NEWSLETTER

RJ2 Technologies Monthly Newsletter
September 2025

1701 Golf Road
Suite T3-300
Rolling Meadows, IL 60008

(847) 303-1194

www.rj2t.com

In this newsletter:

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.

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.

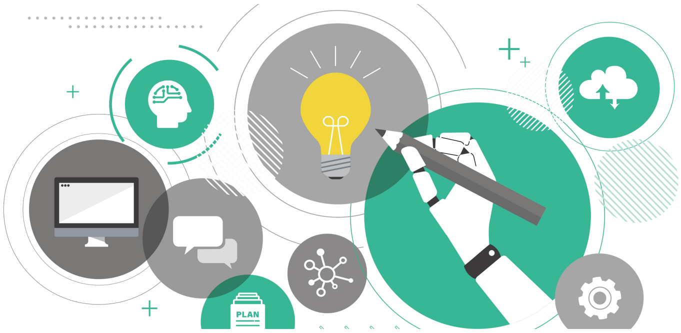
A New Threat: Prompt Injection

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 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 business to hackers, compliance violations, or worse.

Need help with AI?
Call RJ2 Technologies at (847) 303-1194 or email marketing@rj2t.com for more information.

Get Fresh IT News Weekly with RJ2 Technologies!

Follow us on our social media pages for more IT content, latest tech trends, company updates, tech tips and more. Connect with the RJ2T family and show your support!

@RJ2Technologies @RJ2Technologies @RJ2Technologies

@RJ2Technologies @RJ2Technologies532

Why Phishing Attacks Spike In The Summer

You and your employees may be getting back from vacation, but cybercriminals never take a day off. In fact, data shown in studies from vendors ProofPoint and Check Point indicate that phishing attempts actually spike in the summer months. Here's how to stay aware and stay protected.

Why The Increased Risk?

Attackers use your summer travel bug to their advantage by impersonating hotel and Airbnb websites, says Check Point Research. They've uncovered a sharp increase in cyberthreats related to the travel industry – specifically, a 55% increase in the creation of new website domains related to vacations in May 2025, compared to the same period last year. Of over 39,000 domains registered, one in every 21 was flagged as either malicious or suspicious.

August/September is also back-to-school time, which means an uptick in phishing attempts imitating legitimate university e-mails, targeting both students and staff. While these threats might not affect your industry directly, there's always a chance that employees pursuing their master's degree or planning a vacation will check their personal e-mail on their work computer – and it takes only one wrong click for cyberattackers to have access to all of your business's data.

What To Do About It

While AI is making cybersecurity stronger and workflows smoother, it's also making phishing attacks more convincing. That's why it's important to train yourself and your team on what to look for, to avoid clicking on a malicious link.

Safety tips to prevent attacks:

- Keep an eye out for shady e-mails. Don't only check for misspellings and poorly formatted sentences in the body of e-mails; AI can write e-mails for attackers just like it can for you. Also examine the e-mail address of the sender and the text of the link itself, if visible, to make sure everything looks legitimate.
- Double-check URLs. Misspellings in the link text or unusual domain endings, like .today or .info, can be an indicator of an attack. Domain endings like these are often used in scam sites.
- Visit websites directly. It's always better to search for the website yourself, rather than clicking on links in any messages or e-mails.
- Enable Multifactor Authentication (MFA). Setting up MFA ensures that even if a breach does occur within your company, your login credentials will remain protected – and so will any data secured behind them.
- Be careful with public WiFi. If you need to use public WiFi, use a VPN for additional protection when accessing secure information, like booking portals or bank accounts.
- Don't access personal e-mail on company devices. Accessing personal e-mail, messaging or social media accounts on business devices increases your risk. Keep personal accounts on your personal devices, and work-related accounts on the work devices.
- Ask your MSP about endpoint security. Endpoint detection and response (EDR) software can monitor your desktops and mobile devices, detect and block phishing attempts and malicious downloads, and alert your MSP immediately in the event of a breach, drastically limiting your data's exposure.

Phishing attempts become more sophisticated every day, and AI is only speeding that process along. Because of this, it's essential to keep your team well-informed of the risks; knowledge is the best defense against phishing attacks. Stay informed and stay safe!

Call RJ2 Technologies at (847) 303-1194 or email marketing@rj2t.com for more information.

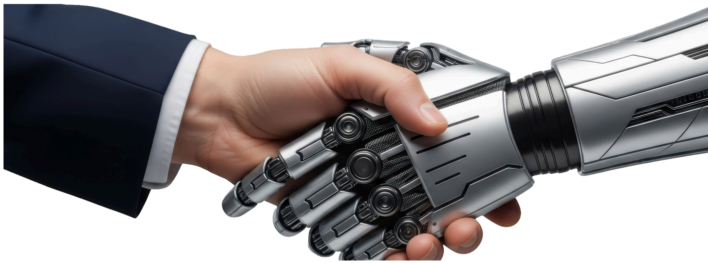
Vendor Partner Highlight - Hatz AI

This month we are excited to highlight Hatz.AI, a powerful solution for secure, scalable. and easy-to-use AI platform designed for businesses. This solution helps businesses streamline operations and elevate the customer experience.

RJ2 Technologies is proud to partner with Hatz.AI as it provides private, organizationally managed access to multiple large language models (LLMs), ensuring your data stays protected while enabling advanced AI capabilities. It's built with compliance and security at its core, giving businesses peace of mind as they adopt AI.

To learn more about this partnership please call RJ2 Technologies at (847)-303-1194 or email marketing@rj2t.com

Get To Know Your Artificial Intelligence: Generative AI vs. Agentic AI



Artificial intelligence seems to come with a new buzzword every week. You'd be forgiven for getting lost among the jargon. Generative AI… agentic AI… large language models… it's no wonder many business owners feel overwhelmed. But at the heart of it are two types of AI that could change how businesses like yours work:

- Generative AI
- Agentic AI.

And no, they're not the same thing.

Generative AI is the type most people have come across by now, such as Chat GPT. Simply put, it creates something when asked, whether that's writing text, generating images, or summarizing reports. It's great for saving time on routine tasks. But it's reactive. It waits for instructions. You ask, it delivers.

Agentic AI takes things further. This is AI that doesn't just wait for a prompt, it acts. Give it a goal, and it can figure out what to do, plan the steps, and get on with the job.

Imagine AI that helps reduce customer churn by spotting patterns in data, testing ideas, and even launching follow-up campaigns, all without your constant input.

Both types of AI can be powerful tools for businesses:

Generative AI boosts productivity by helping create content or ideas faster.

Agentic AI helps businesses work smarter by taking initiative and handling tasks more independently. But with that extra autonomy comes the need for more oversight. Agentic AI relies on good data and clear guardrails to make sure it acts in the right way.

So, is it for you?

Whether it's AI that creates or AI that acts, these tools can support your team and help your business run more efficiently… so long as they're used thoughtfully.

If you're interested in seeing how AI could boost productivity in your business, we can help. Get in touch. **Call RJ2 Technologies at (847) 303-1194 or email marketing@rj2t.com for more information.**