idea LOGICAL

APR 2026

LogicalTalk

Making sense of what's new in IT

Would your business survive a serious cyber attack?

It's not a comfortable question, and it's one many small and medium sized business owners assume they never really need to answer.

Cyber attacks feel like something that happens to other people. Big brands. Global companies. Organisations with huge IT teams and budgets. The reality is very different.

Recent research shows that a worrying number of businesses believe they simply wouldn't survive a major cyber incident. That might sound dramatic, but it's a fair reflection of how exposed many businesses still are.

Cyber attacks have changed. They're no longer just a hacker guessing a password. Attacks today are faster, more targeted, and often designed to shut a business down completely.

Ransomware, for example, is a type of attack where criminals lock your systems and demand payment to unlock them. If you can't access your data, your systems, or your customer information, normal business stops very quickly.

What's interesting is that most business leaders know the risk is rising. Many openly admit they expect their staff to fall for a phishing attack.

Phishing is when a fake email or message pretends to be legitimate, tricking someone into clicking a link or handing over login details.

That single mistake can be all an attacker needs. Despite this awareness, the basics are still being missed.

Password reuse is a big one. If someone uses the same password at work and across multiple personal accounts, one breach can quickly turn into many.

Cyber criminals know this, which is why stolen passwords are so valuable.

Basic cyber awareness training is another gap. Many employees have never been shown what to look out for or how to spot common scams.

But it's not all doom and gloom. High-profile attacks have made business owners more alert, especially around newer threats like AI-driven scams and deepfake video calls that pretend to be senior leaders. That growing scepticism is healthy.

The most important thing to understand is that surviving a cyber attack doesn't need expensive tools or complex technology.

Preparation is your best tool.

Simple steps like strong, unique passwords and regular staff training make a real difference.

did you know...

Microsoft wants to be a good neighbour?

AI data centres continue to pop up around the world. It comes as no surprise that some communities are starting to ask questions.

These facilities can place heavy demands on local electricity, water supplies and land, which has raised understandable concerns.

In response, Microsoft has announced a new "Community-First AI Infrastructure Plan". It promises to be a better neighbour by covering infrastructure costs, reducing and replenishing water use, being open with communities, and investing in local jobs, training and services wherever new data centres are built.

416 410 5030

connect@idealogical.com

idealogical.com

Tech Facts

1

Anguilla has accidentally struck digital gold. Thanks to the global AI boom, over a million .ai website domains are now registered... and Anguilla controls them. That brings in around $70 million a year - roughly a fifth of the government's total income. Even big names like Google and Perplexity pay for them.

2

The modern internet might look very different if not for one generous decision. In April 1993, Tim Berners-Lee persuaded scientific research organisation, CERN, to release the World Wide Web into the public domain. That meant anyone could use it for free, with no licenses or fees. Many historians see this moment as the true birth of the web and a huge reason it spread so fast.

3

The first recorded death caused by an industrial robot happened in 1979. A 25-year-old factory worker named Robert Williams was killed by a robotic arm at a Ford Motor Company plant in Flat Rock, Michigan. The tragic incident led to a landmark court case and a record compensation payout at the time. And it permanently changed how seriously safety around robots in factories is taken.

Technology Update

Microsoft Teams should feel faster and more reliable

Microsoft has confirmed a behind-the-scenes performance upgrade for Teams on Windows. And it's more important than it sounds.

Teams is being re-engineered so that call handling (one of its most demanding tasks) runs in its own dedicated process.

By separating calls from the rest of the app, Teams should start faster, use system resources more efficiently, and deliver smoother meetings.

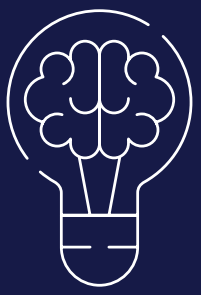
There's no change to how Teams looks or works, but you may need to update security or device management tools, so the new process isn't mistakenly blocked.

"Don't be intimidated by what you don't know. That can be your greatest strength and ensure that you do things differently from everyone else."

Sara Blakely,
Businesswoman
and Philanthropist

NEW TO

MICROSOFT



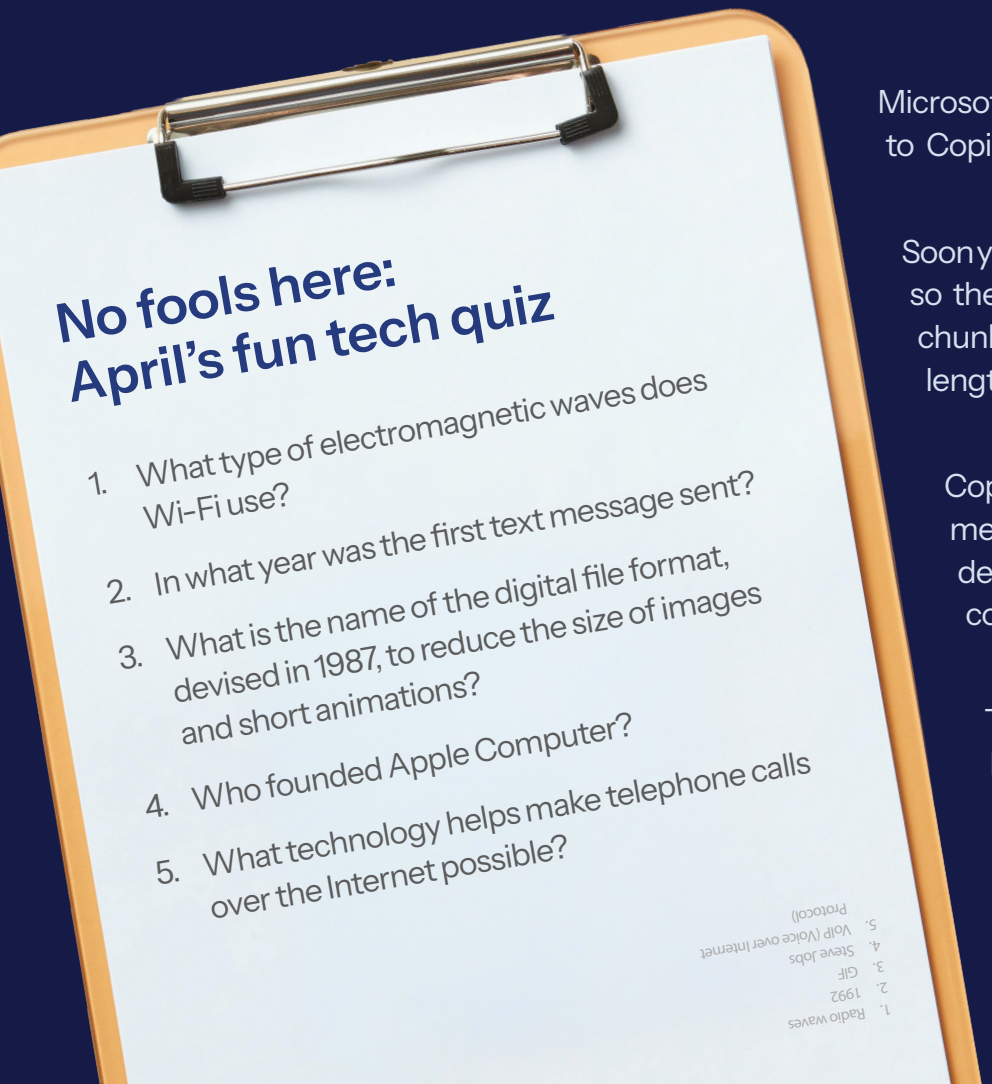
Copilot gets smarter (again)

Microsoft is rolling out a set of practical upgrades to Copilot designed to make it more useful for everyday work.

Soon you'll be able to pin important conversations so they don't get lost, work with much longer chunks of text, and ask Copilot to summarise lengthy chats or turn them into usable documents.

Copilot is also gaining a more advanced memory feature. It can remember helpful details from past conversations, with clear controls so you can see, manage or delete what it remembers.

These updates are inspired by how Microsoft CEO, Satya Nadella, uses Copilot. They're already gradually rolling out.



No fools here: April's fun tech quiz

1. What type of electromagnetic waves does Wi-Fi use?
2. In what year was the first text message sent?
3. What is the name of the digital file format, devised in 1987, to reduce the size of images and short animations?
4. Who founded Apple Computer?
5. What technology helps make telephone calls over the Internet possible?

1. Radio waves
2. 1992
3. GIF
4. Steve Jobs
5. VoIP (Voice over Internet Protocol)

The real reason you're struggling with AI

AI has become a regular topic in business conversations.

It comes up in meetings, strategy days and vendor pitches.

Yet for all the talk, many organisations are still struggling to turn AI from an interesting idea into something that genuinely helps people do their jobs.

In many organisations, AI is stuck in a trial phase.

Someone experiments with a tool. A small pilot runs for a few weeks. Then progress slows. The AI works, but businesses struggle to move from experimentation to everyday use. The return on investment everyone expects stays just out of reach.

Uncertainty is usually to blame.

Leaders worry about security, privacy and compliance. They're unsure what data AI tools are allowed to see or how decisions are being made. Others admit they don't yet have a clear business case, so AI becomes something interesting rather than something essential.

Another big factor is confidence.

Many employees are curious about AI, but also nervous. They worry about making mistakes, relying on the wrong answers, or using tools incorrectly.

Without clear guidance, people either avoid AI altogether or use it quietly and inconsistently. That creates risk and limits the benefits.

It's a shame, because when AI is used properly, the gains are very real. Teams can respond to customers faster, spot issues earlier, analyse data more easily and reduce time spent on repetitive admin.

In technical areas, AI can help monitor systems, improve security, and surface problems before they turn into outages. These are practical, everyday improvements that add up quickly.

The businesses seeing progress tend to take a steady, human-first approach. They set clear rules around how AI should be used, what it can and can't do, and where human judgement still matters. They focus on giving staff training and reassurance, not just new tools.

AI becomes a support act, not a replacement.

AI projects don't usually stall because the technology isn't ready. They stall because people aren't. If you need help giving your team the confidence to use AI effectively, get in touch.

Q&A

Q: Should we use AI tools in our business, or wait until things settle down?

A: Start now. The key is using approved tools, setting clear rules, and making sure data is protected.

Q: What does zero trust mean?

A: It's a security approach where nothing is trusted by default. Every person and device must prove who they are every time.

Q: Do we need to control which apps staff can install?

A: Yes. Unapproved apps may store data insecurely or create hidden risks. A managed app list keeps everything safer and easier to support.

idea LOGICAL