Tax Season Scams Are Surging - How Accountable Institutions Can Stay Ahead

By Sameer Kumandan, MD of SearchWorks

As tax season ramps up across South Africa, so too does a spike in criminal activity - from phishing emails and fake SARS auto-assessments, to attempts to impersonate clients or breach compliance systems.

It is a peak period for opportunistic scams targeting individuals and sophisticated fraud attempts against financial institutions, in what has become prime hunting ground for scammers. SARS has ramped up its scam warnings, issuing multiple alerts in July alone, addressing attempts to mimic refund audits, letters of demand and auto-assessments, all of which use SARS branding and real phrasing to appear legitimate. The official SARS 'Scams & Phishing' log lists several distinct scam codes issued during July 2025, demonstrating a marked increase in fraudulent activity.

Cybersecurity firm Kaspersky reports that phishing accounted for 67% of cyber incidents among South African organisations over the past year - with a 29% year-on-year increase in such scams recorded as tax season opened.

For businesses, especially accountable institutions handling large data volumes and transactions, the risks are twofold: they may be targeted directly or indirectly impacted through compromised clients.

Accountable institutions have a legal obligation to detect and report suspicious activity, making tax season an especially demanding and high-pressure time. To stay ahead, accountable institutions must understand the risks and adopt a proactive, technology-enabled and compliance-focused approach.

"Tax season has always been a hotspot for fraud, but the level of sophistication we're seeing today is unprecedented," says Sameer Kumandan, MD of SearchWorks. "Scammers are mimicking real SARS communication down to the last detail - and unless organisations strengthen their verification processes, they risk being caught off guard."

For accountable institutions, high data volumes and tight deadlines create opportunities for fraudsters, which is why it's important to be extra diligent about verification, due diligence and compliance processes.

Four strategic focus areas for staying ahead of fraudsters this tax season:

Strengthen identity verification processes

Tax-season scams often involve impersonation - making robust identity verification a frontline defence. Accountable institutions should ensure their Know Your Customer (KYC) protocols include multi-factor authentication (MFA), biometric ID verification, and

real-time document validation against trusted data sources. Dormant, inactive, or high-risk accounts should be reverified before any transactional activity is permitted.

Keep customer records and risk profiles current

Fraud often exploits outdated or incomplete records. Institutions should continuously refresh customer data and risk scores, synchronise records across departments, and use machine learning tools to flag anomalies. Data hygiene is more than a compliance requirement - it's a strategic shield against social engineering.

Leverage technology for real-time monitoring

Transaction monitoring shouldn't be reactive. Use real-time analytics to flag unexpected login behaviour (such as geolocation shifts or device changes), unusually high transaction volumes, or rapid movement in new accounts. Institutions should also monitor for red flags around SARS refund timelines, when fraudulent withdrawals are most likely to spike.

Prioritise education and fraud awareness

Internal teams and clients are often the weakest security link - but also the most scalable defence. SARS regularly publishes updated scam alerts on its website, which institutions should actively circulate. In-house phishing simulations, seasonal fraud briefings, and client education campaigns can significantly reduce vulnerability.

Ultimately, tax season is a pressure test - not only for compliance teams, but for the systems and habits that underpin them. Institutions that invest in proactive monitoring, smarter verification, and