February 2026

IT Radix Resource

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

Cabin Fever is Cozy—Cyber Fever is Costly

We continue our 2026 theme of surviving a journey through the digital wilderness this cold month of February. Our focus is on shelter—your first line of defense against the elements and those nefarious digital predators. Just like a reinforced trail shelter is your safe haven on your route, keeping you and your possessions dry and protected, a strong cybersecurity posture with layers of safeguards, is how you keep your business safe, secure, and protected when threats arise.

Cyberthreats are ubiquitous and more troubling with each passing day. Your staff and your business are threatened whether on the warehouse floor, at the central office, in the cloud, or even at a remote location—home or a vacation cabin nestled in the woods. The savvy management professional puts layers of digital shelters in place that function as the walls, roofs and locks that keep everything secure.

Let's review these key elements of a cybersecurity shelter program:

Sturdy Walls: Often overlooked, strong and complex passwords are vital to your entire security posture. Weak or reused passwords leave your tent door wide open. Your passwords are just like locks on your forest hideaway; make them strong or risk anyone walking right in and raiding your pantry!

Fortifications: Beams, trusses, posts, and studs support a roof. In the same way your business needs multiple layers of cybersecurity support. These include:

- **Firewalls**. Your security gate watching every movement in and out.
- **Endpoint Antivirus Software**. Your motion sensor alerting you if something moves when it should not.
- **Multi-Factor Authentication**. Two forms of ID at the ranger station.
- **Backups**. Your emergency supplies stored at a satellite location in case your main retreat is damaged.
- **Cloud Security Enhancements**. Extra guy lines and stakes to secure you from high winds.
- **Data Encryption**. Your locked safe is inside, ensuring valuables are safe even if someone crosses the threshold.

Continued on page 2

Take Note

Our Team Deserves Your Valentine Love Too!

IT Radix service professionals are sometimes the heroes of your day. They love hearing about when they have swooped in and given you the assist you needed to keep chugging along. Has a team member helped you recently?

Don't keep it a secret! Share a quick "Shout-Out" here:

www.it-radix.com/shout-out

We'll pass your love along.

Did You Know...

Cupid may have his arrow, but even he needs a bow to make the magic happen. At IT Radix, teamwork works the same way. That is why it's a core value. Each member of our staff brings unique strengths, and together, as a team, we create the best solutions for our clients. For us, teamwork isn't just strategy, it's a core value supporting every success.

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

Cyber Fever is Costly

Continued from page 1

- **Zero Trust**. That peephole in the cabin door allowing you to verify anyone trying to enter.
- **Security Awareness Training**. Like teaching your fellow hikers how to spot hazards and avoid bad trails

Maintenance: Even the strongest cabin in the woods needs tender loving care and maintenance to do repairs or avoid catastrophes, especially because the weather (and cyberthreats) is constantly changing. That is why it is vital to ensure all relevant security patches and updates are always put in place to close vulnerabilities, just like a crack in a cabin wall. Other maintenance recommendations include periodic review of who has access to key data, running internal and external vulnerability scans, and penetration tests.

Don't brave the digital wilderness alone. IT Radix can guide you through the must-have protections that keep your organization safe, secure, and ready for whatever comes next.

Proudly folded & sealed by Central Park School

Let's Get Physical (with Your IT Security)

Olivia Newton-John's song "Physical," was not about Information Technology, but it should have been! Physical security of your IT hardware should not be overlooked. Let's warm up and flex those physical security muscles!

Best Practices to "Get Physical"

- **Access Control**
  - » Lock server rooms and closets—no open gym policy here!
  - » Use keycards, PINs, or biometric systems for VIP access.
- **Device Security**
  - » Secure servers in locked racks—it's your strong core.
  - » Use cable locks for PCs—equipment needs a good spotter.
- **Surveillance**
  - » Install CCTV cameras and motion sensors—workout mirror.
- **Inventory Management**
  - » Maintain an up-to-date asset list—track your reps!
  - » Tag devices for tracking—RFID is your personal trainer.
- **Environmental Controls**
  - » Fire suppression systems—don't let things get too hot.
  - » Climate control for server rooms—stay cool under pressure
  - » Surge protectors and UPS systems—power is endurance.
  - » Shred documents—as exhilarating as losing those pounds
- **Policies and Training**
  - » Train employees to lock unattended devices and report suspicious activities. It's a workout plan keeping all on track.

Physical Security + Cybersecurity = Complete Protection

Combining both physical and cybersecurity gives you true peace of mind—like cardio and strength training working together.

Refer a Friend and Share the Love!

We cherish having you in our family and now invite you to extend the joy! For each organization that becomes a client, we will send a donation to your choice of charity. Also, as an introduction to our services, your referral will be offered a FREE Network Assessment (a $600 value).

www.it-radix.com/refer-a-friend

SPECIAL OFFER: Refer a Friend and IT Radix Will Donate to Your Choice of Charity

When Good Love Goes Bad

Are You Still in the Right Tech Relationship?

Every great business relationship starts with a flurry of excitement and wishes for a bright future! But just like in love, sometimes what we think is true affection turns into complacency, or worse—betrayal. For your business, that is a liability you do not need. It is smart to consider your business relationships to be sure that they continue to serve you. Consider the following.

Obsolete Technology in The House?

Remember the day five years ago when the IT professional wheeled in that new server! Perfection! Today, it may be approaching "End of Life" meaning the vendor no longer supports security upgrades. That is a security risk you do not need. While loyalty in a relationship is admirable, think about whether hanging on to technology that has "always been good to us" is right for the long term.

Is Your Vendor Seeing Others?

Your vendors are your trusted partners and advisors. Are they worth it? Do they prioritize cybersecurity the way you do? Have you asked them for a copy of a security audit they have conducted? Perhaps they are sharing some of the great ways you conduct business with your competitors? Trust is important in any relationship because it creates security and stability. You would not want your significant other to share sensitive information with others, neither should your business partners.

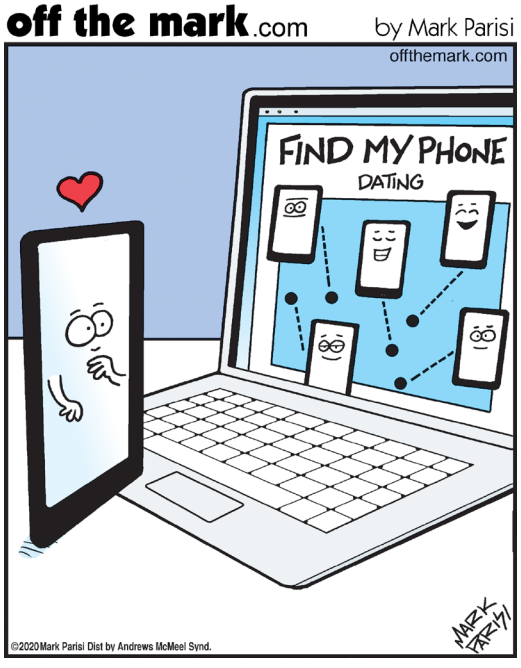
Do You Put Too Much Faith in Staff?

A trusted loyal staff is a cherished thing. But overconfidence in the reason to trust another can be devastating if it is not warranted. Every relationship needs to be nurtured, including that connection you have with your staff about the importance of cybersecurity. Keep your staff educated and alert about how to avoid the latest cyberthreats. And reward them when they do things right. Their devotion to you and your goals will only increase!

Is There a New Head-Turner in Town?

The latest "new thing" in business is Artificial Intelligence (AI). It is the shiny new love that is capturing the attention of everyone! Overuse of AI tools without proper oversight might mean that the blind date with the new hottie turns into a train wreck of legal and compliance issues. It is best to get to know the new attraction slowly before deciding this relationship is right for you.

Just like any partnership, your tech environment deserves a little attention to keep the spark alive. If you're questioning whether your tools or vendors are still treating you right, IT Radix can help you sort the keepers from the heart breakers ensuring that you have a healthy technology love life!



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

49 S. Jefferson Road
Whippany, NJ 07981

In This Issue

- The must-have protections you need in place to keep your organization safe and secure
- Achieving true peace of mind with both physical security AND cybersecurity
- How is your tech relationship?

February 2026

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

Reid's Rules...

Reid knows that just like old bones and forgotten toys pile up in his doghouse, your browser cache can fill up with leftovers from websites you've visited.

While those bits and pieces help pages load faster, they can also store sensitive info longer than you'd want—almost like leaving your best buried bones uncovered for anyone to stumble upon!

Giving your cache a regular cleanup keeps old logins, personal details, and outdated files from sticking around. Plus, it helps your browser run faster and fetch the freshest version of every site. Think of it as tidying up the yard and reburying your treasures properly: quick, refreshing, and a simple way to keep your digital world safe and secure.

Love Isn't the Only Thing in the Air...

Apple AirPods' Bluetooth Eavesdropping Problem

A flaw in Apple AirPods was discovered that allowed attackers to connect to your device and potentially listen in—yikes! The good news? Apple released a firmware update for both AirPods and Beats to close the loophole. To stay protected, be sure your devices are up to date.

How to Update Your AirPods or Beats

Most updates install automatically when your earbuds are paired with your iPhone or iPad. To encourage the update, place your AirPods or Beats in their case with the lid open, keep them near your iPhone or iPad, and make sure your device is connected to Wi-Fi and charging. Updates usually complete quietly in the background.

Want to double-check? Go to **Settings > Bluetooth**, tap the **(i)** next to your device, and look for the Firmware Version. If it's not the latest release, give it a little more time—it should download shortly.

