

Inside This Issue

- Hackers Hate These 6 SMB
Cybersecurity Tricks
Pages 1 and 2
- Free Cyber Security Audit
Page 2
- Rocking the Business World
Page 3

wccxtcertified.com



Cyberside Chat

Smart Sharing: Location Updates Without Oversharing

Instead of sharing your location 24/7, choose “Share trip progress” in Google Maps or “Share ETA” in Apple Maps to send updates only when you’re on the move. It’s a simple, practical way to keep friends or family in the loop and stay safe during late-night rides or busy travel days.

Are You Using AI to Create Charts Yet?

You don’t need to be a design expert; you just need to know how to ask the right questions. Try prompting, “What type of chart or visual would work here?” to let AI help you turn data into clear, impactful visuals in seconds.

Innovative Tech Trends to Explore In 2025

Forget smart vacuums—2025 brings AI-powered communication coaches, advanced collaboration tools, and next-level wearable tech to transform business operations.

- 1. **AI Communication Coaches:** These tools provide real-time feedback on tone, body language, and phrasing during video calls, helping professionals improve communication and engagement. *Why it matters:* They democratize professional development, leveling the playing field for smaller businesses.
- 2. **Advanced Collaboration Tools:** AI-driven meeting

summaries, instant translation, and integrated team chats streamline remote work. *Why it matters:* They break language barriers and improve team efficiency.

- 3. **Wearable Tech:** Smart glasses, watches, and sensor-embedded clothing enhance productivity and safety in industries like logistics and healthcare. *Why it matters:* Wearables provide instant data, reducing errors and improving response times.

Embrace these innovations to future-proof your business and simplify your life in 2025!

TECHNOLOGY TIMES

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

Volume XIX, Issue 4 — April 2025 — Covington, LA

Fluffy Robot for Your Bag: Cute or Creepy?

One of CES 2025’s quirkiest (creepiest?) reveals was the Mirumi robot—a part-owl, part-sloth companion that clips to your bag and swivels its head to watch others as they stroll by. Created by Yukai Engineering, it’s equal parts adorable and unsettling—perfect for sparking conversations or just freaking out strangers on your commute.

Hackers Hate These 6 SMB Cybersecurity Tricks (And Why They Work)



The perception that SMBs have limited resources, smaller budgets and often a “that won’t happen to us” mindset makes them attractive to hackers. Although it’s true that SMBs don’t have the resources of Fortune 500 companies, you don’t need that kind of money to protect your business. Here are six simple strategies hackers hate because they’re affordable, surprisingly easy to set up and *highly* effective.

1. Two-Factor Authentication

The #1 way hackers get access to business accounts is through stolen credentials. Two-factor authentication (2FA) and multifactor authentication (MFA) have existed since the mid-2000s and remain among the best ways to protect your information. 2FA requires things to log in—your passwords and a second factor, like a text message code. If a hacker guesses or steals your password, they still can’t get past that second layer of protection. Many platforms, including Google Workspace and Microsoft 365, already offer 2FA for free. Still, it’s underutilized by SMBs, with an MFA adoption rate of only 34% or less, compared to 87% among large companies, according to JumpCloud’s 2024 IT Trends Report. 2FA is very

simple and effective—don’t sit this tip out!

2. Updates

Cybercriminals love outdated software because it’s full of unpatched vulnerabilities they can capitalize on. Ransomware attacks are notorious for targeting vulnerabilities in operating systems and applications months *after* security patches are available. Set up automatic updates for your systems, apps and software so you’re always running the latest version. Employee awareness training, regular reminders and even revoking access until patches are installed can help hold employees accountable.

3. Employee Training

Over 90% of data breaches start with phishing e-mails, CISA reports. Designed to look like real e-mails from banks, retail companies or coworkers, they are stuffed with harmful links designed to steal your passwords and data. Cybercriminals bank on naive employees who can’t tell real e-mails from fake ones, and AI is making these e-mails even harder to detect. Regular employee awareness training is one of the top defenses against phishing

Continued on Page 2...

April 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.

...Continued from Page 1.

attacks and can reduce phishing risks from 32.5% to 5% in 12 months, according to a recent study by KnowBe4. Research shows that the most effective employee awareness training includes real-world examples, simulated attacks and regular reinforcement through short, interactive training sessions.

4. Data Encryption

The modern world operates on data, and encrypting this data is the most effective method to protect it. In fact, most cybersecurity insurance policies require it. Encryption is like turning your information into code that only authorized people can unlock. Even if hackers intercept your e-mails or customer data, encryption keeps it useless to them. SMBs often hesitate due to costs or complexity, but modern tools like Google Workspace and Microsoft 365 make it simpler and more affordable.

5. Limit Employee Access

Every employee with open access to every folder, file and document significantly increases the risk of accidental (or intentional) changes to your system. Setting up limited access can feel inconvenient initially, but it doesn't have to disrupt employee

workflows. An experienced IT team will ensure that employees can run all the applications they need while having access only to what's necessary. For example, a marketing intern doesn't need the ability to access payroll data or network settings. If employees need access to complete specific tasks or projects, consider using a system that grants temporary admin access. Once their project is done, the access goes away.

6. Data Backups

Ransomware is one of the biggest threats facing SMBs today, with 46% having experienced attacks, according to a recent report by OpenText Cybersecurity. Hackers lock up your data and demand payment to get it back, but even payment isn't a guarantee you'll see your data again. Use the 3-2-1 rule—keep three copies of your data on two different types of storage media, with one stored off-site, such as in the cloud or on an external hard drive disconnected from your main network. Just as important: test your backups regularly. Nothing's worse than restoring your data after an attack, only to discover that your backups are incomplete or corrupted.

These simple, cost-effective strategies are a nightmare for hackers and a boon for SMBs looking for more peace

of mind. If any of these strategies are missing from your cybersecurity, now is the time to integrate them into your business.

FREE CYBER SECURITY AUDIT

Free cyber security audit will reveal where your computer network is exposed and how to protect your company now!

