

When Tech Sparks Catch Fire

Technology Advancements Fuel Changes

One small creative spark can turn a new idea into something that dramatically changes how we all do business. For small businesses in New Jersey, the last few years have been full of developments that have dramatically altered how each of them uses technology.

The Cloud Lit Up the Business World

Remember when working from anywhere was rare? Then came cloud applications, Microsoft Teams, SharePoint, and other cloud tools—and suddenly remote work lit up the business world in an instant. Collaboration ignited, making teamwork easier and more affordable than ever.

Zero Became the Safest Word in IT

IT Security has long been built on putting up walls and strictures that impede access. That strategy worked well for decades. Only recently, though, did that get flipped on its head and the idea of Zero Trust emerged. With Zero Trust, every user must prove that they and their device are safe—every single time. It's like keeping that bucket of water near the fire just in case, because you cannot trust the fire will not spread.

What might be the most important innovation in IT for small businesses over the next few years? The answer is clearly the further growth and expansion of AI.

Aye Aye for AI

Just over the last two years, AI went from an isolated flicker to a blazing bonfire. Only recently have small businesses begun to adopt AI in various forms and use it for customer service, marketing, and automation. It is reducing workloads and downtime, facilitating response times, and sparking innovative ideas. Imagine how the cave dwellers felt when they first saw fire. That is how AI feels to most of us in business today. And the flames of AI are growing!

Continued on page 2



Take Note

March 31 is World Backup Day

... a great reminder to do more than just glance at your daily backup report. Make sure your backups are current—and ask your key vendors (including SaaS providers): how, where, and how often *your* data is backed up. A ransomware attack, deletion, or vendor outage could turn “got you covered” into “sorry, that data is gone.” Backups should be boring...and absolutely reliable.

Did You Know...

Making sound business decisions keeps us cool under pressure and prevents sparks from igniting—ensuring security and stability for our clients. We do this because our clients deserve steady guidance, not rushed reactions.

It protects their time, budget, and peace of mind so they can focus on business growth.



Tech Sparks Catch Fire

Continued from page 1

Generative AI: Generative AI is what most of us are familiar with at this point. It creates content including images, code, and video. It will continue to add new features and benefits—entirely new things unknown to us. It does this by learning and leveraging patterns it learns over time.

Agentic AI: Agentic AI is unfamiliar to most of us, but it takes AI a step further than the current. It doesn't just generate content, it acts autonomously to achieve goals. These systems can make decisions, complete tasks, and even coordinate workflows without constant human input. Think of it as fire that not only burns but moves on its own, reshaping the terrain as it goes. This autonomy means businesses must plan carefully for governance, security, and ethical use. AI will power cybersecurity well beyond its current capabilities. Like wilderness fire management, the successful growth of AI will have to be well regulated and tightly controlled.

Ready to enjoy the heat and avoid the flames? Contact IT Radix today and let's help you keep your business burning bright—not burning out.

Reduce Risks with a Solid Backup Strategy



Heading out on our March journey through the digital wilderness, we are confident because we have a backup plan in case something awry happens. The same applies to your important business and financial data, without a solid backup strategy, you're taking unnecessary risks.

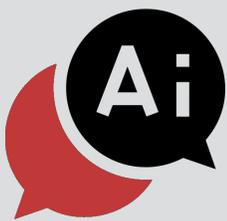
Imagine hiking with only one route mapped out. If that trail closes, you're stuck, journey over. Similarly, if your single backup fails, recovery becomes a horrible nightmare. Redundancy is your safety net—automated backups, regular test restores and multiple backups keep your information secure.

Files on the Cloud Must be Backed Up Too

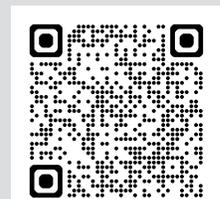
Most people understand and properly backup their personal data locally. Businesses do as well for their local servers on larger storage devices. But backups do not only apply to files stored locally. Cloud computing is now rampant and while it is convenient, it is not foolproof. Lots of people mistakenly think the cloud is a backup—It is not! It is just another file storage location. The key thing to remember is that it is vital for all organizations to have multiple backups in various locations, ideally both local and cloud based.

March 31 is **World Backup Day**, a great reminder to protect your digital life. But don't wait until the end of the month to act. Start today: review your backup plan, ensure cloud files are included, and verify that your system works. Like a well-prepared hiker, you'll be ready for any unexpected detour with these procedures.

Let's Talk About How AI Can Benefit Your Business



Curious how AI could save your team time and boost productivity without adding risk? Book a free, no-pressure conversation with an IT Radix professional and we'll share practical ideas tailored to your business—plus the next best steps if you want to explore further.



www.it-radix.com/ai-talk

SPECIAL OFFER: Complimentary AI Conversation with an IT Radix Professional (expires 4/30/26)

The Four “Cs” of Cybersecurity



As our journey into the digital wilderness continues this month, we set down for the night and prepare a campfire. We need to a) **COLLECT** and gather the wood, b) **CLEAR** the area for safety, c) **CONTAIN** the fire with an adequate boundary, and finally, d) **CARE** and tend to the campfire so it burns safely and steadily—providing safety and security.

Like a successful campfire at the end of a long hike, strong security habits provide warmth and security for your business. Here are Four “Cs” of Cybersecurity to keep your organization safe:

1. Communication

A good campfire starts with gathering everyone together—and so does security. Make it a standing topic in meetings, newsletters, and chats. Encourage employees to share concerns and report suspicious activity. Open dialogue builds awareness and accountability.

2. Compliance

Just as you follow fire safety rules to keep the flames under control, policies keep your business secure. Review and update them regularly. Track training and make compliance a shared responsibility. When everyone plays their part, gaps disappear.

3. Continuity

A campfire is comforting because you know it will last throughout the night. Likewise, continuity planning ensures your business survives the unexpected. Keep backups current, have a recovery plan, and make sure everyone knows what to do when trouble sparks.

4. Culture

Finally, make security part of your DNA—like the tradition of ending a hike around the fire. Celebrate good practices and make them part of everyday operations.

Build these Four “Cs” into your routine, and your business will glow with the steady light of security—like a campfire that turns uncertainty into comfort and confidence. Reach out to IT Radix today for s’more cybersecurity solutions for your business!

Banish IT Snakes



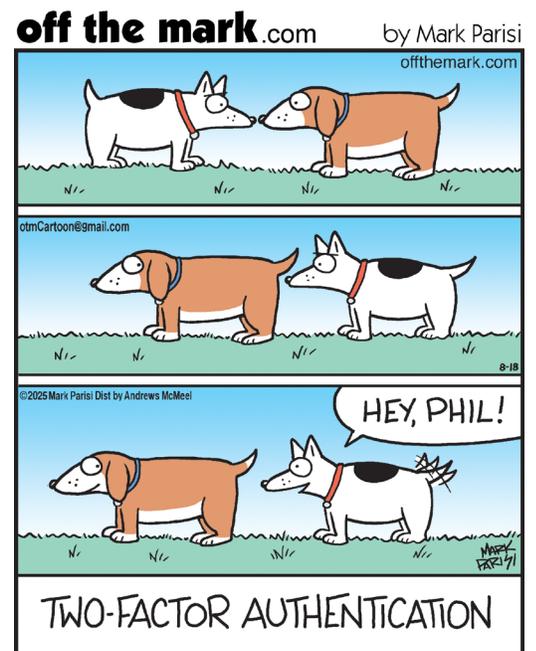
Continued from page 4

apps and tools—lurks in the grass, adding risk and reducing visibility. Meanwhile, **poor backups** can turn a small incident into a full-blown disaster when your safety net isn’t there.

Not all snakes are cybercriminals—some simply choke productivity and create stress. **Slow Wi-Fi** and **network bottlenecks** are sluggish snakes strangling your team’s momentum. **Compliance gaps** can bite too, bringing fines and stress. Finally, a **lack of cybersecurity training** leaves employees unaware of the dangers hiding in plain sight.

Let IT Radix help you chase these snakes out of your network! Schedule your free IT Network Assessment today and keep your business ssssssafe and ssssssecure.

Proudly folded & sealed by Central Park School



In This Issue

- Technology advancements fueling changes for small businesses
- Why backing up your cloud files is important
- Strong security habits every business needs to stay safe

March 2026



Reid's Rules...

Follow Reid's sniff test... if it smells off, don't take a bite!

Phishing emails and malware often look normal, but they're really bait—designed to steal passwords, money, or data. Don't be fooled by promises of "tasty treats" like gift cards, refunds, prizes, or "free upgrades." They're meant to lure you in.

Also beware of the digital version of a long walk or car ride: "Click here to access your account." Watch for urgency, odd wording, strange links, and unexpected attachments.

Verify unusual requests with a known contact and report anything suspicious to IT Radix.

Banish IT Snakes From Your Network — St. Patrick Style!

Legend says St. Patrick drove the snakes out of Ireland. While your office might not have actual serpents in the server room (thankfully), most IT networks have a few "IT snakes" hiding in the tall grass—quietly causing damage and getting ready to strike.

Let's start with the snakes that strike first—and spread fastest. **Viruses and malware** are venomous vipers that slow systems down, steal data, and create chaos. Then there are **phishing emails**—sneaky serpents that slither into inboxes and trick employees into handing over passwords or payments. **Outdated software** and **unpatched systems** are frequently overlooked snakes that leave security holes wide open.

Even a strong network can get nipped when the basics are left unguarded. **Weak passwords** are like leaving the garden gate open. **Shadow IT**—unauthorized

Continued on page 3