

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

2nd November #191

New for this Week

- Another 3: **revenera, cymulate & CleanShot** to buy from FirstMarketPlace
- **DarkWeb Weekly Intelligence Report #191**- it been a **Hacktober**!!
- **5 Years from your Notebook Battery?** - Yes it **is** possible and even longer!
- **CoPilot Credits** -check before you sign!
- **Azure Capacity Checklist** - Very important to read and ask for help
- **MFA** - Not a good idea to mark your own homework!
- **Windows Teams** - Also getting leaner for 8GB
- **PHP2SHELL** - Keep checking the 5 doors - a summary of where we are.
- **Phishing gets personal** - AI helps attacks get more targeted
- **AI Notetakers** - Way more serious than what you think

- 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.

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 #191

Last Week's Top Stories

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.**

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

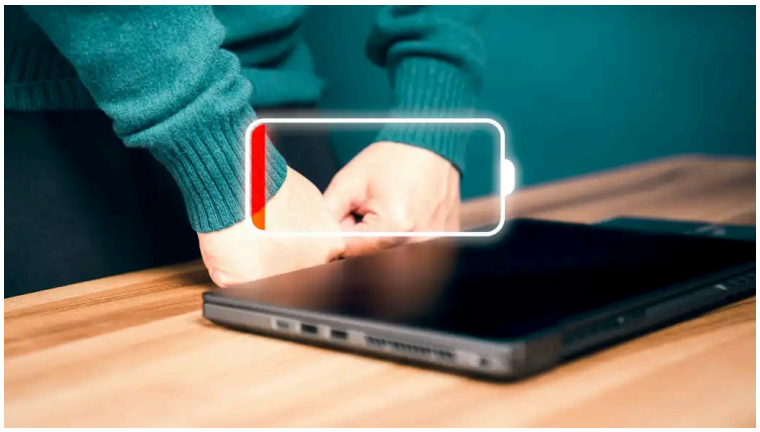
CTA - Sponsored message from FirstMarketPlace

revenera
cymulate
CleanShot

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



FIVE years from your notebook..... without replacing the battery?

If you expect your notebook to last FIVE years, why not plan for the battery to last as well?

P.S. This is also why 32 GB remains the minimum - you need to try and get through 5 years without upgrading the memory as well!!!!

Back in 2021, I wrote about managing notebook batteries to extend their life.
As companies try to keep their notebooks working for longer, that advice is even more relevant..... and PCWorld has revisited the subject.

In a **Philips Research laboratory test**, cells charged 100% managed around 550 cycles, **compared with an estimated 900 when charged to 80%,** before maximum capacity fell to 80% of the original.

Even with the smaller charges, the 80% test delivered about 41% more total charge before reaching that point.

Let's do the maths.....

For a user consuming roughly half a battery's original capacity per working day, the **test figures translate to approximately 3½ years versus just over FIVE years before reaching that capacity benchmark.**

That could mean no replacement battery, no labour, no downtime, and no opening the notebook to replace parts during its five-year life!

Cleaning the fans is another story..... for another day!

BUT..... this is a calculation based on a laboratory test, not a guarantee.
Battery age, heat, usage and the notebook model all affect the result.
Obviously, an 80% charging limit also means less running time between charges.

So where are the settings?

Dell: Look for Adaptive or Primarily AC Use in Dell Optimiser, MyDell or the BIOS.

HP: On supported business notebooks, Battery Health Manager can limit charging to around 80%.

Lenovo: Vantage or Commercial Vantage can set charging thresholds. Lenovo suggests 80% or less for notebooks that remain plugged in.

Choose the setting for the user. Someone travelling may need a full charge; a notebook that lives on a docking station probably does not.

Before ordering a battery, check its health and charging settings. A battery at 80% health may still be perfectly usable..... but if it is swollen, stop using the notebook and get qualified help immediately.

Please contact your First Technology Group account manager to connect you with FTG's hardware and managed services specialists. They can review your notebook fleet and help apply suitable charging policies.

CTA - Sponsored message from First Technology Group

Want your battery to last? Avoid these mistakes

Microsoft News



Copilot Credits..... check BEFORE the meter starts!

Microsoft has published the November 2026 Copilot Credits Guide, with this month's update expanding the SharePoint section to include OneDrive.

The revised section explains which everyday activities are included with a Microsoft Copilot licence and which advanced tasks consume additional Copilot Credits. Large-scale document reviews, complex AI workflows and near real-time metadata processing can all bring consumption charges.

BUT..... having a Copilot licence does NOT mean every AI task is included!

Checking one document and repeatedly processing thousands of files are very different workloads..... even when both begin with an innocent-looking request!

The guide covers pay-as-you-go billing and an annual credit pre-purchase option. Buying ahead can attract discounts, but unused credits expire at the end of the annual term.
Spending controls and usage reports are available..... somebody still needs to configure them and act on the results.

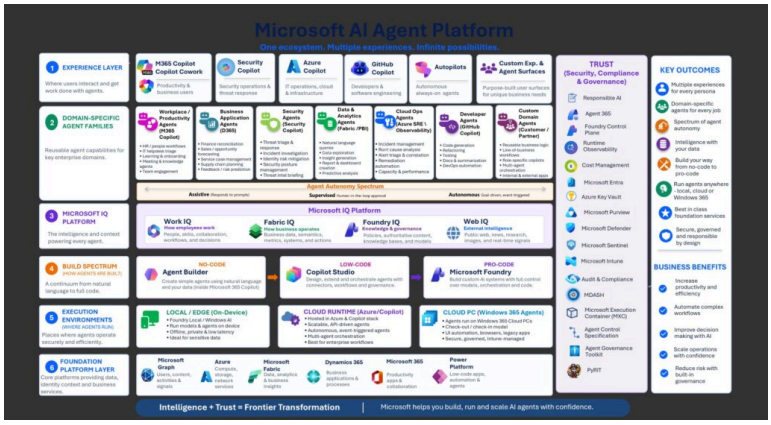
This is why companies MUST engage the experts when deciding how to combine licences and credits.
Start with existing entitlements, identify the business processes worth improving, test representative workloads and estimate ongoing consumption. Then choose the purchasing approach, configure controls and train users.

Please contact your First Technology Group account manager to engage their Microsoft licensing and AI specialists. Ask for a practical plan covering licensing, expected consumption, implementation and ongoing reviews.

Expert advice can help avoid paying for capabilities already included, buying credits that expire unused, or running an impressive automation whose costs exceed its benefits..... clever AI should improve the business, not simply become more efficient at spending its money!

CTA - Sponsored message from First Technology Group

Microsoft CoPilot Credits Guide November 2026



Azure Capacity Checklist, Agent Teammates, Sovereign Cloud

Mary Jo Foley's latest Directions on Microsoft article connects Azure capacity constraints, digital teammates, Microsoft's expanding agent ecosystem and sovereign cloud. It is a complicated subject, but I REALLY urge anyone planning AI deployments to read it in full.

This reinforces the message TOP STORIES keeps repeating..... AI MUST be fit for purpose.

An assistant drafting a reply and an agent sending emails or progressing a purchase approval have very different responsibilities. The model, company knowledge, permissions, human oversight and cost all need to suit the task.

Customers REALLY need a capable partner to help bring these decisions together.
Start with the business process and the result required, then select and test the appropriate solution.
Agree who owns it, train the people using it, and keep checking accuracy, security, consumption and business value as usage grows.

BUT..... sovereignty needs considerably more attention than choosing a local data centre!

Check where information is stored AND **processed (which is what FTG's AI Factory in SA can do)**, who can access it, who controls encryption keys and how critical operations continue during disruption.

Apply the controls each workload actually requires, and establish which capabilities are available for production use today. A feature promised for the future cannot satisfy a requirement you have now.
Microsoft's **sovereignty update** illustrates why those distinctions need careful assessment.

Even finding sufficient cloud capacity becomes part of this discussion. Moving a workload to another region needs checking against its residency requirements, performance and cost.

Then add Microsoft's commercial push. Its current promotions explicitly link E7 upgrades with Copilot Studio capacity packs, alongside Azure consumption offers starting on 2 November.
Subscription PLUS consumption..... the digital colleague comes with a meter!

A promotion can improve the business case. Customers still need the combined cost of licences, usage, infrastructure, implementation and support assessed, including after promotional benefits expire.

Please contact your First Technology Group account manager to start the conversation with their AI, Microsoft licensing, security and cloud specialists. Ask for a coordinated plan that makes the agents effective for the work required, applies sovereignty correctly and measures the ongoing return on the investment.

CTA - Sponsored message from First Technology Group

Directions: Azure Capacity Checklist, Agent Teammates, Sovereign Cloud

---

MFA - you sure there are no holes? Get others to mark your home-work



Multi-Factor Authentication (MFA) needs to be implemented properly, and then checked by somebody independent.
As I have warned before..... marking your own homework is a risky habit when access to your business is at stake!

A recent Japanese survey by security firm Act reinforces the point.
Among respondents reporting account compromise or suspected incidents, 43% said MFA had been temporarily disabled or excluded for the affected account.

Another 21.4% reported problems with the authentication method or its settings. These are self-reported findings, including suspected incidents, but they are a useful reminder of how protection can fall through the gaps.

BUT..... saying “MFA is switched on” does not establish which accounts, applications and access routes it actually protects.
That temporary exception created during a migration may still be there.....

Get professional help with the implementation. If your own team has already done it, get somebody independent of that work to check the result.
Even very good IT teams benefit from a fresh pair of eyes.

A proper review should examine coverage, exclusions, administrator accounts, authentication methods, enrolment and recovery processes.
It should also test whether the controls work as intended, rather than simply confirming that the settings look right.
Microsoft’s **own incident-response guidance** describes how attackers exploit exclusions and gaps in access policies.

And this applies beyond Microsoft..... other cloud services, remote access and business applications deserve the same attention, regardless of whose MFA solution you use.

Ask for written findings, prioritised fixes and verification afterwards. Schedule further reviews as systems change, and keep users trained to recognise suspicious sign-in requests and unexpected MFA prompts.

Please contact your First Technology Group account manager to arrange for FTG’s security specialists to review your MFA implementation. Get somebody else to mark the homework..... before an attacker finds the mistakes!

CTA - Sponsored message from First Technology Group

MFA: Misconfigurations and Exclusions are plentiful

Security



PHP2SHELL..... Keep checking the 5 doors!

This three-minute guide (see link below) reinforces last week’s warning.....

PHP can hide inside websites, business applications and third-party software. Updating the obvious web server can leave other vulnerable copies untouched.

Keep checking ALL 5 doors.....

- The barn door (underlying software),
- Front door (applications)
- Windows (plugins and extensions)
- Back door (existing compromises), and
- Key under the mat (accounts, passwords and MFA).

Prioritise internet-facing systems, verify that fixes are running and investigate suspicious activity.

Take vulnerable services offline where immediate patching is impossible.

BUT..... a firewall does NOT replace patching, and a patch does NOT evict an attacker already inside!

Ask your First Technology Group account manager to coordinate the checks with FTG's security, infrastructure and application specialists.

CTA - Sponsored message from First Technology Group

Channelinsider: PHP2SHELL What you need to Know

Phishing gets personal..... and the weakest link is still HUMAN!



KnowBe4's latest research records a 41.1% annual increase in targeted spear-phishing, while overall phishing rose 29.8%. Criminals are researching their victims and creating convincing requests around familiar people, companies and workplace routines. In Q3 2026, attacks were twice as likely to originate from legitimate infrastructure as in the previous quarter. **A trusted platform can carry a very untrustworthy request!**

The attack can even involve a genuine sign-in process, with the victim persuaded to authorise an attacker's session or grant access to company information.
The employee sees something familiar..... and supplies the permission the criminal needs.

Then comes the pressure. Your account will be blocked. A payment needs immediate approval. Somebody claiming to be IT support needs your help NOW.
Criminals exploit trust, authority and fear to make people act before thinking. The moment you feel pressured to hurry is precisely when you need to slow down.

BUT..... "be careful" is hardly a training programme!

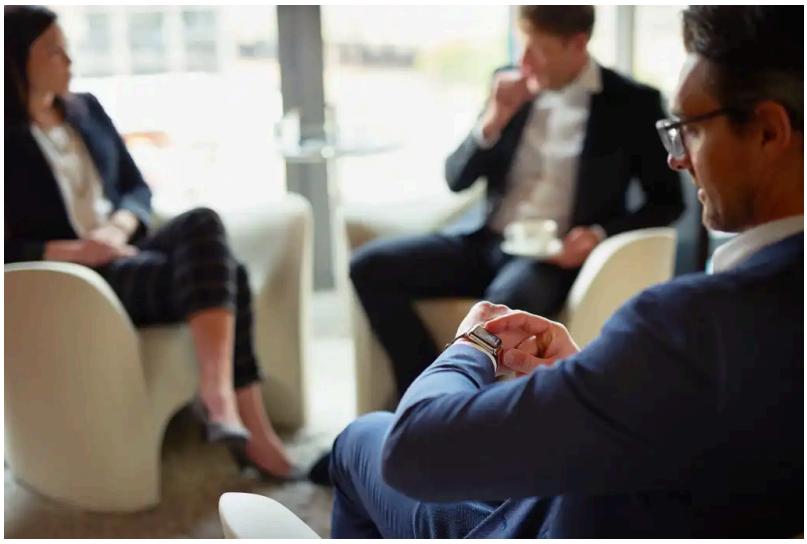
Staff need regular, practical and continuously updated TRAINING, using examples relevant to their jobs. Practise pausing, checking unexpected requests through a known contact route, following normal approval procedures and reporting suspicious activity immediately, including after a mistaken click. **Make asking for help easy and free from blame.**
Technical controls must support people, because nobody can spot EVERY attack.

Please contact your First Technology Group account manager to connect with FTG's security specialists and review ongoing staff training alongside email protection, identity security and application permissions. The criminals keep updating their methods..... staff preparation needs to keep pace!

CTA - Sponsored message from First Technology Group

RedmondMag: Phishing attacks jump 41%

Cloud & AI



AI notetakers..... The Microphone is already on the wall!

In TOP STORIES #175, I warned that controlling meeting bots was only part of the problem.
CIO's latest report extends that warning to phones, watches and wearables, and consider the television on the boardroom wall..... supposedly just a display..... well maybe not.....

In their September investigation, **Gamers Nexus and Level1Techs** demonstrated how compromised LG smart TVs could capture room conversations and conference-call audio.
One demonstration captured room audio while the screen appeared off.

LG denies continuous recording during normal operation and says voice processing requires activation.
The security demonstrations involved equipment the researchers had taken control of.

The business lesson..... equipment you consider passive may contain microphones, software and network connections.
Your confidentiality assessment must include the room itself, including home offices, customer premises and hotel meeting rooms.

AI notetakers have real value. BUT..... telling people "please do not record" cannot substitute for practical policies, controls and training.

Management, staff, customers, service providers, contractors and visitors must understand the rules..... including for devices THEY bring.

Those rules need to cover:

- **Approved tools and devices**.
  Review security, cloud storage, access, model-training terms and personal accounts. Include meeting-room equipment.

- **Recording boundaries**.
  Define disclosure, permission, objections, sensitive discussions and agreed exceptions. Cover live transcription and AI summaries too.

- **External parties**.
  Explain expectations through invitations, visitor information and relevant customer and supplier agreements. Guide staff attending meetings elsewhere.

- **Records and sharing**.
  Control access, distribution, retention and deletion, including provider-held copies

and legal preservation requirements.

- **Accuracy and responsibility.**
  Assign someone to check important notes, decisions and actions before use. Microsoft warns that AI meeting content can be inaccurate or incomplete. Microsoft's guidance.

Then audit TVs, remotes, webcams and voice assistants alongside laptops. Check microphones, disable unnecessary voice features, install security updates and restrict network access.
Train staff to challenge unexpected recording and report concerns.

For South African businesses, address POPIA's requirements around lawful processing, notification, security, retention and transfers abroad.
Involve your legal and privacy advisers.

A dark screen is not a security control..... and a policy nobody understands will not protect the conversation.

Please contact me for consulting and guidance on assessing your exposure, developing practical AI notetaker policies and **helping people understand their responsibilities.**

CIO: AI Notetaker risk is an everywhere problem

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!