



Cyber news that bites back

Issue 7 • July 2026

WHAT THE HACK?

NEWS

**CYBER
SECURITY
AND CYBER
RESILIENCE
INSIGHTS
FROM
ICTS LEGAL
SERVICES**

**SANLAM
CORPORATE:
THIRD-PARTY
DATA
BREACH
NOTIFICATION**

**ASI: PHISHING
ATTACK**



Dear Valued Clients and Colleagues,



A Never-Ending Story

The cyber threats keep coming, much like that classic tale of persistence (and occasional chaos). In this quick inter-month update, we spotlight two fresh incidents from the SA pensions/insurance space. Stay informed, stay vigilant – because data protection is never “set it and forget it.”



Sanlam Corporate: Third-Party Data Breach Notification

Sanlam has issued a transparent communication to members about unauthorised access to a project and task management system used by a third-party service provider. Although Sanlam's own systems were not breached, some personal information entrusted to them was affected.

Potentially impacted data (varies by member):

Surname

ID number

Sanlam activated its incident response protocols immediately, working with the provider, cybersecurity experts, and internal teams. They're coordinating holistically and monitoring for any further risks. No evidence of public sharing or unlawful use so far.

Key takeaway: No immediate action needed on your benefits, but monitor accounts and communications. Sanlam will never ask for passwords, PINs, or OTPs via unsolicited channels.

Protect yourself:

- Be wary of unexpected emails/SMS/calls requesting info.
- Verify before sharing details.
- Report suspicions to your bank and SAFPS (www.safps.org.za).
- Contact Sanlam Corporate Client Care: SCClientCare@sanlam.co.za or 0861 223 646.

Listen to this very carefully:

From a Joint Standard 2 perspective, your role as the governing body of a Fund or a business is to have oversight and test your 3rd-party providers. Simple "we are compliant" letters are not sufficient!

ASI: Phishing Attack

ASI reports a sophisticated phishing incident where a reputable client's account was used to compromise an employee mailbox. Malicious emails were sent from ASI's domain on 1 July 2026 via Outlook Web Access from overseas.

No client data exfiltration or broader system compromise detected so far – classified as a security incident (not a full data breach), but investigations continue. The mailbox was quickly secured.

ASI's response actions:

Testing Gaps Are the Biggest Risk

- Enhanced monitoring and threat detection.
- Enrolled Microsoft 365 in a dedicated SOC.
- Strengthened email security, authentication, and geo-restrictions.
- Additional staff training on phishing/social engineering.

Advice: Delete the suspicious email if received. If you interacted with links/attachments/QR codes/credentials, contact your IT team immediately. Continued vigilance on unexpected comms is essential.

Questions? rcl@asi.co.za.

The Bottom Line

These incidents underscore the interconnected risks in our ecosystem – third parties, email compromises, and persistent adversaries. For pension funds and trustees: Review vendor controls, update incident response plans, and keep member education front and centre.

The story continues... but with better defences, we can write a happier ending.

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



Closing joke of the day:

Q: Why did the hacker go broke?

A: Because he used up all his cache!

(And in the world of pensions, that's one asset you definitely don't want to lose.)



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.