Our mobile phones are no longer just a communication device - it is a bank card, a password vault, an email gateway and a digital identity. In South Africa, cybercriminals are increasingly using Remote Access Trojans (RATs) to silently take control of mobile phones and steal funds directly from banking apps. For individual **Funds Protect** and **Cyber Protect** policyholders, understanding this growing threat is essential to protecting both their money and their personal information.

Your client is a potential target If they use their phone for:

- Mobile banking
- Approving payments
- Receiving OTPs (one-time PINs)
- Email or WhatsApp

What Is a RAT?

A Remote Access Trojan (RAT) is malicious software that gives criminals remote control of a mobile phone without the user knowing. Unlike obvious viruses, RATs are designed to stay hidden. Once installed, a RAT can:

- Read SMS messages (including banking OTPs)
- Access banking apps
- Capture passwords
- Monitor emails
- Record screens
- Initiate transactions

How Are South Africans Being Targeted?

Common tactics currently circulating include:

- Fake courier delivery SMS links
- “Your bank account has been locked” messages
- Fraudulent SARS refund notifications
- Fake load-shedding or municipal apps
- WhatsApp verification scams
- Fake security updates for banking apps

The link looks legitimate. You click once. The RAT installs silently. Criminals may then monitor user activity for days or weeks before stealing funds.

How Funds Are Stolen

A typical attack works like this:

1. Clicking on a malicious link.
2. The RAT installs in the background.
3. The attacker monitors user banking activity.
4. When the user logs in, they capture their credentials.
5. They intercept OTPs.
6. Funds are transferred out of bank accounts.

By the time your client realises something is wrong, the money may already be gone.

Warning Signs A Phone May Be Compromised

- Battery draining unusually fast
- Phone overheating
- Strange pop-ups
- Irregular banking login alerts
- SMS messages sent without the user’s prior knowledge
- Unknown apps installed

How This Relates to Your Client's Policy

Funds Protect

This policy is designed to respond to a loss of funds from your client's bank account due to the fraudulent conduct of a third party by way of:

- Online banking fraud
- Phishing attacks
- Social engineering scams

Cyber Protect Personal

In addition to the cover provided under the Funds Protect policy, this policy may also respond to:

- Identity theft
- Data breach support
- Incident response services

Each claim is assessed based on the facts and policy wording.

If your client suspects a compromise:

- ✓ Contact the bank immediately
- ✓ Change all passwords
- ✓ Notify the incident hotline as soon as possible (For Cyber Protect clients only)
- ✓ Do not wipe the phone until advised (if forensic investigation is required)

Avoiding RAT attacks

- ✓ Never click links in unsolicited SMS or Whatsapp messages
- ✓ Use the bank's official app downloaded only from the Apple App Store or Google Play
- ✓ Enable biometric authentication on all apps and devices
- ✓ Use authentication apps instead of SMS OTPs where possible
- ✓ Keep the phone's software updated
- ✓ Do not install apps from unknown sources
- ✓ Avoid approving large payments on unsecured public Wi-Fi

Final Thought

Cybercrime no longer starts on a laptop - it starts in our pockets. Our mobile phones are now one of the most valuable assets criminals target. Staying alert and acting quickly can make the difference between a near miss and a financial loss.

Phishield UMA (Pty) Ltd has taken the strategic decision to deactivate the **Cyber Protect Business** product on all third-party vendor platforms.

What This Means

- No new business will be accepted on third-party platforms.
- No renewals will be processed on third-party platforms.
- All new business and renewals will be handled directly through Phishield.

All quote requests may now be submitted to *quotes@phishield.com*

Funds Protect Personal, Funds Protect Business and Cyber Protect Personal products are unaffected – its business as usual on the vendor platforms for these products.

Why This Change Is Necessary

The cyber insurance market is evolving at an unprecedented pace. Pricing dynamics, threat patterns, claims trends, and coverage expectations change rapidly - particularly in the South African SME and corporate cyber space. Due to system limitations on third-party vendor platforms, Phishield has been unable to update rates, benefits, and underwriting criteria quickly enough to remain fully responsive to market developments.

Hosting **Cyber Protect Business** directly through Phishield allows us to:

- Implement rate adjustments immediately
- Enhance cover limits without delay
- Refine underwriting strategy in real time
- Ensure competitiveness and sustainability
- Respond faster to emerging cyber threats

Product Enhancements Since Initial Deployment

Since the product was first deployed on vendor platforms, several important enhancements have been made:

- Revised and reduced rates
- Increased cover limits for Data Restoration costs and Cyber Extortion events
- Improved underwriting strategy to strengthen risk selection and competitiveness
- Enhanced overall product positioning in line with current cyber risk exposures

By migrating administration directly to Phishield's internal platform (Nimbis), we can ensure brokers and policyholders benefit from the most current version of Cyber Protect Business at all times.

Migration of Active Policies

Brokers with active Cyber Protect Business policies on third-party platforms will be contacted individually. Our team will assist with the seamless migration of policies onto the Phishield Nimbis system. The objective is to ensure:

- Continuity of cover
- No disruption to clients
- Improved policy management efficiency
- Access to the latest product enhancements

We appreciate the continued support of our broker partners and remain committed to ensuring that **Cyber Protect Business** remains competitive, responsive, and aligned with the realities of today's cyber threat landscape.

For any queries, please contact your Phishield representative or email *quotes@phishield.com*.

The training format used during 2025 proved to be very successful and will continue for 2026. To book a training slot, please click on one of the links below:

Commercial Lines Training (Monday's 09:00 – 10:00)

https://calendly.com/inze-phishield/phishield-commercial-training

Commercial lines products covered:

ü Cyber Protect Business

ü Funds Protect Business

ü Funds Protect Plus

ü Funds Protect Trust

Domestic Training (Friday's 09:00 – 10:00)

https://calendly.com/inze-phishield/phishield-domestic-training

Personal lines products covered:

ü Cyber Protect Personal

ü Funds Protect Personal

Should you have any queries related to the booking of training, please contact Inze via email at inze@phishield.com.

Should you require in-person training or training on a day which is not scheduled, your training requirements may be accommodated provided there are a sufficient number of persons attending the training.

CLAIM SCENARIO

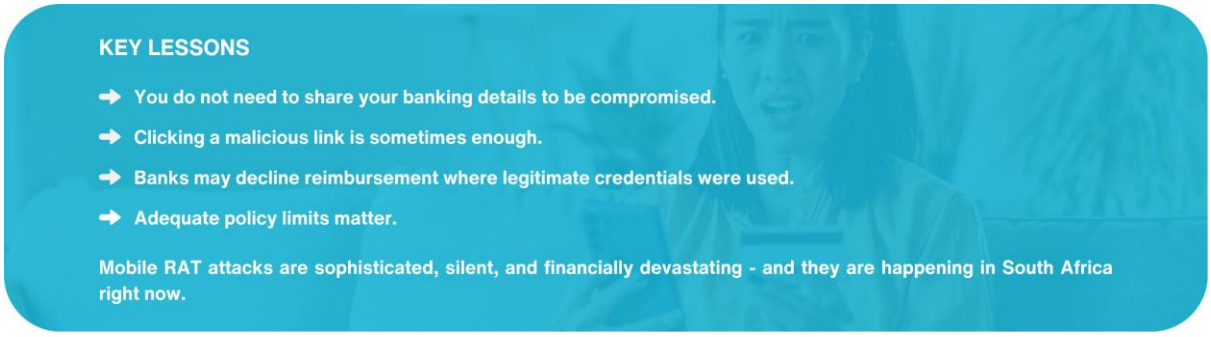
The following is a real-life example of a loss suffered by one of our policyholders because of a Remote Access Trojan (RAT) attack.

The client received a phone call from an individual posing as a customer service agent from South African Airways. The caller informed her that she qualified for a 60% discount on flights for the next twelve months as part of a promotional campaign. During the call, she was sent a link via WhatsApp, which she clicked on while still speaking to the "agent." She did not provide any banking details, passwords, OTPs, or personal information during the call. Unbeknown to her, the link installed malicious software on her mobile phone.

Several hours later, when she opened her banking app to make a payment, she noticed that her account balance was significantly lower than expected. Upon reviewing her transaction history, she discovered multiple unauthorised transactions totalling over R130,000 had been processed from her account.

The client immediately lodged a fraud investigation with her bank. The bank declined her reimbursement request, stating that the transactions had been authenticated using her legitimate security credentials.

The client then submitted a claim under her Phishield policy and was able to recover a portion of her loss. Unfortunately, her policy limit was lower than the total amount stolen, leaving her partially uninsured for the shortfall.



WE'RE HERE TO ASSIST YOU!

If you have any questions, please reach out to your **Phishield Business Development Manager:**

Inze Strydom

073 160 5502

inze@phishield.com

phishield

+27 (0) 10 312 5257

Fourways View Office Park
Block C | 1210 Sunset Boulevard
Fourways, 2055