TECHNOLOGY TIMES
Insider Tips To Make Your Business Run Faster, Easier And More Profitably

SPOOKED BY AI THREATS?

HERE'S WHAT'S ACTUALLY WORTH WORRYING ABOUT

AI is rapidly advancing – and bringing with it a whole new way to do business. While it's exciting to see, it can also be alarming when you consider that attackers have just as much access to AI tools as you do. Here are a few monsters lurking in the dark that we want to shine the light on.

Dopplegängers In Your Video Chats – Watch Out For Deepfakes

AI-generated deepfakes have become scarily accurate, and threat actors are using that to their advantage in social engineering attacks against businesses.

For example, there was a recent incident observed by a security vendor where an employee of a cryptocurrency foundation joined a Zoom meeting with several deepfakes of known senior leadership within their company. The deepfakes told the employee to download a Zoom extension to access the Zoom microphone, paving the way for a North Korean intrusion.

Creepy Crawlies In Your Inbox – Stay Wary Of Phishing E-mails

Phishing e-mails have been a problem for years, but now that attackers can use AI to write e-mails for them, most of the obvious tells of a suspicious e-mail, like bad grammar or spelling errors, aren't a good way to spot them anymore.

Threat actors are also integrating AI tools into their phishing kits as a way to take landing pages or e-mails and translate them into other languages. This can help threat actors scale their phishing campaigns.

However, many of the same security measures still apply to AI-generated phishing content. Extra defenses like multifactor authentication (MFA) make it much harder for attackers to get through, since they're unlikely to also have access to an external device like your cell phone.

Security awareness training is still extremely useful for reducing employee risk, teaching them other red-flag indicators to look for, such as messages expressing urgency.

continued on page 2...

...continued from cover

Skeleton AI Tools – More Malicious Software Than Substance

Attackers are riding on the popularity of AI as a way to trick people into downloading malware. We frequently see threat actors tailoring their lures and customizing their attacks to take advantage of popular current events or even seasonal fads like Black Friday.

So, attackers using things like malicious "AI video generator" websites or fake malware-laden AI tools doesn't come as a surprise. In this case, fake AI "tools" are built with just enough legitimate software to make them look legitimate to the unsuspecting user – but underneath the surface, they're chock-full of malware.

For instance, a TikTok account was reportedly posting videos of ways to install

"cracked software" to bypass licensing or activation requirements for apps like ChatGPT through a PowerShell command. But, in reality, the account was operating a malware distribution campaign, which was later exposed by researchers.

Security awareness training is key for businesses here too. A reliable way to protect your business is to ask your MSP to vet any new AI tools you're interested in before you download them.

Ready To Chase The AI Ghosts Out Of Your Business?

AI threats don't have to keep you up at night. From deepfakes to phishing to malicious "AI tools," attackers are getting smarter, but the right defenses will keep your business one step ahead.

Protect your team from the scary side of AI ... before it becomes a real problem.

4 'MAGIC' STRATEGIES TO BECOMING A BUSINESS LEGEND

Former NBA player Earvin "Magic" Johnson Jr. is known for his strong work ethic. Here are four strategies Magic used to build his empire that will help you achieve your goals and dreams in your business.

1. Refuse To Lose

When Magic left basketball for business, many assumed his fame made it easy. The truth was different. He struggled, made mistakes and faced rejection. "I could get the meetings," he said, "but people didn't take me seriously." He used his own money at first, but when he sought outside funding for growth, banks turned him down for three years.

Eventually, he secured a loan and invested wisely, launching his career to the next level. Ironically, the banks that once rejected him now seek his business and he often declines. Magic's takeaway: success isn't about name recognition; it's about showing a solid strategy, clear ROI and value creation.

2. Rivals Make You Better

Magic's rivalry with Larry Bird is one of basketball's most famous. "I disliked the Celtics and Larry because you have to in order to beat them," he said. But Bird's relentless work ethic pushed Magic to match him. "I knew Larry was taking 1,000 shots a day, so I had to take 1,000 shots a day. He got better, so I had to get better."

The same applies to business. Competitors force you to sharpen your skills, innovate and work harder. They can keep you awake at night but that pressure can elevate your performance.

3. Elevate Your Game

"It takes the same amount of time to do a million-dollar deal as a billion-dollar deal," Magic often says. For him, every opportunity must align with his brand, values and long-term goals. He uses a clear set of criteria: if a deal doesn't check enough boxes, it isn't worth pursuing.

Aligned values, shared revenue goals and a commitment to giving back are his markers for success. He teaches that clarity on what fits your company ensures stronger partnerships and sustainable growth.

4. Don't Let Good Enough Be Enough

Magic believes in constant evaluation and improvement. Every new business begins with a SWOT analysis (Strengths, Weaknesses, Opportunities, Threats). He doesn't stop there—he runs SWOTs on his executive team and even on himself. "I want to be a better man, husband, father, grandfather and CEO," he said. He constantly asks, "Can this team take me where I want to go tomorrow?" That mindset ensures that both he and his businesses are always evolving, never settling.

The Bigger Picture

Magic Johnson's transition from NBA superstar to successful entrepreneur was not smooth or guaranteed. He faced rejection, adapted and pushed himself the way he once did on the court. His story is a reminder that perseverance, competition, discipline and self-reflection can help anyone elevate their game—whether in sports, business or life.

SHINY NEW GADGET OF THE MONTH

LeafyPod AI-Powered Planter

LeafyPod is an intelligent planter designed to simplify plant care using real-time environmental monitoring. Powered by AI, it tracks soil moisture, sunlight exposure and watering cycles to maintain peak plant health all without the guesswork.

Perfect for office lobbies, clinics or workspaces seeking to improve air quality and add a touch of natural calm, LeafyPod blends smart technology with biophilic design. Its sleek, minimalist look makes it as stylish as it is functional.

CARTOON OF THE MONTH

"It's just a welcome mat. That doesn't count."

Marchese Computer Products, Inc.
"The Technology Experts"
220 Ellicott Street
Batavia, NY 14020

November 2025

This monthly publication is provided courtesy of Paul Marchese, President of Marchese Computer Products, Inc.

We Specialize in Security and Technology solutions for Small and Medium Businesses in our area.

We look forward to helping you achieve all your technology goals in 2025 and beyond!

4 HABITS EVERY WORKPLACE NEEDS

Most cyberattacks don't happen because of elite hackers breaking through firewalls. They happen because of small, everyday mistakes — like an employee clicking a bad link, skipping a software update, or reusing a password that's already been stolen in another breach.

The good news? A few simple habit changes can dramatically reduce your company's risk. Here are four cybersecurity habits every workplace should adopt:

1. Communication

Cybersecurity shouldn't live solely in the IT department. Talk about it openly and often. Share examples of phishing emails in your next staff meeting or circulate alerts about new scams in your industry. When security becomes a regular part of conversation, it feels less like a chore and more like a shared priority.

2. Compliance

Following regulations like HIPAA or PCI isn't just about avoiding fines — it's about protecting trust. Even if your business isn't heavily regulated, your customers still expect their data to be safe. Review your policies regularly, document staff training, and make compliance a shared responsibility across departments.

3. Continuity

If your systems went down tomorrow, how quickly could you recover? Continuity planning ensures you're prepared. Test your backups often, outline a ransomware response plan, and rehearse recovery steps so your team knows exactly what to do when minutes matter.

4. Culture

Your employees are your strongest defense. Encourage strong, unique passwords (or password managers), require MFA on all accounts, and celebrate employees who spot phishing attempts. When security feels like a team win, everyone becomes more vigilant.

Security Is Everyone's Job

Keeping your business safe isn't just about software or hardware – it's about people. By building strong habits around communication, compliance, continuity and culture, you're not just avoiding threats, you're creating a workplace that takes security seriously every day.