



Digital Mosquitoes Can Suck Your Business Dry

Keep Malware, Phishing, and Ransomware from Taking a Bite Out of Your Business

Imagine you're halfway up a scenic trail, backpack loaded, boots laced, and the only thing buzzing in your ear is a blood-thirsty mosquito treating your neck like an all-you-can-eat buffet. Welcome back to our journey through the digital wilderness. Except instead of mosquitoes, you've got malware, ransomware, phishing scams, and breach attempts all looking for a free meal—your data. The solution? Cyber bug spray! It works way better than the citronella candles your uncle swears by each year at the family picnic.

Endpoint Protection

Start with a proper coat of endpoint protection. Think of tools like Huntress ITDR and ETDR. They function as industrial-strength DEET. These bad boys patrol your laptops, servers, and that suspiciously old iPad in the break room, swatting ransomware, and malware before they can sink their little digital fangs in. If something bad does land on you, it is immediately isolated.

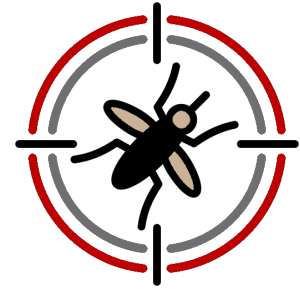
Network Protection

Put up some network-level protection—a good firewall acts as your secure web gateway. It keeps the worst of the wilderness out, so your team isn't accidentally wandering into shady websites or opening emails titled "Urgent: Your Invoice Is Overdue."

Ongoing Maintenance

Don't skip the reapplication schedule. Just like real bug spray wears off after a few sweaty hours, software patches and updates are non-negotiable. Turn on automatic updates, or you're basically hiking in flip-flops and underwear. And no one wants to see that! Leverage working with an IT Managed Services provider like IT Radix to help with this and all the other bug spray recommendations in this article!

Continued on page 2



Happy 250th Birthday America!

This month, America's got a fresh new spark! While the Founders rocked quills, we've got digital magic. Technology has handed us a "liberty upgrade," freeing us from offices and old gatekeepers.

Now, we carry the whole world in our pockets, allowing us to learn, work, or master a hobby from anywhere. It's a modern revolution that sparks connection, curiosity, and ultimate independence to live life at our own joyful rhythm!

That's worth celebrating!

Did You Know...

At IT Radix, we believe in having a positive attitude. It creates an uplifting environment where our team thrives and actually enjoys solving challenges. That upbeat energy is contagious—our clients feel it through faster and better solutions and peace of mind that comes from a team that genuinely likes what they do and cares about our clients' success.



Digital Mosquitoes

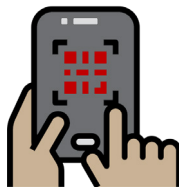
Continued from page 1

Staff Training

And for the final ounce of prevention, add employee training and multi-factor authentication (MFA). These are the digital equivalents of long sleeves, tucked-in pants, and a hat with a net. A quick monthly phishing drill turns your team from “easy targets” into “those annoying humans who actually spot the fake emails.” MFA adds that extra “sorry, mosquito, you still need my six-digit code” barrier.

For most New Jersey based small businesses, a decent cybersecurity “bug spray” subscription costs less per month than your office coffee fund. The return on investment? No 3 a.m. “we’ve been ransomed” phone calls and the ability to actually enjoy running your business instead of constantly scratching digital bites.

You do not have to hike through today’s cyber wilderness alone. With the right protection in place, your business can stay focused on the trail ahead instead of swatting away nonstop threats. Contact IT Radix and let’s talk about how to keep your business protected.



Cracking the QR Code

What Is a QR code? Ever seen those funky, square barcodes on posters or products or even in an email or website? That’s a QR code!

You can scan it with your phone to visit a website, download a file, or even add an event to your calendar. They’re super handy and can be found everywhere, from business cards to snack bags. (We even have one for our special offer below.) But they are not all sugar and spice and can be harmful.

How Cybercriminals Use QR Codes

Sadly, cybercriminals can use QR codes just like phishing links. They can create malicious QR codes that lead to harmful websites or download malware onto your device. These fake codes can be shared via email, social media, or even printed on flyers and stickers.

Tips to Safely Use QR Codes

- **Be cautious:** Don’t scan QR codes from unknown or sketchy sources. If it promises a free iPhone, it’s probably a scam!
- **Use a scanner app:** Choose one that shows a preview of the link before you open it. This helps you decide if it’s safe.
- **Trust your instincts:** If the URL looks weird, asks for a login, or seems unrelated, close your browser right away.

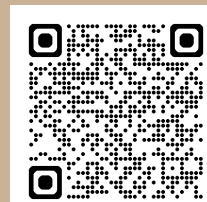
QR codes are handy, but one quick scan can cause big trouble. IT Radix is here to help with practical cybersecurity guidance to keep your team safer. Reach out anytime to help your business scan smarter and stay safer!



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.



www.it-radix.com/ai-security

SPECIAL OFFER: Free Microsoft AI Security Assessment (Expires 8/31/26)

Unauthorized Apps Are Risky Business



Your employees may not mean to create cyber-security problems, but the unauthorized apps they use every day could be doing exactly that.

This issue is called Shadow IT. It happens when employees use software, apps, or cloud services that have not been approved or reviewed by IT. That might include personal Google Drive or Dropbox accounts, unapproved collaboration tools, messaging apps, or even AI tools used without security checks.

Most people are not trying to break the rules. Usually, they are just trying to work faster, solve a problem, or avoid tools that feel outdated or clunky. The trouble is that these shortcuts can open the door to serious security risks.

When IT does not know a tool is being used, it cannot properly secure it. That can lead to sensitive data being shared in unsafe places, missing security updates, compliance issues, malware infections, and account hijacking. Even one unapproved app can create a weak spot that cybercriminals are happy to exploit.

Here's How to Manage Shadow IT

Start by giving employees a clear list of approved software and making it easy to request new tools when needed. Put policies in place to limit unauthorized app downloads on company devices. Just as important, educate your team so they understand that convenience should never come at the expense of security. On the technical side, network monitoring and strong endpoint protection can help your IT team spot risky activity and respond before it becomes a bigger problem.

Shadow IT is not just an IT issue. It is a business risk that can lead to downtime, data loss, and compliance headaches if left unchecked.

The best defense is to get ahead of it. Contact IT Radix for a complimentary Network Security Assessment and let us help you uncover unauthorized apps, identify vulnerabilities, and strengthen your defenses before Shadow IT turns into a full-blown security headache.

Delegate to Claude Cowork

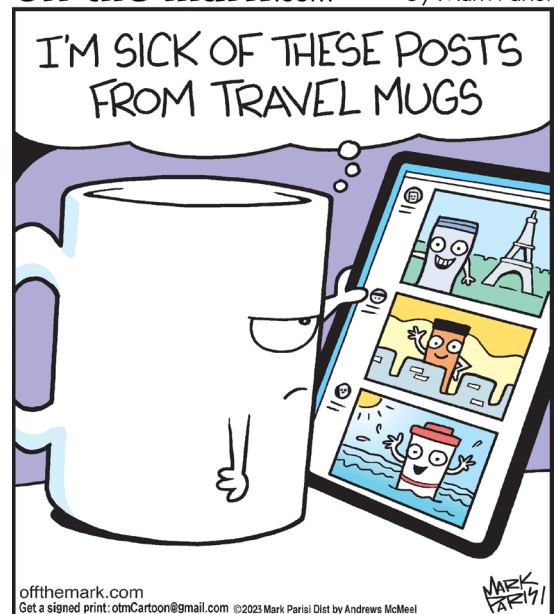


While many of us think of AI as a more advanced version of a search engine, things are shifting toward actual project management. Anthropic is leaning into this shift with their latest release: **Claude Cowork**.

Claude is an AI teammate that can research a topic, organize information, draft content, and work through projects with you. It is way more than "here's an answer." It carries work forward. For businesses like yours, that could mean less time spent digging through notes, summarizing documents, or starting from a blank page.

As with any AI tool, it is still important to think about security, permissions, and how company information is handled before rolling it out. AI can be a big help, but it works best with the right guardrails in place. IT Radix is here to help pave the way.

off the mark.com by Mark Parisi



In This Issue

- How to keep cyberthreats from taking a bite out of your business
- How cybercriminals are using QR Codes
- How to manage Shadow IT

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

July 2026



Reid's Rules...

Hi, Reid here, your friendly office IT dog with a nose for Canine Intelligence. When it comes to AI, my first rule is simple: **keep AI on a short leash.** Stay close to what matters most in your business. Start with familiar routines like sales follow-ups, data sniffing (analysis), forecasting, or customer support. Train your AI with clean, well-labeled data—no mystery kibble.

When AI behaves, reward it with feedback loops so it learns good tricks. Always keep a human in the loop, or it might sprint off after squirrels. Roll AI into your daily walks (workflows), fetch small wins first, and track results like treats earned. Lock down your data bowls, watch for bias (bad habits spread fast), and teach the whole pack. Do that, and AI becomes your best business buddy.

Apple Pay Scam Alert: Don't Panic and Pay



Scammers are sending fake Apple Pay fraud alerts designed to make people panic and act fast. These messages may claim there is suspicious activity on your account and urge you to call a number or click a link.

If you do, you may reach a scammer pretending to be Apple, your bank, or an investigator. Their goal is to pressure you into sending money or sharing personal information.

Watch for these red flags: unexpected alerts, pressure to act immediately, requests for passwords or codes, and instructions to move money.

If you get a suspicious message, do not respond. Check your account directly and contact Apple or your bank through official channels.

When in doubt, slow down. Scammers create urgency. Do not let them. IT Radix is here to help you stay safe.