idea LOGICAL

JUN 2026

LogicalTalk

Making sense of what's new in IT

Where are your files really going?

When people talk about "moving to the cloud", it can sound like a single decision, but there are a few different ways to do it. The right choice depends on how your business works.

At its simplest, cloud storage means your data isn't stored on a single computer or server in your office.

Instead, it's stored in secure data centres run by providers (like Microsoft) and accessed over the internet.

That's what allows you to open files from anywhere, share them instantly, and collaborate in real time, but not all cloud setups are the same.

The most common approach is what's known as the public cloud. This is where your data is stored on shared infrastructure managed by a provider. Tools like Microsoft 365 and OneDrive fall into this category.

You're effectively renting space in a highly secure, always-available environment, without needing to maintain any hardware yourself.

At the other end of the spectrum is private cloud.

This is where the infrastructure is dedicated to your business, either hosted on-site or in a data centre.

It offers more control and can be useful for organizations with specific security or compliance requirements. But it also comes with more responsibility and cost.

Some businesses sit somewhere in the middle with a hybrid setup.

That might mean everyday files and collaboration tools live in the public cloud, while more sensitive systems or data are kept in a private environment.

It gives you flexibility to balance accessibility, control, and risk.

Whichever route you take, the benefits tend to be similar:

- Your team can access what they need from anywhere
- You can scale storage up or down without buying new equipment
- And your data is protected by enterprise-grade security, including encryption and multiple backups across different locations

The important thing is that "the cloud" isn't a one-size-fits-all solution.

The way it's set up should reflect how your business operates, what data you handle, and how your team works day to day.

did you know...

staying connected is a good thing?

A senior Microsoft executive has confirmed engineers are exploring ways to make it easier to set up a PC without needing a Microsoft account. Nothing is confirmed yet, but it shows the setup experience is evolving.

That said, using a Microsoft account still unlocks the full benefits of Windows, including seamless access to Microsoft 365, cloud storage, and built-in security features.

So, while more choice may be on the way, most businesses will still get the best experience by staying connected.

416 410 5030
connect@idealogical.com
idealogical.com

Tech Facts

1. A humanoid robot can now play tennis and rally with human players using a new training method called LATENT. This teaches it from small snippets of human movement rather than perfect data. The result is a robot that can react in real time, return shots consistently, and even place the ball strategically during play.

2. Back in Windows 95, installing new software could accidentally break your system by replacing important files with older versions. Microsoft's solution was simple. Windows kept hidden backup copies and restored anything that got overwritten after the installation finished, all without telling you.

3. Most people know what AI is, but many still aren't convinced they need it. A recent study found that while awareness is high, around two-thirds of sceptical users don't see a real need for AI on their devices. The biggest concerns are privacy and cost, not complexity. Interestingly, younger people are far more open to it, while older groups are more cautious.

Technology Update

Joining a Microsoft Teams meeting gets less frustrating

Microsoft is phasing out those familiar CAPTCHA checks (the "prove you're not a robot" tests) and replacing them with a smarter system that detects bots automatically.

Instead of making every user jump through hoops, the system will flag anything suspicious and let the meeting organizer decide what to allow.

That's a win. Less friction for you and your people, and better control behind the scenes.

"The most effective way to do it, is to do it."

Amelia Earhart,
Aviation Pioneer

NEW TO

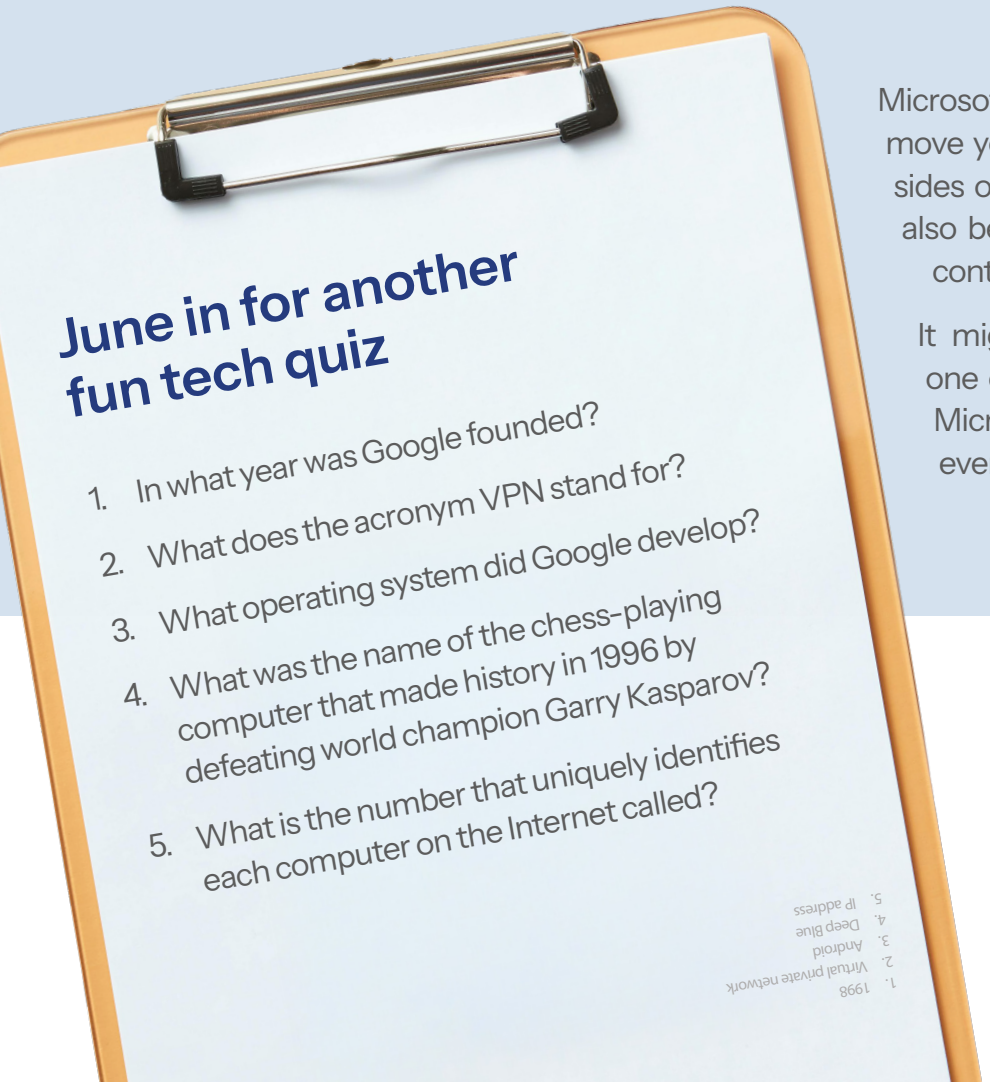
MICROSOFT

AI

A familiar feature returns to Windows 11

Microsoft has confirmed you'll soon be able to move your taskbar again, placing it at the top or sides of your screen, not just the bottom. You'll also be able to adjust its size, giving you more control over how your desktop looks and feels.

It might sound like a small change, but it's one of the most requested updates. It shows Microsoft is focusing more on usability and everyday experience, not just adding new features.



Everyone's talking about AI, but what are the risks?

Do you feel like you're being nudged towards AI from every direction right now?

Business owners, managers, even staff are all seeing the same thing: New tools promising to save time, reduce workload, and make life easier.

And in many cases, they do.

But behind the excitement, there's another conversation happening.

"What could go wrong?"

Interestingly, most businesses already know there are risks. But many are moving ahead anyway, often because they feel they can't afford to fall behind competitors.

That creates an uncomfortable situation.

AI tools are becoming more powerful, and in some cases, more independent.

You might have heard of an "AI agent". This is a tool that can take actions on your behalf, like accessing files, sending messages, or interacting with other software.

And it's where one of the biggest concerns comes in.

If an AI tool has access to your systems, it also has access to your data.

Without the right controls, there's a risk that sensitive information could be shared unintentionally.

The AI has the potential to follow instructions too literally or be tricked by what's known as a "malicious prompt". That could be something as simple as a cleverly written email that causes the AI to behave in a way you didn't expect.

There's also the issue of visibility.

In many businesses, different teams are experimenting with different AI tools. Some are approved. Others aren't.

Over time, it becomes harder to track what's being used, what data is being shared, and where it's going. This is often called "shadow AI", and it's becoming increasingly common.

On top of that, the technology itself is evolving quickly. Faster than most organisations can comfortably keep up with from a security or policy point of view.

All of this might sound concerning, but it doesn't mean you should avoid AI. Rather, you should approach it with structure.

Choose approved tools, set clear rules around data use, and make sure someone has oversight of how AI is being used across the business.

And if you need guidance on any of this, don't be afraid to ask for help. If you'd like to talk about how AI can help your business, get in touch.

Q&A

Q: What's the biggest security risk for small businesses?

A: Usually people, not technology. Weak passwords, phishing emails, and poor access control cause most issues.

Q: Should my business be using AI yet?

A: Yes, but in a controlled way. Start with trusted tools and clear guidelines rather than letting everyone experiment freely.

Q: My team keeps using new tools. Is that a problem?

A: It can be if it's unmanaged. It's best to standardise tools so you keep control of data and security.

idea LOGICAL