



Essential Digital Gear for Your Business Climb

For a New Jersey business owner, sometimes the journey toward success and growth can feel like a long trek that includes an ascent up an unpredictable mountain. Your survival may depend on what you've packed in your backpack before heading out. You need a backpack that protects you without slowing your pace.

Here is what to pack to navigate safely:

The Compass: Managed Identity

In the wilderness, losing your way is the quickest path to disaster. In the digital world, losing your identity—or your passwords—is the equivalent. A business-grade password manager like Keeper is your compass. It ensures that even if you're navigating unfamiliar terrain, your credentials are secure, unique, and encrypted. It prevents the "reused password" trap, which is the most common root on the trail that causes "digital" hikers to stumble.

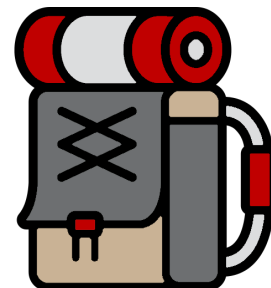
The Multi-Tool: Integrated Platforms

Sometimes as a business manager you must cut through a lot of stuff just to get to the core of what you want to do. You don't want a separate tool for every vine you need to cut. For a small- or medium-sized organization, consolidation is key. Platforms like Microsoft 365 Business Premium function as your Swiss Army knife. By combining your communication (email) and collaboration (SharePoint), document storage, and device management (Intune) into one kit you are set! Adding Microsoft Teams ensures that if a "digital predator" strikes one area, the rest of your kit is ready.

The Mosquito Netting: EDR & ITDR

Some threats don't just hide; they strike aggressively in groups—like mosquitoes after sunset. Phishing links, ransomware, and identity-based attacks are the predators to repel. Endpoint Detection and Response (EDR) and Identity Theft Detection and Response (ITDR) function as your digital sentinel, continuously monitoring endpoints and identities to detect and neutralize threats before they can cause harm. By stopping malicious activity and compromised credentials at the source, you protect your team—even when working on public Wi-Fi.

Continued on page 2



Think IT Through!

Artificial Intelligence (AI) can be a great tool for saving time and working smarter, but it also creates new security risks. Sensitive company information may be exposed when entered into public AI tools. Cybercriminals are also using AI to create more convincing phishing emails.

A little caution goes a long way.
Is your business prepared?
IT Radix is here to help.

Did You Know...

Having fun is part of how we do our best work. We want our client relationships to feel productive, positive, and genuinely enjoyable. Bringing humor, energy, and a light-hearted spirit to each day helps us build stronger connections, solve problems with care, and make success feel even better for everyone involved.



Essential Digital Gear

Continued from page 1

The Emergency Flare: Cloud Backup

Even the most prepared hikers can face a total washout. If ransomware locks your path, you need a way to signal for help and restart. A “set it and forget it” backup solution like Datto is your emergency flare. It ensures that no matter how bad the storm gets, your data is tucked away in a dry, safe cave, ready to be recovered so you can resume the climb.

The summit of business growth is within reach, but the trail is unforgiving. Pack smart, keep your kit light, and ensure every member of your group knows how to use the tools in their pack.

No one wants to discover halfway up the mountain that they packed the wrong gear. If you are not sure whether your business has the right digital backpack essentials in place, IT Radix is here to help. We can help you strengthen security, simplify your tools, and make sure your team is ready for whatever the trail brings. Reach out to us for a conversation about building a smarter, safer pack for the journey ahead.

Happy hiking!

Your Accountant is Stressed. Hackers Know It!



Tax extension deadlines in September and October can bring a second wave of pressure for accountants, bookkeepers, and business owners. Documents are being gathered, questions are flying, and hackers are paying attention too.

Phishing attempts often increase during tax time because cyber-criminals know people are moving quickly. Their messages are not always dramatic or obvious. They are designed to look like everyday business requests at the exact moment people are most likely to scan, assume, and react.

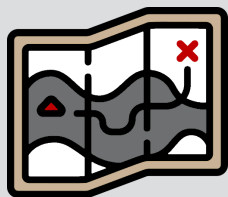
Hackers are not only targeting accounting firms. They are targeting the chaos around them. Clients rush to send sensitive documents. Staff may shortcut normal checks. “Just send me the file” can replace the usual caution. That is exactly the environment scammers love.

These attacks may look like an email from “your accountant” asking you to resend tax documents, a vendor claiming their bank information has changed, a DocuSign request that needs your signature today, or an urgent message from a traveling executive. They feel normal, which is why they work.

The best defense is to slow down when something feels urgent. Verify payment changes by phone using a trusted number. Confirm sensitive requests through a second channel. Remind your team that it is okay to pause, double-check, and ask questions.

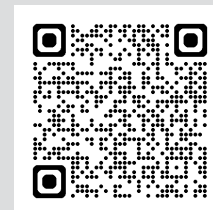
Tax extension deadlines may be stressful, but your security habits do not have to be. As deadlines approach, remind your team to slow down, verify requests, and stay protected. IT Radix is here to help.

Windows Server 2016 EOL ... Time to Hit the Trail



Windows Server 2016 reaches End of Life (EOL) in January 2027. Once that date arrives, security updates and support disappear, leaving your business exposed on a risky stretch of trail.

Let IT Radix help you map the route ahead with a free assessment. We'll review your environment and give you a clear, practical roadmap for what comes next. No pressure. No confusing detours. Just friendly guidance to help you stay ahead of EOL.



www.it-radix.com/server

SPECIAL OFFER: Free Windows Server 2016 Assessment (Expires August 31)



Is That Really Your Kid?

As August rolls around and college students start packing up for campus life, parents have plenty on their minds. Between move-in day, meal plans, and making sure that extra-long twin sheet set actually fits, there is one more thing worth preparing for: scam messages that pretend to come from your child.

One of the most common versions is often called the “Hi Mom/Dad” scam. It usually starts with a text from an unfamiliar number claiming to be your son or daughter. The story sounds urgent but believable. Maybe their phone broke, maybe they are locked out of an account, or maybe they need money right away for an emergency. These scams work because they are designed to trigger a parent’s natural instinct to help first and question later.

That tactic is paying off for criminals. The Federal Tax Commission (FTC) says consumers reported \$15.9 billion in fraud losses in 2025, including more than \$3.5 billion lost to imposter scams, while the FBI reported more than \$20 billion in cybercrime-related losses that same year. The agency also reported that impersonation scams remain one of the most common fraud categories.

The warning signs are often subtle. The text comes from a number you do not recognize. The greeting feels a little off. The writing style does not sound like your child. There may be pressure to act immediately, a suspicious link, or a request to send money to an unfamiliar account. The best first move is simple: pause. Do not rush. Try contacting your child through their usual number, ask a question only they would know, or request a quick video call. The FTC also advises not replying to unexpected texts and not clicking links in those messages.

Scammers can use AI-generated voices to mimic a child on the phone, and a little healthy skepticism can save a lot of stress and money. Consider setting up a family code word for real emergencies before your student heads off to school. And always remember to avoid oversharing on social media and keep personal details private.

At IT Radix, we believe staying safe online starts with staying informed. If you ever have questions about suspicious messages, online scams, or smart ways to protect your family and business, we are here to help.

Screen Time Survival Tips

Continued from page 4

a comfortable 90-degree angle. Your shoulders should feel at ease.

The 60-Second Solo: Every hour, stand up and shake it out. Reach for the sky, touch your toes, or do a quick lap around the room. It resets things and gets the blood moving.

Talk More, Type Less: Give your fingers a break by using voice-to-text for emails or notes. It keeps your hands relaxed and forces you to sit up straight while you speak.

Kill the Blue Light: That screen glow tells your brain it’s high noon. Switch to “Night Mode” early and put the devices away well before bedtime.

Need help making tech work more comfortably for your team? IT Radix is here to keep your systems, and your people, running smoothly.



In This Issue

- Survival essentials for your digital backpack
- What you can do to stay safe from AI-generated identity scams
- Security habits during stressful times

August 2026

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



Reid's Rules...

It's August and the Dog Days of Summer have arrived! I'm flopping on the cool tile with my tongue out like a flag, panting harder than the creaky fan on my old Windows 95 laptop. Gotta stay cool! Turns out your servers and computers hate the heat too—they get sluggish, overheat, and crash right when you need them most.

So, here's my #1 rule for beating the Dog Days: **give your tech some shade!** Clear the dust bunnies from vents, check the server room AC, and make sure nothing's blocking the airflow. While you're at it, update everything and avoid fetching files on random public Wi-Fi (that's just drinking from a muddy puddle). A little summer belly rub (maintenance) now keeps your systems cool and your business running smoothly.

Screen Time Survival Tips

We spend too much time in front of computer screens. Our eyes and necks weren't designed for that. To keep your biological systems from feeling like outdated software, try these simple maintenance tips:



Give Your Eyes a Passport: Every 20 minutes, stare at something 20 feet away for 20 seconds. It's like a mini vacation for your focus muscles preventing "digital fog."

The Conscious Blink: Screens turn us into staring statues. Make a point to blink often; it's nature's way of refreshing eye moisture.

Stack It to the Ceiling: If you're looking down, your neck is working hard. Prop your screen up on a stack of books or a stand until the top of the monitor meets your eye line.

The T-Rex Arm Rule: Keep your keyboard and mouse close enough that your elbows stay at

Continued on page 3