CTTS TECH TALK

YOUR TECHNOLOGY NEWSLETTER

AUGUST 2025


JOSH


SARA


KURT


MICHELLE


CHAIM


KEN


EVAN


KURT


NICHOLAS

Cyberthreats are evolving fast—especially in your inbox.

This month, we're highlighting how AI-powered phishing attacks are getting smarter and harder to spot, and what your business can do to stay protected.

You'll also learn why cyber insurance alone isn't enough. We break down how your IT strategy and insurance coverage should work together to defend your business, minimize risk, and ensure you're ready if the worst happens.

If you haven't reviewed your cybersecurity plan lately, now's the time.

INSIDE THIS ISSUE

TECH NOTES

ADVANCED TECH

BIZTECH

CTTS, Inc. 557 S. Interstate 35, Suite 201, Georgetown, TX 78626
www.CTTSonline.com | (512) 388-5559

TECH NOTES
FROM JOSH WILMOTH

AI Isn't Coming for Your Job...
But It Might Be Coming for Your Inbox

***"The best way to predict the future is to prepare for it."* — Peter Drucker**

Let's talk about the productivity killer that no one really wants to admit is winning the war against your calendar: your inbox.

In the last month alone, I've had more conversations with business owners about email overload than anything else—and not just spam, but smart-looking phishing attacks, spoofed invoices, fake DocuSigns, and calendar invites from "IT Support" (which, spoiler alert, wasn't us).

Why the spike? AI.

Hackers are now using AI to craft emails that sound like you, look like your team, and even mimic real past conversations. These aren't the "Nigerian prince" scams of old—they're modern, smart, and scarily convincing.

And if you're still relying on your inbox rules and a spam folder to catch the bad guys, you're basically trying to stop a Tesla with a tricycle.

Here's the Deal:

The email threat landscape has changed. Your email security should too.

What most CEOs don't realize is this:

The #1 attack vector for businesses in 2025 is email.

Your team clicks one wrong link, and boom—your systems, your clients' data, and your bank account could be on the line. Ransomware doesn't knock before it enters.

But there's good news:

At CTTS, we've seen firsthand how the right tools can cut through the noise and stop attacks before they start.

Since switching to our advanced email protection platform (called Shield), my own inbox is 40% quieter. Fewer interruptions. Fewer "Hey, did you send this?" Teams messages. And a lot fewer heart attacks at 4:45 p.m.

We're not just filtering spam—we're using behavioral AI to detect the stuff that slips past traditional filters. It learns how your team communicates and flags anything weird. And if you're already a CTTS client, we can migrate you to this at no extra cost.

Want to Know If You're Vulnerable?

Shoot me a note. We'll run a quick (and painless) audit of your current email protection, show you where gaps exist, and help you lock it down.

Because let's face it—if hackers are using AI to level up, it's time we do too.

Ready to stop email threats before they start? Call us today at (512) 388-5559 or visit CTTSonline.com to get protected.

Help Us Celebrate August Birthdays at CTTS!

Josh Wilmoth

Michelle Quick

ADVANCED TECH

Cyber Insurance 101:
Protecting Your Business from the Unexpected

Cyberattacks can strike without warning, and when they do, the fallout can be costly. Lost data, disrupted operations, and a damaged reputation are just a few of the challenges businesses face after a breach.

That's where cyber insurance comes in. It helps cover the financial hit from cyber incidents like ransomware, phishing attacks, or data leaks.

But here's the catch: not all policies are the same, and coverage depends heavily on your company's security practices.

What Does Cyber Insurance Cover?

A good cyber insurance policy may help pay for:

- Recovering lost data and restoring systems
- Legal and regulatory costs
- Notifying affected customers and monitoring their credit
- Lost income due to downtime
- Ransomware payments (sometimes)

However, having a policy in place doesn't guarantee a payout. If your business isn't following cybersecurity best practices, your claim could be denied.

Why Claims Get Denied

Insurers will review your cybersecurity setup before approving a claim. Common reasons claims are denied include:

- Weak or missing security tools
- Unpatched software or outdated systems
- Poor recordkeeping of your cybersecurity processes
- No clear plan for responding to an attack

In short, if your defenses weren't strong before the incident, your insurer may not help after the fact.

How to Improve Your Cyber Readiness

To stay protected—and to keep your insurance coverage reliable—make sure your IT strategy includes:

- Multi-factor authentication (MFA)
- Regular data backups and endpoint protection
- Timely updates and patch management
- A documented incident response plan
- Ongoing employee cybersecurity training
- Periodic risk assessments

How CTTS Can Help

That's where we come in. At CTTS, we work with businesses like yours to meet and exceed the cybersecurity standards insurers expect. From daily IT support to long-term strategy, we'll help you build a secure foundation, so if an incident does happen, you're not left unprotected.

Need help making sure your business is cyber-insurance ready? Let's talk. CTTS is here to help you prepare, prevent, and respond.

Windows 10 Support is Coming to an End!
Schedule a PC Review with CTTS Today!

BIZTECH

Why Smart Businesses Combine Cyber Insurance and IT Strategy

Cyberthreats are becoming more advanced, especially with the use of AI by hackers. That's why having both a strong IT strategy and cyber insurance isn't just smart—it's essential. One protects your systems, the other protects your bottom line.

When combined, they form a powerful shield that keeps your business safe and running, even when the unexpected happens.

How IT and Cyber Insurance Work Together

Many business owners think of IT and cyber insurance as separate tools. In reality, they're most effective when used together. A strong IT strategy helps reduce your risk of an attack—and shows insurance providers that your business takes cybersecurity seriously.

Here's how your IT provider plays a key role in both protection and insurance readiness:

Assess Security Gaps

Your IT partner can evaluate your current defenses, identify risks, and create a plan to strengthen weak spots. This step shows insurers you're proactive about protecting your data.

Put Best Practices in Place

With help from an experienced IT team, your business can implement vital security tools like multi-factor authentication (MFA), firewalls, and access controls—many of which are now required by insurance providers.

Document Policies and Plans

Proper documentation matters. Insurers look for written security policies and incident response plans when evaluating coverage and claims. Your IT provider can help you get these in place.

Prepare for the Worst

A solid incident response plan ensures your team knows exactly what to do during an attack. Testing and refining this plan with your IT partner helps you recover faster and shows insurers you're ready.

Stay One Step Ahead

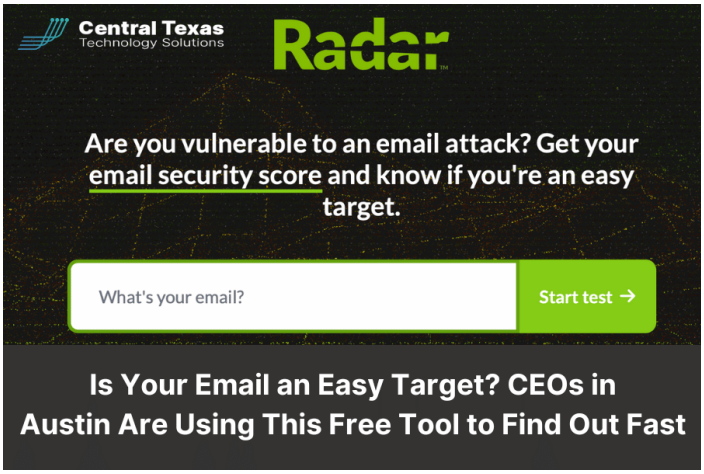
Cyberthreats are always changing. That's why continuous monitoring and regular updates are essential. Ongoing support from your IT provider keeps your defenses up-to-date and insurance-ready.

Partner With CTTS for Peace of Mind

At CTTS, we help Central Texas businesses align their IT strategies with cyber insurance requirements—so you're not only protected, but also prepared.

Let's simplify the process, fill in the gaps, and build a strong foundation for your business.

Ready to strengthen your security and safeguard your insurance coverage? Let's talk.



Run Your Free Email Security Test Today:
https://ctts.email.security/radar

Central Texas
Technology Solutions

CTTS, Inc. 557 S. Interstate 35, Suite 201, Georgetown, TX 78626
www.CTTSonline.com | (512) 388-5559