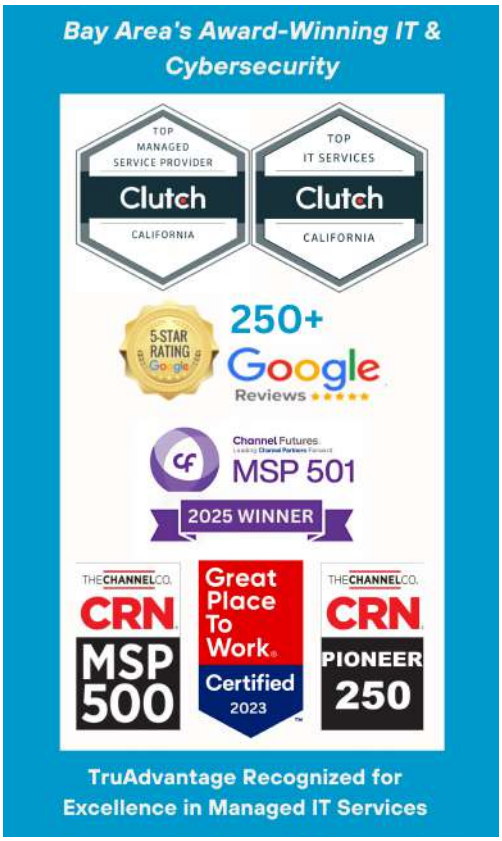
modern business IT.advisor
"Insider Tips To Make Your Small Business Run Faster. Easier, and More Profitably"



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.

For businesses, these types of scams are turning existing verification processes upside down. To identify them, look for red flags such as facial inconsistencies, long silences or strange lighting.

Creepy Crawlies In Your Inbox – Stay Wary Of Phishing Emails

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

Continued on Page 2 ...

NOVEMBER 2025

Kayvan Yazdi,
CEO of TruAdvantage

OUR MISSION:

To become a trusted partner to our clients and impact their success by delivering technology, education, and process.

... continued from Cover

Threat actors are also integrating AI tools into their phishing kits as a way to take landing pages or emails 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.

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 researchers later exposed.

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.

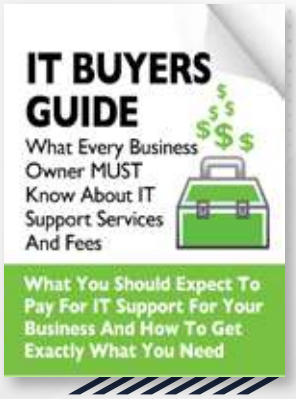
Protect your team from the scary side of AI ... before it becomes a real problem.

FREE REPORT DOWNLOAD

The Business Owner's Guide To IT Support Services And Fees

You'll learn:

- The three most common ways IT companies charge for their services and the pros and cons of each approach
- A common billing model that puts ALL THE RISK on you, the customer, when buying IT services; you'll learn what it is and why you need to avoid agreeing to it
- Exclusions, hidden fees and other "gotcha" clauses IT companies put in their contracts that you DON'T want to agree to
- How to make sure you know exactly what you're getting to avoid disappointment, frustration and added costs later on that you didn't anticipate



Claim your FREE copy today at truAdvantage.com/itbuyersguide

CARTOON OF THE MONTH

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 and started in business, people thought he had it easy, but he struggled, made mistakes and even failed. There was a lot of pain and frustration. People wanted his autograph, so they'd take a meeting but didn't take him seriously. "I could get the meetings," Magic said. "Magic Johnson got me that part, but Magic Johnson also played a role against me getting deals, too … I used my own money in the beginning, but then I wanted growth and sustainability. I wanted to go for bigger deals, and I needed other people's money to accomplish that, but they all turned me down."

It took him three years before he was finally able to get a loan. He made wise investments with that money, which took him to a whole other level in business where he is today. And all those banks that turned him down? They all want to do business with him now, and he is the one turning them down.

"It's not about name recognition," Magic said. "It's not about anything other than you having a solid business strategy. Show them how they're going to get a return on their investment and also how you're going to drive ROI."

2. Rivals Make You Better.

Magic Johnson and Larry Bird's heated rivalry is famous and well documented and added fuel to the long-standing feud between the Celtics and the Lakers. "I disliked the Celtics and Larry because you have to in order to beat them," Magic said. "But your competitor can make you better. I knew Larry Bird was taking 1,000 shots a day, so I had to make 1,000 shots a day. I knew he was working on a new move, so I had to work on a new move. I knew he was going to come back better, so I knew I had to come back better. So, I owe Larry Bird a lot because he made me better. And it's the same in business. Your competitor can make you better. You're going to work harder. They'll keep you up at night sometimes because you wonder what he is going to do next."

3. Elevate Your Game.

"It takes the same amount of time to do a million-dollar deal as a billion-dollar deal," Magic said.

His point is that you must have guidelines on what deal fits within your brand, within your system and within your company. "I've given everybody the guidelines on what I'm looking for in a deal," Magic said, "and if you can check only five of the 10 boxes, then we shouldn't be doing a deal."

For Magic, when the brands are aligned, the core values are aligned, and the revenue that they both want is aligned, along with a component to give back, that is an indication a deal will work out.

4. Don't Let Good Enough Be Enough.

Whenever he starts a business or buys one, he does a SWOT analysis right away. (A SWOT Analysis is a framework for identifying your Strengths, Weaknesses, Opportunities and Threats.) This helps him improve and grow. Not only does he do a SWOT on his executive team to see if his companies are headed in the right direction, but he also does a SWOT on himself. "I run a personal SWOT on myself because I want to be a better man, a better husband, a better father, a better grandfather and a better CEO," Magic said.

As he looks to the future, he says the question he is asking is, "Can this team take me where I want to go tomorrow? I'm asking myself that because I want to make sure when we get back to normal, I can get where I want to go," Magic said.

SHINY NEW GADGET OF THE MONTH

Tech Gadget: 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.

3031 Tisch Way,
Suite 110 Plaza West
San Jose, CA 95128

INSIDE THIS ISSUE

4 HABITS

EVERY WORKPLACE NEEDS

Most cyberattacks don't come from elite hackers. They happen because of everyday mistakes — like clicking a bad link, skipping an update or reusing a stolen password.

The good news? Small daily changes can add up to strong protection. Here are four cybersecurity habits every workplace should adopt.

1. Communication

Cybersecurity shouldn't just be IT's job. Talk with your team regularly about risks and prevention. This could mean:

- A quick reminder in a meeting on spotting phishing emails.
- Sharing news of a recent scam so staff stay alert.

When security becomes a normal topic, it feels less like "extra work" and more like second nature.

2. Compliance

Rules matter — whether it's HIPAA, PCI or protecting customer data. Compliance is about more than avoiding fines; it's about protecting trust. Even outside regulated industries, customers expect you to keep their data safe. Falling short can damage both reputation and revenue. To stay on track:

- Review policies regularly.
- Keep records of training and updates.
- Treat compliance as a shared responsibility, not an IT checkbox.

3. Continuity

If systems fail tomorrow, how fast could you recover? Continuity means being prepared:

- Ensure backups run automatically and are tested.
- Have a plan for ransomware or downtime.
- Practice recovery steps before you need them.

Even testing the restoration of a single file can prove your plan works.

4. Culture

Your people are the first line of defense. Building a security culture means weaving safe habits into daily work. Examples include:

- Encouraging strong, unique passwords or password managers.
- Requiring MFA (multifactor authentication).
- Recognizing employees who spot phishing attempts.

When security feels like a team effort, everyone improves.

Security Is Everyone's Job

Protecting your business isn't just about software or hardware — it's about people. By building habits around communication, compliance, continuity and culture, you reduce risks and create a workplace that takes security seriously every day.