TECHNICAL FRAMEWORK
TECHNOLOGY FOR GROWTH

(970) 372-4940
info@techframework.com
https://techframework.com

A Second Brain for Your Business Tech

TECH INSIDER
May 2025

Corporate

- 8 Quick Wins to Protect Your Business from a Data Breach
- That Email Isn’t From Who You Think: How to Spot Fake Messages That Look Real
- Too Many Tools? Here’s How App Overload Is Slowing Down Your Business
- A Second Brain for Your Business Tech

Personal & Home-Office

- A Physical Key for Your Digital Life: What Is a Yubico Security Key?
- Why You Shouldn’t Keep Passwords in a Notebook (or Your Head)
- How to Make Your Home Wi-Fi Safer in Under 30 Minutes

CORPORATE

A Second Brain for Your Business Tech

Is your business tech running you—or are you running it?

At Technical Framework, we’ve launched a smarter way to manage your IT: the **Tech Bar**. Located in Downtown Fort Collins, the Tech Bar is a **by-appointment**, hospitality-style space where **clients and friends** can get expert help without the jargon, delays, or confusion.

Whether you're a team of one or 100, the Tech Bar offers:

- **Live product demos**
- **Walk-up IT consultations**
- **Workshops for business tools & automation**
- **A hands-on space to explore solutions that fit your workflow**

We designed the Tech Bar to be more than tech support—it’s where your business tech gets connected, protected, and elevated. Come see how a visit to our Tech Bar can become the smartest part of your business week.

☐ **123 N. College Ave, Suite 140, Fort Collins**
☐ (970) 372-4940

☐ techframework.com
☐ **Let us know you're coming so we'll save you a seat!**

PERSONAL & HOME-OFFICE

A Physical Key for Your Digital Life: What Is a Yubico Security Key?

You've probably heard of two-factor authentication (2FA)—the extra step that protects your accounts after you enter your password. Usually, it's a code sent by text or an app. But there's a smarter, more secure way: using a physical security key.
One of the best known is the Yubico Security Key, a small device that plugs into your computer or phone and verifies your identity instantly. No codes. No waiting. Just tap—and you're in.

How It Works

The Yubico key looks like a USB stick, but instead of storing files, it acts as a physical proof that *you* are the person trying to log in.
It works with:
- Google and Microsoft accounts
- Password managers like 1Password or Bitwarden
- Banking sites, government portals, and more
- Social platforms like Facebook and Twitter

When logging in, you simply plug in the key and tap it. If you don't have the key, access is denied—even if someone has your password.

Why It's Better Than 2FA Codes

- No codes to copy or intercept – Eliminates phishing risks
- No waiting for texts or emails
- Works even without cell service
- One key works across multiple accounts
- Much harder for hackers to fake or bypass

It's like having a house key for your digital world—and nobody can pick the lock.

Is It Easy to Use?

Yes. Setup usually takes just a few minutes per account. Once it's in place, login becomes faster—not slower. You can carry the key on your keychain, backpack, or keep a backup stored safely at home.
There are versions with USB-A, USB-C, NFC (for phones), and even Bluetooth support, depending on what devices you use.

Who Should Consider One?

- Anyone using cloud-based email or storage
- Remote workers handling client data
- Business owners with financial or admin access
- Anyone who wants a simple, secure login method
- People tired of dealing with endless login codes

How Technical Framework Helps

We help users identify their most sensitive logins and set up hardware-based 2FA using tools like Yubico keys. Whether you're protecting business data, personal accounts, or a shared household, we'll walk you through choosing the right model and getting it configured safely.

→ Ready to upgrade from SMS codes to physical protection? Schedule a session at TechFramework.com.

DALL-E prompt: A modern office desk with a laptop displaying a locked password icon, surrounded by a notebook, coffee mug, plant, and smartphone—illustrating secure password management in a clean, tech-savvy style.

PERSONAL & HOME-OFFICE

Why You Shouldn't Keep Passwords in a Notebook (or Your Head)

Most people have dozens—sometimes hundreds—of passwords. Email, banking, shopping, work accounts, cloud storage, streaming services, and more. It’s no wonder many users still rely on sticky notes, spreadsheets, or memory to keep track.

But here’s the problem: convenience doesn’t equal security.
If your passwords are easy to access, they’re also easy to steal. And if you reuse them, a single data breach on one site can expose everything else.

What Could Go Wrong?
- A stolen Amazon password reveals your saved cards
- A reused email password lets hackers reset your bank login
- A single malware infection captures passwords saved in your browser
- A lost or stolen notebook gives a thief everything they need

The result? Locked accounts, identity theft, financial loss, and a lot of stress.

What You Need Instead: A Password Manager

A password manager is like a digital vault. You remember *one* strong master password, and it remembers the rest—securely encrypted and synced across your devices.

Here’s what it can do for you:
- Generate strong, unique passwords for every website
- Autofill login info so you don’t waste time typing
- Store sensitive notes, like Wi-Fi credentials or license keys
- Work across devices, so you're covered at home and on the go
- Warn you about reused or weak passwords

It’s safer, faster, and actually easier than doing it yourself.

Which One Should You Use?

There are many great options available—some built into browsers, others as dedicated apps. Most offer both free and paid plans depending on the features you want.

The key is to choose one that:
- Works on all your devices
- Has good reviews and strong encryption
- Offers two-factor authentication
- Is easy for you to use consistently

Once you switch, you’ll wonder how you ever managed without it.

How Technical Framework Can Help

Not sure where to start? We help home-office users choose and set up password managers that fit their comfort level and lifestyle. Whether you want a guided walkthrough, a quick setup, or just a recommendation, we’ll help you protect your digital life without the overwhelm.

**→ Give your memory a break—and your accounts a serious upgrade.
Book a password security session at TechFramework.com.**

CORPORATE

8 Quick Wins to Protect Your Business from a Data Breach

A data breach doesn’t just hit big corporations—it happens to small businesses every day. And when it does, the impact is personal: stolen client data, fraudulent charges, locked accounts, and a serious hit to your reputation.

Many businesses don’t realize they’ve been breached until it’s too late. But the steps you take *after* a breach are just as important as the ones you take to prevent it.
Here’s a quick-response checklist that can limit the damage and help you bounce back faster.

If You Receive a Breach Notification:

1. Change Your Passwords Immediately

5. Review the Details of the Breach
What data was exposed? Was it email addresses, passwords, credit cards, or full identity info? Understanding the scope helps guide your next steps.

6. Install or Update Cybersecurity Tools
Make sure your antivirus, firewalls, and device protections are current. Breaches are often followed by new phishing or malware attempts.

7. Be Alert for Follow-Up Scams
Attackers often follow up with emails pretending to “help” you. Be skeptical of any messages offering refunds, fixes, or security scans.

8. Update All Your Devices and Software
Breaches often exploit outdated

Focus on affected accounts first, then update any others that used the same or similar login credentials.

2. Turn On Multi-Factor Authentication (MFA)
MFA makes it much harder for attackers to use stolen passwords. Most platforms support it—just toggle it on in your settings.

3. Check All Bank and Credit Accounts
Look for suspicious charges or transfers. Even small amounts could be a test run by fraudsters.

4. Freeze Your Credit (If Needed)
If personal info like your SSN or tax ID was exposed, freezing your credit can block new accounts from being opened in your name.

systems. Keep everything up to date to close security holes and prevent reinfection.

How Technical Framework Helps

We don't just clean up after the fact—we help you stay protected year-round. From breach response to ongoing monitoring, we give small businesses the same level of protection large companies expect—without the overhead.

→ Want to see where your weak points are before something happens?

Book a security checkup at TechFramework.com.

DALL-E prompt: A modern office desk featuring a laptop with a phishing email on screen labeled "FAKE EMAIL" and a warning icon. The workspace includes a coffee mug, smartphone, spiral notebook, and potted plants, with a wall clock and cityscape visible through the windows. The scene uses a consistent flat design and muted blue-green color palette.

CORPORATE

That Email Isn't From Who You Think: How to Spot Fake Messages That Look Real

Small businesses get hit hardest when a fake email slips through. It might look like it's from a vendor, a coworker, or even your bank. But one wrong click, and you're dealing with stolen credentials, wire fraud, or worse.

Cybercriminals have gotten smart. They don't send sloppy scams anymore. Today's phishing emails look nearly perfect—polished logos, real names, legit-sounding content. And they don't always ask for money. Sometimes all it takes is opening a file or clicking a link.

Red Flags to Watch For

• Unexpected attachments – Especially from contacts you weren't expecting to hear from

• Generic greetings – "Hi Customer" instead of your name

• Malware installed on your network
• Client data leaks
• Real financial losses

It's not just a nuisance—it's a business risk.

What Small Businesses Can Do

Staying safe doesn't require hiring a security team. It starts with small, smart habits:

• Hover over links before clicking – Check where they *actually* lead

• Verify requests – If something seems off, call the sender

• Use strong, unique passwords – And store them securely

• Turn on multi-factor authentication – Especially for email and banking

• Train your team – A quick monthly

- Minor spelling changes – A domain like paypaI.com instead of paypal.com (look closely)

- Urgency or threats – "Act now or your account will be locked"

- Out-of-character requests – A team member asking for gift cards or a quick wire transfer

Even smart people fall for these. And if your team isn't trained to catch them, it's only a matter of time.

The Cost of One Click

One phishing email can lead to:
- Locked accounts
- Compromised passwords

reminder or example goes a long way

How Technical Framework Helps

We help small businesses avoid email-based threats with layered protection and team awareness. That includes smart filters, proactive alerts, and simple checklists to keep everyone on the same page.
No scare tactics—just the tools and habits that work.

→ Want to test how secure your email setup really is? Schedule a no-pressure review at techframework.com.

PERSONAL & HOME-OFFICE

How to Make Your Home Wi-Fi Safer in Under 30 Minutes

Your home Wi-Fi network is the digital front door to everything you do online. If it's not secured properly, hackers can spy on your activity, steal your information, or even access devices like smart cameras, thermostats, and baby monitors.

The good news? You don't need to be a tech expert to make your home network safer. Just a few simple steps can lock things down and give you peace of mind.

1. Change Your Wi-Fi Password
If you're still using the default password that came with your router, change it now. Choose something strong, unique, and hard to guess. Avoid using names, birthdays, or simple patterns.

2. Rename Your Network (SSID)
Routers often broadcast their brand in the network name (like "Netgear123" or "LinksysXYZ"), which tells hackers what type of device you're using. Rename it to something generic and boring.

3. Turn On WPA3 Security (If Available)
Check your router's settings and make sure the wireless security type is set to WPA3 or WPA2 at minimum. If it's still on WEP, it's outdated and insecure.

4. Update Your Router's Firmware
Manufacturers release updates to patch vulnerabilities. Log into your router settings and look for a "Firmware Update" or "Check for Updates" option. It's usually under "Advanced" or "Administration."

5. Disable Remote Management
Most people never need to access their router remotely. Turn off remote management to block outside access from the internet.

6. Separate Your Devices
Create a guest network for visitors. Also, consider putting smart home devices (like Alexa or smart plugs) on a separate network from your main computers and phones.

7. Reboot Regularly
Some malware lives in memory and disappears when you reboot. Restarting your router every week or two is a simple preventive step.

8. Use a Strong Router Admin Password
This is different from your Wi-Fi password. It's what you use to log into the router settings page. Make sure it's not "admin" or "password."

How Technical Framework Can Help

Need help with a messy setup or aging equipment? We assist home-office users with network assessments, hardware upgrades, and step-by-step Wi-Fi hardening. If you're not sure what your current router is protecting (or not protecting), we can help you find out.

→ Keep your network safe and private. Schedule a home Wi-Fi checkup at TechFramework.com

CORPORATE

Too Many Tools? Here's How App Overload Is Slowing Down Your Business

Small businesses rely on more tools than ever—email, calendars, CRMs, task trackers, online forms, cloud storage. The goal? Efficiency. The result? A scattered, disconnected mess.

Every day, you spend time manually moving information between systems. Copying customer info into three different tools. Searching for files. Creating reminders. Updating spreadsheets. It feels necessary, but it’s not progress—it’s friction.

Where App Overload Slows You Down

- Entering the same details across multiple platforms
- Missing appointments due to disconnected calendars
- Forgetting follow-ups because your CRM isn’t in sync
- Searching endlessly for documents that never landed where they should
- Wasting mental energy switching between tabs and dashboards

This kind of disjointed workflow isn’t just inconvenient—it’s expensive. It costs time, accuracy, and missed opportunities.

The Fix? Not Fewer Tools. Smarter Tools.

Modern platforms like Microsoft 365, Google Workspace, HubSpot, and Shopify are built to work together. When connected correctly, they can:

- Share customer data across systems automatically
- Sync bookings and meetings in real time
- Route files to the right person or location instantly
- Trigger reminders and next steps without your input

The result is a seamless experience—less clicking, less copying, and fewer things slipping through the cracks. Your business flows faster, with fewer mistakes and more headspace to focus on what matters.

How Technical Framework Helps

We help you get your apps and platforms working together—quietly, behind the scenes—so you can focus on delivering your service, not wrestling with your systems.

No new software. No learning curve. Just smoother, faster workflows that free up hours of your week.

→ Curious how much time you’re wasting on manual tasks?

Book a free workflow discovery session at techframework.com.

Technical Framework maintains an **A+** rating with the **BBB** A+ BBB

FORT COLLINS AREA CHAMBER OF COMMERCE

GREELEY AREA CHAMBER OF COMMERCE