www.digeteks.com **NOVEMBER 2025** 





















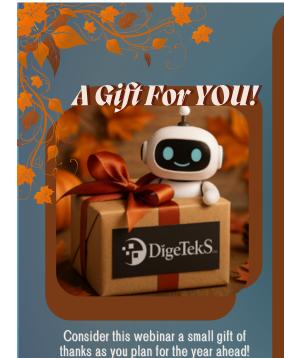






# DĭgeTekS... TECH CHRONICLE





To show our appreciation, we're inviting you to a FREE webinar:

## Build a Virtual Employee with Al

In this webinar you will learn how to:



Create a custom AI bot built specifically for YOUR business needs.



Free up valuable time, boosting productivity.



**Empower your team with** practical, real-world AI tools.

Don't Just **Imagine A** Virtual Employee.

Make It Your Reality.

Scan HERE To **Build YOU** Virtual **Employee!** 



# **Business Leaders are Giving Thanks for Smart Tech** (and smarter security)

AI is changing the way we do business, and while there's a lot to be thankful for, there's also reason to stay alert.

Cybercriminals have access to the same tools we do, which means it's more

important than ever to stay vigilant and protect what you've built.

Here are three AI threats to keep in mind and a few ways to "stuff" your defenses.



## Deepfakes In Disguise

AI-generated video deepfakes are becoming alarmingly realistic, and scammers are using them to impersonate

continued on page 2...

Tech Chronicle NOVEMBER 2025



## Black Friday & Cyber Monday Are Coming Don't Let Cybercriminals Cash In

The holiday season brings big deals, and big risks. As online shopping spikes around Black Friday and Cyber Monday, cybercriminals gear up to exploit the chaos. Before you hit "Add to Cart," take a minute to protect your personal and financial data.

## SHOPPING TIPS FOR A SAFE SEASON

## 1. Shop from reputable sites only.

Stick to well-known retailers. If that "too-good-to-be-true" offer pops up in your feed, it probably is. Check the URL for "https" and avoid clicking links from social media ads or emails you weren't expecting.

#### 2. Watch for fake sites and scams.

Cybercriminals clone real websites to trick shoppers. Always navigate directly to a retailer's official site instead of following pop-up ads or promotional links.

## 3. Use strong unique passwords.

Never reuse passwords across accounts. Better yet, use a password manager to generate and store complex ones securely. 4. Enable Multi Factor Authentication (MFA).

Adding MFA is like locking your front door and setting an alarm — it drastically reduces the chance of unauthorized access.

5. Avoid public WiFi for purchases.

Shopping from a coffee shop? Wait until you're on a secure network. Public Wi-Fi is a playground for hackers looking to intercept payment info.

**BONUS TIP:** Monitor your accounts Keep an eye on your bank statements and email alerts for unusual activity throughout the season. Quick action can stop fraud before it snowballs.

...continued from cover

executive and trusted contacts.

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.

## Phishy Emails With A Polished Look

AI tools can now craft perfect emails without typos or broken grammar, making phishing harder to spot. These scams may even translate seamlessly across languages, allowing attackers to scale their operations globally.

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.

## Fake AI Tools That Take More Than They Give

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.

## In The Spirit Of Gratitude

This Thanksgiving, be thankful for your cybersecurity team — or your MSP partner — that helps keep your data, your business, and your peace of mind protected yearround.

Strong security habits aren't just good housekeeping; they're a daily practice of protecting what matters most.



Tech Chronicle NOVEMBER 2025



## 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 Al-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.





Tech Chronicle NOVEMBER 2025



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.

#### 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.

4 · Get More Free Tips, Tools And Services At Our Website: www.digeteks.com · (833) 976-3137