tier). If your passwords live in a notes file or spreadsheet, you're wide open — and protect the manager itself with a passkey or authenticator app on the master account.

**A WORD ON BREACHES**

Even password managers can be targeted — one major provider suffered a serious breach of encrypted vault backups in 2022. The lesson isn't to avoid managers; it's to choose a reputable one, use a long unique master password, and turn on the strongest login protection available.

A SECOND LOCK

# Two-Factor Authentication

2FA (or MFA) adds a second step beyond your password, so a stolen password alone isn't enough to get in. It's no longer optional. Not all second factors are equal:

- **Text-message (SMS) codes** — better than nothing, but vulnerable to "SIM-swap" attacks where a criminal hijacks your phone number.
- **Authenticator apps** — a rotating code on your device; no phone number to hijack. A strong, free upgrade over SMS.
- **Hardware security keys** (such as a YubiKey) — highly resistant to phishing; the strongest option for your highest-value accounts.

PRIVATE CONVERSATIONS

# Secure Texting

Standard text messaging is not private — messages can sit on carrier servers, and the link between sender and receiver isn't always encrypted. **Signal** (signal.org, free) is a widely respected, strong default: it encrypts every message end-to-end **by default**, so not even Signal can read them, and it offers disappearing messages and encrypted calls. Use it alongside your normal texting app.

> **A COMMON MISCONCEPTION**
>
> Telegram is often called "secure," but its ordinary chats are **not** end-to-end encrypted — only its one-on-one "Secret Chats" are, and group chats never are. If privacy is the goal, Signal is the clearer choice.

MAIL, LOCKED DOWN

# Secure & Private Email

**Proton Mail**, based in Switzerland, is a well-regarded privacy-focused option, with end-to-end encryption and options like password-protected and self-destructing messages. End-to-end protection is strongest when your recipient uses a compatible service or you send a password-protected message; ordinary email to any address is less protected. Other reputable names include **Tuta** (formerly Tutanota), **Posteo**, and **Hushmail**. You don't have to move everything — many people keep their everyday inbox and use a secure account for sensitive correspondence.

CLOSE THE DOORS

# PC & Mac Patching

Patching means applying the software updates that fix flaws — including the security holes attackers actively exploit. Operating systems and everyday apps (Office, Adobe, QuickBooks) all need timely updates. Windows and macOS install OS updates automatically by default, but automation can fail, and some **applications may not auto-update reliably**. The best solution is monitored, systematic patching through a professional or IT provider. On your own: keep the OS current through **Windows Update** / **Software Update**, use a tool like **Ninite** for Windows apps, and update Mac apps through the **App Store**.

IF IT'S LOST OR STOLEN

# Full Disk Encryption

Full Disk Encryption (FDE) scrambles everything on your drive, so a thief who takes the device can't read your data. It's a free, built-in feature: **BitLocker** on Windows (shown as "Device Encryption" on Windows Home editions) and **FileVault** on macOS. Two things must be in place first, or FDE can lock *you* out:

- **Save your recovery key** — separate from your login password. If the computer asks for it and you don't have it, the data is gone.
- **Have a current, tested backup** — so if the worst happens, you can recover (see the next page).

KNOW WHEN YOU'RE TARGETED

# Identity Theft Protection

Identity theft protection alerts you — by phone, email, or text — to signs your identity may be misused, such as a new credit inquiry, dark-web exposure, or a change in public records. No service catches every attempt, but the early warning is valuable. A good service covers four areas. Reputable providers include **Aura**, **Identity Guard**, and **LifeLock**.

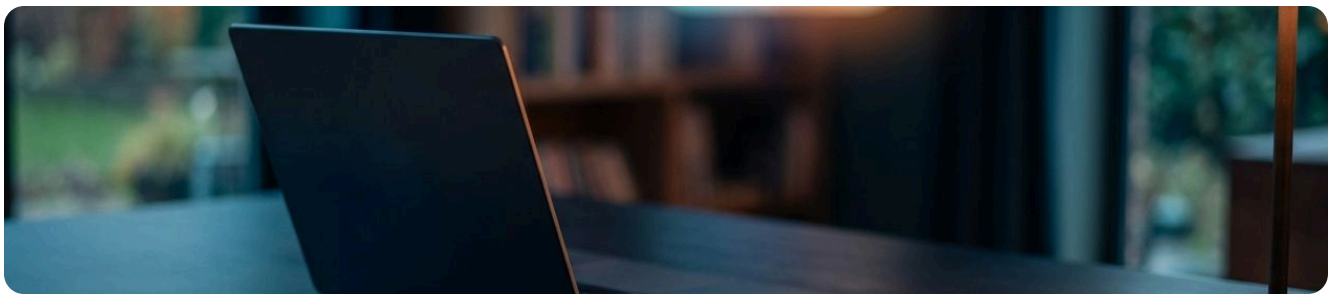
- **Credit monitoring** — watches your reports at Equifax, Experian, and TransUnion and flags new accounts, address changes, and score shifts.
- **Identity monitoring** — scans public records, the dark web, and more for activity tied to your name, address, or details.
- **Recovery assistance** — a dedicated agent who does the legwork of restoring your identity.
- **Identity theft insurance** — reimburses recovery costs; often available as a rider on homeowners/renters insurance.

### CHECK WHAT YOU ALREADY HAVE

You may already carry identity-theft coverage through your bank, credit card, or insurer. Confirm before paying for a duplicate.

THE MOST IMPORTANT PAGE

# Backups & Recovery



Best practices reduce your risk, but a breach or hardware failure can still happen — which is why backup and recovery is the single most crucial part of personal security. And a backup only counts if you can actually restore from it.

- **Recover successfully** — periodically restore a few random files to prove your backup works.
- **Recover in reasonable time** (Recovery Time Objective) — how long to rebuild if a device is lost or destroyed?
- **Recover the right version** (Recovery Point Objective) — yesterday's file or one from six months ago? Choose a service that keeps enough history.

### SYNC IS NOT BACKUP

Services like **OneDrive**, **Google Drive**, and **Dropbox sync** your files — they mirror every change across your devices. If a file is deleted, corrupted, or encrypted by ransomware, that change syncs everywhere too, and your only good copy can vanish. A real **backup** keeps separate, versioned copies you can restore from an earlier point in time.

### FOR MAXIMUM PRIVACY

Look for **zero-knowledge** (private-key) encryption, so not even the provider can read your data. **iDrive** offers a private-key option; **Backblaze** is a simple, unlimited option with a private-key setting (though its restore process has caveats, so it isn't a strict zero-knowledge equivalent). Follow a **3-2-1** rule: three copies, on two types of media, one of them off-site.

THE NEW THREAT

# AI-Era Scams

Artificial intelligence has made scams faster, cheaper, and far more convincing — here's what to watch for.

Criminals now use inexpensive AI tools to **clone a voice** from a few seconds of audio and to write flawless, personalized scam messages at scale. Federal authorities have warned of "family in distress" calls that sound exactly like a loved one, and of highly convincing impersonation of officials and companies.

## How to protect yourself

- **Agree on a family code word** — a private word only real family knows, to confirm identity on an urgent call.
- **Hang up and call back** on a number you already have. A real relative or bank will answer; a scammer won't.
- **Distrust urgency.** "Right now, don't tell anyone, pay this way" is the signature of a scam.
- **Slow down on links and messages** — AI makes phishing look perfect. Verify through a known channel first.

**REPORTED LOSSES ARE REAL**

Reported losses from these scams already run into the hundreds of millions of dollars, and older adults are hit hardest. A ten-second pause defeats most of them.

THE COMMON THREAD

# Good Habits

The most important element in cybersecurity isn't hardware, software, or a subscription. It's us.

Human action can undo any technology-based protection. It's impossible to predict every mistake that leads to a breach, but one root cause runs through nearly all of them: a rush to act instead of pausing to evaluate. Build the pause into your routine, and you've addressed the single biggest risk you face.

- Pause before you click, pay, or share — especially when something feels urgent.
- Verify unexpected requests through a channel you already trust.
- Keep devices updated, backed up, and protected — the boring habits are the ones that save you.
- When in doubt, ask a professional. There's no penalty for checking.

**(970) 372-4940** · help@TechFramework.com · techframework.com
123 N. College Ave #140, Fort Collins, CO 80524