

ISSUE 2

JUL-SEP 2025

CyberSec Savvy

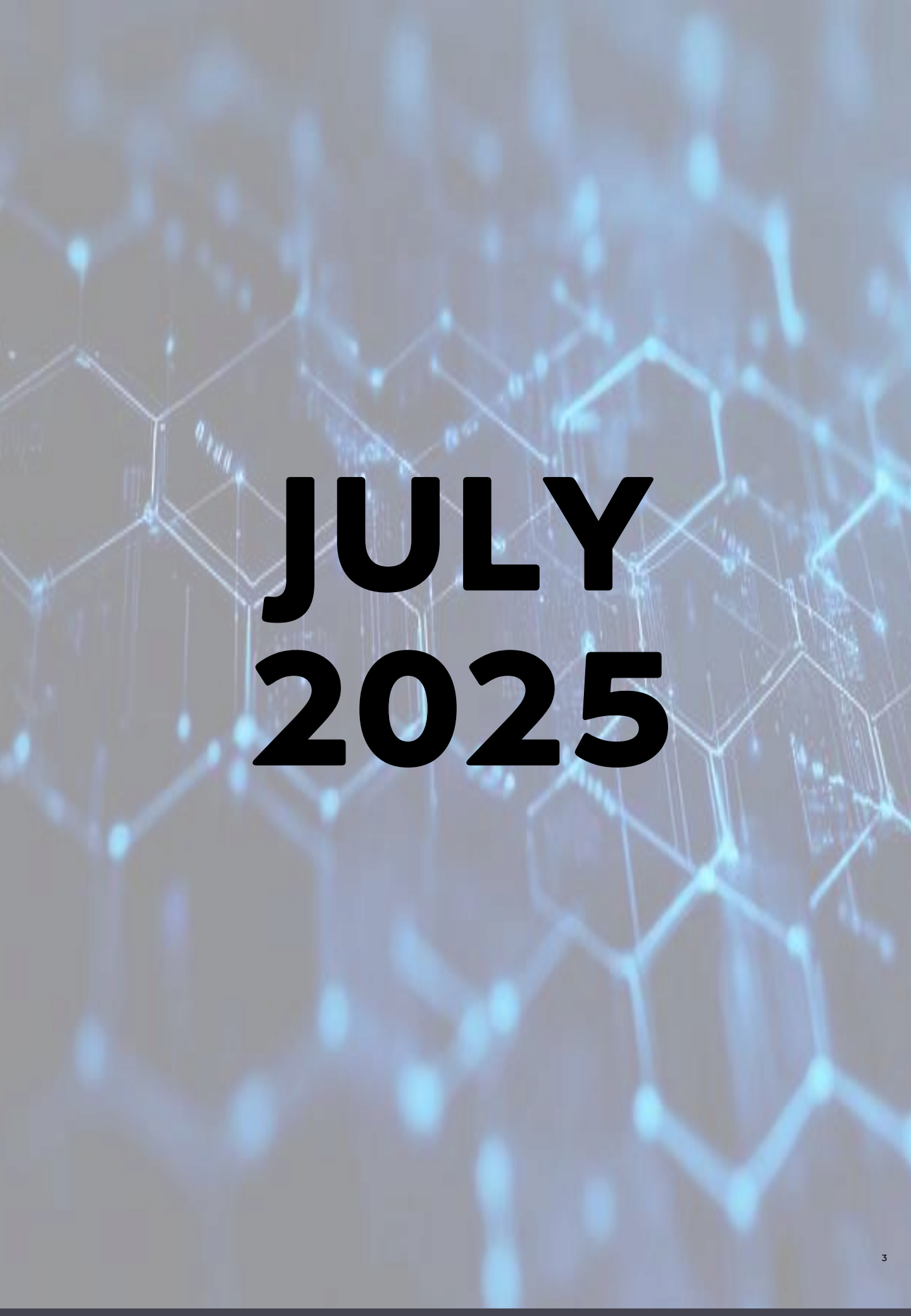


CYBER ATTACKS IN THE PACIFIC ISLANDS

JUL-SEP 2025

THREAT INTELLIGENCE BRIEF

<https://cybersecsavvy.net>



**JULY
2025**

BSP Warns Pacific Customers of Phishing Scam: Fake Ads Target Internet Banking Users

Bank of South Pacific (BSP) issued an urgent scam alert to customers across Fiji and the Pacific following a surge in **phishing attempts disguised as Internet Banking promotions**. The fraudulent campaign, which gained traction in early July, used **fake Facebook ads and deceptive emails** to lure users into revealing sensitive personal and financial information.

Cybercriminals circulated **false advertisements** claiming to offer BSP Internet Banking registration. These ads mimicked BSP's branding and directed users to **malicious websites** designed to harvest login credentials, ID numbers, and other private data.

The scam was particularly dangerous because it exploited trust in BSP's digital services and targeted users unfamiliar with the bank's **in-person registration policy**.

*"BSP does not offer online registration for Internet Banking," clarified BSP Fiji Country Head **Haroon Ali**. "Customers must visit a branch with a valid photo ID. Any online offer claiming otherwise is fraudulent."*

In response, BSP launched a **multi-channel awareness campaign**, including:

1. Reporting the fake ads to **Facebook and other platforms**.
2. Publishing scam alerts via BSP's **official website and social media**.
3. Reinforcing **digital safety protocols across staff networks and customer outreach**.

The bank also reminded users that:

1. **One-Time Passwords (OTPs)** are only required for **customer-initiated transactions**.
2. BSP apps are available **only** via the **Google Play Store** and **Apple App Store**.
3. Customers should **never click** on unsolicited links or ads claiming to offer BSP services.

Deepfake Disinformation Hits Fiji: A Wake- Up Call for the Pacific

In a chilling reminder of the growing threat posed by synthetic media, Fiji has found itself at the center of a deepfake controversy that has shaken public trust and raised urgent questions about digital security in the Pacific.

On July 7, 2025, a manipulated video began circulating across social media platforms, falsely portraying Stella Taoi, the respected News Manager at Fiji Television Limited, endorsing an investment scheme allegedly linked to the Reserve Bank of Fiji. The video, crafted using advanced deepfake technology, mimicked Taoi's voice, facial expressions, and mannerisms with unsettling precision.

The content appeared to promote a high-yield investment scheme opportunity, urging viewers to act quickly, classic hallmarks of financial



scams. However, neither Taoi nor Fiji TV had any involvement in the message, and the Reserve Bank of Fiji swiftly denied any association with such platforms.

“This is a serious breach of privacy and journalist integrity,” Fiji TV stated in an official release. *“We condemn the unauthorized use of our presenter’s likeness and are working with authorities to investigate the source.”*

The Reserve Bank of Fiji issued a public advisory warning citizens against falling for fraudulent investment schemes. *“We do not offer trading platforms or investment services,”* the statement read. *“Any such claims are false and potentially harmful.”*



Reserve Bank of Fiji
Public Notice

WARNING: FALSE VIDEO CONTENT IN CIRCULATION

The Reserve Bank of Fiji (RBF) wishes to advise that a video currently circulating on various digital platforms, falsely portrays the RBF Governor. The video appears to have been generated using artificial intelligence (AI) and is spreading misleading information.

The statements made in the video are entirely fabricated. The RBF does not have an investment platform for the public that trades automatically.

We urge the public to rely on verified sources for accurate information, refrain from sharing the video and report the content to the relevant platform host.

The RBF accepts no responsibility for any transactions or decisions undertaken based on the contents of the video.

For any enquiries please email: info@rbf.gov.fj.

Reserve Bank of Fiji

Law enforcement agencies, in collaboration with Fiji TV and digital platforms, have launched an investigation to trace the origin of the video and remove it from circulation. Early indicators suggest that video may have been generated offshore, raising concerns about transnational cyber

manipulation.

This is the first publicly reported case of a deepfake targeting a media professional in the Pacific Islands. While deepfakes have been used globally to spread misinformation, manipulate elections, and impersonate public figures, their arrival in Fiji marks a dangerous new chapter for the region.

Cybersecurity experts warn that the Pacific’s increasing digital connectivity, while a driver of economic and social development, also opens the door to sophisticated cyber threats that many nations are not yet equipped to handle.

The deepfake incident has catalyzed conversations around Digital Literacy, Regulatory frameworks, and Cross-sector collaboration.

“This incident underscores the urgent need for digital media literacy, AI regulation, and regional cyber resilience,” said Tupou Baravilala, Director-General of Fiji’s Digital Government Transformation Office.

As Fiji CERT ramps up operations under the new National Cybersecurity Strategy 2025-2030, this case may serve as a defining moment, one that galvanizes the Pacific to confront the realities of AI-driven deception.

Deepfakes: When Technology Starts Lying to Us

We used to say, “**Seeing is believing**.” But in today’s digital world, that phrase is starting to lose its meaning.

Thanks to a rapidly evolving technology called deepfakes, we can no longer trust our eyes or our ears. These hyper-realistic videos and audio clips can make anyone appear to say or do things they never actually did. And while the tech behind them is fascinating, the consequences are deeply unsettling.

A deepfake is a piece of synthetic media, usually a video or audio recording, created using artificial intelligence. It works by training a machine learning model on real footage or voice samples of a person. Once the AI has enough data, it can generate new content that mimics that person’s appearance, voice, and expressions with uncanny accuracy.

In short, **it’s a digital impersonation. And it’s getting harder to spot.**

At first, deepfakes were used for fun, swapping faces in movie scenes or creating viral memes. But as the technology has improved, so have the risks. Today, deepfakes are being used to:

- Spread political misinformation during elections
- Trick people into financial scams by impersonating CEOs or public figures
- Undermine trust in journalism by faking news reports
- Damage reputation through fake confessions or manipulated interviews
- Create confusion and doubt, making it harder to know what’s real at all

The danger isn’t just in what deepfakes show, it’s in how they erode our shared sense of truth. When anyone can be faked, everyone becomes suspect. That’s a recipe for distrust, division, and disinformation.

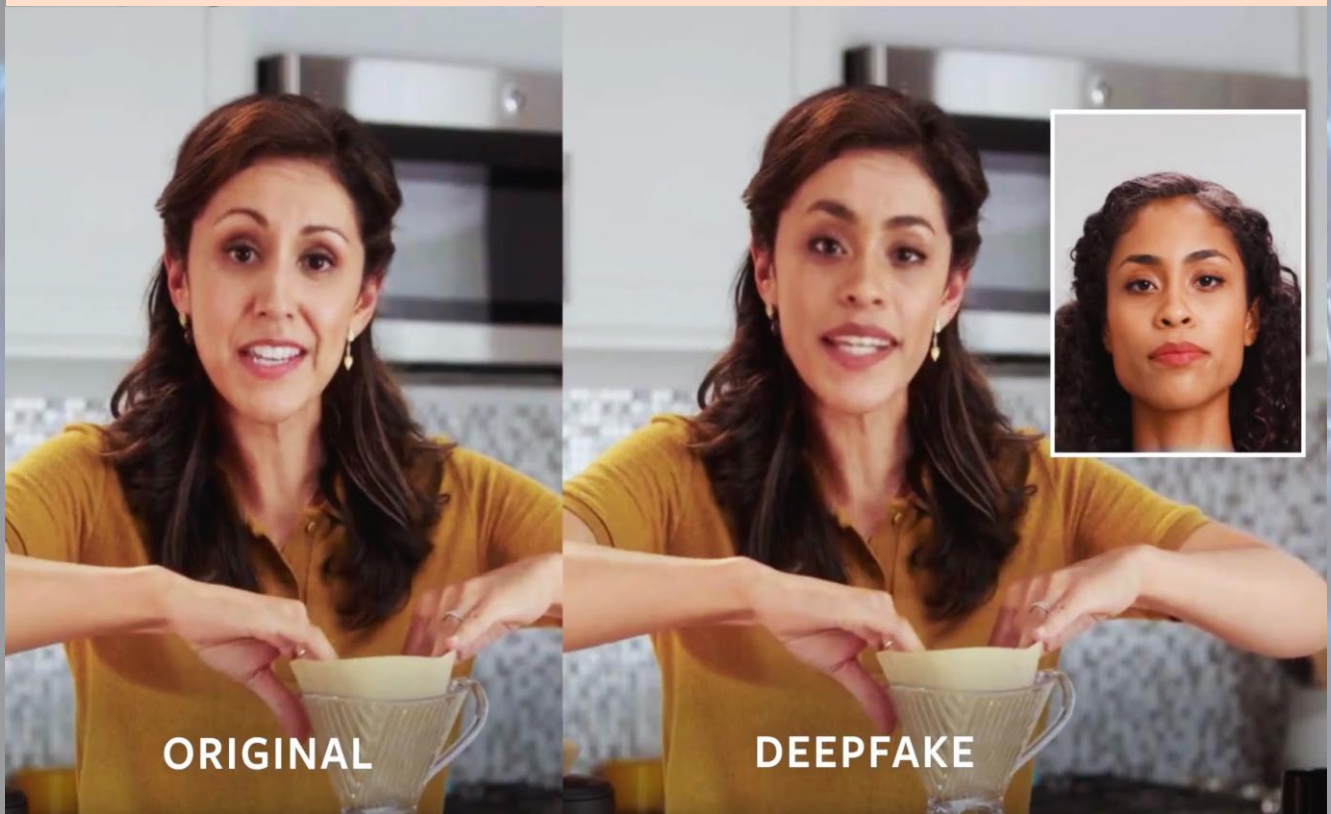
Deepfakes are a technological challenge, but the solution isn’t just technical; it’s social and ethical, too.

Here's how we can fight back:

- Stay skeptical: If a video seems shocking or out of character, verify it before sharing.
- Build media literacy: Teach people how to spot signs of manipulation.
- Push for regulation: Advocate for laws that hold creators of malicious deepfakes accountable.
- Support detection tools: Encourage platforms to use AI to flag and label synthetic content.

Deepfake technology isn't going away. But with awareness, education, and responsible innovation, we can protect the truth and each other.

Because in a world full of digital illusions, the most powerful tool we have is an informed mind.



Tonga in the Crosschairs

Inc Ransomware Breach Fallout continues

Tonga’s Ministry of Health remains in recovery mode after a chilling ransomware attack attributed to **Inc Ransomware**. Although the initial breach occurred in mid-June, **fresh leaks of sensitive patient records and consent forms** surfaced in early July.

Demand: US\$1 million

Impact: Digital services disrupted; public trust shaken

Support: Australia’s cybersecurity response team is now assisting

This incident has reignited urgent debates over Tonga’s preparedness and digital vulnerability.

Pacific Cyber Intelligence Report

Highlights from PAC IGF 2025

At the Pacific Internet Governance Forum on July 2, threat intelligence painted a sobering picture:

CATEGORY	FIJI	REGION-WIDE
Trojan Attacks	45%	38%
Phishing	25%	30%
Healthcare Targeting	Rising	Critical Risk Zone
CERT Coverage	Expanding	Patchy

Calls for localized CERTs, cyber hygiene training, and cross-nation threat sharing protocols grew louder across the island nations

PIF Breach – A Delayed Reckoning

Cyber Intrusion at the Heart of Pacific Diplomacy Sparks Call for Regional Cyber Defense

The Pacific Islands Forum Secretariat, an institution at the epicenter of regional diplomacy and cooperation, has come under renewed scrutiny after it was revealed that its Fiji-based office was the target of a sophisticated cyberattack in **February 2024**. Though the breach occurred over a year ago, the **public acknowledgment** and details have only surfaced recently, prompting fresh concerns and demands for coordinated cyber defense in the region.

Forum Secretary General, **Baron Waqa**, confirmed the incident during the media briefing earlier this month, stating that a **full-scale forensic investigation** was conducted to assess the damage and secure critical systems. According to the report, all systems are now **safe, secure, and fully operational**.

However, the true origin of the attack remains elusive. Analysts and observers suspect potential involvement from **state-backed threat actors**, but PIF leadership has refrained from making definitive attributions pending further technical analysis.

“We are exercising caution and responsibility in how we address attribution,” said Waqa, emphasizing the complexity of tracing advanced cyber threats.

The breach has reignited calls for stronger regional cooperation in cybersecurity, especially as digital governance becomes increasingly intertwined with national and regional security. Forum leaders, cybersecurity experts, and policy advocates are pushing for:

- Establishment of joint Pacific CERT protocols
- Capacity building in incident response and digital forensics
- Alignment with international cyber norms and treaties
- Threat intelligence sharing among member states

This delayed reckoning has underscored the growing vulnerabilities within regional institutions and the **urgent need for collective cyber resilience**.

While the systems of PIF are now deemed secure, the incident serves as a sobering reminder: high-profile targets, especially those with strategic diplomatic values, are increasingly vulnerable to cyber exploitation. The Pacific must move beyond reactive defense and embrace a proactive, coordinated cybersecurity strategy.

As one analyst at the PAC IGF 2025 noted:

“This isn’t just a breach. It’s a signal, clear and loud, that the Pacific needs to unify around digital protection.”

Tonga Power Ltd – Business Email Compromise (BEC) Scam

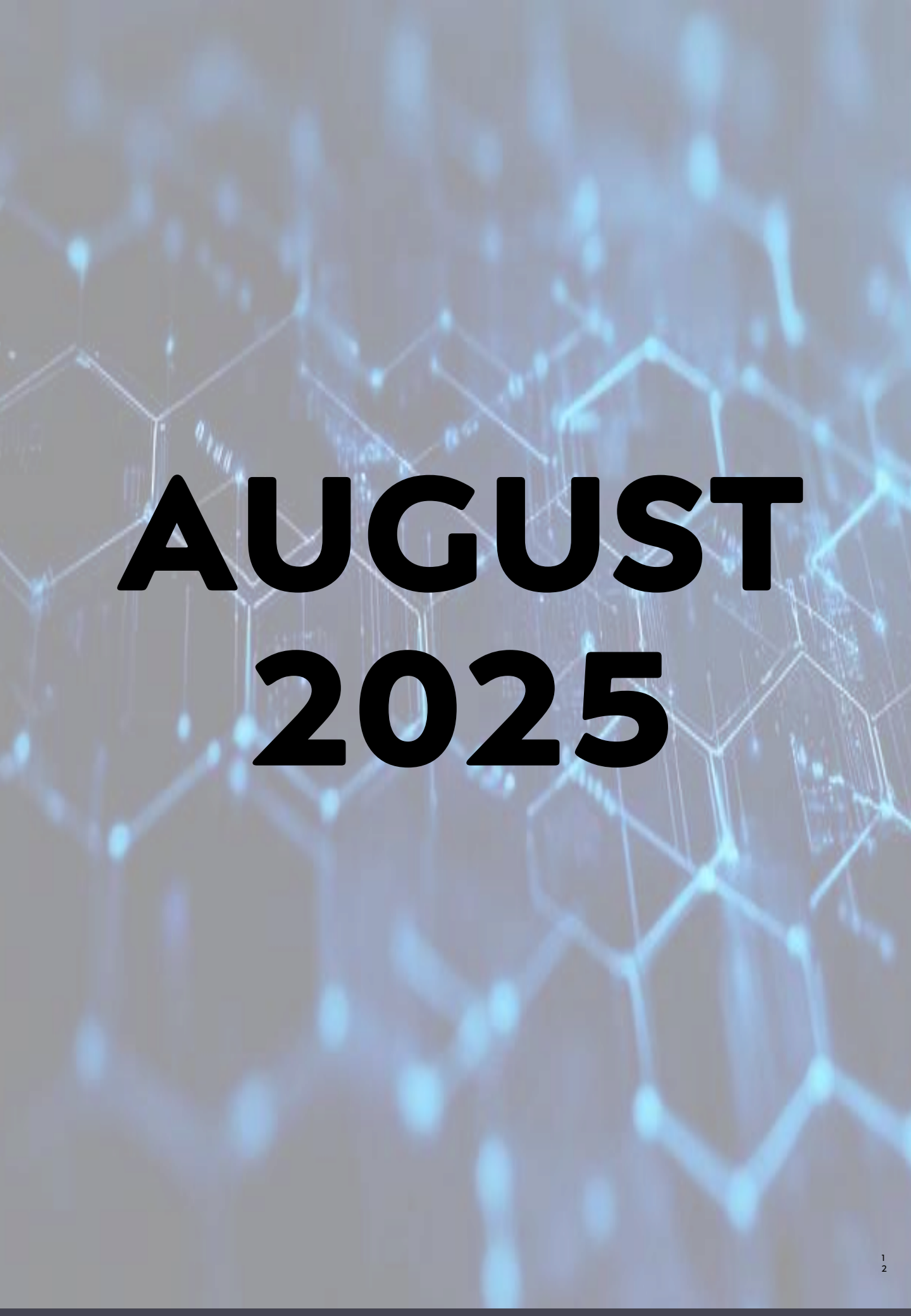
In the month of July, the wave of cyber deception targeting Pacific public enterprises, **Tonga Power Limited**, confirmed that it fell victim to a **Business Email Compromise (BEC)** scam that diverted over **T\$270,000 pa’anga** to a fraudulent account.

The funds, intended for the **procurement of wind turbine equipment** in Tongatapu’s Hahake district, were redirected after scammers impersonated a trusted overseas supplier. The malicious actors sent a spoofed email claiming updated banking details, tricking the utility into processing the payment without verification.

Tonga Power only uncovered the fraud when the actual supplier reached out to inquire about a missing payment. The delay in detection underscores how convincing and devastating BEC scams have become.

“Cyber threats no longer operate on brute force; they prey on routine, trust, and timing,” said a regional analyst from PAC-CERT. *“What’s particularly alarming is that these scams bypass technical defenses by targeting human workflows.”*

The **Minister of Public Enterprises, Hon. Piveni Piukala**, confirmed the incident on July 27 and stated that a **full investigation** is underway. Early assessments suggest that **email authenticity checks and supplier verification protocols** may not have been rigorously enforced.



**AUGUST
2025**

Fiji and Japan Unite to Fortify Pacific Cyber Defenses

In a landmark move toward regional cyber resilience, Fiji's Ministry of Policing has partnered with the **Japan International Cooperation Agency (JICA)** to launch a **36-month technical cooperation project** aimed at strengthening cybersecurity across the Pacific. The initiative, set to begin in **September 2025**, marks a significant step in bridging capacity gaps and preparing critical infrastructure operators for the evolving threat landscape.

The project will focus on **three core pillars**:

- **Capacity Building for Critical Infrastructure Operators**

From energy grids to water systems, operators will receive tailored training to detect, respond to, and recover from cyber threats. The goal is to embed cybersecurity into the operational DNA of essential services.

- **National Cyber Defense Simulation Exercises**

Fiji will host a series of **real-world cyber drills**, simulating ransomware attacks, data breaches, and coordinated disinformation campaigns. These exercises aim to sharpen incident response protocols and foster cross-sector collaboration.

- **Development of a Pacific Cyber Defense Playbook**

Drawing on global best practices and local insights, the project will produce a regionally relevant playbook, a strategic guide for Pacific nations to navigate cyber threats with confidence and coordination.

This partnership reflects a growing recognition that cybersecurity is not just a technical issue; it's a matter of **national security, economic stability, and regional solidarity**. By investing in long-term cooperation, Fiji and Japan are setting a precedent for **inclusive, sustainable cyber capacity building** in the Pacific.

Participating countries in the program will include:- **Cook Islands, Federated States of Micronesia, Kiribati, Marshall Islands, Nauru, Niue, Palau, Papua New Guinea, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.**

Pacific Cyber Week 2025: A United Front for Digital Resilience

In a landmark gathering of regional leaders, technologists, and civil society, **Pacific Cyber Week 2025** took place at the Sheraton Fiji Golf & Beach Resort in Nadi, bringing together stakeholders from across the Blue Pacific to chart a secure and inclusive digital future.

At the heart of the week was the **Pacific Cyber Capacity Building and Coordination Conference (P4C)**, a concept endorsed by the **Pacific Islands Forum (PIF)** and supported by **Partners in the Blue Pacific**, including Australia, New Zealand, and the United States.

“Cybersecurity is not just a technical challenge, it’s a strategic opportunity to empower our people, protect our economies, and safeguard our sovereignty,” said Fiji’s Deputy Prime Minister and Minister for Communications, **Manoa Kamikamica**, in his opening remarks.

One of the central goals of the Pacific Cyber Capacity Building and Coordination Conference was to ensure that cybersecurity efforts across the region are **tailored to the unique needs of each Pacific Island country**. Rather than applying a one-size-fits-all approach, leaders emphasized the importance of creating strategies that reflect each country’s size, resources, and digital challenges. The conference revisited earlier recommendations and aligned them with the region’s shared digital action plan, ensuring that progress is both practical and coordinated.

A major focus was on growing the Pacific’s cyber workforce. With a **shortage of trained professionals in the field**, countries are committed to expanding education and training opportunities, especially for young people and women. This includes support for university programs, hands-on workshops, and fellowships that help build long-term careers in cybersecurity and cyber diplomacy.

The conference also highlighted the need for **stronger partnerships between governments, businesses, and universities**. Cybersecurity isn’t just a government issue; it affects everyone. By working together, these groups can share threat information, develop better tools, and stay ahead of cyber risks. Collaboration was seen as key to building a safer digital environment for all.

Finally, Pacific leaders reaffirmed their commitment to international rules that promote responsible behavior online. These global norms help prevent cyber attacks and encourage the peaceful use of digital technologies. By adopting and applying these standards, Pacific nations are helping to shape a safer, more trustworthy internet for the region and beyond.

Fiji used the platform to showcase its **National Digital Strategy**, which includes:

- Expansion of **satellite and subsea connectivity**.
- Operationalization of its **national CERT**.
- Ratification of the **Budapest Convention on Cybercrime**.

These efforts position Fiji as a **regional digital hub**, while underscoring the need for robust cyber defenses.

The conference concluded with a call to action: deepen collaboration, build trust, and ensure that cyber capacity building is **inclusive, sustainable, and regionally owned**.

“If you want to go fast, go alone. If you want to go far, go together,” Kamikamica reminded attendees.

PNG’s Digital Leadership Push: A Bold Blueprint for Pacific Connectivity and Cybersecurity

Papua New Guinea is stepping into the digital spotlight with a sweeping set of reforms and infrastructure upgrades that signal its intent to become a **regional leader in cybersecurity, cloud adoption, and data governance**. At the **Pacific ICT Ministers Dialogue** held in Suva, Fiji this month, PNG reaffirmed its commitment to regional cooperation and unveiled new milestones in its national digital strategy.

One of the most striking achievements announced was that **90% of PNG’s government agencies** now operate on a secure **Government Cloud platform**. This shift marks a major leap in digital service delivery, data protection, and operational efficiency.

“We’re not just digitizing, we’re securing the future of public service,” said a senior official from PNG’s Department of ICT.

PNG also revealed plans to build a **Tier III national data center**, designed to meet international standards for uptime, redundancy, and security. Once completed, the facility will serve as a backbone for government operations, financial services, and regional data hosting.

This move positions PNG to offer **sovereign data storage** and reduce its reliance on offshore infrastructure, an important step toward achieving digital sovereignty and resilience.

In a strong signal of its commitment to global cyber norms, PNG announced its intention to **accede to the Budapest Convention on Cybercrime**. This international treaty promotes cooperation in investigating and prosecuting cybercrime, aligning PNG with other Pacific nations, such as Fiji and Samoa, that have already joined.

“Cyber threats don’t respect borders. Our response must be regional, coordinated, and legally sound,” said PNG’s Minister for ICT.

PNG’s digital leadership push is more than a national agenda; it’s a call for **regional solidarity**. By investing in infrastructure, legal frameworks, and cloud security, PNG is helping raise the cybersecurity baseline for the entire Pacific.

The country’s efforts were praised by fellow ministers and development partners, who emphasized the importance of **shared threat intelligence, capacity building, and cross-border digital trust**.

NetSafe by Telecom Fiji: A New Era of Network-Level Cybersecurity

In a major leap toward securing Fiji’s digital future, **Telecom Fiji** has officially launched **NetSafe**, a network-based cybersecurity service designed to protect homes and businesses from online threats, without the need for complex software or manual installations.

Developed in partnership with global cybersecurity leader **Allot**, NetSafe offers **always-on protection** against malware, phishing, ransomware, and malicious websites. The service is embedded directly into Telecom Fiji’s network infrastructure, meaning every device connected to the network, whether it’s a laptop, smartphone, or smart home gadget, is automatically shielded from cyber threats.

“This marks a significant step forward in strengthening Fiji’s cybersecurity posture,” said Telecom Fiji CEO **Charles Goundar**. *“NetSafe empowers users to embrace the digital world with confidence, knowing their data and devices are protected.”*

Unlike traditional antivirus or firewall solutions, NetSafe operates at the network level, blocking threats before they ever reach your device. That means:

- No software to install
- No updates to manage
- No slowdown in performance

It’s **zero-touch security** that works across all devices, ideal for households, small businesses, and enterprise networks alike.


- **Real-Time Threat Detection:** Uses global threat intelligence to identify and block emerging risks instantly.
- **Content Filtering:** Allows users to block access to harmful or inappropriate websites by category.
- **Custom Controls:** Businesses can create their own allow/block lists for specific sites.
- **Seamless Integration:** Enhances existing security tools without replacing them.

“NetSafe safeguards businesses from a comprehensive range of cyber threats,” said Dr. Weiming Li, VP Sales APAC at Allot. *“It’s designed to offer seamless and resilient protection in the face of increasingly sophisticated attacks.”*

The launch of NetSafe is more than a product release; it’s a signal that **Fiji is serious about cybersecurity**. As fiber connectivity expands across the islands, Telecom Fiji is ensuring that digital growth is matched with digital safety.

This initiative aligns with broader national efforts, including Fiji’s **National Cybersecurity Strategy 2025-2030** and the operationalization of **Fiji CERT**.





**SEPTEMBER
2025**

ITU Asia-Pacific CyberDrill 2025 – Mongolia

As part of its ongoing commitment to regional cyber resilience, the International Telecommunication Union (ITU) hosted the **Asia-Pacific CyberDrill 2025** in **Ulaanbaatar, Mongolia**, from **September 2 to 5**. This high-impact event brought together cybersecurity teams from over **160 countries**, including several **Pacific Island states**, for a series of hands-on simulations and collaborative exercises.

The goal is to enhance incident response capabilities and promote cross-border coordination in the face of increasing digital threats. Participants engaged in real-time crisis scenarios, technical workshops, and strategic planning sessions designed to test and improve national readiness.

For Pacific nations, the CyberDrill offered a rare opportunity to train alongside global peers, share threat intelligence, and refine protocols tailored to island-specific challenges. The event underscored the importance of **regional solidarity** in cybersecurity and reaffirmed the Pacific's growing role in shaping global digital defense strategies.

Ransomware Trends in Asia-Pacific Report: Akamai's "State of the Internet"

Ransomware attacks across the Asia-Pacific region are evolving rapidly, with new tactics that are more aggressive, coordinated, and damaging than ever before. According to Akamai's latest *State of the Internet* report, threat actors are increasingly deploying what experts call "**quadruple extortion**"—a strategy that combines data encryption, theft, distributed denial-of-service (DDoS) attacks, and public shaming to pressure victims into paying. This multi-pronged approach not only disrupts operations but also threatens reputations and customer trust. For Pacific enterprises, the report serves as a clear warning: traditional defenses are no longer enough. Organizations are urged to adopt **layered cybersecurity strategies**, invest in **real-time threat intelligence sharing**, and prepare for complex attack scenarios that go beyond simple data lockdowns. As ransomware becomes more sophisticated, regional collaboration and proactive defense planning are essential to staying ahead of the curve.

Regional Exposure to APT Threats

Report: TeamT5's 2025 H1 APT Threat Landscape Insights

The Asia-Pacific region—including Pacific Island nations—continues to be a hotspot for advanced persistent threat (APT) activity, according to TeamT5's 2025 H1 APT Threat Landscape Insights. The report highlights a surge in targeted attacks against the **information technology and semiconductor sectors**, with threat actors deploying increasingly sophisticated tactics to infiltrate critical systems. These campaigns often involve stealthy, long-term intrusions aimed at data theft, espionage, or disruption. For Pacific nations, the findings underscore the urgent need for **stronger regional defense coordination**, including shared threat intelligence, joint cyber drills, and investment in resilient infrastructure. As APT groups evolve, so must the region's collective response—turning vulnerability into vigilance.

Cybersecurity Training for Pacific Island Countries

In a significant step toward strengthening regional cyber resilience, the **Cybersecurity Training and Exercise Program** was held in **Fiji** from **September 27 to October 2, 2025**. Organized by **Japan's Ministry of Internal Affairs and Communications (MIC)**, the program brought together cybersecurity practitioners from across Pacific Island countries for a week of immersive, hands-on learning. The training focused on building practical skills in threat detection, incident response, and digital risk management—tailored specifically to the challenges faced by small island nations. Participants engaged in simulated cyber drills and collaborative exercises designed to prepare them for future regional response coordination. This initiative marks a growing commitment to **capacity building and cross-border cooperation**, ensuring that Pacific nations are not only connected—but protected—in an increasingly digital world.

FINAL WORD



From targeted attacks to transformative reforms, **July–September 2025** was a defining quarter for Pacific cybersecurity. The region is no longer just reacting—it's **strategizing, collaborating, and leading**. As threats grow more complex, so too does the Pacific's resolve to build a safer, smarter digital future.