TALK NERDY TO ME

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!

- Jason Horne
CEO

THE "SESSION COOKIE" HIJACK: WHY MFA CAN'T ALWAYS SAVE YOU

MFA is a strong front-door lock. But it's not the only thing that decides whether someone can get in.

After you sign in, your browser keeps you logged in using a session token (often stored as a cookie). It's the digital version of a wristband at an event: once you've been checked, the wristband proves you belong there. If an attacker steals that wristband, they may not need to beat your MFA prompt at all.

That's the core of session cookie hijacking. The attacker isn't "cracking" MFA. They're skipping it by replaying your already authenticated session.

This isn't a reason to stop using MFA. It's a reason to stop treating MFA as the finish line.

Why MFA Isn't a "Game Over" Control

MFA is still one of the best upgrades most businesses can make, but it doesn't end an attack on its own. The reason is that attackers don't always try to beat the login step. They try to go around it.

Cloudflare notes that "attackers are finding new ways to circumvent MFA" and that modern incidents are rarely one isolated technique. They're "part of a chain of attacks."

In other words, MFA can block a lot of credential theft, but it doesn't automatically protect what happens after a user successfully signs in.

That's where session cookie hijacking comes in.

What a Session Cookie Is and Why Attackers Want It

When you sign into a web app, the site needs a way to remember that you've already proved who you are. That's what a session is: a temporary "logged-in" state that saves you from entering your password and MFA code on every click.

Kaspersky explains that session hijacking is "sometimes called cookie hijacking" because cookies are commonly used to store the session identifier that keeps you authenticated.

Proofpoint describes session tokens as digital "keys" that let a user stay authenticated. It warns that stealing valid tokens lets attackers impersonate legitimate users and potentially bypass authentication measures "like MFA." That's why session cookie hijacking is so highly leveraged.

If an attacker can steal the cookie or token that represents your active session, they're not trying to defeat the login process. They're attempting to reuse what you already completed and access the same apps and data as if they were sitting at your keyboard.

How Session Cookie Hijacking Actually Happens

- AiTM phishing – Adversary-in-the-middle (AiTM) phishing is the "proxy login" trap. You think you're signing into a normal service, but you're actually signing into a lookalike page that sits between you and the real site. The attacker relays the login in real time, so everything appears to work, including MFA.
- Browser-in-the-Middle session stealing. It's similar in spirit, but it's even more "hands- on" from the attacker's side. Instead of stealing a password and running away, the attacker effectively places themselves in control of the browsing session.
- Cookie theft from the endpoint. Not every session hijack starts with a fancy proxy. Sometimes the attacker simply steals session data from the device itself, allowing attackers to impersonate legitimate users.

MFA is a Baseline, not a Finish Line

MFA is still essential. It blocks a huge amount of credential theft and makes basic account takeover harder. But session cookie hijacking is a reminder that attackers don't always try to defeat the login step. Sometimes they reuse what happens after it.

The practical response is layered and realistic. When those controls work together, MFA stops being a checkbox and becomes a strong baseline backed by protections around the session itself.

NETGEAR NIGHTHAWK M7 PRO

NETGEAR NighthawkM7 Pro is a premium 5G mobile hotspot that delivers fast internet on the go and shares it via WiFi 7 for laptops, phones, and other devices.

It supports up to 64 connections and includes a 2.5GB Ethernet port plus USB-C tethering for more reliable performance.

With a touchscreen and removable battery, it's built for travel, client work, or backup internet when your main connection fails.

THE "BACKUP EXIT" STRATEGY: CAN YOU MOVE YOUR DATA WITHOUT THE VENDOR'S HELP?

Signing up for a SaaS platform is usually the easy part. A few clicks, a credit card, and you're in. The first real test of a SaaS relationship isn't onboarding. It's the exit.

For many small businesses, the front door is wide open, but the emergency exit is bolted shut.

Your business data isn't sitting in one system. It's spread across platforms, integrations, plug-ins, and automation. When one vendor changes pricing, terms, features, or risk profile, you don't just "switch tools." You either move your data cleanly, or you stay stuck.

This is where a backup exit strategy matters. It's a pre-planned method for extracting and migrating your data without relying on vendor hand-holding, surprise costs, or emergency timelines.

The Financial Cost of the "Proprietary Trap"

A weak exit plan doesn't just slow innovation. It quietly increases operating costs because you end up paying for a setup you can't easily change.

When you're locked into a vendor, spending becomes sticky. You can't right-size quickly, consolidate tools, or move workloads to a better-fit platform without turning it into a major project. That's how waste hangs around.

The real cost isn't the monthly invoice. It's the lack of options. When your data can't move easily, every renewal, pricing change, or product shift becomes a forced decision instead of a strategic one.

A true backup exit strategy flips that dynamic. It gives you the ability to migrate on your timeline, reduce duplicate tooling, and make cost decisions based on value rather than inertia. In practical terms, it turns "we can't leave" into "we can compare, choose, and move when it makes sense."

Securing the Move

Once you decide to move your data, the migration itself becomes a high-risk moment. Not because migrations are inherently unsafe, but because they concentrate exactly what attackers want:

- High-privilege access
- Lots of open sessions,
- A lot of data moving at once

During a data move, your team is often signed into multiple admin-level tools at the same time. An attacker doesn't need to "crack" your password if they can steal the session token that proves you're already authenticated.

Cloudflare notes that attackers are finding ways to circumvent MFA as part of broader attack chains, which is why the safest approach is layered rather than relying on one control.

To protect your backup exit migration:

- Use phishing-resistant sign-ins where possible.
- Tighten session controls so privileged sessions expire sooner and re-authentication is required for risky actions.
- Treat device health as part of access: run the migration from a managed, patched, protected device.
- Monitor for suspicious access during the move.

Contact us and we'll help you identify portability gaps and create a practical exit plan you can actually execute.

MICRO-SAAS VETTING: THE 5-MINUTE SECURITY CHECK FOR BROWSER ADD-ONS

Browser add-ons have a funny reputation. They feel "small." A quick install. A tiny productivity boost. But in practice, a browser extension is like a micro-vendor sitting inside your browser session. It can see what you see, interact with the pages you open, and sometimes access the same cloud apps your business runs all day.

That's why a five-minute check matters. Not because every extension is bad, but because it only takes one over-permissioned add-on-or one bad update-to turn "helpful" into exposure.

Why Browser Extensions Are a High-Leverage Risk

Browser extensions sit in the most sensitive place in modern work: the tab where your staff live all day.

That matters because extensions aren't just "apps". They're granted special authorizations inside the browser which makes them attractive targets that's disproportionate to how "small" they feel.

When an extension can read and modify what happens in the browser, it can potentially see data in cloud tools, capture what's typed into forms, or alter content on a page.

The 5-Minute Extension Check

1. Vet the developer like a real vendor. If you can't clearly tell who built it and how to contact them, don't install it on a work browser.

2. Read the description like a contract. If it's vague about what it does or what data it touches, treat that as a red flag.

3. Permission sanity check. Broad "read and change data on all websites" access is rarely justified for a simple productivity tool.

4. Watch for permission creep. If an extension suddenly asks for new permissions, pause.

5. Decide: approve, avoid, or escalate. Approve clear, least-privilege tools. Avoid vague and over-permissioned ones. Escalate anything touching sensitive systems.

QUICK RED FLAGS FOR FAKE RECRUITMENT SCAMS

LinkedIn recruitment scams don't succeed because staff are careless. They succeed because the outreach looks normal, the process feels familiar. Use this checklist as a quick pause button before engaging, clicking, or moving the conversation forward.

- Vague job description, unclear role details, or "we'll share specifics later."
- Pressure to move fast: "limited slots," "complete today," "fast-track hiring."
- Push to move off LinkedIn quickly onto WhatsApp/ Telegram/personal email.
- Requests for money, fees, gift cards, crypto, or "equipment purchases."
- Requests for verification codes.
- Requests for sensitive personal info early, like ID scans or bank details.
- Any request for non-public company information (org charts, client lists, internal tools).

THE "LEGACY DEBT" AUDIT: THE OLDEST RISKS TO FIND FIRST

Legacy debt doesn't show up as a single big failure. It shows up as "small, normal" exceptions that stack up until something breaks at the worst possible time.

Here are your first steps to identify the highest-leverage legacy risks:

1. End-of-support edge devices:
Old firewalls, routers, VPN gateways, and exposed management interfaces.

2. Obsolete products:
Anything past support that can't receive security updates.

3. Servers with drifted basics:
Delayed patching, unnecessary services, weak admin controls, untested backups.

4. Quick move:
Start with internet- facing devices. Replace what's unsupported and isolate what you can't replace yet

"CLEAN DESK" 2.0: HOME OFFICE SECURITY DEFAULTS THAT PREVENT REAL INCIDENTS

A modern "clean desk" is about stopping physical-to-digital shortcuts to secure your home office tech.

Use these defaults as a baseline:

- Lock the screen every time you step away with a short auto-lock timer as well as a manual lock habit.
- Don't share work devices with family or guests.
- Store laptops like they're valuable.
- Keep home routers supported and patched.
- Replace the end-of-support gear.
- Use strong sign-ins and MFA everywhere.
- Keep browsers and extensions controlled.
- Patch laptops quickly and restart when prompted.
- Use device protection on endpoints.
- Treat AI automation like a power tool with approvals for payments, exports, and account changes.
- Make reporting easy for suspicious messages, weird sign-ins, or unexpected prompts.

In 2026, the home workspace isn't a side setup. It's part of your business perimeter.

TUNE INTO "THIS WEEK IN TECH" WITH JUSTIN SHURLEY!