



Hidden Threats Leave Digital Footprints

Imagine you're hiking a quiet trail early in the morning. No wind, just the crunch of your boots. Suddenly, you spot a set of deep, fresh tracks crossing the path ahead. They're not fresh enough to make you panic, but they're too fresh to ignore. Do you keep strolling blindly, or do you take a closer look?

Welcome back to our journey through the digital wilderness. As we head into **Cybersecurity Awareness Month** this October, it's the perfect time to talk about tracking, because in your business' IT environment, the biggest threats don't crash through the trees making a ton of noise. They move silently, and they leave footprints.

Not Every Threat Sets Off an Alarm

Most northern New Jersey businesses already have the basics in place—think of firewalls and antivirus as your digital shelter and bug spray. That stuff is essential. But modern cybercriminals aren't smash-and-grab burglars; they act like experienced poachers. They move slowly, blend in with the day-to-day, use stolen credentials, and completely bypass standard alarms. That means something could be hanging out in your network right now without triggering a single warning.

What "Tracks" Look Like in Your IT Environment

In the woods, a single dent in the mud might be nothing. A line of them? That's another story. In your business, digital tracks look like a staff member logging in at 3:00a.m., someone accessing files they've never looked at before, or random chunks of data trickling out to an unfamiliar country. On their own, these glitches don't scream "emergency!" But when you connect the dots, they point to a problem you want to solve before it solves you.

Knowing What's Native to Your Woods

Smart hikers know the difference between a harmless deer track and a bear print. Your business needs that exact same awareness. You and your IT team must have a clear picture of what "normal" looks like. Who is supposed to be logging in? Which apps actually belong? Once you

Continued on page 2



October is Cybersecurity Awareness Month!

Strong cybersecurity isn't a one-and-done checkbox. It's an ongoing practice—staying vigilant with updates, smart habits, training, and proactive monitoring. The threats never stop evolving, so neither should your defenses.

IT Radix is here to help keep your business protected all year long. Let's make security a habit, not a hassle! Need help? Give us a call.

Did You Know...

WOW Service is how we turn "good enough" into "how did IT Radix do that?!" It means faster fixes, crystal-clear communication, and reliability you can count on every time. We sweat the small stuff—so you don't have to—creating standout experiences that grow into lasting, trusted partnerships.



Animal Tracks in Network

Continued from page 1

map out your everyday environment, the strange stuff sticks out like a sore thumb. Without that blueprint, everything just blends into the background noise.

Catch the Signs Early

Cyberattacks usually start with quiet scouting, not a massive crash. The longer a threat goes unnoticed, the more damage it does. Catching those early footprints keeps your business safe, keeps your data secure, and saves you an absolute fortune in emergency recovery costs.

That's exactly why IT Radix recommends a step back to examine what's happening across your network—not just what triggers alarms, but what quietly slips by unnoticed. If something were quietly moving through your network today, would you even know?

Connect with IT Radix for a security check, and let's read the tracks before they turn into trouble.

Proudly folded & sealed by Montgomery Academy

The Smart Way to Use AI



AI tools can save your team time, but they work best when you set clear boundaries. Think of AI as a helpful new intern: it can handle routine tasks, but it still needs guidance and review.

Start with a few practical uses. AI can summarize long email threads and draft replies, turn meeting notes into action lists, and help organize reports by highlighting trends or unusual activity. These tools can make a busy day more manageable, but they should support your team, not replace good judgment.

Keep Sensitive Data Out of AI

Do not paste sensitive information into public AI tools. Customer data, employee information, passwords, financial details, and confidential documents should stay out of prompts. Assume data sent to an AI tool lives forever and act accordingly. It is also important to create an approved list of AI tools so employees know what is safe to use.

Before any AI-generated content is shared with a client, posted online, or used to make a business decision, a person should review it carefully. AI drafts...humans decide.

You do not need a massive AI overhaul to get started. Choose one or two time-consuming tasks, put the right guardrails in place, and expand slowly as your team learns what works without creating unnecessary risks or headaches.

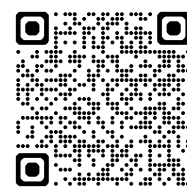
Not sure where to begin? Contact IT Radix today. We are happy to help your business use AI safely and productively every day.

What's lurking in your Microsoft 365 Account? Our free Microsoft 365 Cybersecurity Audit will identify if you are exposed.



At no cost or obligation, our highly skilled team of IT pros will conduct a Microsoft 365 Cybersecurity Audit to uncover any hidden risks.

Once completed, we'll prepare a customized report that will identify specific vulnerabilities and provide an action plan for getting them addressed fast.



www.it-radix.com/cs-audit

SPECIAL OFFER: Microsoft 365 Cybersecurity Audit (expires 11/30/26)

Four Simple Ways to be Safer Online



Cybersecurity can feel overwhelming, but protecting yourself online does not have to be complicated. A few practical habits can make a real difference and help reduce your risk of common scams and online threats.

Here are four simple ways to improve your online safety:

1. **Use strong, unique passwords.** Using the same password for multiple accounts is like using one key for every door. If one account is compromised, the others may be at risk too. Create a different password for each account and consider using a password manager.
2. **Pause before you click.** Scammers often create a sense of urgency with messages claiming your account is locked or immediate action is required. Taking a few seconds to stop, look closely, and verify the message can help you avoid a costly mistake.
3. **Review app permissions.** Not every app needs access to your location, contacts, microphone, or camera. Limiting access reduces your digital footprint and your risk.
4. **Freeze your credit.** A credit freeze can make it much harder for someone to open a new account in your name if your personal information is stolen.

These habits can also help protect you when using public Wi-Fi, payment apps, or shared devices.

ONE More Thing...

The above are smart ways to stay safe. But staying ahead of every evolving and more sophisticated cyberthreat requires more, and it's a challenge to keep up. Partnering with an experienced Managed Services Provider like IT Radix gives you and your business access to dedicated cybersecurity experts. This means you can focus on growing your business while knowing your digital assets are protected by industry-leading security practices.

Navigating the ever-changing cybersecurity landscape doesn't have to be overwhelming when you have a trusted partner like IT Radix guiding the way!

Is It REALLY You?

Continued from page 4



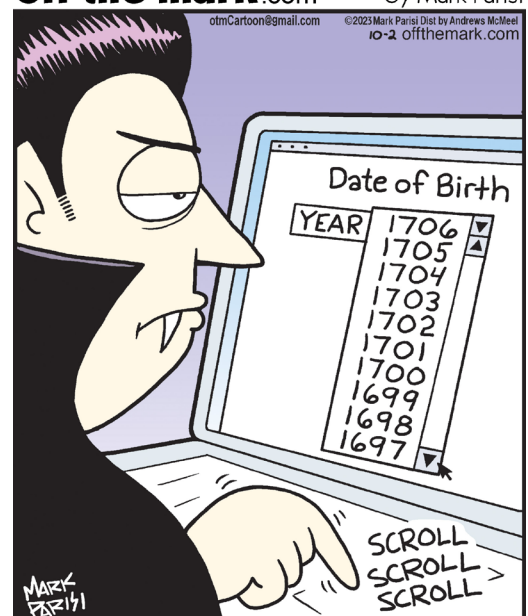
This October—**Cybersecurity Awareness Month**—is a great time to tighten things up before your identity starts making decisions without you.

Here are a few simple ways to stay ahead:

- Use strong, unique passwords and change them regularly
- Turn on Multi-Factor Authentication wherever possible
- Review accounts, systems, and apps access regularly
- Pay attention to unusual alerts or activity
- Confirm urgent requests face to face or by calling a known phone number

A few good habits can stop a lot of strange problems before they start. Contact IT Radix today to help make sure your team's accounts, access, and security settings are buttoned up.

off the mark.com by Mark Parisi



In This Issue

- If something were quietly moving through your network today, would you even know?
- How to safeguard your business while using AI
- 5 Simple ways to be safer online

October 2026



Reid's Rules...

Woof! I've been keeping watch, and I've noticed some humans still use the same password everywhere.

That's like leaving the doghouse door wide open and hoping no one wanders in!

Here's how I protect the pack:

- 🐾 Use one strong master password that only you know.
- 🐾 Give every website its own unique password. (Think of it as leaving a different scent trail at every stop.)
- 🐾 Let a password manager do the fetching and remembering for you.

A good password manager keeps your logins locked up tight, autofills them safely, and saves you from chasing your tail trying to remember them all.

IT Radix Family and Friends
321 Delighted Clients Drive
Geekville, NJ USA

Is It REALLY You?

Imagine opening your email and seeing... **your own obituary!**

The Good News: You are still very much alive.

The Bad News: Your identity, bank account, and online accounts may have just entered the danger zone.

Welcome to the weird world of identity theft, where things can get ridiculous and stressful fast. Cybercriminals are very good at pretending to be someone else, including you. Suddenly, everyday people are getting bills for medical procedures they never had, alerts for logins they never attempted, or messages about "urgent" gift card requests they definitely did not send.

These situations may sound extreme, but they happen more often than you think. They usually start small: one breached website, one reused password, one suspicious login, or one "I'll review that later" moment. Bit by bit, someone can piece together enough information to cause real trouble.

Continued on page 3