

SARS eFiling Profile Hijacking

See below correspondence from SARS regarding the recent hijacking of eFiling profiles:

"Dear Stakeholder,

Cases reported to SARS from multiple entry points are escalated to the Cybercrime Task Team (CCTT) via an internal Remedy Incident Management process. Each case is then actively investigated by various specialised teams to rectify the matter and return the profile to the rightful owner. Additionally, consultants from our Digital Channels division, working in the CCTT, makes contact with the affected taxpayer/stakeholders to acknowledge the complaint, assist with contact details changes and, if required, request any additional documents.

SARS Criminal Investigations and the SARS Anti-Corruption Unit are also pursuing these matters. This involves, amongst others, engaging with banks to close accounts that were opened fraudulently and to reverse refunds payments made into these accounts.

Should it come to your attention that the problem has recurred, please advise SARS via the return email as provided by the consultants from CCTT, citing the relevant reference numbers and attach any supporting information"

*Please advise your members to take the appropriate security precautions to safeguard their eFiling login credentials (viz usernames and passwords). eFiling usernames and passwords should **NOT** be shared by multiple employees within an organisation; and members are to ensure that access to eFiling profiles by unauthorised employees is revoked. SARS will in the coming months rollout security enhancements to the eFiling login procedures. This will be communicated to you in due course."*

9 November 2021