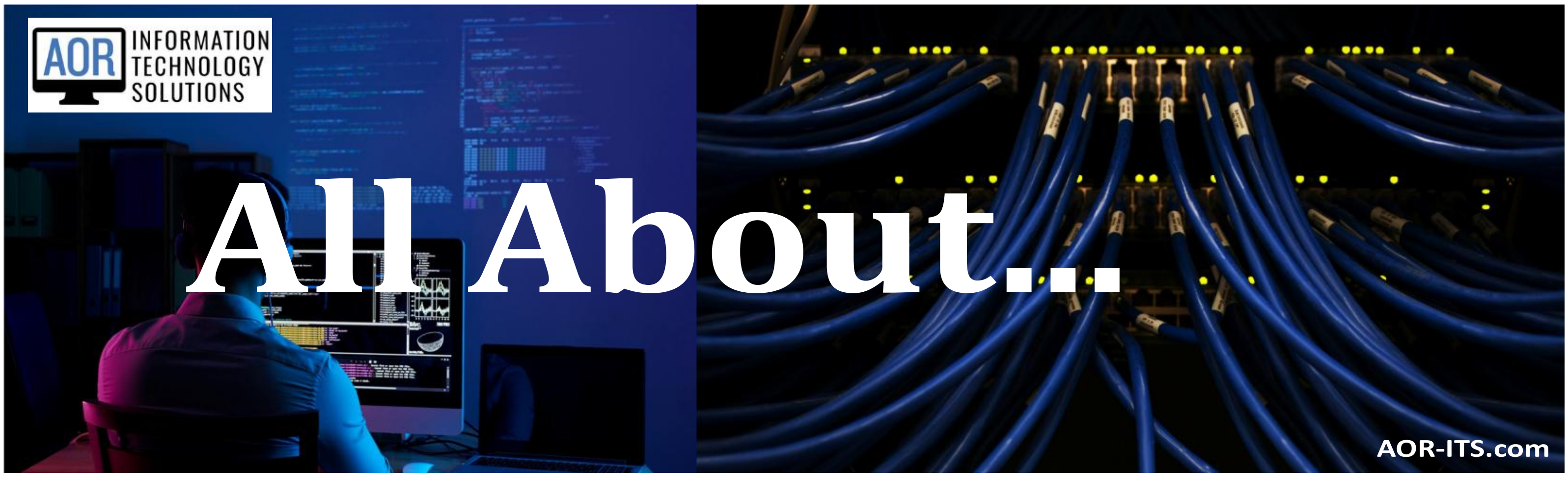

# Is Your Business Inadvertently Training AI On How To Hack You?

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.

Let's have a quick conversation to make sure your AI usage isn't putting your company at risk. We'll help you build a smart, secure AI policy and show you how to protect your data without slowing your team down. Book your call now.

**AND click here to book your FREE Cybersecurity Assessment**

**Questions? Call our Glenside, PA office today at 267-699-2551. Or visit us on the web at AOR-ITS.com to learn more about our proven managed IT solutions, including cybersecurity, for small local businesses.**