TECHNOLOGY TIMES

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

IS YOUR BUSINESS TRAINING AI TO HACK YOU?

There's a lot of excitement about artificial intelligence (AI) right now, and for good reason. Tools like ChatGPT, Google Gemini and Microsoft Copilot are popping up everywhere. Businesses are using them to create content, respond to customers, write e-mails, summarize meetings and even assist with coding or spreadsheets.

AI can be a huge time-saver and productivity booster. But, like any powerful tool, if misused, it can open the door to serious problems – especially when it comes to your company's data security.

Even small businesses are at risk.

Here's The Problem

The issue isn't the technology itself. It's how people are using it. When employees copy and paste sensitive data into public AI tools, that information may be stored, analyzed or even used to train future models. That means confidential or regulated data could be exposed, without anyone realizing it.

In 2023, engineers at Samsung accidentally leaked internal source code into ChatGPT. It became such a significant privacy issue that the company banned the use of public AI tools altogether, as reported by *Tom's Hardware*.

Now picture the same thing happening in your office. An employee pastes client financials or medical data into ChatGPT to "get help summarizing," not knowing the risks. In seconds, private information is exposed.

A New Threat: Prompt Injection

Beyond accidental leaks, hackers are now exploiting a more sophisticated technique called prompt injection. They hide malicious instructions inside e-mails, transcripts, PDFs or even YouTube captions. When an AI tool is asked to process that content, it can be tricked into giving up sensitive data or doing something it shouldn't.

In short, the AI helps the attacker – without knowing it's being manipulated.

Why Small Businesses Are Vulnerable

Most small businesses aren't monitoring AI use internally. Employees adopt new tools on their own, often with good

continued on page 2...

...continued from cover

intentions but without clear guidance. Many assume AI tools are just smarter versions of Google.

They don't realize that what they paste could be stored permanently or seen by someone else.

And few companies have policies in place to manage AI usage or to train employees on what's safe to share.

What You Can Do Right Now

You don't need to ban AI from your business, but you do need to take control.

Here are four steps to get started:

1. Create an AI usage policy.

Define which tools are approved, what types of data should never be shared and who to go to with questions.

2. Educate your team.

Help your staff understand the risks of using public AI tools and how threats like prompt injection work.

3. Use secure platforms.

Encourage employees to stick with business-grade tools like Microsoft Copilot, which offer more control over data privacy and compliance.

4. Monitor AI use.

Track which tools are being used and consider blocking public AI platforms on company devices if needed.

The Bottom Line

AI is here to stay.

Businesses that learn how to use it safely will benefit, but those that ignore the risks are asking for trouble.

A few careless keystrokes can expose your businessto hackers, compliance violations, or worse.

BILLY BEANE

SHARES HIS WINNING DATA-DRIVEN STRATEGY FOR BUSINESS

A failed 2001 draft led former Oakland A's General Manager Billy Beane to overhaul how he managed talent—sparking a transformation that revolutionized baseball and inspired industries worldwide.

Using a data-driven strategy, Beane turned the low-budget Oakland A's into consistent playoff contenders. The team won seven American League Western Division titles and made 10 postseason appearances, all while operating with one of the lowest payrolls in Major League Baseball.

Beane's approach, known as the "Moneyball" philosophy, emphasized objective analysis over tradition and intuition. It gained widespread recognition through a best-selling book and Oscar-nominated film chronicling his unconventional path to success.

At a recent leadership event, Beane outlined how businesses can adopt similar principles to build high-performing teams despite resource limitations.

Make Data-Backed Decisions

"Baseball had been tracking stats since the 1800s, but none of it influenced decision-making," Beane said. "I turned running a team into a math equation." He replaced gut instinct and subjective scouting with analytics, reshaping how talent was evaluated.

Identify Undervalued Assets

"There's a championship team you can afford—you just need to find what others undervalue," Beane explained. He focused on on-base percentage, a metric more predictive of winning than traditional stats, uncovering overlooked players who delivered strong results.

Be Relentless With Execution

"You can't go back and forth," Beane said. "If you commit to data, you have to use it every time." His team stayed disciplined throughout each season, trusting the math to guide decisions rather than reacting emotionally to short-term outcomes.

Maximize The Middle

Rather than spending big on stars, Beane focused on building depth. "We couldn't afford top players, so we made sure we didn't have bad ones," he said. "A strong middle roster outperforms one with gaps."

Hire Differently

Beane recruited talent from outside traditional pipelines. One example was hiring a Harvard economics major as assistant GM—unusual in a role typically filled by former players. This fresh thinking helped the A's stay ahead.

Redefine Culture With Data

"If we did what everyone else was doing, our results would match our budget," Beane said. "We challenged the norm, used data to value skills differently and changed our outcomes."

Lead With Transparency

"Data explains decisions," he noted. "Even when you're not always right, clarity builds trust."

Level The Playing Field

Beane's philosophy proves that success isn't solely dictated by budget. With innovation, discipline and a data-first approach, even smaller organizations can compete with giants.

As he put it: "Data isn't an opinion. It's a fact."

SHINY NEW GADGET OF THE MONTH

Logitech MX Mechanical Wireless Keyboard

The Logitech MX Mechanical Wireless Keyboard delivers a premium, quiet typing experience with tactile mechanical switches for precise, low-noise feedback. Its low-profile, full-size layout enhances comfort and ergonomics, while smart backlit keys illuminate as your hands approach, adapting to lighting conditions. Seamlessly pair with up to three devices across multiple operating systems via Bluetooth or the Logi Bolt receiver. Customizable through Logi Options+, it supports efficient workflows, and its rechargeable battery lasts up to 15 days with lighting or 10 months without.

CARTOON OF THE MONTH

"I'm just sayin' a little conflict resolution trainin' might not be unwarranted."

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

September 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!

WHY PHISHING ATTACKS SPIKE IN THE SUMMER

You and your employees may be returning from summer vacations, but cybercriminals never take time off. In fact, studies from ProofPoint and Check Point show phishing attempts actually spike during summer months. Here's what you need to know to stay protected.

Why The Increased Risk?

Attackers exploit summer travel by impersonating hotel and Airbnb websites. Check Point Research found a 55% increase in newly created travel-related domains in May 2025 compared to last year. Of over 39,000 domains registered, one in 21 was flagged as suspicious or malicious. Phishing also rises during back-to-school season, when fake university emails target students and staff. Even if your business isn't directly tied to these industries, risks remain—employees checking personal email on work devices can give attackers a path into your company's data. It only takes one click.

What You Can Do

While AI has strengthened cybersecurity, it has also made phishing attacks more convincing. That's why training is critical. Teach your team to recognize red flags and practice safe online behavior.

Key safety tips:

- Double-check URLs—misspellings or unusual domain endings like .info or .today are common in scams.
- Scrutinize emails for odd sender addresses and questionable links.Visit websites directly instead of clicking links.
- Enable multifactor authentication (MFA) for added login protection.
- Use VPNs on public WiFi when accessing sensitive accounts.
- Keep personal email and social accounts off company devices.
- Ask your MSP about endpoint detection and response (EDR) software to monitor and block threats.

Phishing is growing more sophisticated daily, and AI is fueling that growth. The best defense is awareness. Keep your team informed, stay cautious, and stay safe.

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

September 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!

WHY PHISHING ATTACKS SPIKE IN THE SUMMER

You and your employees may be returning from summer vacations, but cybercriminals never take time off. In fact, studies from ProofPoint and Check Point show phishing attempts actually spike during summer months. Here's what you need to know to stay protected.

Why The Increased Risk?

Attackers exploit summer travel by impersonating hotel and Airbnb websites. Check Point Research found a 55% increase in newly created travel-related domains in May 2025 compared to last year. Of over 39,000 domains registered, one in 21 was flagged as suspicious or malicious. Phishing also rises during back-to-school season, when fake university emails target students and staff. Even if your business isn't directly tied to these industries, risks remain—employees checking personal email on work devices can give attackers a path into your company's data. It only takes one click.

What You Can Do

While AI has strengthened cybersecurity, it has also made phishing attacks more convincing. That's why training is critical. Teach your team to recognize red flags and practice safe online behavior.

Key safety tips:

- Double-check URLs—misspellings or unusual domain endings like .info or .today are common in scams.
- Scrutinize emails for odd sender addresses and questionable links. Visit websites directly instead of clicking links.
- Enable multifactor authentication (MFA) for added login protection.
- Use VPNs on public WiFi when accessing sensitive accounts.
- Keep personal email and social accounts off company devices.
- Ask your MSP about endpoint detection and response (EDR) software to monitor and block threats.

Phishing is growing more sophisticated daily, and AI is fueling that growth. The best defense is awareness. Keep your team informed, stay cautious, and stay safe.