truadvantage

800-650-4144 • truAdvantage.com

modern business IT.advisor

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

Bay Area's Award-Winning IT & Cybersecurity

TruAdvantage Recognized for Excellence in Managed IT Services

SEPTEMBER 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.

IS YOUR BUSINESS TRAINING AI HOW 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*.

Continued on Page 2 ...

... continued from Cover

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 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 whom to go to with questions.

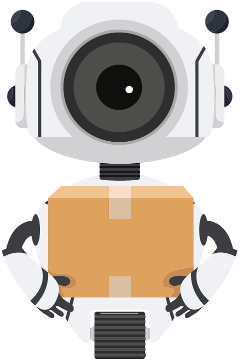
2. Educate your team.
Help your staff understand the risks of using public AI tools and how threats like prompt injection work.

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.

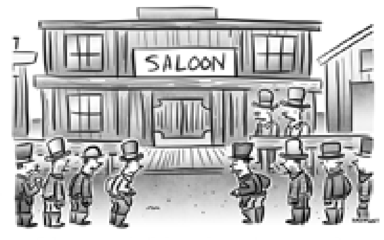
The Bottom Line

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 business to hackers, compliance violations, or worse.

CARTOON OF THE MONTH



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

BILLY BEANE

SHARES HIS WINNING DATE-DRIVEN STRATEGY FOR BUSINESSES

A disastrous 2001 MLB draft led former Oakland A's General Manager Billy Beane to overhaul how he managed talent — an approach that ultimately revolutionized not only his team but the game of baseball itself.

Using a groundbreaking, data-driven strategy, Beane transformed the Oakland A's into consistent contenders, achieving seven American League Western Division titles and 10 playoff appearances. This was accomplished despite having one of the smallest payrolls in Major League Baseball.

This methodology became known as the "Moneyball" philosophy, popularized by the bestselling book and Oscar-nominated film that detail Beane's journey from overlooked GM to management icon. His success has inspired leaders across industries to rethink how they assess and build teams.

At a recent event, Beane shared how businesses can apply his data-first philosophy to build winning teams — even when resources are limited.

Make Data-Driven Decisions

"Baseball has tracked player stats since the 1800s, but few used that data for actual decision-making," Beane said. "I turned running a baseball team into a math equation." By relying on objective analysis rather than gut instincts or traditional scouting, Beane changed how teams evaluate players — building one of the most efficient rosters in sports.

Find Undervalued Metrics

"There is a championship team you can afford," he asserted. Beane realized that statistics like on-base percentage had a stronger correlation with wins than traditional metrics like batting average. By identifying undervalued stats, he was able to uncover hidden gems passed over by other teams.

Commit To Consistency

"You can't go back and forth," Beane said. "You have to use data every single time." Once the season started, Beane didn't panic or change course. His team stuck to its data-backed strategy. "Using data is like having the answers to the test. It's only effective if you follow it consistently."

Maximize Existing Resources

Rather than chasing expensive superstars, Beane focused on eliminating weaknesses. "We couldn't afford the top talent, so we made sure we didn't have bad players," he said. "A balanced roster of solid contributors can outperform a top-heavy one."

Expand Hiring Criteria

Beane also brought in nontraditional candidates. One notable hire was Paul DePodesta, a Harvard economics major with no playing background, who became a key architect of the A's strategy. "He wasn't what people expected—but he changed the way we operated."

Challenge The Status Quo

"If we ran our team like the other 29 teams, we were destined to finish where our payroll ranked," Beane explained. "We had to challenge baseball's traditions and redefine how we valued players — through data."

Manage Emotions

Beane avoided watching games live to prevent emotion from clouding judgment. "I didn't want decisions made in the heat of the moment. I trusted the numbers."

Lead With Clarity

"Data lets you explain why a decision is being made," he said. "Even if it's not always right, it brings transparency and alignment."

Build Custom Metrics

Beane's team developed proprietary models to assess players' current and future performance. "We built systems to measure process—not just results," he noted.

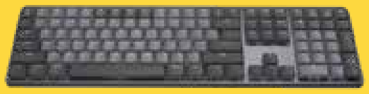
Leveling the Playing Field

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 the 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.

truadvantage

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

INSIDE THIS ISSUE

WHY PHISHING ATTACKS SPIKE IN THE SUMMER

As you and your team return from summer vacations, cybercriminals remain hard at work. In fact, phishing attacks often spike during the summer, according to research from ProofPoint and Check Point.

Why The Increase?

Hackers take advantage of summer travel habits by impersonating hotel and vacation rental websites. Check Point Research reported a 55% increase in newly registered vacation-related domains in May 2025 compared to the same time last year — over 39,000 in total. Alarmingly, 1 in 21 of these were flagged as suspicious or malicious.

Late summer also marks back-to-school season, which brings a wave of phishing emails mimicking university communications — targeting both students and staff. While these may seem unrelated to your business, the real risk lies in employees checking personal e-mails on work devices. One wrong click can expose your entire company's data.

What You Can Do

While AI helps improve cybersecurity, it also makes phishing emails harder to spot. Training your team to recognize threats is essential.

Tips to Stay Safe:

Scrutinize e-mails. Don't rely on spotting typos — AI can generate clean, polished messages. Instead, examine sender addresses and hover over links to check their authenticity.

- **Watch for suspicious URLs.** Domains like .info or .today often signal scam websites.
- **Type URLs yourself.** Rather than clicking on links, visit websites by typing the URL directly.
- **Enable MFA.** Multifactor authentication protects login credentials and the data behind them — even if passwords are compromised.
- **Use VPN on public WiFi.** This adds a layer of security when accessing sensitive info away from the office.
- **Keep work and personal devices separate.** Avoid checking personal e-mails or social media on work machines.
- **Ask about endpoint protection.** Tools like EDR software can detect and block threats, alerting IT teams instantly and minimizing damage.

Phishing tactics are evolving fast, especially with AI. Regular education and vigilance are your best defense. Stay sharp — stay safe.