JULY 2026
Fitzgerald, Georgia

asyst YOU Technology

TECH TALK

"Insider Tips to Make Your Business Run Faster, Easier and More Profitable"

INSIDE THIS ISSUE:

We love technology and we love helping people.

Give me a call today for a quick (non-salesy) chat to find out whether my team and I can help you better secure your data and get more out of your existing technology!

- **Scott Spivey**

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.

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. Many will set up email forwarding rules to silently copy future emails to themselves, extending their access even after the stolen session expires.

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 business applications, those become targets too.

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.

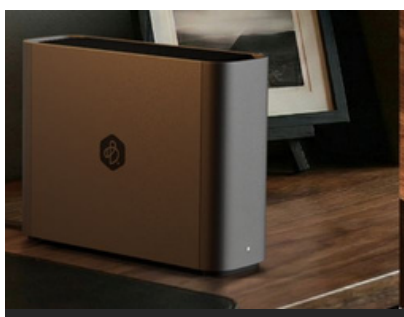
Session timeout policies matter more than you might think. Shorter session durations mean stolen cookies expire faster, limiting the attacker's window. Some advanced security solutions can also bind sessions to specific devices or network conditions, making stolen cookies useless when used from a different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

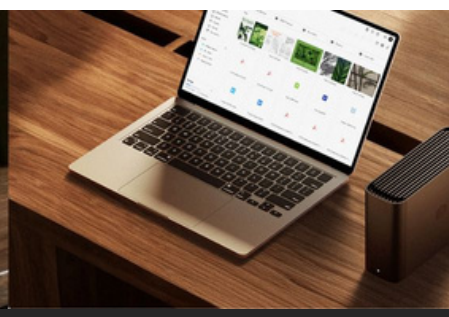
Employee training needs to evolve beyond "don't click suspicious links." Your team should know to verify the actual URL before entering credentials, watch for subtle signs that a login page might be fake,and report anything unusual immediately.

Regular security audits of email accounts catch the telltalesigns of compromise. The sooner you catch these indicators, the less damage attackers can do.

Getting Help with Modern Authentication Threats

If you'd like help assessing your current authentication security or training your team to assess these attacks, contact us. We help businesses like yours stay protected against threats that evolve faster than traditional security can keep up.





SYNOLOGY BEESTATION

Synology BeeStation is a compact, plug-and-play personal cloud device that gives teams simple, private storage for work and photosat home or in the office.

Set it up in minutes, then access files from phone, desktop, and web apps. With local storage and easy sharing, it keeps data under your control without monthly fees.

It's ideal for replacing shared drives and cloud plans while keeping files on a box you own withstraightforward controls.

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 expense scan turn a simple platform switch into a budget-busting nightmare.

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.

Second, ZDNet points out that "organizations must factor in these potential expenses, alongside the costs of re-platforming and retraining, when evaluating SaaS solutions." Expect a 20-30% productivity dip as your team adapts.

Third, there's the opportunity cost of leadership time. Your decision- makers will spend 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? 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.

Finally, budget for portability from day one. Set aside 10-15% of your annual SaaS spend as an "exit fund". This financial cushion transforms vendor lock-in from a trap into a calculated business decision.

Contact us to discuss your specific situation and get a realistic estimate of what your exit options actually cost.

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. Here's how to conduct a practical audit of your legacy IT systems.

• 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. Document your software licenses, cloud subscriptions, and any custom applications built years ago that still run critical processes.

• 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? Systems that pose security risks or could halt business operations should rise to the top of your priority list.

• Calculate the True Cost of Keeping It

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.

• 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 and longer-term projects that address foundational issues. Set clear timelines, assign ownership, and establish metrics.

Contact us if you'd like help conducting a thorough legacy IT audit or developing a modernization strategy that fits your budget and timeline.

THE 5-MINUTE BROWSER EXTENSION CHECK

A quick five-minute vetting process can help you separate legitimate tools from potential security risks.

1. Verify the publisher identity. Check if the extension comes from a known company or developer.
2. 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.
3. Read recent user reviews. Look for patterns of complaints about suspicious behavior,performance issues, or recent changes after updates.
4. Check the last update date. Extensions abandoned for over a year may contain unpatched securityvulnerabilities.
5. Search for the extension name plus "security" or "malware".
6. Examine the privacy policy. Carefully review what data is collected and how it is shared.

RED FLAGS FOR FAKE LINKEDIN RECRUITMENT SCAMS

Knowing what to watchfor can save your employees and your business from a costly breach.

- The recruiter's profile looks too generic or too perfect.
- The job offer seems unrealistically good.
- They pressure you to respond immediately. Scammers create artificial urgency to bypass your critical thinking.
- They ask for personal or financial information early. Real companies conduct this through secure HR systems after extending offers.
- Communication quickly moves off LinkedIn to apps like Whatsapp or Telegram.
- They ask you to download software or click suspicious links.
- The company details don't check out. Search for the company independently, not through links they provide.

HOME OFFICE SECURITY DEFAULTS EVERY REMOTE WORKER NEEDS

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
- Remove sticky notes containing passwords, Wi-Fi credentials, or access codes from your monitor and desk area
- Clear your desk of client files, financial records, and proprietary documents
- Position your monitor so it's not visible through windows or to anyone passing by your workspace
- Use a privacy screen filter if you work in shared living spaces or areas with foot traffic
- Keep work devices physically separate from personal devices and family members' access
- Establish a dedicated charging station for work devices

Support Tickets:

For the best service, please use the smiley face on your desktop taskbar to create a ticket.