CTTS TECH TALK

YOUR TECHNOLOGY NEWSLETTER

JUNE 2025


JOSH


SARA


KURT


MICHELLE


CHAIM


KEN


EVAN


KURT


WILSON


NICHOLAS

Phishing and social engineering attacks have evolved. AI now helps cybercriminals craft emails, voicemails, and even fake videos that look and sound real - making them harder to spot and more dangerous than ever.

Inside this issue, you'll learn:

- **Why your current security tools might not be enough**
- **How AI is helping hackers craft smarter, more believable attacks**
- **And the #1 way businesses like yours are getting compromised (hint: it's not your firewall)**

Let's make sure your business is prepared, not just protected.

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

What Got You Here Won't Get You There (And That's a Good Thing)

If you've been with CTTS for a while, first—thank you. We don't take that lightly.

You're probably someone who saw early on that technology is more than just email and printers—it's the engine that keeps your business running, growing, and protected.

But here's the hard truth we're seeing in 2025:

The tools and strategies that worked even two years ago aren't cutting it today.

Cybersecurity threats have gotten smarter. AI is changing the pace of everything. And the expectations your customers and employees have? They're not slowing down.

As a business owner, that means doing what you've always done - **but better, faster, and more securely.**

And here's the good news: **you're not starting from scratch.**

Because you're already working with us, you have a head start. But even the best-run systems need a tune-up. And most of the businesses we serve have gaps they don't even know about—until we shine a flashlight on them.

Here's What We're Seeing (Even in Well-Run Businesses):

- Old devices quietly ticking toward Windows 10 end-of-life (October 2025)
- Microsoft 365 tools not being used to their full potential (Teams Phone, anyone?)
- Backups that work... until they don't (yes, we test them)
- Security tools in place, but no one's sure who's managing them
- Support tickets getting answered—but without addressing the root issue

That's Why Mid-Year Is the Perfect Time to Reassess

Think of it like a mid-season check-in.

Are we still supporting you in the areas that matter most? Are there tools you're paying for but not using? Are your systems future-proofed for the next six months—or are they slowly dragging down your team?

Let's Talk. Not Sales Talk - Real Talk.

We're offering our existing clients **a free 30-minute Tech Alignment Session** this month. It's a no-pressure review where we:

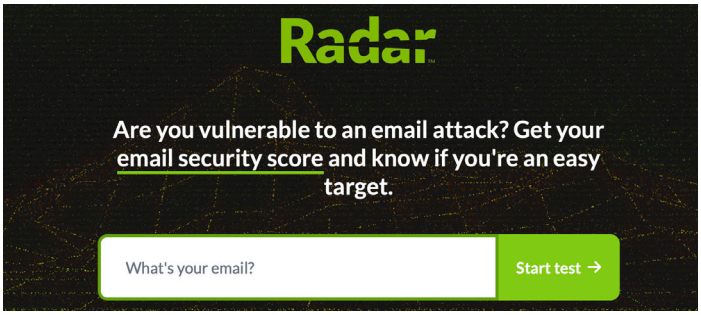
- Show you what's working well
- Flag hidden risks
- Recommend quick wins and long-term improvements
- Give you clarity, not a sales pitch

You might walk away thinking, "We're in great shape." Or you might realize there's a gap that's been quietly costing you time, money, or peace of mind.

Either way, you'll know. And we'll make sure you have a plan.

Schedule Your Tech Alignment Session Before July 1

We've got limited slots available. Call us at (512) 388-5559 or visit www.CTTSonline.com to grab your spot. Because what got you here, **won't get you there!**



At CTTS, we've helped hundreds of businesses across Central Texas secure their email systems, and one thing we know for sure: what you don't know about spam protection can hurt you.

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

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

ADVANCED TECH

The Alarming Reason Social Engineering Attacks Are So Effective

Hint: It's not your firewall - it's your people.

It's June 2025, and while most businesses are busy embracing AI tools to speed up workflows and automate the boring stuff, cybercriminals are using those same tools for a different kind of efficiency: tricking your employees into letting them walk right through the front door.

They're not hacking your systems - they're hacking your staff.

This tactic is called **social engineering**, and it's hands-down one of the most successful (and dangerous) cyberattack methods we see today. Why? Because it doesn't need code. It doesn't need a backdoor. It just needs a moment of trust… and a click.

Why This Works So Well (And Why It's So Dangerous)

Let's be honest, your team's busy. They're handling meetings, invoices, customer requests, and 117 unread emails. Social engineers count on this chaos. They send an email that looks like it came from your CFO, your IT provider, or even you… and it says something like:

- "Urgent: I need you to send a payment before 2 p.m."
- "Unusual login detected—reset your password here."
- "Your invoice is overdue—click to view."

It looks normal. It feels routine. But it's anything but.

Here's how social engineering plays on human instincts:

- **Authority** – "This is from your CEO. Do it now."
- **Urgency** – "Your account will be locked."
- **Fear** – "Your data's been compromised."
- **Greed** – "Claim your refund now."

These messages don't stand out as threats. That's what makes them so effective.

How to Fight Back (And Actually Win)

The best defense isn't just firewalls and antivirus software, it's your people. When your employees know what to look for, your business becomes a much harder target.

Here's how we help our clients stay ahead:

Security Awareness Training – Regular, real-world training so your team knows a fake when they see one.

Phishing Simulations – We test your defenses the safe way—with fake phishing emails that turn into coaching opportunities.

MFA Everywhere – A second layer of security that blocks attackers even if a password gets compromised.

Clear Reporting Paths – Make it easy for your team to say, "Hey, this feels off." Early detection = no disaster.

Here's one more thing that works surprisingly well: **slowing down.** Most social engineering emails are designed to get your team to act fast and think later. If you encourage your employees to pause and verify, you've already cut the risk in half.

You're Not Paranoid - You're Just Prepared

Whether your company has 10 employees or 200, you're a target. But you don't have to be an easy one.

CTTS helps CEOs and business owners take practical steps to protect their team, data, and bottom line. If you're unsure how exposed your business is—or if your current MSP hasn't talked to you about social engineering threats lately—now is the time.

Schedule a no-pressure consultation with our team.

We'll assess your current cybersecurity posture, explain where you're vulnerable (in plain English), and give you clear next steps to strengthen your defenses.

Call us at (512) 388-5559 or visit www.CTTSonline.com. Let's make sure the only thing your team clicks on… is **"Forward to IT."**

BIZTECH

AI Is the New Hacker: What Business Owners Need to Know Right Now

If you've been reading headlines lately, you've probably seen the same buzzword pop up over and over: AI.

Most of the stories are about productivity, automation, or how it's changing the way we work. And that's true—it is. But here's the part that doesn't make the evening news: **AI is also changing how cybercriminals attack your business.**

At CTTS, we're seeing it firsthand. And I'm here to tell you: this is not a "someday" problem. This is happening now.

The Rise of AI-Driven Cybercrime

For years, phishing emails were filled with typos and broken grammar. You could spot them from a mile away. Today? Not so much.

AI can now write perfect emails. It can mimic writing styles, clone voices, and even generate video of someone saying something they never actually said. We've seen AI-generated voicemails from "CEOs" asking accounting teams to wire money. We've seen deepfake videos used to manipulate vendors. And we've seen small businesses—right here in Central Texas—get caught off guard.

This isn't about a guy in a hoodie guessing passwords anymore. It's about machine intelligence moving faster than most companies can keep up with.

What You're Facing Today:

- **AI-Generated Phishing Emails** – Written in perfect English, tailored to your industry, and sometimes even referencing real client names.
- **Voice Cloning** – Using as little as 3 seconds of audio, hackers can recreate your voice (or mine) to request passwords, money transfers, or access.
- **Image and Video Deepfakes** – It's now possible to fake Zoom calls, recorded messages, and even ID badges using AI.
- **Smarter Malware** – AI can detect your antivirus patterns and change itself in real time to slip past defenses.
- **Hyper-Personalized Attacks** – LinkedIn, company websites, and public records are used to generate AI content that feels real because it is based on your data.

What's Coming Tomorrow? It's Already Here.

The biggest mistake we see businesses make is assuming they're too small to be a target. That thinking is outdated. AI doesn't care if you have 10 users or 1,000—it just needs one person to click the wrong link.

And if you think this is moving fast now? Just wait. AI threats are getting faster, cheaper, and harder to detect by the day. In a year, we'll likely see fully autonomous attack bots scanning the web, generating phishing content on the fly, and executing attacks without human oversight.

Scared? You should be a little. But fear isn't the solution - **a plan is.**

What You Can Do (And What We're Doing to Help)

At CTTS, we're investing heavily in AI—not just to keep up, but to stay ahead. We're integrating AI-powered security tools that can identify threats in real time, stop deepfake attempts before they spread, and detect behavioral red flags inside your systems before they turn into breaches.

But the most important tool in your toolbox? **An aware, trained team.**

We're helping business owners across Central Texas educate their people on what AI-powered threats look like, how to respond, and how to spot red flags before the damage is done. We offer live training, real-time testing, and ongoing monitoring to make sure your business stays protected - even as the threat landscape evolves.

Let's Get Ahead of This - Together

This isn't the time to play defense. It's time to build a smarter offense.

If you haven't reviewed your cybersecurity strategy in the last 6 months, it's time. AI won't wait—and neither should you.

Let's put your security posture to the test.

Give us a call or schedule a time at www.CTTSonline.com.

We'll assess your risks, make a clear plan, and help you build the kind of resilient business that can stand up to whatever tomorrow brings.

AI is the biggest business accelerator and the biggest threat we've seen in years. Let's make sure your business is ready for both.

Central Texas
Technology Solutions

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