It's happening, **whether you like it or not**

AI tools are becoming a normal part of the working day.

Someone uses one to tidy up a report. Someone else asks a chatbot to summarize meeting notes. A team member installs an AI browser extension because it helps them work faster.

Most of this happens with good intentions.

But some businesses have no visibility of it at all.

This is known as "shadow AI".

It describes employees using AI tools that haven't been approved, reviewed, or properly managed by the business.

In many ways, it's like shadow IT, where staff adopt their own software without involving the IT team.

The difference is that AI tools can interact with company information in deeper ways.

Employees may paste confidential documents into public chatbots, connect AI assistants to email accounts, or allow AI tools to access files and calendars without fully understanding what happens to that data afterwards.

The motivation is easy to understand. These tools save time, reduce admin, help people get through work more efficiently.

So, banning AI outright rarely works.

If employees feel the tools genuinely help them, they often continue using them secretly. At that point, the business loses even more visibility and control.

The better approach is usually to accept that AI is now part of modern work, then guide people towards safer, approved options.

Newer AI systems are becoming more capable very quickly. Tools are no longer limited to generating text or summaries. They can search files, access systems, organize information, trigger workflows… and even carry out actions automatically.

Without proper oversight, that creates obvious security and compliance concerns.

For businesses using Microsoft 365, approved tools like Copilot offer a safer route because they sit inside existing permissions and security controls.

That doesn't remove risk completely, but it does give businesses much better visibility over how AI is being used.

Whatever tools you're using, the important thing is not to ignore the issue.

If you need better oversight on how your team is using AI tools, we can help.

Get in touch.

Productivity tool of the month

Power Automate makes everyday tasks easier

You know those small repetitive jobs that eat away at your day?

Renaming files, sorting attachments, copying information from one place to another, opening the same apps every morning….

Power Automate, built into Windows 11 Pro, can handle those kinds of tasks automatically.

And better yet, you don't need to know how to code. You can create simple automations using drag-and-drop tools or even record yourself doing a task once and let Power Automate turn it into a reusable workflow.

It's one of those tools many businesses already have but rarely realize how much time it could save them.

Install it from the Microsoft Store.

?A

Q: Are smaller businesses really targeted by hackers?

A: Absolutely. Many attacks are automated and look for easy opportunities, regardless of business size.

Q: What's the easiest way to make staff more cyber aware?

A: Regular short reminders and training tend to work better than one big annual session. People are more likely to remember guidance that fits into day-to-day work.

Q: Does our Wi-Fi need a separate guest network?

A: If you have visitors, yes. It reduces the risk of someone accidentally accessing company devices, files, printers, or other sensitive parts of the network.

This is how you can get in touch with us:

CALL: (661) 750-8402 | EMAIL Daniel@GoldenHillsIT.com

WEBSITE: www.GoldenHillsIT.com

AUGUST 2026

Your monthly newsletter, written for humans not geeks

TECHNOLOGY INSIDER

The threats hiding in the tools **you use everyday**

How do you imagine a cyberattack?

A sophisticated hacker breaking through layers of security? Using advanced tools that no regular business could possibly defend against?

The reality is usually way less glamorous.

Many breaches start with something small. A forgotten account that was never removed. A laptop that missed an update. A security setting that was switched off and never switched back on.

These are the kinds of gaps attackers actively search for because they're far easier to exploit than forcing their way through a heavily protected system.

In other words, the danger often comes from the things nobody realized were a problem.

One of the biggest changes in cybersecurity right now is the growing focus on identities.

Instead of attacking systems directly, criminals increasingly target usernames and passwords.

Once they gain access to a legitimate account, they can move through a business much more easily because, from the outside, it looks like a normal user logging in.

That can happen surprisingly quickly. In some cases, ransomware attacks have escalated within hours of the initial breach.

The challenge is that modern businesses are complicated.

Staff work remotely. Devices move between home and office. New software gets introduced. Small gaps appear naturally, unless someone is constantly monitoring them.

Even security tools themselves can become blind spots.

You may have protection installed, but if it is misconfigured, outdated, or partially disabled, it creates a false sense of security.

Attackers also rely heavily on something known as "living off the land" techniques. This means using legitimate tools already built into Windows and Microsoft 365 to carry out malicious activity.

Because those tools are commonly used by IT teams every day, suspicious behavior can blend into normal activity more easily.

Artificial intelligence is likely to accelerate this problem.

AI tools can help criminals identify weaknesses faster, automate attacks, and adapt techniques more quickly than before.

But many of the most effective protections are still the basics done well.

Strong passwords, multi-factor authentication, regular updates, controlled access permissions, and ongoing staff awareness training remain some of the strongest defenses available.

If you'd like help spotting and closing small security gaps before somebody else finds them, get in touch.

DID YOU KNOW…

that might not really be support?

The FBI has warned businesses about a cybercrime group pretending to be IT support staff.

Attackers have reportedly gone as far as turning up in person at offices after first contacting staff by phone. They pose as technicians fixing a problem, then copy sensitive files onto external drives and install malware in the background.

Staff awareness and clear verification processes for visitors and support requests are just as important as technical security controls.

TechFacts

1 A study found that many employees exaggerate their AI skills at work. Around two-thirds of workers admitted overstating their AI knowledge. They feel pressure to appear more employable or future-ready. Among younger workers, that number rose to 80%. Most said they plan to learn the skills eventually… they just don't want to look behind in the meantime.

2 China has started operating an underwater data center sitting 35 meters beneath the ocean surface. Instead of using huge air-conditioning systems to keep servers cool, the facility uses naturally cold seawater surrounding the sealed server pods. The site reportedly contains around 2,000 servers and is powered partly by offshore wind energy.

3 A company reportedly spent an astonishing $500 million in a single month on AI tools after forgetting to set usage limits for employees. According to reports, staff were freely using AI systems like Claude across the business, with costs spiraling in the background.

INSPIRATIONAL QUOTE OF THE MONTH

"If you're not failing every now and again, it's a sign you're not doing anything very innovative."

Woody Allen,
filmmaker and actor.

NEW TO

MICROSOFT

Microsoft may quarantine infected devices

A new security feature is being tested in Microsoft Defender for Endpoint.
It can automatically isolate a compromised device before an attack spreads across the network.

If suspicious activity is detected, the affected computer can be cut off from the rest of the business, while remaining connected to Microsoft's security systems for monitoring and investigation.

The goal is to slow attackers down quickly, helping prevent ransomware, data theft, and wider disruption.

Technology update

Google's AI overhaul

Google is giving Search its biggest overhaul in more than 25 years, of course, building in more AI.

The search box is being redesigned to handle longer, more conversational questions, along with AI-powered suggestions and image-based searches.

Google says traditional website links will still appear, but AI-generated summaries are expected to play a much bigger role in what people see first.

Debug your tech knowledge for this month's quiz...

1. What was the first item to be scanned using a barcode?
2. Which company popularized the term "Tablet PC" in 2001?
3. What was the name of the first social networking site launched in 1994?
4. What was eBay.com originally called?
5. What is a technical term for the "brain" of the computer?

The answers are below.

1. Wrigley's gum
2. Microsoft
3. GeoCities
4. Auctionweb
5. CPU (Central Processing Unit)