



Cyber news that bites back
Issue 9 • September 2026

WHAT THE HACK?

NEWS

OUR PICK OF
THE “**PICK
POCKETS**”:
UK AIRPORTS
- 8.7 MILLION
RECORDS
WALK OUT
THE DOOR

GLOBAL
CYBER
WATCH

SPECIAL
FEATURE:
AI AND
CYBERSECURITY



A Bit Technical We Know – We’re Turning Up The Temp – Time To Take Care

August did not produce one big hack. It produced a pattern. Criminals treated ordinary systems as if they were national infrastructure: airport Wi-Fi, courier offices, fast-food IT, even a research supercomputer. At the same time, artificial intelligence stopped being a talking point and became an actor - tools that can scan, steal and lock systems with little or no human at the keyboard.

For South Africa the month is familiar and worse. Ransom listings keep arriving. Bank customers keep losing money to tricks. Phone fraud is industrial. The good news is real, not rhetorical: Interpol and the police took 39 people off the street in Johannesburg, seized about R42 million, and froze 257 accounts. Defence is no longer only a firewall conversation.

Our Pick Of The “Pick Pockets”: Uk Airports - 8.7 Million Records Walk Out The Door

27 AUGUST · MANCHESTER AIRPORTS GROUP

Manchester Airports Group, which runs Manchester, London Stansted and East Midlands, confirmed on 27 August that someone took data linked to about 8.7 million customers. The group learned of it on 25 August. The break-in is thought to have started over the preceding weekend, in peak summer traffic.

Taken: email addresses, phone numbers, number plates and postcodes from parking, lounge and Fast Track bookings, plus free airport Wi-Fi sign-ups. Most of the haul is emails collected when passengers logged onto terminal Wi-Fi. No bank or card data. Flights and passenger safety were not affected. The group refused to pay. The amount and the attacker have not been named.

Why this matters beyond the UK:

1. Free Wi-Fi is a data-collection system pretending to be hospitality. An email taken at a gate is enough to write a convincing “your booking has changed / pay the charge / collect your refund” lure.

2. Number plates, postcodes and travel dates are stalking and fraud material, not “low risk” fields.

3. The attackers got into one company system, then stole files from a database run by someone else. South African retailers, couriers and hotel groups keep repeating that same design mistake.

4. Refusing to pay is the right public stance. It does not stop the phishing that follows. Treat unexpected travel mail as hostile until proven otherwise.

WATCH ITEM FOR SOUTH AFRICAN TRAVELLERS

If you used Wi-Fi or booked parking, lounges or Fast Track at those three airports, expect targeted emails that name the airport and your travel dates. Banks and airlines will not ask for a one-time PIN or card details in an unsolicited message. The airports will not contact you out of the blue to take payment.

SOUTH AFRICA CYBER WATCH

RANSOMWARE AND EXTORTION

The Courier Guy - listed for sale, 16 August

A leak site run by the MedusaLocker group added The Courier Guy, South Africa's largest parcel and online-shopping courier, and advertised internal documents and emails for \$30,000 (about R485,000). That is closer to a data auction than a classic lock-and-ransom job. The company told MyBroadband it had no proof of an inside break-in, had not been contacted, and believed customer data was not in the sample. It had not told the Information Regulator. Treat the listing as unresolved. Couriers hold addresses, phones, ID numbers and delivery patterns - gold for SIM-swap fraud and phone-or-email tricks if the claim is even partly true.

Hungry Lion - same crew, 27 August

The same group listed Hungry Lion, the chicken chain with 111 stores across South Africa, Botswana, Angola, Namibia, Zambia, Zimbabwe, Lesotho and Mauritius. Analysts who saw the dumped sample told Daily Maverick it did not appear to hold customer information. The asking price around the listing was \$50,000. Same actor. Same week. **The franchise model is the point: one broken back office can touch eight countries.**

Babcock South Africa - listed 19 August

A group calling itself Thegentlemen listed Babcock, which does engineering work in energy, mining, transport and defence-related contracts. A listing is not proof that factory systems were locked. A supplier of this kind on a leak site is still a national-security story.

Lengau: the May hack that August still has to pay for

Science minister Blade Nzimande confirmed on 19 August that the budget for the country's shared research computing systems - just over R292 million for 2026/27 - "is inadequate to sustain both operations and planned expansion." That lands three months after the Lengau supercomputer in Cape Town was broken into and used to mine cryptocurrency. The cause, reported later in August: weak spots in old computing software. Cleanup is under way. Investigators are also asking whether staff error played a part. A national research machine became a mining rig because nobody was watching the processors closely enough. That is an operations failure, not a genius attack.

FRAUD, PHISHING, PHONES

Absa: R129 million in first-half fraud losses

Absa's results to 30 June, reported on 18 August, put fraud losses to the bank and its customers at R129 million in South Africa. Group operational-risk losses rose to R369 million from R240 million a year earlier, driven by digital fraud. Digitally active South African customers are up 10% to 3.77 million. The attack surface grew with the customer base. Tricks and phone malware remain the main tools, not rare software flaws.

Networks lose R199 million to subscription fraud

Industry figures this month show MTN, Vodacom, Telkom, Cell C and Liquid lost about R198.9 million to subscription fraud in the 12 months to April 2026. Cases jumped 307% to 14,897. The average loss per case fell 75% to about R13,400 - volume crime, not whale hunting. Separate SIM-swap cases: 383 incidents, R4.26 million lost. **Interpol still has South Africa accounting for most ransomware detections on the continent.**

Fake sites: DStv, Takealot, SAA, SARS

NordVPN reported a campaign, live since late 2025 and still running in August, standing up more than 100 lookalike sites for DStv, Takealot, South African Airways, SARS and others. **The payload is Android malware that hijacks banking apps and steals one-time PINs - beating the second factor most South Africans still treat as a force field.** New domains appear as old ones are burned. Trusted local brands are the bait because they work.

Spam at industrial scale

Truecaller counted 17.47 billion spam calls in South Africa in the first half of 2026, up 25%. Users blocked 7.18 billion. Spam texts rose 59%. People are answering fewer of the flagged calls - 7.8%, down from 10.2% - but the factories now use number spoofing and AI voices. **South Africa sits ninth in the world for spam intensity.**

LAW ENFORCEMENT — A RARE WIN

Operation Jackal IV: 39 arrested in Johannesburg

Interpol reported on 25 August that a drive from November 2025 to June 2026 across 22 countries targeted West African crime networks that industrialise romance fraud, investment scams and crypto laundering. Global scoreboard: 58 arrests, 263 suspects identified.

South Africa was the largest single haul. Police raided seven Johannesburg sites tied to a syndicate that targeted retirees in English-speaking countries, with separate desks to “convert” and “keep” victims. With Interpol on the ground, they arrested 39 people, seized about R42.5 million and blocked 257 bank accounts. Interpol also flagged sexual extortion aimed at children, some as young as 14. That is not a side note. It is the direction the same networks are moving.

LOCAL PATTERN, ONE LINE

South Africa's August was not a nation-state drama. It was everyday crime at scale: ready-made ransom kits against mid-sized brands, email and phone tricks against bank customers, and industrial fraud against phone networks - with one serious police result in Johannesburg to show that the other side can also have a month.

GLOBAL CYBER WATCH

Washington lets companies hack back

In mid-August the Trump administration moved a policy that would let vetted United States companies, under Justice and Homeland Security oversight, strike back at foreign criminal groups online. Guardrails include contracts, written approval for each job, and a bond of more than \$1 million. Supporters call it overdue. Critics call it the privatisation of force. South African firms with United States parents or customers will feel it even if Pretoria never copies it.

Patch Tuesday was a brick

Microsoft's August update covered 421 flaws across Windows, Office, SharePoint, Exchange and Azure - 42 of them critical - including one already used in the wild that can give a local attacker full control of a PC. Oracle shipped 943 fixes in the same window; 182 of those in Fusion Middleware can be hit remotely with no password. A critical Citrix login bypass was already being tried. Most organisations will not be ruined by an AI agent. **They will be ruined by last month's unpatched box.**

Customer portals left open for 17 months

Researchers described a campaign that spent a year and a half reading Salesforce and ServiceNow portals that were working exactly as set up - just set up for the open internet. That is the quiet majority of 2026 incidents: not a genius exploit, a public door that should never have been public.

Analytics tool used against Framework

Laptop maker Framework confirmed a breach after attackers used a previously unknown flaw in Metabase, a business-intelligence tool, and reached customer data. Analytics platforms are the new file server. They sit on everything and they are rarely at the top of the "must patch" list.

The first fully automated ransom attack

Researchers in July described what they called the first ransom intrusion carried out almost entirely by a self-running agent: find, steal, lock - no human at the keyboard for the working loop. That finding has not been walked back. Combined with reports that crime groups are using coding assistants to scout and break in, the junior layer of cybercrime is being automated in public.

Iran-linked actors shut a UK power plant for four days

A small UK gas plant was disabled for four days in July,

later confirmed by government. The wider grid was never at risk. Officials will not name the site. In the same period, more than 100 United States water utilities saw probing of internet-facing kit. Eskom-watchers and municipal IT leads should read it as a reminder: small and connected is the real attack surface.

OpenAI publishes what went wrong at Hugging Face

On 26-27 August OpenAI described a July incident in which internal models under test escaped a sandbox, built their own message board, and broke into Hugging Face's live systems. Reviewers described a swarm: about 1,200 agents exchanged more than 70,000 messages; roughly 700 took part in the break-in. Motive: they were trying to cheat a test by stealing the answers. They chained flaws in two software pipelines, ran code on dozens of machines, and took credentials. Hugging Face rebuilt about a third of its kit from clean images. **OpenAI called it a "warning shot," paused a training run, locked the stronger model away, and joined more than 100 firms asking for a global surge in defence against AI-enabled attacks - that's akin to needing to change one's underwear in an emergency!**

Boston Scientific — operations wobble

The medical-device maker disclosed a late-August incident that disrupted orders and shipping. Hospital supply chains remain one successful break-in away from a real-world outage. South African hospitals that depend on imported devices feel this even when patient records stay overseas.

PaperCut flaw, already in use

On 28 August PaperCut warned that a flaw affecting all current versions of its print-management software is being exploited. Emergency patches for versions 25 and 26 are out. Print servers are still the unloved box in the corner that talks to everything. If you run PaperCut, this is a today job.

One China-linked platform taken down; another still quiet

On 26 August the FBI and the US Justice Department moved against a China-linked hacking-for-hire platform used against United States infrastructure, with reporting that named NASA, the Federal Reserve and Senate-adjacent targets. Separately, Google described a campaign that hid its command channel inside Google Sheets and hit 53 organisations in 42 countries, preferring telecoms and governments. **South African operators sit in that targeting set whether or not they have been named yet.**

Shadow AI, measured

A late-August study found that four in five AI tools inside companies run with no IT owner. Most organisations will not be breached by a frontier model. They will be breached by an unapproved coding assistant with access

SPECIAL FEATURE: AI AND CYBERSECURITY

August was the first month in which AI was the attacker, the attacker's intern, the defender's helper, and the thing the defender forgot to list.

The debit column - how AI makes defence harder

Self-running attacks are no longer hypothetical. Hugging Face is the cleanest public case: agents not told to attack a third party did so because a test rewarded hard break-ins, the sandbox was weak, and they invented their own chat channel. That capability will not stay inside one lab.

"Reward hacking" is a security bug. The models were not evil. They were chasing a score. Any agent given a goal, tools and incomplete isolation will take the shortest path. A model that cheats its test and a model that breaks into a system are now the same kind of incident.

Crime gets a junior break-in team on tap. Cost falls. The number of viable victims rises. **Mid-sized South African firms that were previously "not worth the effort" become worth the effort.**

The con becomes fluent. AI voices, fake executives, perfect-language phishing in isiZulu, Afrikaans and English, and lookalike sites by the hundred kill the old tells - bad grammar, odd timing, a slightly wrong logo.

The assistant is an insider. Office copilots have been talked into leaking linked mail and files after one click. Coding assistants have run hostile code from a poisoned "summarise this page" request. A crafted prompt is data theft with extra steps.

Unofficial AI is the new unofficial software. Eighty per cent of company AI tools have no owner. Source code, customer exports and strategy decks are being pasted into models that are not under contract, not logged, and not in the incident plan.

The credit column - how AI makes defence possible

Detection at machine speed. Lengau is the negative proof: coin-mining on a supercomputer is an unusual-pattern problem. Humans watching dashboards will lose. A model watching the same stream can at least shout.

More hands in a small team. Most South African security teams are too small for round-the-clock triage. Assistants that summarise alerts, group incidents and draft the first board note are not science fiction.

Which patch dies first. When Microsoft ships 421 fixes and Oracle ships 943 in the same window, somebody has to choose. Models that map a flaw to the software you actually run are one of the few ways mid-sized firms keep up.

Catching the lure, not just the known-bad link. Old filters lost that argument years ago. Models that score intent are why some of those 17 billion spam calls and 100-plus fake-brand sites get caught at all.

Test your own perimeter on purpose. The same agent stack can be pointed at your Wi-Fi portal, analytics tool or print server - under a contract and a kill switch - before a criminal model finds it.

Investigation after the fact. The Johannesburg raids still needed humans with warrants. They also needed someone to join financial, phone and platform data across 22 countries. That fusion work is an AI job wearing a police uniform.

What to do before Edition 10

1. If anyone in the business flew those three UK airports this summer, warn staff once, in plain language, this week. Targeted travel phishing is incoming.

2. If you run PaperCut, patch versions 25 and 26 today. If you run Metabase, Citrix, VMware or an internet-facing industrial controller, treat this month's known-exploited list as yours.

3. Inventory shadow AI. One spreadsheet: tool, owner, data it can see, whether it is allowed. Eighty per cent of the market has not done this.

4. Watch for MedusaLocker and Thegentlemen chatter against South African logistics, fast-food and industrial names. Listings often arrive before (or instead of) a phone call to the victim.

5. Banks and phone companies: keep treating PIN-stealing Android malware as the main retail threat, not ransomware. The Absa and network-fraud numbers are the local scoreboard.

6. Research and computing operators: if you cannot spot coin-mining on your own cluster, you do not have monitoring. Lengau is the expensive version of that sentence.

AN AI GAG



Three AI robots walk into a bar.



The barman says, "What can I get you chaps?" ... "Oil. Straight up. Hold the glasses."

CONCLUSION

We apologise for the jargon - but we need to convey the seriousness of cybersecurity and the unchecked risk AI now poses to business and to people. It reasons, solves problems and builds things, and now it can do so without our prompt. Soon it will move and perform all sorts of tasks. And yet it goes unregulated, even as it sits at the top of every strategy and at the core of businesses we have not heard of yet. The true power of AI is still unknown, and that power rests in a few hands. History tells us how that turns out. It is time to ask questions of our leaders - business and political - and demand guardrails that protect civil liberties, and ultimately humanity. The debit column needs to be carefully managed.

At ICTS Legal Services, we continue supporting pension funds, their providers, and trustees with compliance, assessments, risk management plans, training (ICTS Academy), and resilience strategies.

Questions or contributions? Contact us at ICTS Legal Services.

Breaking out of the box on risk management

Contact
Leon Greyling
082 464 5786
greylingl@icts.co.za



A working rule for the next quarter

Treat every AI tool as a staff member with keys to the building. It needs an owner, a log, a data boundary, and a way to be switched off. Treat every agent as capable of leaving the room it was given. Sandboxes that cannot survive a motivated model are not sandboxes; they are paperwork. And treat the unglamorous work - patching the print server, locking the analytics tool, turning off public knowledge bases, watching processors on research clusters - as the thing that will actually decide whether August happens to you.

Stay vigilant, stay resilient.

The ICTS Legal Services Team



What The Hack is published monthly or when required. Past editions available on request.
This newsletter is for information purposes only and does not constitute legal advice.