May 2026

IT Radix Resource

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

Campfire Tales from the Digital Dark

Shadows in Your Inbox

Our digital journey continues and we have set the campfire for the night. Gather 'round for some scary stories! See the shadows dance behind the trees? In the woods, we fear noises in the night. But in the office? The real monsters aren't under your desk. They hide in your inbox, disguised as a friend, or worse.

Here are a few real-life campfire stories of digital horror:

The QR Code Curse

In a quiet accounting office, a staffer's eyes lit up. An email arrived: "Congratulations on your bonus! Scan QR code to claim." They pulled out their phone, scanned the code, and BOOM, a hacker used that scan to slip into their email account like a ghost through a wall. Our sensors screamed; we saw a login from a suspicious data center and slammed the door shut, resetting everything before the "ghost" could steal anything. The breach was contained, but the chill remains.

The U-Haul Phantom

Purchasing received an urgent client email. They needed $100,000 in materials delivered immediately to a trailer in a dark parking lot. The helpful staff sent the goods. We found no digital breach. This was a "the call is coming from inside the house" situation: a disgruntled ex-employee using insider knowledge is believed to be the culprit.

The Invisible Impostor

One C-level manager spent six months funding a shadow. The emails looked identical to a known vendor's address. Only much later did they realize that a lowercase "l" was actually a capital "I." The manager sent invoice payments straight into a monster's pocket. No software could stop this, only heightened awareness. It was a psychological trick. By the time the lights came on, the money was long gone.

The Sketchy Meeting

Finally, a manager received a "Teams Meeting" invite from IT. They clicked "Join," but no coworkers were there. Within seconds, their mouse began to

Continued on page 2

Take Note

World Password Day is May 7

...A perfect reminder to give your logins a quick tune-up. Strong, unique passwords help block hackers from sneaking into your accounts. If you've reused passwords (no judgment), now is a great time to change them—and consider a password manager for extra peace of mind. Additionally, consider using Passkeys with systems where they're supported. Call us today to learn more!

Did You Know...

At IT Radix, putting clients first isn't a slogan—it's how we work every day. We get to know each user, listen closely, and stay agile so you get the right solution for your unique situation.

In a world full of automation, we believe authentic human connection still matters most.

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

Campfire Tales

Continued from page 1

move on its own. A hacker had hijacked the session and was taking total control of the machine. We caught the unusual traffic and shouted, "GET OUT!" We remediated the computer just as the hacker was reaching for the files.

The moral of the story? Campfire tales are fun—until your business becomes the next one. If an email feels "off" (odd link, urgent request, tiny typo), step back and verify before you click. Contact IT Radix today for help in identifying the potential shadows in your inbox.

Give Your Passwords a Glow-up!

Updating your passwords doesn't have to be boring—try a fun passphrase like:

GiraffesDance@Dawn!47
<or>
CoffeeBeforeEverything2026!

longer = stronger
more fun = more memorable
regular updates = improved protection

Introducing... Carrie

Carrie comes to IT Radix with nearly two decades of experience in the IT/MSP world. She brings 19 years of hands-on industry knowledge to the table. She has a deep expertise in operations, finance, and client support. Along the way, she became known for keeping the behind-the-scenes details organized, accurate, and moving in the right direction.

In her current role on our Account Management Team, Carrie focuses on what every client appreciates: clear, correct, and transparent billing that matches the services they receive. Billing accuracy and procurement are her specialties, especially when it comes to monthly recurring changes and the complex shifts that can happen over time. She's detail-oriented, process-driven, and steady under pressure—great assets for helping our team stay aligned and our clients feel confident in their invoices. Carrie shares that her favorite part of working at IT Radix is "working with a supportive team of coworkers always willing to step in and help with any question or challenge."

When she's off the clock, Carrie's all about fun! She crafts detailed Comic-Con cosplays, builds Legos, paints, snowboards, bakes, and loves decorating cupcakes! She's also a big live music fan (she's seen Streetlight Manifesto 30+ times), a proud "crazy cat lady," and a delighted "professional aunt" to her friends' kids. She is also working towards her degree in Accounting.

Carrie's personal philosophy centers on empathy, connection, and showing up for people in meaningful ways. She believes in kindness, patience, and making sure the people around her feel supported and valued, whether that's at work, home, or her community.

Carrie's Favorite Quote: "Be the reason someone feels seen."

Let IT Radix Make Password Management Easier (and Safer)!

Keeping track of passwords is harder than ever... and an automated, cloud-based password manager that can be used by all your staff working onsite or remotely is the solution!

IT Radix's Password Management Solution allows you to securely store, generate, and share passwords without sticky notes or spreadsheets.

www.it-radix.com/pword

SPECIAL OFFER: 15% Off Setup Fee for IT Radix's Password Management Solution — New Subscriptions Only (Expires 6/30/26)

Are You Managing Your Vendor Security Risks?

Innovative businesses often reflect on what's gone right and what needs improvement. Managing vendor security risks should not be overlooked. Vendors play an essential role in your business's success, but they also present a severe cybersecurity risk if you don't vet and monitor them effectively, especially if they handle sensitive data.

Many businesses rely on trusted vendors, such as cloud services or file-sharing tools, to carry out day-to-day operations. If that vendor gets hacked, your sensitive data is suddenly exposed.

Vendor breaches are more than annoying—they could also lead to data loss, diminished customer loyalty, or even legal issues. Consider adding these best practices to manage your vendor risk:

1. **Review Vendor Contracts**. Like you, vendors need to be held accountable for following industry-standard practices. Make sure they spell out security basics (encryption, secure storage, incident response protocols) so everyone knows the expectations.
2. **Conduct Vendor Security Audits**. If you haven't done it recently, it's time for a thorough security audit of your high-risk vendors. Make sure they're implementing strong cybersecurity measures, such as multi-factor authentication, encryption, and regular system updates. Knowing where your vendors stand gives you a better handle on your own security.
3. **Monitor For Emerging Risks**. Cyberthreats evolve quickly and so do the risks your vendors face. Regular monitoring of your vendor's security practices, like tracking vulnerabilities or breaches, will keep you on top of any emerging threats.
4. **Update Your Vendor List**. It's time to clean house. Cut ties with vendors who aren't living up to your security standards and tighten your relationship with those who are proactive about protecting your data. Create standardized onboarding and offboarding processes for vendors, so old vendors don't have unwarranted access to your organization.

Vendor risk doesn't have to feel overwhelming. IT Radix can help you vet vendors, strengthen contracts, and stay on top of emerging threats. Let's chat and lock down a simple plan to protect your data.

Why You Should Worry About Vendor Security Risks

- **Legal Liability**. You remain legally and financially responsible for data breaches even if the security failure happened at your vendor.
- **Supply-Chain Attacks**. Hackers use smaller vendors as a "back door" to infiltrate larger, more secure client networks.
- **Access Overload**. Too many admin rights let attackers use stolen vendor credentials to move freely through your systems.
- **Email Fraud**. Scammers compromise vendor accounts to send invoices or payment instructions to steal funds.
- **Dormant Accounts**. Forgotten vendor logins left active after a project ends serve as unmonitored permanent entry points for hackers.

Proudly folded & sealed by Central Park School

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

In This Issue

- Real-life IT security horror stories
- How to avoid vendor breaches
- Meet our newest team member—Carrie!

May 2026

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

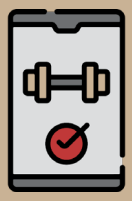
Reid's Rules...

Q: Why was the Office Dog sent to the doghouse?

A: Because he clicked a link in an email promising "Unlimited Tennis Balls & Mailman Schedules—Click Now!" He gave it one enthusiastic click, and now the entire office network has a worse case of "digital fleas" than a stray in the Pine Barrens! It happened because the top dog did not enforce "obedience training" for his staff and a digital fence to catch mistakes.

In Jersey, we don't let strangers over the gate without a bark! To keep your business from chasing its tail after a breach, you need smart humans who have gone through "training" on cybersecurity awareness. Don't let a clumsy paw lead to the doghouse. Security Awareness Training should be the rule of paw!

Are Fitness Apps Tracking YOU?



Fitness apps like Fitbit and Nike Training Club are great for tracking progress—but they can also track YOU! Recent research found that **75% of popular fitness apps analyzed share user data with third parties**, which can include identifiers used for ad tracking and profiling. And it's not just "workout stats"—many apps collect details like location, device IDs, and usage behavior that can paint a pretty clear picture of your routines.

The good news... you have more control than you think. Take two minutes to review the app's permissions and privacy settings. Disable location access unless you truly need it, limit "share with partners" options, and turn off ad tracking where available. Also, double-check any connected accounts (Google/Apple/Facebook) so you're not accidentally oversharing.

A little privacy tune-up keeps your fitness goals on track—without broadcasting your life to advertisers.

