April 2026

IT Radix Resource

large enough to *deliver*
small enough to *care*

Don't Let Your Data Get Muddy

As we trudge forward this spring on our journey through New Jersey's digital wilderness, we know that April's unpredictable weather is the price we pay for a lush, green landscape. While "April showers bring May flowers," for New Jersey businesses, the influx of spring activity can also bring a flood of "muddy" data into your systems on top of some of the muck that might have accumulated over the years.

Think of your company's network like a mountain stream: it's the lifeblood of your operation but, without proper filtration, can quickly become contaminated. Your data can include numerous duplicates, outdated records, and even hidden or forgotten security vulnerabilities. Just as a hiker uses a purification tablet to ensure their water is safe to drink, you need a data hygiene strategy to ensure the information driving your decisions is clear. By cleaning now, you aren't just tidying up, you're planting the seeds for a season of healthy, sustainable growth.

Here are steps you can take to "purify" your digital data.

- **Hunt for and remove duplicate files and file names**. They function as silt slowing down the flow of information.
- **Review your contacts in your email client and your customer management system**. Remove duplicates as well as inclusions that are no longer important to you.
- **Remove old files and folders before a certain date**. Move them all into an archive so that you can access them if necessary. If not, they just sit there, making your surface open to cyberattack even bigger.
- **Physically clean your server room including all equipment**. Too much dust can lead to overheating and breakdowns.
- **Update all patches**. This is an ongoing recommendation, but especially important as part of a larger network "cleanse."
- **Examine access control to key data**. Ensure that only the right people have the keys to the well.

Continued on page 3

Take Note

Go Green with IT Radix and Free Electronics Recycling

Drop off your e-waste at our IT Radix office during the month of April between 10am-4pm. Acceptable items here: www.it-radix.com/recycling

Over the years, our April recycling event has kept 20+ tons of e-waste out of landfills—and recycled properly. Let's make 2026 our biggest collection yet—join us and help keep yesterday's tech out of the trash.

Did You Know...

We strive to make a positive difference for our clients, staff and community every day. Positive actions create meaningful change. In April we make a difference by helping our clients recycle e-waste. Look at the *Take Note* box above for more information on how you can help us change things for the better.

IT Radix Resource large enough to *deliver* small enough to *care*

Talk Nerdy to Me

Recover Closed Tabs

While in your browser, restore your most recently closed tab by pressing:
Ctrl + Shift + T
Hit it again to reopen earlier tabs in the order they were closed.

IT Radix

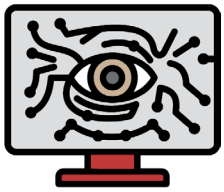
Recover Closed Tabs (Like Magic)

Ever close the wrong browser tab (or lose them all after a crash)? No worries—you can bring them back in seconds.

In your browser, press Ctrl + Shift + T to restore your most recently closed tab. Hit it again (and again) to reopen earlier tabs in the order they were closed.

Consider it your quick "undo" button for the web.

Is Your Business Training AI to Hack You?



There's a lot of excitement about artificial intelligence (AI) right now, and for good reason. Tools like ChatGPT, Google Gemini, and Microsoft Copilot are popping up everywhere. Businesses are using them to create content, respond to customers, write emails, summarize meetings, and even assist with coding or spreadsheets.

AI can be a huge time-saver and productivity booster. But, like any powerful tool, if misused, it can open the door to serious problems—especially when it comes to your company's data security. Even small businesses are at risk.

Here's The Problem

The issue isn't the technology itself. It's how people are using it. When employees copy and paste sensitive data into public AI tools, that information may be stored, analyzed, or even used to train future models. That means confidential or regulated data could be exposed, without anyone realizing it.

In 2023, engineers at Samsung accidentally leaked internal source code into ChatGPT. It became such a significant privacy issue that the company banned the use of public AI tools altogether, as reported by Tom's Hardware. Picture the same thing happening in your office. An employee pastes client financials or medical data into ChatGPT to "get help summarizing," not knowing the risks. In seconds, private information is exposed.

AI Risks Are Rising. Are You Ready?

AI tools are changing the way we work—but they can also open the door to new risks. To help you stay protected, IT Radix is offering a **Free Microsoft AI Security Assessment** for a limited time.

We'll take a quick look at how AI is being used in your business and point out where hidden vulnerabilities may be putting your data or reputation at risk. No jargon, no pressure—just practical insights to keep you secure. Don't wait until it's too late.

SPECIAL OFFER: Free Microsoft AI Security Assessment (Expires 5/31/26)

www.it-radix.com/ai-security

A New Threat: Prompt Injection

Beyond accidental leaks, hackers are now exploiting a more sophisticated technique called prompt injection. They hide malicious instructions inside emails, transcripts, PDFs, or even YouTube captions. When an AI tool is asked to process that content, it can be tricked into giving up sensitive data or doing something it shouldn't. In short, the AI helps the attacker—without you knowing it's being manipulated.

Why Small Businesses Are Vulnerable

Most small businesses aren't monitoring AI use internally. Employees adopt new tools on their own, often with good intentions but without clear guidance. Many assume AI tools are just smarter versions of Google. They don't realize that what they paste could be stored permanently or seen by someone else. And few companies have policies in place to manage AI usage or to train employees on what's safe to share.

What You Can Do Right Now

You don't need to ban AI from your business, but you do need to take control. Here are four steps to get started:

1. Create an AI usage policy. Define which tools are approved, what types of data should never be shared, and who to go to with questions.
2. Educate your team. Help your staff understand the risks of using public AI tools and how threats like prompt injection work.
3. Use secure platforms. Encourage employees to stick with business-grade tools like Microsoft Copilot, which offer more control over data privacy and compliance.
4. Monitor AI use. Track which tools are being used and consider blocking public AI platforms on company devices if needed.

The Bottom Line

AI is here to stay. Businesses that learn how to use it safely will benefit, but those that ignore the risks are asking for trouble. A few careless keystrokes can expose your business to hackers, compliance violations, or worse.

IT Radix is here to help you avoid AI pitfalls.

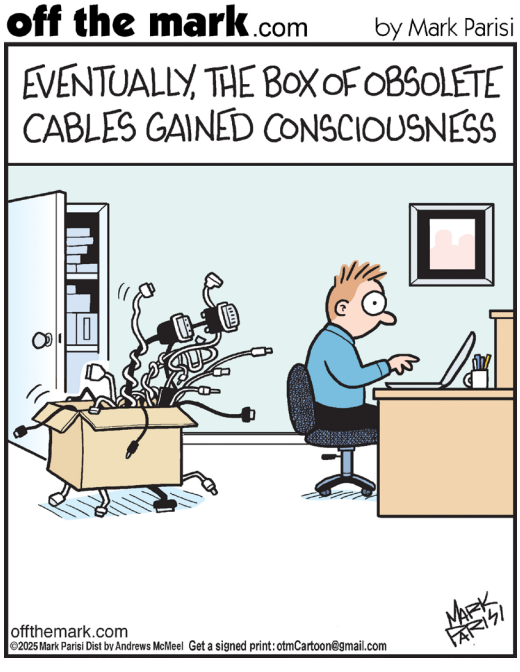
Don't Let Data Get Muddy

Continued from page 1

Purifying things leads to data integrity (clear water), cybersecurity (less attractive to parasites), and compliance (leaving no trace).

Just as April's rains prepare the soil for a vibrant May, a rigorous commitment to data hygiene clears the path for success. By treating your network with the same care a hiker gives to a freshwater source, you ensure that every decision—from local marketing to financial forecasting—is built on a foundation of purity and precision.

Don't let "muddy" data drown your potential. Let IT Radix help you clean now so you can truly bloom tomorrow.



IT Radix
large enough to *deliver*
small enough to *care*
49 S. Jefferson Road
Whippany, NJ 07981

In This Issue

April 2026

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

Reid's Rules...

It's time to clean out Reid's doghouse...

As April kicks off—prime season for fresh starts and longer walks—it's a great time to give your IT network a quick "spring grooming." Take a moment to review what's outdated or under performing and schedule a routine network health check. A little cleanup now keeps your systems running as smoothly as a well trained pup on a leash.

Reid's rule of paw: if it's old, noisy, or slowing everyone down, it's probably time to tidy it up—or replace it. Clear out unused accounts, remove old software, and make sure updates are current. Like a clean doghouse, a healthy network is safer, calmer, and built to last. Now *that's* something to bark about!

Don't Let Your Checks Get Cooked

Check fraud is on the rise—even as fewer people use paper checks. In fact, the Associated Press reported that check fraud incidents increased by 11% in 2025 compared to the prior year, despite a 7% drop in checks overall.

So, what's happening? Criminals aren't just stealing checks from mailboxes anymore. A growing tactic is "**check cooking**," where a thief snaps a photo of a check, then uses easy, off-the-shelf tools to alter the payee and amount. From there, they can deposit a counterfeit version through a mobile banking app—or even sell the stolen check details online.

How to protect yourself: Use credit cards or digital payments whenever you can. If you must send a paper check, avoid leaving it in your mailbox. Drop it directly at the post office (or inside a secure mail slot). Better yet, if the business is local, pay in person at the register.

