TECH TALK
MONTHLY

Stilwell Support
Expert Support with Wallet-Friendly Solutions

JULY 2026

HOME OFFICE SECURITY DEFAULTS EVERY REMOTE WORKER NEEDS

More in this edition:

- What attackers do after they've already beaten your MFA
- A 5-minute audit that reveals which browser extensions are spying on you
- The expensive surprise waiting when you try to leave your SaaS provider
- How to spot fake recruiters targeting your employees on LinkedIn

stilwellsupport.com 239.376.0075 info@stilwellsupport.com

What's Inside

Page 1:

- ***After the Login: What Happens When MFA Gets Bypassed***

Page 2:

- ***The Hidden Cost of SaaS Backup: Planning Your Exit Strategy***

Page 3:

- ***The 5-Minute Browser Extension Security Check***

Page 4:

- ***Red Flags for Fake LinkedIn Recruitment Scams***

Page 5:

- ***The 4-Step Legacy IT Debt Audit Your Business Needs***

Page 6:

- ***Home Office Security Defaults Every Remote Worker Needs***

Dear Fellow Business Owner 👋

I hope this newsletter finds you and your team thriving. As remote and hybrid work continues to be the norm for so many of us, I've been thinking a lot about the small security gaps that emerge when our offices become our living rooms. This month's cover story tackles something we don't talk about enough: the physical security of home workspaces.

It's easy to focus on firewalls and password managers while forgetting that a Post-it note with credentials or an unlocked laptop during a doorbell ring can be just as risky. The reality is that home offices blend our professional and personal lives in ways that create unexpected vulnerabilities—not because our families are threats, but because we're simply not in a controlled office environment anymore.

Inside this issue, you'll also find practical guidance on MFA bypass tactics, the true cost of SaaS data, browser extension risks, and more. As always, we're here to help you stay secure without the overwhelm. Here's to building better habits, one small default at a time.

John Stilwell
Owner, Stilwell Support

DID YOU KNOW ?

According to IBM, 19% of data breaches are caused by compromised credentials left physically exposed, costing businesses an average of $4.5 million per incident.

GET IN TOUCH

239.376.0075

stilwellsupport.com

info@stilwellsupport.com

AFTER THE LOGIN: WHAT HAPPENS WHEN MFA GETS BYPASSED

Multi-factor authentication is supposed to be the lock on your digital front door. But what happens when an attacker finds a way around it—not by breaking the lock, but by walking in right behind someone who just unlocked it? Session cookie hijacking lets attackers do exactly that, and the real damage begins after they're already inside your systems, moving through your business undetected.

How Attackers Steal the Keys After You've Already Unlocked the Door

The technique is called Adversary-in-the-Middle (AiTM), and it works like a digital pickpocket. According to Cloudflare, these attacks involve "intercepting and relaying authentication requests and session cookies between the user and the legitimate service, allowing them to steal the session cookie after the user has successfully authenticated, including MFA, and then use that cookie to impersonate the user."

Think of a session cookie as a backstage pass your browser receives after you log in successfully. It tells the system "this person already proved who they are, let them through." When an attacker steals that pass, they don't need your password or your phone for MFA—they just walk in as you.

The attack typically starts with a phishing email that looks legitimate. When you click the link, you're taken to a fake login page that looks identical to the real one. But here's the twist: when you enter your credentials and complete MFA, you're actually logging into the real service—the attacker's fake site is just sitting in the middle, passing everything through while copying your session cookie for themselves.

What Attackers Do Once They're Inside

This is where things get serious. The Microsoft Security Blog notes that "once a user enters their credentials and completes MFA, the adversary intercepts the session cookie and can use it to authenticate to the web service as the user, even if the user changes their password, gaining access to the user's mailbox and other sensitive data, leading to business email compromise (BEC) and other attacks."

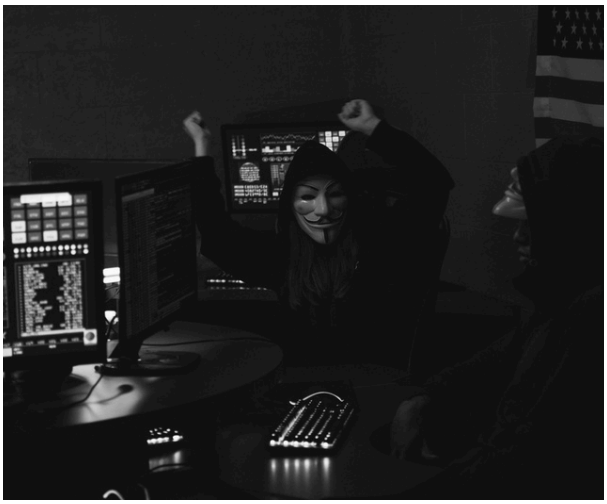
Once inside your email account, attackers typically work fast. They'll scan your inbox and sent items to understand your business relationships, ongoing projects, and payment processes. They're looking for invoices, wire transfer instructions, and conversations about money. Many will set up email forwarding rules to silently copy future emails to themselves, extending their access even after the stolen session expires.

Business email compromise is often the next step. Attackers might impersonate you to request urgent wire transfers, change payment details with vendors, or trick employees into sharing sensitive information. Because the emails come from your actual account—not a spoofed address—they're incredibly convincing.

Some attackers also use compromised accounts to move laterally through your organization. They'll access shared documents, cloud storage, and internal systems. If your email account has admin privileges or access to other business applications, those become targets too.

Why Traditional Defenses Miss This Attack

The reason session hijacking is so effective is that it bypasses the security measures most businesses rely on. You had a strong password—didn't matter. You used MFA—still got compromised. Even changing your password after the attack won't kick the attacker out, because they're using your session cookie, not your credentials.



Traditional security tools often miss this activity because, from the system's perspective, it looks like you're legitimately logged in. The attacker is using valid authentication tokens, so there's no failed login attempt to trigger an alert. They're accessing your account from a different location or device, but many businesses don't have monitoring in place to catch those anomalies.

Protecting Your Business Beyond the Login Screen

The good news is that session hijacking can be detected and prevented with the right approach. Modern security tools can monitor for suspicious session behavior—like a user suddenly accessing their account from two different countries simultaneously, or unusual patterns of email forwarding and deletion.

Session timeout policies matter more than you might think. Shorter session durations mean stolen cookies expire faster, limiting the attacker's window. Some advanced security solutions can also bind sessions to specific devices or network conditions, making stolen cookies useless when used from a different context.

Employee training needs to evolve beyond "don't click suspicious links." Your team should know to verify the actual URL before entering credentials, watch for subtle signs that a login page might be fake, and report anything unusual immediately—even if they're not sure.

Regular security audits of email accounts can catch the telltale signs of compromise: unexpected forwarding rules, unfamiliar devices with active sessions, or access from unusual locations. The sooner you catch these indicators, the less damage an attacker can do.

Getting Help With Modern Authentication Threats

Session hijacking and MFA bypass attacks represent a new generation of threats that require a new generation of defenses. If you'd like help assessing your current authentication security, implementing session monitoring, or training your team to recognize these sophisticated attacks, contact us. We help businesses like yours stay protected against threats that evolve faster than traditional security can keep up.

THE HIDDEN COST OF SAAS BACKUP: PLANNING YOUR EXIT STRATEGY

When you commit to a SaaS platform, you're not just choosing software—you're choosing a relationship that could cost thousands to exit. Most small business owners focus on monthly subscription fees, but the real financial risk lurks in what happens when you need to leave or back up your data elsewhere. Data egress fees, reformatting costs, and migration expenses can turn a simple platform switch into a budget-busting nightmare. Understanding these costs upfront isn't pessimism; it's smart financial planning.

The Real Price Tag of Moving Your Data

The sticker shock of leaving a SaaS vendor often catches businesses off guard. According to TechTarget, "the cost of moving data out of a SaaS vendor can be substantial, especially for large datasets, due to data egress fees and the potential need for data reformatting." These aren't minor line items—for a business with years of accumulated data, egress fees alone can run into thousands of dollars.

Consider what you're actually paying for: Every gigabyte transferred out, every API call to extract your information, and every hour spent reformatting data to work with a new system. A company with 50 employees might have 500GB or more of data spread across email, file storage, and business applications. At typical egress rates, that's a significant unexpected expense before you've even paid for the new platform.

Three Cost Centers Most Businesses Overlook

Beyond the obvious egress fees, three additional cost centers can derail your budget. First, there's data transformation—your information rarely exports in a format that's immediately usable elsewhere. You'll need technical resources to convert, clean, and verify data integrity, which means either paying your IT team for overtime or hiring consultants.

Second, ZDNet points out that "organizations must factor in these potential expenses, alongside the costs of re-platforming and retraining, when evaluating SaaS solutions." Retraining isn't just about learning new buttons; it's about lost productivity during the transition period. Expect a 20-30% productivity dip for at least two weeks as your team adapts.

Third, there's the opportunity cost of leadership time. Your decision-makers will spend dozens of hours evaluating alternatives, overseeing migration, and troubleshooting issues. That's time not spent on revenue-generating activities or strategic planning.

Building a Cost-Effective Exit Strategy Now

The best time to plan your exit is before you fully commit. Start by asking potential SaaS vendors specific questions: What are your data egress fees? In what formats can data be exported? Is there an API for automated backups? Get these answers in writing before signing.

Next, implement regular, automated exports of your critical data to neutral storage you control. This

doesn't mean abandoning the SaaS platform's built-in backups, but rather maintaining a parallel copy in a standard format. The incremental cost of cloud storage for these exports is minimal compared to emergency extraction fees.

Finally, budget for portability from day one. Set aside 10-15% of your annual SaaS spend as an "exit fund" that covers potential migration costs. This financial cushion transforms vendor lock-in from a trap into a calculated business decision. You're not locked in if you can afford to leave.

Making Lock-In Work for You

Some degree of vendor integration is inevitable and even beneficial—it's how you get the full value from sophisticated platforms. The goal isn't to avoid commitment entirely, but to ensure that commitment is voluntary rather than financial coercion. When you know exactly what leaving would cost, you can negotiate from a position of strength and make informed decisions about when to stay and when to switch.

Document your exit strategy in a simple one-page plan: where your data lives, how to extract it, what formats you need, and what the estimated costs are. Update this annually as your data volume grows. This exercise alone often reveals surprising dependencies or identifies data you're storing unnecessarily.

If you'd like help evaluating your current SaaS commitments and building a cost-effective backup exit strategy, we work with businesses to create practical plans that balance convenience with financial flexibility. Contact us to discuss your specific situation and get a realistic estimate of what your exit options actually cost.

THE 5-MINUTE BROWSER EXTENSION SECURITY CHECK

Why Browser Extensions Deserve a Second Look

Browser extensions can boost productivity, block ads, and streamline workflows—but they also have access to nearly everything you do online. Many extensions can read your passwords, track your browsing history, and access sensitive business data. The good news? A quick five-minute vetting process can help you separate legitimate tools from potential security risks.

What Makes Extensions Risky?

Extensions operate with elevated permissions inside your browser. Unlike regular websites, they can monitor your keystrokes, modify web pages, and transmit data to third parties. Kaspersky emphasizes that before installing any extension, you should always check the publisher's reputation, read user reviews, scrutinize the requested permissions, and review the privacy policy to understand how your data will be handled. For small businesses where employees access financial systems, customer databases, and proprietary information through their browsers, a compromised extension can become a gateway to your entire network.

The 5-Minute Vetting Checklist:

- **Verify the publisher identity:** Check if the extension comes from a known company or developer with a verifiable web presence and contact information.
- **Review the permission requests:** If a simple calculator extension asks to "read and change all your data on all websites," that's a red flag. Permissions should match functionality.
- **Read recent user reviews:** Sort by newest first and look for patterns of complaints about suspicious behavior, performance issues, or recent changes after updates.
- **Check the last update date:** Extensions abandoned for over a year may contain unpatched security vulnerabilities. Active maintenance is a good sign.
- **Search for the extension name plus "security" or "malware:** A quick web search can reveal if security researchers have flagged the extension or if it's been removed from stores previously.
- **Examine the privacy policy:** Cloudflare recommends that users only install extensions from official stores and carefully review what data is collected and whether it's shared with third parties.

Take these five minutes before clicking "Add to Browser"—your business data is worth the wait.

RED FLAGS FOR FAKE LINKEDIN RECRUITMENT SCAMS

LinkedIn has become a primary hunting ground for scammers posing as recruiters. These fraudsters create convincing fake profiles to steal personal information, financial data, or even trick victims into laundering money. Knowing what to watch for can save your employees—and your business—from a costly breach.

Watch for these warning signs:

- **The profile looks too generic or too perfect.** Microsoft Security warns that scammers often create fake profiles using stolen photos and vague job descriptions. Check if the recruiter's profile has a sparse work history, few connections, or recent account creation date.
- **The job offer seems unrealistically good.** According to Proofpoint, opportunities that promise exceptionally high pay for minimal work or vague responsibilities are classic bait. If it sounds too good to be true, it probably is.
- **They pressure you to respond immediately.** Legitimate recruiters understand candidates need time to consider opportunities. Scammers create artificial urgency to bypass your critical thinking.
- **They ask for personal or financial information early.** Proofpoint notes that requests for bank details, Social Security numbers, or copies of identification documents before a formal interview process are major red flags. Real companies conduct this through secure HR systems after extending offers.
- **Communication quickly moves off LinkedIn.** Be suspicious if the recruiter immediately pushes conversation to WhatsApp, Telegram, or personal email. Legitimate recruiters typically use company email addresses and established platforms.
- **They ask you to download software or click suspicious links.** Microsoft Security identifies this as a common tactic to install malware or steal credentials. Legitimate recruitment processes don't require downloading unfamiliar applications.
- **The company details don't check out.** Search for the company independently—not through links they provide. Verify the recruiter actually works there by calling the company's main number or checking their official website's staff directory.

THE 4-STEP LEGACY IT DEBT AUDIT YOUR BUSINESS NEEDS

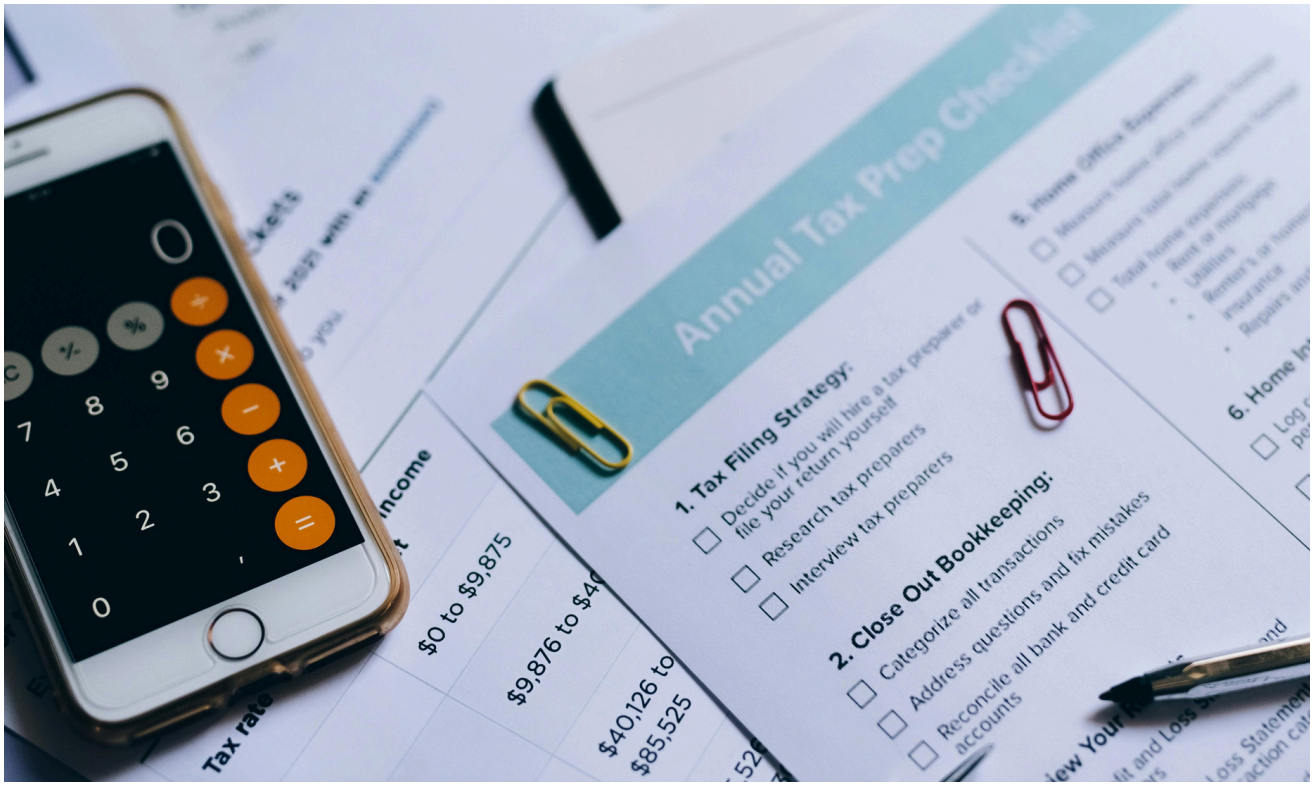
Legacy systems and outdated technology create hidden costs that drain your budget and slow your business down. If you're running software that hasn't been updated in years, relying on hardware past its prime, or patching together workarounds to keep things running, you're carrying technical debt. According to TechTarget, "A technical debt audit involves systematically identifying, assessing, and prioritizing areas of technical debt within an organization's IT landscape. This process helps organizations understand the scope and impact of their debt, enabling them to create a strategic plan for remediation." Here's how to conduct a practical audit of your legacy IT systems.

1. **Inventory Your Current IT Assets.** Start by creating a complete list of every system, application, and piece of hardware your business uses. Include the age of each asset, its current version, the vendor's support status, and who depends on it daily. This isn't just about servers and computers—document your software licenses, cloud subscriptions, and any custom applications built years ago that still run critical processes.

2. **Assess Business Impact and Risk.** For each item in your inventory, evaluate how it affects your operations. Ask: What happens if this system fails tomorrow? Does it handle sensitive customer data? Is it connected to other critical systems? CIO.com emphasizes that "assessing the impact of technical debt on business operations" and "prioritizing remediation efforts based on risk and value" are essential steps in managing technical debt effectively. Systems that pose security risks or could halt business operations should rise to the top of your priority list.

3. **Calculate the True Cost of Keeping It.** Legacy systems cost more than their maintenance contracts. Factor in the staff time spent on workarounds, the productivity lost to slow performance, the security vulnerabilities that put you at risk, and the opportunities you're missing because your systems can't support new capabilities. Compare these ongoing costs against the investment required to modernize or replace the system.

4. **Create a Prioritized Remediation Roadmap.** Based on your risk assessment and cost analysis, build a realistic plan for addressing your technical debt. Some systems may need immediate replacement, while others can be phased out gradually. Budget for both quick wins that deliver immediate value and longer-term projects that address foundational issues. Set clear timelines, assign ownership, and establish metrics to track your progress.



If you'd like help conducting a thorough legacy IT audit or developing a modernization strategy that fits your budget and timeline, contact us to discuss your specific situation.

HOME OFFICE SECURITY DEFAULTS EVERY REMOTE WORKER NEEDS

Working from home has blurred the line between personal and professional space, but your security posture shouldn't blur with it. Whether you're in a dedicated home office or working from the kitchen table, establishing baseline security defaults protects both your company's data and your own peace of mind.

Core defaults to implement immediately

- Lock your computer screen every time you step away—even for 30 seconds to grab coffee or answer the door
- Set your computer to auto-lock after 5 minutes of inactivity as a backup to manual locking
- Store all physical documents with sensitive information in a locked drawer or filing cabinet when not actively in use
- Remove sticky notes containing passwords, Wi-Fi credentials, or access codes from your monitor and desk area
- Position your monitor so it's not visible through windows or to anyone passing by your workspace
- Clear your desk of client files, financial records, and proprietary documents at the end of each workday
- Use a privacy screen filter if you work in shared living spaces or areas with foot traffic
- Shred sensitive documents rather than tossing them in household trash or recycling
- Keep work devices physically separate from personal devices and family members' access
- Establish a dedicated charging station for work devices that's out of reach of children, guests, or household visitors

CISA emphasizes that you should "ensure that sensitive information is not left unattended or visible to unauthorized individuals. This includes physical documents, sticky notes with passwords, and information displayed on computer screens." The same principle applies whether unauthorized individuals are external threats or simply family members who shouldn't have access to confidential business information.

These defaults aren't about distrusting your household—they're about building habits that protect you regardless of circumstance. A locked screen prevents your curious teenager from accidentally seeing employee salary data. A clear desk means the plumber who's fixing your sink doesn't glimpse client contracts. Physical security measures create layers of protection that complement your digital safeguards.

Thank You!

Thanks for taking the time to read this month's newsletter. We hope you picked up a few helpful tips or ideas to make your tech work a little smarter for you.

If you ever have questions, or just want a second opinion on anything IT-related, we're only a phone call or email away.

CONTACT US BELOW

239.376.0075

info@stilwellsupport.com

stilwellsupport.com

Stilwell Support

Expert Support with Wallet-Friendly Solutions.