June 2026

AvTek Chronicle

Insider Tips To Make Your Business Run Faster, Easier and More Profitably

Bitcoin ATM Scams Are Rising Across Texas — Here's What You Need to Know

A growing wave of cryptocurrency scams is impacting communities across East Texas and the nation, with criminals increasingly using Bitcoin ATMs to pressure victims into making fast, irreversible payments. While these scams often target individuals, they also highlight a broader cybersecurity challenge businesses cannot afford to ignore: social engineering attacks are becoming more sophisticated, more believable, and more financially damaging.

Recent incidents in Smith County, Angelina County, and Polk County show how quickly these scams can escalate. In one Lindale case, scammers impersonated law enforcement officials and convinced an elderly resident to deposit $13,000 into a Bitcoin kiosk to avoid arrest. Similar scams in Lufkin involved spoofed sheriff's office phone numbers, threats related to missed jury duty, and instructions directing victims to local cryptocurrency machines.

Why Bitcoin ATM Scams Are Growing

Bitcoin ATMs allow users to convert cash into cryptocurrency within minutes. Unfortunately, scammers exploit the speed and irreversibility of crypto transactions to move stolen funds before victims realize they've been deceived.

According to national fraud data cited in the research, losses tied to Bitcoin ATM scams have increased dramatically since 2020, with older adults disproportionately affected. Many victims are pressured into acting immediately through fear-based tactics involving:

- Threats of arrest or legal action
- Claims of compromised bank accounts
- Fake government or law enforcement impersonation
- Requests for secrecy and urgency
- Instructions to remain on the phone during the transaction

Once the cash is deposited into the kiosk and converted into cryptocurrency, recovery becomes extremely difficult.

What Businesses Should Learn From These Scams

Although these incidents often target consumers, the tactics mirror the same social engineering methods used against businesses every day. Cybercriminals rely on urgency, impersonation, fear, and confusion to bypass normal decision-making processes.

For organizations in regulated industries like healthcare, financial services, legal, and construction, the risks are even greater. Employees who are not properly trained may unknowingly expose sensitive information, approve fraudulent transactions, or fall victim to phishing and ransomware attacks.

This is why cybersecurity today must go beyond firewalls and antivirus software. Businesses need a layered strategy that includes:

- Employee cybersecurity awareness training
- Multi-factor authentication (MFA)
- Identity and access management controls
- Ongoing vulnerability monitoring
- Documented compliance and risk management procedures
- Incident response planning

Red Flags Everyone Should Know

Whether at home or at work, these warning signs should never be ignored:

- Someone demands payment using cryptocurrency or gift cards
- The caller claims to be law enforcement or a government agency
- You are pressured to act immediately
- The caller insists you stay on the phone
- You are told not to discuss the situation with anyone else
- You are instructed to withdraw cash and visit a Bitcoin ATM

Legitimate organizations will never demand payment through cryptocurrency.

How Businesses Can Reduce Cyber Risk

Social engineering attacks continue to evolve because they target human behavior rather than technology alone. Organizations that regularly educate employees and maintain strong cybersecurity governance are far better positioned to prevent costly incidents.

AvTek Solutions helps businesses build stronger cyber resilience through services including:

- Managed IT and Security Services
- Cybersecurity Awareness Training
- Compliance Readiness Programs
- Vulnerability Management
- Identity & Access Management
- Data Backup and Recovery
- Virtual CSO (vCSO) Advisory Services

By combining proactive security measures with ongoing compliance guidance, businesses can better protect both their operations and the people they serve.

Final Thoughts

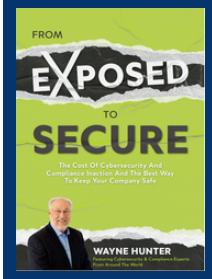
Bitcoin ATM scams are no longer isolated incidents — they are part of a nationwide fraud trend fueled by increasingly sophisticated social engineering tactics. The same manipulation techniques being used against individuals are also being used to infiltrate businesses, compromise accounts, and trigger financial loss.

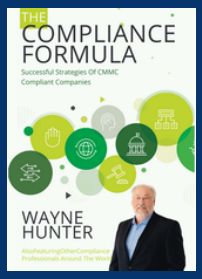
Education, awareness, and proactive cybersecurity planning remain the best defense.

Storm Season is Here: Is Your Backup Strategy Ready?

Summer storm season can bring more than heavy rain and power outages — it can disrupt operations, impact productivity, and put critical business data at risk. Whether it's severe weather, flooding, or unexpected downtime, businesses need more than just backups; they need a recovery plan they can rely on. Now is the perfect time to review your disaster recovery strategy, verify backups are functioning properly, and ensure your team knows what to do if systems suddenly go offline. A proactive approach today can help minimize downtime and keep your business running when unexpected disruptions happen tomorrow.

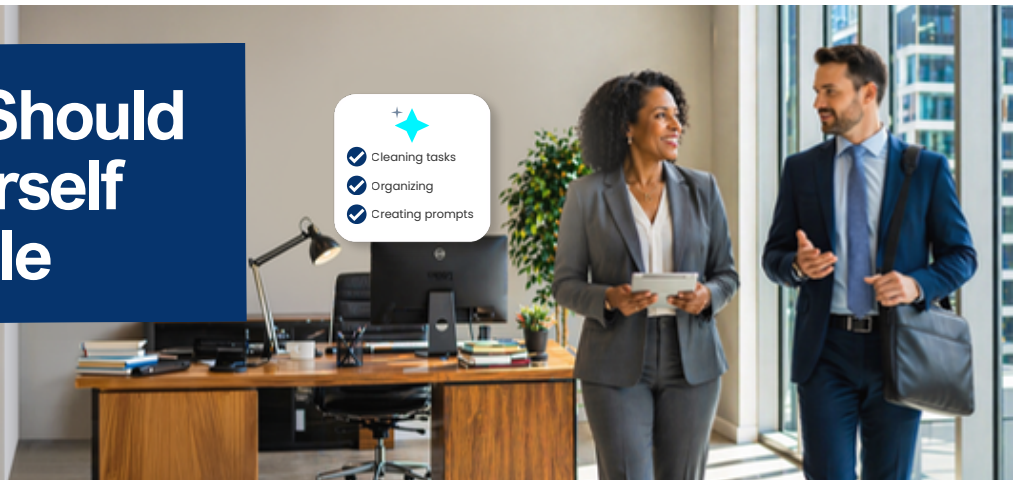
HAVE YOU READ WAYNE'S BOOKS?





Available on Amazon
*****except for Exploited! Email Katie to ask for a copy!***

The Tasks You Should Stop Doing Yourself and Let AI Handle



For many business owners, time doesn't disappear suddenly. It fades into the background. Your day gets swallowed by small, repeatable work that feels necessary in the moment. You answer routine emails, follow up on requests and check in on things that should be fine without you.

The issue isn't that you're doing too much. It's that you're still doing work your business should be able to handle on its own. AI can handle predictable tasks, so your time stays where it matters.

PROBLEM #1: ROUTINE EMAIL RESPONSES

Your inbox may look overwhelming, but most are variations of the same few questions you answer again and again. Availability questions, basic inquiries and routine follow-ups keep coming in, and you keep answering them. Each reply feels quick, but it pulls you back into reaction mode.

AI can reply to repetitive emails based on how you've handled them before. Common questions get answered without your involvement. Instead of reacting to every message, you stay focused on conversations that need you.

PROBLEM #2: CUSTOMER INQUIRY TRIAGE

When every customer request comes to you first, response time becomes tied to your availability. That slows things down when you're in a meeting or simply away.

With AI handling incoming requests, inquiries are sorted, prioritized and directed to the right person without passing through you. Each request arrives where it belongs, already categorized before your team sees it. You stay out of the flow unless a situation genuinely requires a direct response.

PROBLEM #3: INTERNAL FOLLOW-UPS AND REMINDERS

If progress depends on you checking in, you become the bottleneck. You end up chasing updates instead of focusing on decisions that move the business forward.

AI handles routine follow-ups, tracks progress and prompts the right people. Work moves without you, and you step in only when it matters.

PROBLEM #4: BASIC REPORTING AND STATUS CHECKS

Logging into multiple systems to understand what's going on is a time drain.

The problem usually isn't that you need more data. It's that the right data isn't laid out clearly, so you have to go find it.

AI compiles and monitors simple reports, giving you a clear view of what matters without having to dig through multiple platforms. It flags anything that looks off early so you can act quickly.

PROBLEM #5: FIRST DRAFTS OF CONTENT AND COMMUNICATION

Starting from scratch takes longer than most owners realize. Client updates, proposals and internal messages often take longer to begin than to finish. The delay comes from getting something on the page, not from improving it.

Instead of staring at a blank page, AI gives you a working draft to review and send. You stay in control of what goes out and stop wasting energy on blank-page work.

YOUR BUSINESS SHOULDN'T NEED YOU FOR ALL OF THIS

A business that requires your constant input isn't just busy; it's fragile.

When your time is tied up in repeatable tasks, it's harder to step back and grow. AI takes that work off your plate so you can focus on what you do best.

Key Takeaway:
AI isn't about replacing what makes your business work. It's about removing the parts that shouldn't require you, so your focus stays where it matters most.