ICTS
LEGAL SERVICES

Cyber news that bites back

Issue 3 • May 2026

Update

WHAT THE HACK?

NEWS

TWO MAJOR SOUTH AFRICAN CYBER INCIDENTS

SPECIAL UPDATE

Dear Valued Clients and Colleagues,

We promised to keep you abreast of the latest on the cybersecurity (or risk) that we are all faced by. The following two, recently reported, incidents underscore the evolving threat landscape in South Africa's financial and public sectors.

Alexforbes CEO Email Accessed in Business Email Compromise (BEC) Attack

Date of breach: 28 April 2026 (Tuesday)

Target: Dawie de Villiers, CEO of Alexforbes - South Africa's largest retirement-fund administrator and a major player in financial services.

Attackers gained access to De Villiers' work email account and used the legitimate executive address to launch a targeted phishing campaign. Recipients (primarily clients and stakeholders) received emails that appeared to come directly from the CEO. The messages urged them to "review and confirm" an attached PDF document labelled as a "revised order".

This is a textbook Business Email Compromise (BEC) tactic: attackers exploit the trust associated with a senior executive's real email address rather than spoofing it, dramatically increasing the likelihood that victims will open the attachment or follow instructions (often leading to malware installation, credential theft, or fraudulent payments).

Company response

Alexforbes acted swiftly: The compromised account was immediately blocked.

- The company issued direct warnings to affected clients and the broader community.
- Recipients were instructed to delete the emails without opening attachments, avoid clicking any links, change passwords, and run full antivirus scans.
- No evidence has been reported of a wider breach into Alexforbes systems or exposure of client retirement-fund data.

The incident forms part of a worrying pattern of cyberattacks targeting South Africa's financial services sector, where high-value data and trusted executive communications make organisations prime targets.

Why this matters

Even sophisticated organisations can fall victim when a single high-privilege account is breached. It highlights the critical need for email security controls (advanced phishing protection, MFA on email, behavioural analysis) and ongoing staff/client awareness training.

R2 Billion Siphoned from Ekurhuleni Municipality in Major Cyber Heist

Revealed: 6 May 2026 during a parliamentary hearing of the Standing Committee on Public Accounts (SCOPA).
Testifying: City of Ekurhuleni Mayor Nkosindiphile Xhakaza and senior municipal officials.

Hackers exploited a shockingly basic vulnerability: an unprotected Wi-Fi network at the municipality's licensing department. By physically driving near the premises and connecting to the open network, they gained unauthorised access to the City's billing system. Once inside, they manipulated records and siphoned off more than R2 billion in revenue.

The breach reportedly took place over an extended period (references point to activity between 2023 and 2024), allowing repeated, undetected extractions. SCOPA members described the incident as a clear manifestation of organised cybercrime exploiting systemic weaknesses in local-government IT infrastructure.

Key technical failure

No encryption, no network segmentation, and apparently no monitoring or anomaly detection on what should have been a sensitive financial system. The billing system handles critical revenue streams (including water and electricity), making the loss especially damaging to municipal finances and service delivery.

Current status

- Investigations are ongoing.
- The hearing placed the matter firmly on the national agenda, with calls for urgent forensic audits and improved cybersecurity standards across municipalities.
- No public confirmation yet of arrests or full recovery of funds.

Why this matters

This is one of the largest publicly disclosed municipal cyber heists in South Africa. It demonstrates how even "low-tech" entry points (unsecured Wi-Fi) can lead to catastrophic financial damage when core systems lack basic protections. It also exposes the broader risk to public finances and service delivery when local governments lag behind in cybersecurity maturity.

Immediate Lessons for Organisations & Individuals

For businesses (like Alexforbes case): Treat executive email accounts as high-risk assets. Enforce MFA everywhere, use AI-driven email threat detection.

Universal rule: Assume compromise is possible. Verify, don't trust - especially when money or sensitive documents are involved.

For public-sector & municipalities (Ekurhuleni case): Never run unprotected Wi-Fi on operational networks. Segment billing/financial systems, implement continuous monitoring, and conduct regular penetration testing.

Get trained: Train staff/clients/yourself to understand cyber risks and threats, allowing them a better chance to verify unusual requests via secondary channels.

These two incidents show that both private financial giants and public institutions remain vulnerable. South Africa's cyber threat environment is intensifying, and basic hygiene failures continue to enable major losses.

If you need support on any mater related to your cybersecurity and cyber resilience, please get in touch. Retirement funds and their providers MUST take this seriously. Stay safe!

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

What The Hack is published monthly or when required. Past editions available on request.