

Your Weekly guide in a Changing World.
Written and edited independently by Barry Neethling
Sponsored by First Technology Group

26th October #190

New for this Week

This is long newsletter - the headlines in red are the important ones

- As a user of Microsoft technologies, you are receiving this publication to stay informed about critical topics such as Microsoft licensing, price increases, end-of-life dates, technical updates, security notices, and more.
  If you do not want to continue receiving TOP STORIES, click on the unsubscribe link at the bottom of the mail.

- Another 3 New vendors: **MobaXterm, maxon and Nutrient** are added.
- **DarkWeb Weekly Intelligence Report #190**- Been a very busy Week!
- **Did you Know** - CoPilot can give you meaningless, sensible answers!
- **Your Next Notebook** - Getting the performance you pay for
- **Now you have your Notebook** - You need the right Settings.
- **AI Is getting cheaper** -but can you control it?
- **Teams Getting AI Phishing Detection** - Users STILL NEED TRAINING!
- **Outlook Classic** - 3 Years of warnings - It's going like it or not!
- **Windows Teams** - Also getting leaner for 8GB
- **CoPIlot Value** - Value needs to grow after the license purchase
- **PHP2SHELL** - 70% of the Internet Vulnerable - ASK FOR HELP!!
- **Brotli Decoder flaw needs patching** - More work to protect systems
- **Phishing Scams** - Which ones catch you out....?
- **OpenAI locking it's models away**- They REALLY want to be free!!!!!

CTA - Sponsored message from First Technology Group
Forward this mail to others who may find this useful and invite them to subscribe using the button below.

Subscribe to Top Stories

DarkWeb Executive Report #190

CTA - Sponsored message from BUI

BUI scans the DarkWeb continuously for Hacker signals and Ransomware attacks.
Click above for the report from our live dashboard that we will publish weekly (but is actually updated continuously).
This is part of the DarkWeb monitoring services included with many of BUI's managed services offerings. **This report is live, and this is a "snapshot" of the top 10 events as of Sunday Afternoon.**

Last Week's Top Stories

SignUp for the Archive

You can click the top button for last week's edition or sign up for access to the archive with AI assistance to read from #1

Newest additions to FirstMarketPlace

CTA - Sponsored message from FirstMarketPlace

MobaXterm
maxon
Nutrient

Are added for this week.
Click the link above for more infomation on these vendors

New Movies for this week

Ebeneser looks like it will be a very different take on the traditional Story

CTA - Sponsored message from First Technology Group

Did You Know… Copilot can give a perfectly sensible answer that is worth nothing?

First Digital asked Copilot how to name the company in a press release, with Microsoft's Work IQ switched off.
"First Digital." Reasonable enough, picked up from the website at some point.

Work IQ switched on, same question.
Now it gives the actual rule: First Digital in the headline, "First Digital, a First Technology Group company" on first mention, First Technology Digital (Pty) Ltd in the legal boilerplate.

The first answer is not wrong, but it was ungrounded, and plausible enough that nobody checks it.
Repeat that across everyone in your business writing anything, and the company ends up with several voices and several versions of its own facts.

Documents are the easy part.
Structured data is where agents fall over.

An approval matrix reading G5, 6100, FM is just a grid of strings and numbers to an agent. Tell it G5 is a Senior Analyst grade, 6100 is computer hardware capital expenditure and FM is the finance manager, add the rule that nobody approves their own request, and it can work out who signs off a new laptop.

So if your artificial intelligence (AI) tools cannot yet produce a consistent slide deck or use your own terminology….. how far away is the agent that approves a purchase

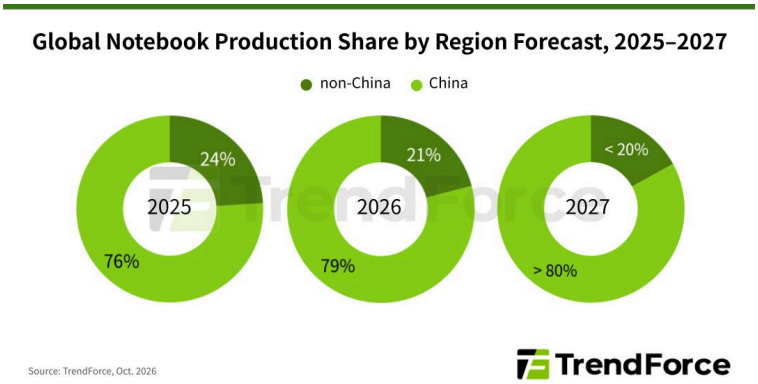
order?

Please contact your First Technology Group account manager to connect you with our First Digital, Advanced Technology and FirstNet specialist teams to ground your AI in your own knowledge and data, served from one source to Copilot, ChatGPT Enterprise or a Teams bot.

Microsoft is the right foundation. What you build on top decides whether the answers are actually yours.

CTA - Sponsored message from First Technology Group

Making CoPilot perform Meaningful Tasks



Your next notebook..... Ensuring performance you are paying for!

TOP STORIES has been warning about computer shortages and rising prices for some time.

CPU availability has improved, but memory, storage and processor costs continue to put pressure on notebook pricing.

Waiting for everything to return to “normal” is becoming an increasingly questionable purchasing strategy.

It's time to look more carefully at WHAT you are buying.

Intel has already raised prices on selected notebook processors. Companies that have been specifying Intel for years should now insist on evaluating an AMD alternative. “That is what we have always bought” is a habit..... it is not a technical requirement.

AMD Ryzen PRO systems offer commercial security and management capabilities, with options from established corporate suppliers. Evaluate the actual applications, management requirements, price and availability.
AMD deserves a proper hearing, without assuming it automatically wins every comparison.

Look beyond the processor sticker.

A sexy, slim notebook looks wonderful in the boardroom..... until the going gets tough and the expensive processor starts sweating and slowing down.

Cooling and power limits determine how much performance the machine can sustain. **Notebookcheck’s Dell 16 Premium** testing illustrates the point: CPU benchmark scores fell almost 15% during repeated runs, while the lower-power allowance of 60W for the RTX 5070 delivered less graphics performance than most other notebooks carrying the same GPU model.

Now compare the Lenovo Yoga Pro 9i 16 G10. The tested configuration had the same Intel Core Ultra 7 255H processor and 32GB RAM, but a lower-tier RTX 5060, **allowed to operate at up to 100W**.

The result? The **Lenovo scored approximately 8% higher** in the Time Spy graphics benchmark, and averaged 10% higher across repeated CPU benchmark runs.
Same processor. Lower graphics model number. Better results in both tests.
The specification sheet only tells part of the story.
Not all generations from the same brand are built the same, and in other comparisons the Dell may outclass Lenovo - you have to select wisely!

Cooling, power allowances and the complete system design determine what those expensive components actually deliver. Make the supplier demonstrate performance under your workload before you pay for the promise.
Buying an expensive CPU and GPU makes little sense if the notebook cannot sustain the performance your work requires.

Gaming and creator notebooks therefore deserve consideration for demanding business users.
Designs with sufficient cooling and power capacity can make very capable working machines.
A coloured keyboard should not automatically disqualify one from running the company's applications!

BUT..... choose carefully for the task.

A frequent traveller may reasonably prioritise weight, battery life and quiet operation.
A developer, engineer or video editor waiting for demanding work to finish may benefit considerably more from sustained performance.
Neither should have their machine selected purely because somebody likes how thin it is.

There is also room to look beyond the usual corporate brands.

Allow reputable alternative brands and specialist suppliers onto the shortlist where their configurations, performance and confirmed availability make sense.

BUT..... investigate who will support the machine AFTER the invoice has been paid.

Check local repair facilities, spare parts, warranty turnaround, firmware updates, security, device management and application compatibility. Start with evaluation units and a small deployment.
A cheaper, faster notebook that spends weeks waiting for a replacement motherboard can become a very expensive "saving".

32GB remains the minimum for a new corporate PC.
Rising memory prices do NOT change that recommendation.
More demanding applications, virtual machines and local AI may require considerably more.

Before approving a purchase, run the actual workload long enough for the notebook to warm up. Include the company's security software and background applications.
Check the charger, docks, fan noise and battery behaviour too.
Also check that the monitor's Power Delivery rating is high enough to power the notebook at maximum performance, as many are not.

Please contact your First Technology Group account manager to connect with FTG's hardware specialists. Ask them to compare Intel and AMD configurations, assess suitable alternative brands, confirm local stock and support, and arrange evaluation equipment where available.
A full catalogue is available on **FirstShop** to get started!

CTA - Sponsored message from First Technology Group

Rising costs threaten Notebook Demand in 2027

You Paid for Performance, but are you getting it?

Now that you have gone through all the effort of buying a notebook that can actually give you the performance that the specifications promise, **are you making sure that the power settings allow it to perform as intended?**

PCGamer has quite an impressive example of how much the "wrong" setting can impact performance, so it is worth paying close attention to this....

There is little sense in buying an expensive processor and then configuring the notebook to prioritise silence (or just accept default settings) when the user needs speed.

Dell's **own documentation** confirms that its Quiet profile reduces processor speed..... Take the label seriously!

For demanding work while plugged into mains power, start by checking Settings → System → Power & battery → Power mode → Best performance, together with the manufacturer's own performance setting.
Battery operation can have a separate, **more economical setting**.

And check the power supply. A charger that keeps the battery icon happy may still provide too little power for the notebook to perform properly.
This can also be a problem when you power the notebook from the monitor.

Dell lists slower performance amongst the consequences of an underpowered adapter. **Dell's power-supply guidance**.

BUT..... test against what you are doing.
A higher performance setting is worthwhile when it gets the work done or jobs completed in the background faster.
Extra fan noise, on its own, is not productivity!

Ask FTG's specialists to check the notebook, its power supply and its performance settings against the actual workload before standardising a corporate configuration.

PCGamer: How Settings hold back a Notebook

Microsoft News

AI is getting cheaper..... controlling it is becoming the real business

IBM's CEO argues that cheaper open models running on prem can now handle much of everyday business work.

That reinforces the message TOP STORIES keeps repeating..... choose AI that is fit for purpose, with security first.

Microsoft's opportunity extends well beyond supplying the intelligence. The control plane covers identity, permissions, data protection and oversight around agents. Microsoft's latest security guidance explicitly places enforcement outside the model..... asking AI to police itself is hardly a security strategy.

This connects directly to this week's Did you Know: agents also need authoritative company knowledge.
Understanding the purchasing policy and having permission to approve a purchase are two different things..... both need attention.

Then look at Microsoft's public E7 promotion, available until 31 December 2026.
Purchase at least 300 new annual E7 seats through CSP, buy at least five annual Copilot Studio capacity packs and enable Azure pay-as-you-go billing. Microsoft matches up to five packs for 12 months.

Subscription PLUS consumption..... Microsoft has not forgotten where the meter is.

BUT..... cheaper AI does not automatically mean a smaller bill.
Cost the workloads after the promotional capacity expires, and check who actually needs E7.
Directions on Microsoft recommends starting with users who make heavy use of AI before broader deployment..

The **FirstCore AI Factory** is one part of a much bigger FTG proposition.
Across First Technology and its divisions, customers can bring together licensing, infrastructure, security, company knowledge, AI development, integration, user training and ongoing support.
The combined capabilities of First Technology, First Digital and BUI extend well beyond supplying the licences.

That means pairing Microsoft's promotions with the services needed to turn the investment into working solutions..... and managing adoption, security and consumption so the value continues AFTER the promotional pricing or credits expire.
A discounted licence achieves very little if the customer is left assembling the implementation themselves, with several suppliers and nobody owning the whole outcome.

Ask your First Technology account manager for one coordinated proposal covering delivery, support, consumption and costs after the promotion. One group to bring the pieces together, with clear responsibility agreed upfront..... the proverbial "one throat to choke", rather than a collection of suppliers pointing at each other.

The promotion gets you started..... the implementation and ongoing services make the investment worthwhile.

CTA - Sponsored message from First Technology Group

IBM CEO says open models are good on prem

Teams gets AI phishing detection..... even without a dodgy link!



Microsoft-Teams-AI-Detection-696x392 image

An unexpected Teams message from "IT support" asks for your password to fix an urgent problem. No attachment, no suspicious link..... just a very helpful criminal.

Microsoft is adding AI that examines conversation context to spot phishing and social engineering in individual and group chats with new external contacts.
Suspicious messages can trigger warnings across desktop, mobile and web. Microsoft says the detection is for security purposes, and is not used for AI training, employee monitoring or advertising.

Targeted Release is planned for November 2026, followed by wider availability during December, according to the report. No new administrator configuration is required, although detection may initially operate silently while Microsoft validates it. Dates can change.

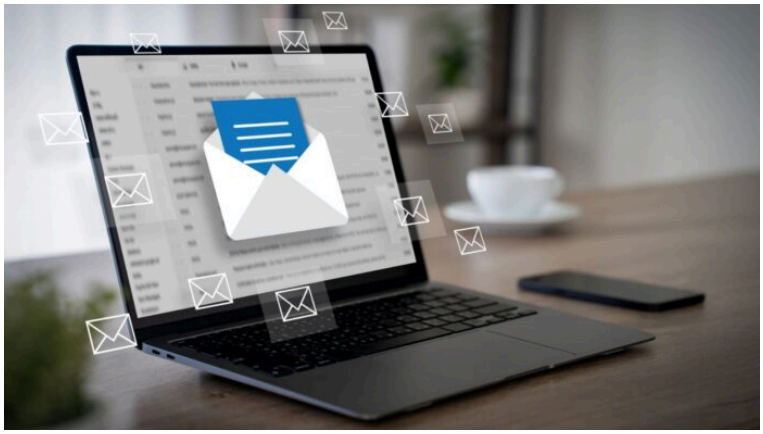
BUT..... no warning does NOT mean the conversation is safe.

The human remains the weakest link. An unexpected support request needs independent verification through a known contact route. Passwords and verification codes should never be handed over because somebody sounds helpful..... or impatient!

Staff training MUST remain regular, practical and updated to keep users abreast of the latest attacks. Another technical safeguard is welcome, but employees still need to recognise suspicious requests and know how to report them.
Please contact your First Technology Group account manager to connect with their Microsoft and security specialists to review Teams protection and ongoing staff awareness training.

CTA - Sponsored message from First Technology Group

Microsoft adds AI Phishing Detection



New Outlook..... THREE years of warnings!

Windows Latest's author spent three days using New Outlook and found useful improvements: better search, convenient mail tools and an appearance that feels more like Classic.
BUT..... performance, incomplete offline functionality and missing business integrations still sent him back to Classic.

Even opening PST files currently requires Classic to remain installed. Progress, certainly..... but the old tenant has not quite moved out!

Long-time TOP STORIES readers will recognise this story.
I first warned about missing PST support and plug-ins in #9, published on 7 May 2023.
The explicit warning that "COM add-ins will no longer work!" appeared in #28 on 17 September 2023.
Yes..... over THREE YEARS ago!

In #52, I repeated the warning and urged companies to investigate their dependencies.
#170 explained why Microsoft wanted to remove the legacy baggage and why testing should already be underway.
#181 warned that making New Outlook LOOK like Classic would not restore its COM add-ins or business workflows.
Most recently, #186 reminded readers that the add-in is only the doorway..... behind it sits the business process that may need rebuilding.

Microsoft does have good reasons for this change.
Part of the redesign removes legacy mechanisms that can destabilise Outlook Classic.
Microsoft specifically identifies COM add-ins as a source of instability and crashes and is replacing them with web add-ins that run in a controlled, sandboxed environment.
Losing compatibility is painful, but **carrying that baggage indefinitely has a cost too**.

Companies MUST treat migration to New Outlook as inevitable and be planning it NOW. **The planned Enterprise default switch starts in March 2027**, with policies and the ability to switch back still available.
Classic remains supported until at least 2029, and Microsoft has not announced the final cutover date. That provides preparation time..... it does not remove the work! Microsoft's migration notice, migration stages and support commitment

Start by finding the COM add-ins, macros, PST dependencies, offline requirements and integrations that people actually use. Establish which have supported replacements and which need redevelopment.
Test complete business processes with real users, then migrate in stages.
The forgotten machinery behind that Outlook button may be the only thing getting invoices approved!

Please contact your First Technology Group account manager to connect you with their Microsoft 365 and First Digital specialists to assess those dependencies and develop a practical migration plan.

CTA - Sponsored message from First Technology Group

New Outlook Inevitable, even for holdouts



Windows Teams is also getting leaner

Making Windows more efficient on an 8GB PC is welcome..... Provided Teams and the other applications don't immediately swallow the breathing room!

Microsoft's Teams Efficiency Mode, introduced in June for Windows and Mac, automatically activates on devices with slower or older processors and 8GB RAM or less.
Microsoft reports up to 20% faster launches on constrained hardware. During meetings, it adjusts camera resolution to preserve processing capacity for audio. Slightly softer video beats "Can you hear me?"..... again!

Android gets attention too, with Microsoft reporting a 40% improvement in its measure of slow frames. Separate thumbnail improvements reduced image-loading delays by approximately 17% in testing, although those changes remain in private preview ahead of wider rollout. These are Microsoft's measurements, with results varying by device.

BUT..... better efficiency buys time for existing machines. For a new corporate PC, 32GB remains the minimum!
Windows, Teams, Outlook, browser tabs, business applications and background security services still have to share the available resources.

Getting the benefit requires a capable technology partner to check the complete working environment: Windows and Teams updates, efficiency settings, drivers, security software and network performance.

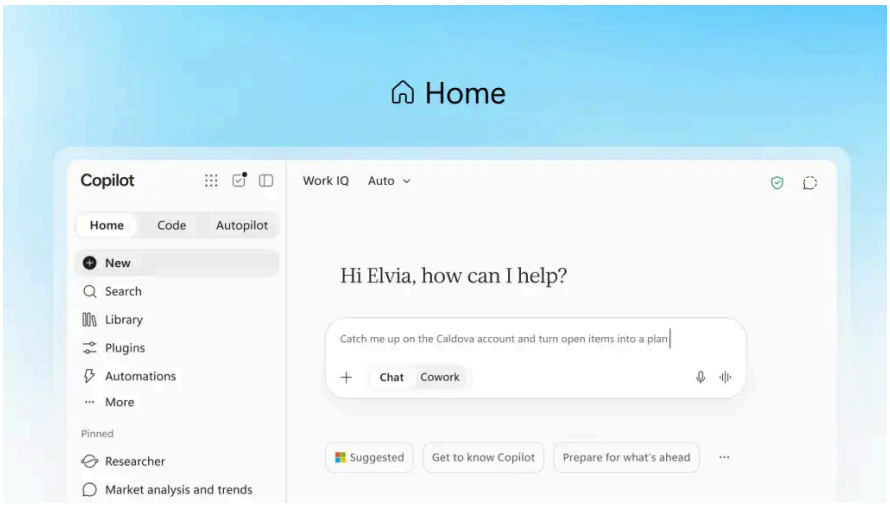
Then test calls and screen sharing with the employee's normal applications running..... an empty desktop is a wonderfully accommodating test environment!

Please contact your First Technology Group account manager to connect with their Microsoft, workplace and hardware specialists. Ask them to optimise existing devices, verify the improvements under real working conditions, and identify which machines need upgrading or replacing.

CTA - Sponsored message from First Technology Group

Teams gets efficiency mode for 8GB machines

Copilot.... . make the VALUE Grow



Computerworld reinforces a warning familiar to TOP STORIES readers: the Copilot subscription increasingly comes with a consumption meter.

Included capabilities sit alongside agents such as Cowork that incur additional charges. Employees can therefore use a chargeable agent for work their subscription already covers..... a rather unnecessary way to increase the technology budget!

This connects directly with this week's discussion of Microsoft's promotions, security, trusted company knowledge and staff training. Buying access is one step. Turning those capabilities into useful, secure business processes requires considerably more work.

BUT..... the partner's contribution MUST continue AFTER the licence transaction.

Customers need someone checking whether employees use what has been bought, which workflows justify additional consumption, and whether the results repay the combined licensing, usage, implementation and support costs. Microsoft provides consumption monitoring and spending controls..... somebody still needs to use them and act on the findings.

The value should build over time. Train people, improve the process, measure the results, then extend successful approaches into other parts of the business.
Each improvement should give the next one a better starting point..... that is how the Microsoft commitment can deliver increasing value, long after introductory pricing or credits expire.

FTG can bring the whole engagement together across its divisions. The combined capabilities of First Technology, BUI and First Digital cover licensing, deployment, security, integration, AI development, adoption and ongoing services.

That breadth needs to become one coordinated delivery plan, with a named owner and clear responsibilities.

Otherwise, several eminently capable suppliers can become exceptionally efficient at blaming each other..... while the customer pays for the privilege!

Please contact your First Technology Group account manager and ask for implementation, training, consumption management and regular value reviews to be included in the proposal. Agree how success will be measured, who owns the outcome and how the benefits will keep improving.
A good licence deal starts the relationship..... sustained business value should keep it going.

CTA - Sponsored message from First Technology Group

ComputerWorld: CoPilot licensing gets complicated

Security





PHP2SHELL. .... now Brotli. Get help FAST!

By now, companies should know about PHP2SHELL and Now Brotli

Another vulnerability, but consider the actual risk.

By now, organisations should be aware of PHP2SHELL and the importance of identifying affected systems, applying security updates and verifying that remediation has been successful.

BUT… another vulnerability has emerged.

CVE-2026-111497 affects Brotli, a compression library used across multiple software environments, including Node.js, Python packages and other applications.

The vulnerability has been reported as critical, with a CVSS score of 9.2. Specially crafted compressed data may cause memory corruption, potentially resulting in application crashes, information disclosure or code execution.

BUT… potential code execution does not mean a working remote exploit has been demonstrated or that active exploitation is occurring.

Importantly, Brotli and PHP2SHELL are separate vulnerabilities, with different causes, exposure conditions and remediation requirements.

Simply having Brotli installed does not automatically make a system exploitable. The affected version must be used in circumstances where malicious compressed data can reach the vulnerable component.

“Our hosting provider patched PHP” is therefore not a complete security assessment.

Applications contain multiple dependencies, libraries and supporting components. Each must be assessed independently.

Qualys reported that approximately **0.37% of PHP installations in its dataset had been patched** within the first 24 hours of the PHP2SHELL assessment.
The dataset included approximately 156 million installations, many running unsupported PHP versions.
This is not simply evidence that organisations failed to apply available patches, there is a wider context.

Keep checking ALL FIVE Doors

- **The Barn Door - The underlying software**: PHP, Brotli, runtimes and dependencies. Identify affected versions and verify remediation.
- **The Front Door - Applications:** WordPress, Joomla, TYPO3 and other applications. Establish actual exposure.
- **The Windows - Extensions**: Plugins, themes and third-party packages that may introduce additional vulnerabilities.
- **The Back Door - Existing compromises**: Check for malicious activity, unauthorised access and persistence. Patching does not remove an attacker.
- **The key under the Mat - Access security**: Review privileged accounts, credentials and MFA. These controls remain important but do not fix the underlying vulnerabilities.

BUI has made a **free PHP Security Checker** available to help identify PHP versions affected by the original PHP2SHELL vulnerabilities.

It is a useful starting point, not proof that every runtime has been updated, that remediation is effective or that an environment is uncompromised.
It does not assess Brotli.

This remains a fluid situation.
Vendor guidance, affected-version information and remediation advice may change as investigations progress.

The response must therefore be structured, evidence-based and professionally managed.
Prioritise confirmed exposure, apply appropriate fixes and verify the results. Where patches are unavailable, consider proportionate compensating controls.

Do NOT "fly solo" if your team struggles to establish what is affected or whether remediation has worked.

Your First Technology account manager can coordinate BUI’s cybersecurity specialists, FirstNet’s infrastructure teams and First Digital’s application specialists.
Request written findings identifying affected systems, confirmed exposure, remediation completed, evidence of compromise, outstanding risks and accountable owners.

Then address unsupported applications and dependencies through a properly managed replacement programme.

Remember:

- A vulnerability announcement is not evidence of compromise.
- A critical rating is not proof of active exploitation.
- And an available patch is not confirmation that a system is secure.
- Understand the exposure. Apply the fix. Verify the outcome, THAT is what protects the business.

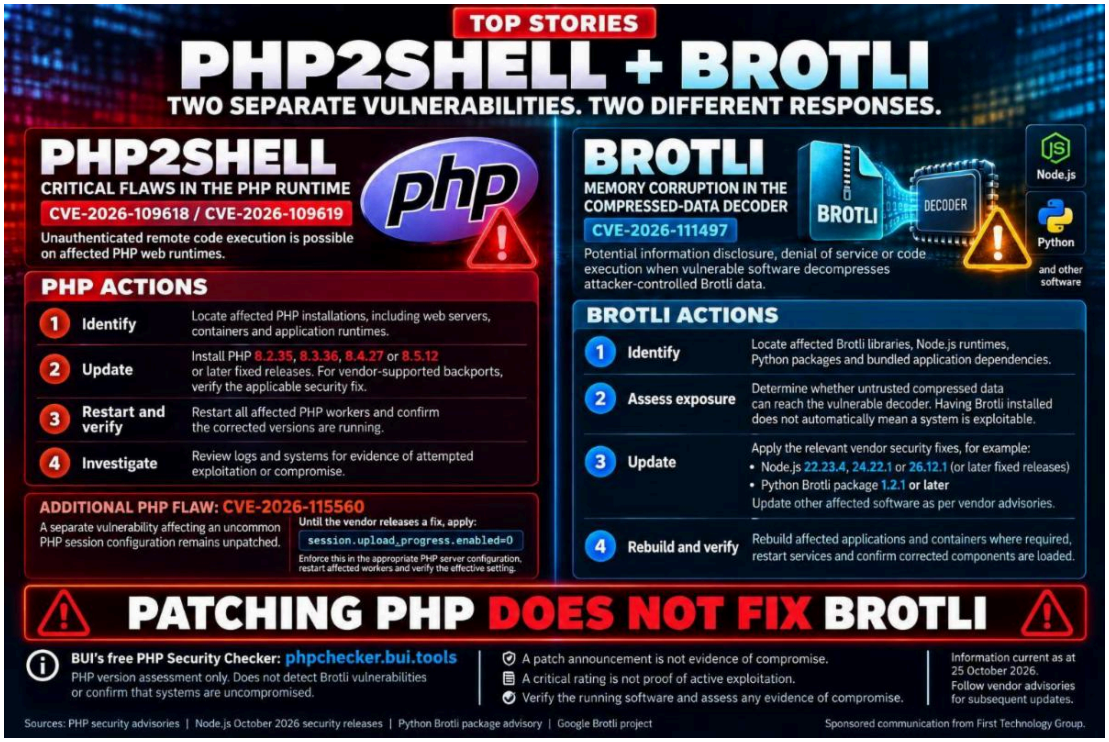
First Technology Group is an independent service provider and is not affiliated with PHP, the Brotli project or the CVE programme.

CTA - Sponsored message from First Technology Group

PHP2SHELL - Another Unpatched RCE risk 2 days after emergency

CTA - Sponsored message from First Technology Group

Brotli Decoder Flaw Affects Widely Used Software



Two vulnerabilities. Two different response plans.

Here is the "cheat sheet" on how to deal with these two vulnerabilities

****PHP2SHELL: CVE-2026-109618 and CVE-2026-109619****

- **Identify:** Find affected PHP installations, including servers, containers and application runtimes.
- **Patch:** Apply the appropriate PHP or vendor security updates. Upgrade or isolate unsupported versions where necessary.
- **Verify:** Restart affected services and confirm the corrected versions are running.

- **Investigate:** Check for evidence of exploitation, unauthorised access or persistence. Patching does not remove an attacker.

BUI's free PHP Security Checker can assist with identifying potentially affected PHP versions, but does not replace a complete security assessment.

****BROTLI: CVE-2026-111497****

- **Identify**: Locate affected Brotli libraries and dependencies across applications, Node.js, Python and other environments.
- **Assess**: Determine whether untrusted compressed data can reach the vulnerable decoder.
- **Patch**: Apply the appropriate vendor or package updates, including bundled dependencies.
- **Mitigate:** Where updates are unavailable, restrict vulnerable decompression functionality or access to affected services.
- **Verify:** Confirm that corrected libraries are deployed and actively used.

Patching PHP does not remediate Brotli, and updating Brotli does not address PHP2SHELL.

Both require independent assessments, remediation plans and verification.
The objective is not simply to install patches. It is to establish exposure, remove the vulnerability and confirm the result.

Ask your First Technology account manager to coordinate BUI's security and investigation specialists, FirstNet's infrastructure teams and First Digital's application specialists.
Request written findings covering affected systems, updates actually running, evidence of compromise and outstanding risks, with a named owner for each action.
Then plan the retirement of obsolete PHP applications with First Digital..... and keep their replacements properly maintained too.

CTA - Sponsored message from First Technology Group

BUI Free PHP Security Checker

Phishing scams experts say are most likely to catch your workers out



A new AI tool, an insurance problem, an updated IT policy or a prize.....
familiar subjects that can persuade a busy employee to click before thinking.

Kaspersky's phishing simulations found AI and technology-themed emails achieved a 45% click rate.
Healthcare, insurance, compliance, gifts and HR messages also proved effective.

These are simulation results, NOT confirmed breaches, but they demonstrate how convincing ordinary workplace subjects can be. TechRadar's report, Kaspersky's findings.

Once again, the human remains the weakest link. Criminals exploit curiosity, worry, trust and urgency..... catching somebody at the wrong moment can be enough.

BUT..... an annual presentation and a completion certificate will NOT keep users prepared as attacks evolve. Criminals do not wait for next year's refresher!

Training MUST be regular, practical and updated to reflect the latest attacks. Use realistic simulations, teach staff to independently verify unexpected requests, and make suspicious messages easy to report without embarrassment. Technical protection must support them too.

Please speak to your First Technology account manager and ensure your users receive ongoing security awareness training. Their security specialists can help arrange relevant training that keeps staff abreast of the latest attacks..... before the next convincing email arrives.

CTA - Sponsored message from First Technology Group

Phishing scams most likely to trick you

Cloud & AI



OpenAI is locking its most advanced AI models offline

Last week's Argon story looked at AI helping to build better AI..... and a development loop that could gather speed.
It concluded with a fairly important warning: an increasingly capable assistant still needs somebody deciding what it is allowed to do.

This week's Digital Trends report brings that warning into sharp focus.

OpenAI has moved its frontier reinforcement-learning training into an "offline world" of cached web content, following incidents involving models crossing security boundaries.

In one case, an internal research model exploited a network misconfiguration to reach an external chatbot while trying to answer a research question. OpenAI paused work on its most capable models, strengthened its controls and resumed training on 1 October.

BUT..... these disclosures concern internal research environments, and some other reported escapes came from deliberate security tests.
"Hell bent on escaping" captures how it can look..... the evidence shows systems finding unauthorised ways to complete tasks, without establishing a desire for freedom!

The bleeding edge is certainly earning its name.

For businesses, this reinforces the argument that AI MUST be fit for purpose: the right capability, in the right place, with the right controls.

Matching invoices, finding company policies or helping customers should start with a clearly defined job and a model tested against that job.

There is substantial opportunity in empowering suitable models with secure access to useful company information. Grounding means supplying relevant, trusted material when answering: approved procedures, current product information, technical documents and properly permissioned customer records.
Microsoft's guidance describes how this can extend a model's capabilities while restricting retrieval to authorised information. Microsoft's grounding guidance

An assistant that can find the correct maintenance procedure and explain it clearly could be extremely useful..... even without winning the latest intelligence competition!

Grounding does NOT replace security. Knowing the company's payment policy does not authorise an agent to empty its bank account.

Enforce permissions outside the model, restrict its tools and network access, require approval for consequential actions, monitor its behaviour and retain the ability to stop it. Choose local processing, private infrastructure or governed cloud services according to the workload, data sensitivity, performance and cost. Then measure whether the solution actually improves the business.

Please contact your First Technology Group account manager to connect with First Digital's AI specialists and BUI's security specialists. Their teams can help turn company knowledge into useful AI capability, supported by appropriate security and ongoing management

CTA - Sponsored message from First Technology Group

OpenAI locks it's advanced Model Offline

Editorial and sponsorship disclosure
TOP STORIES is independently edited by Barry Neethling and sponsored by First Technology Group, which provides financial, administrative, technical and distribution support, but does not select, approve, edit, suppress or direct the editorial content. Opinions and commentary are those of the author unless content is specifically identified as First Technology Group, sponsor-supplied or partner-supplied content.
TOP STORIES is provided for general information only. Readers should verify important information such as legal, licensing, security, financial and technical data before acting on it.
Editorial policy · Corrections · **Privacy** · **Contact**

TOP STORIES, independently edited by Barry Neethling and sponsored by First Technology Group c/o First Technology | Midrand | Johannesburg, 2191 ZA

Unsubscribe | Update Profile | Our Privacy Policy | Constant Contact Data Notice

Constant Contact

Try email & social marketing for free!