JUNE 2026

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

WHY HUMAN HABITS ARE YOUR BIGGEST SECURITY RISK

Most cyberattacks do not start with a sophisticated intrusion. They start with a click on a personal email, a reused password, or a file uploaded to a familiar cloud service because the approved option felt slower.

The Verizon Data Breach Investigations Report found that 68% of breaches involve the human element.

Not a zero-day exploit. Not a brute-force attack on a hardened system. Human behavior, in the course of an ordinary working day.

For businesses running cloud-based workflows across multiple devices, the personal and professional overlap is now the rule. Understanding where that overlap creates risk is no longer optional. It is a core part of modern security strategy.

How Personal Web Habits Create Business Exposure

Personal channels are phishing's preferred territory. Personal inboxes, messaging platforms, and social media feeds are where phishing thrives.

These environments are harder to filter, easier to spoof, and loaded with the emotional triggers that make people act before they think.

When those channels share a device or browser with business systems, a single click can cross the boundary instantly.

Phishing is the most common entry method for attackers precisely because it exploits distraction rather than technical weakness. The target does not need to be careless. They just need to be busy.

Password reuse is one of the most direct connections between personal and professional exposure.

When credentials from a personal account are compromised, attackers run them against business systems automatically. This technique, credential stuffing, is low-effort and highly effective because so many people use the same password across multiple accounts.

Unique credentials for every account, combined with multi-factor authentication, break that chain.

A personal breach has nowhere to go when the work account requires a second factor that the attacker cannot relay.

Why Blocking Behavior Doesn't Work

The instinct is to lock things down: block personal apps, restrict browsing, enforce strict device policies.

In practice, blanket restrictions rarely stop the behavior. They relocate it. Users find workarounds. Unapproved tools move to personal devices. IT teams lose visibility into exactly the activity they were trying to manage.

The risk does not disappear. It moves somewhere harder to see.

Security strategies that assume perfect compliance perform poorly in real workplaces. The goal is not eliminating the overlap between personal and professional digital activity. It is managing it without breaking how people work.

What Actually Reduces Risk

The controls that work are the ones that match how people actually operate.

- **Separate contexts, not people.**
The simplest way to reduce crossover risk is to reduce crossover. Separate browser profiles for work and personal activity, clear guidance on where business accounts should be accessed, and identity boundaries that prevent accidental mixing all reduce exposure without restricting what people do with their time.

- **Design for credential failure.**
Assume passwords will eventually be exposed somewhere. Design for that outcome rather than hoping to prevent it. CISA reports that enabling multi-factor authentication makes accounts 99% less likely to be compromised, even when the underlying password has already been stolen.

Make secure behavior easier than unsafe behavior

Contact us or schedule a consultation to review current controls and identify where the most important gaps are.

BEELINK EQR7

Beelink EQR5 is a compact mini PC that delivers strong everyday performance for work, media, and light productivity tasks at home or in the office.

Powered by an AMD Ryzen processor,it supports smooth multitasking and connects easily to displays,peripherals, and network storage.

With 2.5GbE Ethernet, Wi-Fi 6, and a space-saving design, it's ideal for desks or always-on computing without the bulk of a full desktop.

ADVERSARY-IN-THE-MIDDLE ATTACKS: HOW PHISHING SITES STEAL YOUR ACTIVE LOGIN

You click a link, sign in, approve the MFA prompt, and get on with your day, completely unaware that someone else just logged into your account at the same moment.

That scenario surprises many businesses, particularly those that rely on multi-factor authentication (MFA) to protect cloud accounts. But this is exactly how Adversary-in-the-Middle (AiTM) phishing attacks work. Rather than stealing passwords for later use, these attacks silently hijack an already-authenticated session in real time.

MFA remains a core control, and getting it implemented correctly is still a critical first step for any business.

But AiTM attacks exploit something MFA was never designed to protect: the trusted session that exists after authentication has already completed.

How AiTM Attacks Actually Work

An AiTM phishing site is not a basic replica of a login page. It is a live reverse proxy. The attacker's infrastructure sits between the user and the real authentication service. Every keystroke, redirect, and server response flow through the attacker's system in real time. From the user's perspective, nothing looks wrong.

The page behaves exactly like the real service, with correct branding, working redirects, and a functioning MFA prompt. In most cases, the only clue is a slightly altered URL that goes unnoticed on a mobile screen or when someone is under time pressure.

Session cookies

Session tokens act as bearer credentials. So, whoever possesses the token can access the account, with no password or MFA challenge required.

Once the cookie is stolen, the attacker imports it into their browser and immediately resumes the session. The attacker does not need to log in. They pick up where the legitimate user left off, inside a fully trusted, already-verified session.

What Happens After a Session is Stolen

The aftermath of an AiTM attack tends to be quiet, which is what makes it dangerous.

The attacker is operating inside a legitimate, authenticated session. There are no failed MFA attempts, no unusual login alerts, and nothing in standard sign-in logs to signal a problem.

Research from Proofpoint shows that attackers who gain access through session hijacking commonly create hidden inbox rules to redirect mail, register additional MFA methods to lock in persistent access, monitor email threads for financial conversations, and use the trusted account to launch phishing campaigns against internal colleagues or finance teams.

These follow-on actions are a key reason AiTM attacks are frequently uncovered late, after financial fraud, data exposure, or wider network compromise has already begun.

Stop Protecting Just the Login Screen

Want to review your identity security controls?

Contact us or schedule a consultation to identify the gaps that matter most before an incident does it for you.

HOW "JUST-IN-TIME" ELEVATION HELPS YOUR TEAM HAVE THE SYSTEM CONTROLS THEY NEED

Local administrator rights (the ability to install software, modify system settings, and override security controls) are given to end users far more often than they should. The usual reason is efficiency.

But the practical effect of this often is the opposite: machines that drift from baseline, infections that spread before they are caught, and remediation tickets nobody planned for.

Revoking local admin rights directly removes the root cause of most of those issues.

But I Need to Install Things

The concern about restrictions is legitimate. Users on your network occasionally do need elevated access for specific tasks.

The answer is not to restore permanent admin rights. It is just-in- time (JIT) elevation, where you get temporary elevated access for a defined task. The request is approved through an automated policy or by IT, and the elevation expires automatically once the task is complete.

This keeps users productive and IT informed.

Every elevation request is logged. Unapproved actions do not happen silently. The volume and pattern of requests also become useful data in its own right, revealing exactly which tasks genuinely require escalation and which ones users were performing only because nothing was stopping them.

What Standard Users Can Already Do

Standard accounts support normal application use, browser activity, printing, file access, and the vast majority of day-to-day tasks without any escalation at all.

The friction you may anticipate is usually larger than the friction you actually experience once the change is made and a robust JIT process handles the edge cases.

PROTECTING ACCOUNTS PAYABLE FROM AI FRAUD

Use these tips to strengthen your Accounts Payable (AP) defenses against sophisticated impersonation attacks.

1.Implement Out-of-Band Verification:
Always confirm requests to change bank details or approve urgent payments through a secondary, independent channel.

2.Don't Rely on "The Look":
Assume that a convincing appearance alone is no longer proof of a legitimate request.

3.Be Wary of Voice Cloning:
Require secondary verification for any verbal payment approval.

4.Standardize Verification Habits:
Create a culture where staff feel safe pausing high-risk actions to verify details.

5.Use Layered Access Controls:
Enforce MFA and restrict access to financial systems.

THE PASSKEY MIGRATION CHECKLIST

Transitioning to a passwordless environment doesn't have to happen overnight. Use this checklist to guide your team through a secure and efficient passkey migration.

- **Audit Your Platform Support:** Identify which of your current tools already support passkeys natively.
- **Prioritize High-Risk Users:** Begin your rollout with administrators and power users.
- **Implement a Parallel Authentication Phase:** Allow users to authenticate with passkeys on enrolled devices while keeping passwords as fallback.
- **Bridge Gaps with Password Managers:** For tools that do not yet support passkeys, utilize a password manager.
- **Establish Recovery & Sync Protocols:** Ensure users understand how passkeys sync across their ecosystem (such as iCloud Keychain or Google Password Manager).

SAAS OFFBOARDING: 10 TIPS FOR ELIMINATING "ZOMBIE" ACCOUNTS

Use these 10 tips to conduct a thorough "Zombie" SaaS audit and protect your sensitive data.

- Start your search by pulling a comprehensive list of all SaaS applications connected to your primary identity providers.
- Cross-reference your known inventory with billing records, browser extension installs, and email domains.
- Audit your HR exit records from the past year and check every name against your SaaS inventory.
- Ensure you revoke folder access set to "anyone with the link".
- Check team-provisioned platforms like Salesforce, Asana, and Notion.
- Look for smaller applications employees may have used, such as AI writing assistants, survey platforms, or data visualization tools.
- Replace shared team logins with individual accounts whenever a platform allow sit to ensure a clean audit trail.
- For each identified application, check the admin console to see who is currently active and when they last logged in.
- Establish a quarterly review cadence.
- For all remaining active accounts, ensure MFA is strictly enforced.

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