CD TECHNOLOGY TIMES

Insider Tips to Help Your Business Run Faster, Easier and More Profitably

Thomas Hill, President & Founder

"To build trust, start by doing what you say you will do. As simple as this seems, it's astounding how many people simply don't do what they say they will."

TRIVIA

CONGRATULATIONS

Mary Beth Simmons

Who knew the most popular apple in the US right now is the Gala!

WORRIED ABOUT AI THREATS?

HERE'S WHAT'S ACTUALLY WORTH WORRING 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 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,

continued from cover

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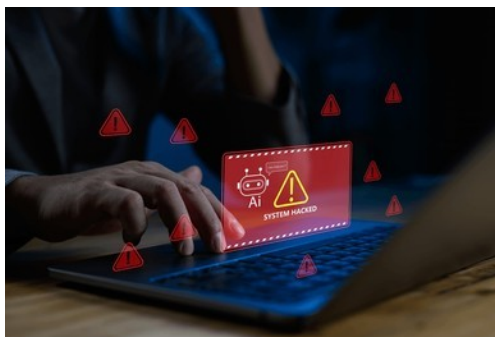
Security awareness training is key for businesses here too. A reliable way to protect your business is to ask your MSP to vet any new AI tools you're interested in before you download them.

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.

11/11   VETERANS DAY

"Mr. Wilson will see you now."

Get More Free Tips, Tools and Services At Our Website: www.CDTechnology.com

4 'Magic' Strategies
To Becoming A Business Legend

Former NBA player Earvin "Magic" Johnson Jr. is known not only for his legendary career on the court but also for his remarkable success in business. 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
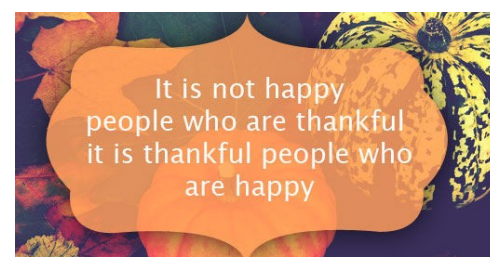
Here is your chance to win Lunch On Us!
This Month's

TRIVIA

Name ~~three two~~ an animal with a key?

Email your answer to RHill@CDTechnology.com

A winner is randomly selected from all correct entries. So it's not to late to submit your answer! Unless it is already December, then you are probably too late.

It is not happy people who are thankful it is thankful people who are happy

FALL BACK ONE HOUR! SUNDAY NOVEMBER 2

CD TECHNOLOGY
10721 Chapman Hwy #30
Seymour, TN 37865

November 2025

INSIDE THIS ISSUE

What You Really Need To Worry About When It Comes To AI | 1

Magic Johnson's Winning Strategies In Business And In Life | 3

You Could Be This Month's Trivia Winner | 2

Does Your Workplace Practice These 4 Critical Habits? | 5

CD TECHNOLOGY - AFFORDABLE IT HELPDESK AND CYBER SECURITY SUPPORT IN 20 MINUTES OR LESS

A Little Holiday Phone Tech Etiquette For Your Businesses

The holidays are stressful enough without technology tripping you up. Customers are trying to squeeze in last-minute errands, employees are juggling family schedules and everyone's expectations are cranked up. Here are two important "Holiday Tech Manners" you want to remember so you don't accidentally frustrate people with easily avoidable tech slip-ups.

1. Update Your Online Hours (Before Your First Angry Phone Call)

You don't want a customer who rushes across town during their lunch break because Google says you're open, only to find your door locked and lights off. Congratulations, you've just created someone's villain origin story.

What to update:

• Your Google Business Profile (the big one!)

• Facebook, Instagram, Yelp – anywhere customers might find you

• Your website banner with a friendly holiday schedule

• Apple Maps (yes, people actually use it)

Sample message: "Happy Holidays! We'll be closed Thursday, Nov. 28 to Sunday, Dec. 1 to spend time with family. We'll be back to regular hours Monday morning, probably with a slight turkey hangover but ready to help!"

2. Test Your Phone Systems

Holiday callers are often in a rush and already stressed. Make sure your voicemail greeting actually matches your hours and doesn't send people on a wild-goose chase.

Sample voicemail: "You've reached [Business Name]. Our office is currently closed for the holiday weekend. Please leave a message and we'll return your call Monday morning. If this is urgent, press 1 to reach our on-call team. Happy Holidays, and thanks for your patience!"

Remember: The goal isn't just to avoid problems – it's to make your customers feel taken care of, even when you're not there.

Want help making sure your systems (and your customer experience) stay polished and professional this holiday season? Let's talk about simple ways to keep everything running smoothly while you enjoy some well-deserved time off.

Book a free discovery call at www.CDTechnology.com.

4 Habits

YOU'RE DUE FOR A TECH UPGRADE

Most cyberattacks don't happen because of some elite hacker. They happen because of sloppy everyday habits – like an employee clicking a bad link, skipping an update or reusing a password that's already been stolen in another breach.

The good news? Small changes in your daily routines can add up to big protection.

Here are four cybersecurity habits every workplace needs to adopt:

1. Communication

Cybersecurity should be part of the conversation, not just something IT worries about. Talk with your team regularly about the risks they might face and how to avoid them.

For example:

- A short reminder in a staff meeting about how to spot a phishing e-mail.
- Sharing news of a recent scam in your industry so people are on alert.

When security becomes a normal part of the discussion, it feels less like "extra work" and more like second nature.

2. Compliance

Every business has rules to follow, whether it's HIPAA for health care, PCI for credit card payments or simply protecting sensitive customer information. Compliance isn't just about avoiding fines, it's about protecting trust.

Even if you're not in a highly regulated industry, your customers still expect you to safeguard their data. Falling short can damage your reputation just as much as it can hurt your bottom line.

Make sure to:

- Review your policies regularly to ensure they match current regulations.
- Keep records of training and system updates.
- Make compliance a shared responsibility, not just an IT checkbox.

3. Continuity

If your systems go down tomorrow, how quickly can your business get back up and running? Continuity is all about being prepared.

Always:

- Make sure backups are running automatically and tested regularly.
- Have a plan in place for what to do if ransomware locks up your files.
- Practice your recovery steps before you need them.

Even a simple test, like restoring one critical file from backup, can prove whether your plan really works.

4. Culture

At the end of the day, your people are your first line of defense. Building a **culture of security** means making good cyber habits part of everyday work.

Some ways to make that happen are:

- Encourage strong, unique passwords (or, even better, password managers).
- Require MFA (multifactor authentication) on all accounts that support it.
- Recognize employees who catch phishing attempts. This reinforces good habits and makes security a team win.

When security feels like a team effort, everyone gets better at it.

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.

Get More Free Tips, Tools and Services At Our Website: www.CDTechnology.com

Blount Partnership Women In Business Luncheon: A time for Encouragement, Growth, and Building Friendships

The Blount Partnership Women In Business Luncheon is one of our (Melissa and Rebekah's) favorite networking opportunities. Led by Sharon Hannum, the bimonthly Women in Business meeting is where Blount County business and professional women share best practices and discuss issues relevant to work and home life.

When the call went out for lunch sponsors, we jumped at the chance to say thank you to Sharon and WIB for what this group means to us. We has a blast serving salad bar and CfA nuggets with pumpkin roll for dessert to everyone.

Getting to mingle and connect with an incredible group of powerful businesswomen is inspiring and Sharon's devotions as well as the guest speakers are always valuable and uplifting. If you are a member of the Blount Chamber, you should defiantly have the women in your organization check out Women in Business. Meetings are every other month noon to 1p.m. You can find out more information at https://blountchamber.com/event/women-in-business/

November in East Tennessee

Welcome
Knoxville Wholesale Granite

We want to officially welcome Knoxville Wholesale Granite to our CD Technology community. Nestled in the heart of Maryville, TN, Knoxville Wholesale Granite is a family-owned and operated custom stone company, that has been transforming spaces with high-quality natural stone since 2012. They specialize in the stone industry with state of the art technology and the fast turn around times! We are happy they have chosen CDT to be their   IT provider.

KNOXVILLE
WHOLESALE GRANITE

Anthem, Arizona Veterans Memorial

On November 11 of each year at exactly 11:11 a.m., the rays of the sun stream through five pillars to perfectly spotlight The Great Seal of the United States, honoring all veterans on their day.

Get More Free Tips, Tools and Services At Our Website: www.CDTechnology.com