ENER SYSTEMS
INFORMATION TECHNOLOGY SERVICES

19295 North 3rd Street, Suite 5
Covington, LA 70433

Inside This Issue

wccxtcertified.com

WORLD-CLASS CUSTOMER EXPERIENCE TRAINED

certified WBENC WOMEN'S BUSINESS ENTERPRISE

JESSE COLE On How To Create Raving FANS

Jesse Cole built the iconic Savannah Bananas brand from nothing by doing things differently. The key to his success was his "fans first" mindset, which centers on creating an incredible experience for each individual fan.

"[Fans] aren't buying because of the product," Cole explained. "They're buying it because of how we make them feel. That's the differentiator."

Here are his takeaways for businesses who want to create raving fans too.

Eliminate Friction.

Put yourself in the customer's shoes and eliminate the friction they experience. Just like Walt Disney used to walk around Disneyland every day to find things to improve, businesses should go through the sales and onboarding process to look for friction points—and reduce them whenever possible.

Entertain Always.

The heart of entertainment is to provide enjoyment, according to Cole. "How do you map the journey for your customers, every step of the way, to provide enjoyment and make their lives better?" he said. Think about the little details; there are many stages of the experience of working with you, from first impressions to onboarding. Try to make every stage remarkable. Those interactions set the tone when someone starts working with you.

Experiment Constantly.

And don't just experiment—try the exact opposite of what's normal. Not every experiment will work, but the ones that do have the opportunity to become groundbreaking successes. And people only remember the successes, not all the failures along the way.

Engage Deeply.

"Do for one, what you wish you could do for many," Cole said. The Magic Castle Hotel in Hollywood is a master of this tactic as well; their CEO says the key is to "listen carefully, respond creatively." By creating tailored experiences for individuals, you show your entire fan base that you care deeply for the people who support you.

Empower Action.

"Stop standing still, start standing up," said Cole. "None of [the rest of it] matters if we don't empower first ourselves, and then our team." To this end, he advised businesses to not underestimate the power of a thank you—to your team, your mentors and your clients—when it comes to building raving fans.

TECHNOLOGY TIMES

INSIDER TIPS TO MAKE YOUR BUSINESS RUN FASTER, EASIER, AND MORE PROFITABLY

Volume XXI, Issue 9 — September 2025 — Covington, LA

SHINY NEW GADGET OF THE MONTH

Logitech MX Mechanical Wireless Keyboard

The Logitech MX Mechanical Wireless Keyboard delivers a premium, quiet typing experience with tactile mechanical switches for precise, low-noise feedback. Its low-profile, full-size layout enhances comfort and ergonomics, while smart backlit keys illuminate as your hands approach, adapting to lighting conditions. Seamlessly pair with up to three devices across multiple operating systems via Bluetooth or the Logi Bolt receiver. Customizable through Logi Options+, it supports efficient workflows, and its rechargeable battery lasts up to 15 days with lighting or 10 months without.

September 2025

René Miller, CEO, and J. Michele Miller, President

OUR MISSION:

To safeguard small and mid-sized businesses from cyberattacks and eliminate any unforeseen IT issues that may arise, allowing your business to prosper without any interruptions.

Is Your Business Training AI to Hack You?

There's a lot of excitement about artificial intelligence (AI) right now, and for good reason. Tools like ChatGPT, Google Gemini and Microsoft Copilot are popping up everywhere. Businesses are using them to create content, respond to customers, write e-mails, summarize meetings and even assist with coding or spreadsheets.

AI can be a huge time-saver and productivity booster. But, like any powerful tool, if misused, it can open the door to serious problems – especially when it comes to your company's data security.

Even small businesses are at risk.

Here's The Problem

The issue isn't the technology itself. It's how people are using it. When employees copy and paste sensitive data into public AI tools, that information may be stored, analyzed or even used to train future models. That means confidential or regulated data could be exposed, without anyone realizing it.

In 2023, engineers at Samsung accidentally leaked internal source code into ChatGPT. It became such a significant privacy issue that the company banned the use of public AI tools altogether, as reported by Tom's Hardware.

Now picture the same thing happening in your office. An employee pastes client financials or medical data into ChatGPT to "get help summarizing," not knowing the risks. In seconds, private information is exposed.

A New Threat: Prompt Injection

Beyond accidental leaks, hackers are now exploiting a more sophisticated technique called prompt injection. They hide malicious instructions inside e-mails, transcripts, PDFs or even YouTube captions. When an AI tool is asked to process that content, it can be tricked into giving up sensitive data or doing something it shouldn't.

In short, the AI helps the attacker – without knowing it's being manipulated.

Continued on Page 2...

...*Continued from Page 1.*

Why Small Businesses Are Vulnerable

Most small businesses aren't monitoring AI use internally. Employees adopt new tools on their own, often with good intentions but without clear guidance. Many assume AI tools are just smarter versions of Google.

They don't realize that what they paste could be stored permanently or seen by someone else.

And few companies have policies in place to manage AI usage or to train employees on what's safe to share.

What You Can Do Right Now

You don't need to ban AI from your business, but you do need to take control.

Here are four steps to get started:

1. Create an AI usage policy.

Define which tools are approved, what types of data should never be shared and who to go to with questions.

2. Educate your team.

Help your staff understand the risks of using public AI tools and how threats like prompt injection work.

3. Use secure platforms.

Encourage employees to stick with business-grade tools like Microsoft Copilot, which offer more control over data privacy and compliance.

4. Monitor AI use.

Track which tools are being used and consider blocking public AI platforms on company devices if needed.

The Bottom Line

AI is here to stay.

Businesses that learn how to use it safely will benefit, but those that ignore the risks are asking for trouble.

A few careless keystrokes can expose your business to hackers, compliance violations, or worse.

Why Not Take 4 Seconds Now To Protect Yourself, Protect Your Company And Protect Your Customers?

Do You Safeguard Your Company's Data And Your Customers' Private Information BETTER THAN Equifax, Yahoo And Target Did?

If the answer is "NO" – you're leaving yourself and your company open to massive liability, millions in fines and lost business, lawsuits, theft and so much more. Because you are a hacker's #1 target. They know you have access to financials, employee records, company data and all that juicy customer information – Social Security numbers, credit card numbers, birthdates, home addresses, e-mails, etc.

Our 100% FREE and 100% confidential, exclusive CEO Dark Web Scan is your first line of defense. To receive your report in just 24 hours, visit the link below and provide us with your name and company e-mail address. Hopefully, it will be ALL CLEAR and you can breathe easy. But if your company, your profits and your customers are AT RISK, we'll simply dig a little deeper to make sure you're protected.

Don't let cybertheft happen to you, your employees and your customers. **Reserve your exclusive CEO Dark Web Scan now!**

Claim Your FREE Dark Web Scan Today At

www.enersystems.com/DarkWebScan/

Thank You!

BEST OF ST. TAMMANY 2025 WINNER

IT/Computer Services

Getting rid of unplanned work...So that others may prosper.

Most of us carry our phones everywhere, trusting them with everything from passwords to private business conversations. But here's the sad truth: phone tracking is far more common – and easier – than most people realize.

Whether it's a jealous partner, a disgruntled employee or a cybercriminal targeting your business, anyone with the right tools can monitor your location, read your messages or even access sensitive business data without you ever knowing. And for business owners, that puts more than just your privacy at risk. It puts your operations, clients and bottom line in danger.

How Phone Tracking Works:

There are several ways someone might track your phone:

Spyware Apps: These can be installed to monitor calls, texts and app usage. Some can even activate your microphone or camera without your knowledge.

Phishing Links: Clicking a malicious link in an e-mail or SMS can silently download tracking software onto your phone.

Location Sharing: Apps with excessive permissions or with social platforms you forgot were still logged in might be sharing your location in the background.

Stalkerware: This spyware is designed to hide in plain sight, often disguised as harmless apps or settings tools.

These methods don't require advanced hacking skills – many are sold commercially under the guise of "monitoring software."

Why This A Big Deal For Business Owners

If you run a company, your phone likely contains more than just personal messages. Think: e-mails with confidential client data, saved passwords, banking access and employee records. A compromised phone can be an open door to your entire business.

The scarier part is the likelihood that you won't realize you're being tracked until it's too late, after an account is drained, a deal is leaked or customer trust is broken.

Consider this: a single data breach costs US small businesses an average of $120,000 (Verizon Data Breach Investigations Report). If your device is the weak link, that breach could start in your pocket any time.

Signs Someone Might Be Tracking Your Phone

Most spyware tools are designed to operate quietly, but there are still signs to watch for:

Battery drain that doesn't match usage
Increased data usage or strange spikes
The phone feels hot when idle
Unexplained apps or icons
Background noise during calls
Frequent crashes/unresponsive screens

These symptoms don't guarantee your phone is compromised, but when paired alongside other unusual behavior, they're worth investigating.

How To Stop Phone Tracking

If you suspect someone is tracking your phone, here's what to do:

1. Run A Security Scan: Use a reputable mobile security app to detect and remove spyware or malware. These tools can also monitor your device in real time and alert you to new threats.

2. Check App Permissions: Go through your app list and review permissions. Disable unnecessary access to location, microphone and camera – especially for apps you rarely use.

3. Update Your Phone: Security updates often include patches for vulnerabilities that spyware might exploit. Make sure your phone is running the latest OS.

4. Perform A Factory Reset: If spyware is confirmed and can't be removed easily, a factory reset is the most thorough option. Just make sure to back up critical data, complete the reset and then change all important passwords.

5. Set Up Security Controls: Use biometric logins (like Face ID or fingerprint) and enable multi-factor authentication on business apps.

Don't Leave Your Phone – And Business – Exposed

Because you're a business owner, your phone is more than a personal device. It's a mobile command center, customer file cabinet and sometimes a virtual vault. That's why keeping it secure should be a priority.

Cybercriminals are opportunists, and a compromised mobile device gives them an easy way in – no firewall needed.