Protect Your Tax Profile

SARS has robust security systems protecting taxpayer's information. Your information held by SARS can only be accessed using proven authentication methods, such as access using unique usernames and passwords and access confirmation using one-time passwords (OTPs). Fraudsters are using a range deceptive methods to get taxpayers to unwittingly provide them with personal information which are used to defraud the taxpayer and SARS. The fraudsters may also use your personal information in such a way that can result in you having increased tax liabilities to SARS and you can even become the subject of a criminal investigation. You have to be vigilant at all times and protect your personal information from falling into the hands of fraudsters

This is how Fraudsters May Contact With You

Fraudsters will use a different ways to contact you, depending on what information they already have about you. They may contact you on your cellphone either by speaking to you directly, and/or by SMS and/or messaging services such as WhatsApp. The person making contact with you may claim to be working at SARS - using the name of a person who does work at SARS - and will indicate that they are contacting you on behalf of SARS. Always be cautious when you receive a call from a person claiming to be from SARS offering to assist with your tax returns, to help you get a tax refund, or wants your personal and/or business information. WhatsApp and similar messages and SMSs may contain links which you are encouraged to click on. These links may contain trojans which fraudsters will use to gain access to you device to steal personal information from you.

You may also receive emails that appear to come from SARS. This can include the email having SARS identifying marks such as the SARS logo. Emails may ask you to contact a particular person whose details may be included and/or it can contain links which you are asked to click on to open. These links can be marked as "Outstanding Debt", "Final Demand" or anything which will compel you to click on the link and may also contain trojans to gain illegal access to your device.

The fraudsters may also send you adverts of their "tax related services" to your phone using SMS or messaging services and/or via email. They also advertise their services on social media platforms such as Facebook. The adverts may also have SARS identifying marks and even fictitious or real company names and addresses. Rates charged for services are either very low or it may be based on a percentage of refunds obtained. These rates are often outside the range changed by legitimate tax practitioners. The fraudsters will ask you for personal information to enable them to assist you and then use the information to defraud you and/or SARS

This is what the fraudsters want from you

The fraudsters want your identity number, your telephone number, your address (physical and/or work), your email address, your income tax number, VAT number or any other SARS reference number associated with you, your SARS eFiling username and password your bank account details, financial statements. In some instances they may even convince you to provide them with copies of your identity document, and proof of address.

This is why the fraudsters want your information

Depending on the amount of information the fraudsters manage to obtain from you, they may use the information for, amongst others:

- Access your eFiling profile and change banking details and mobile phone numbers to divert refunds to another account and to ensure OTPs are received on the mobile phones only they have access to
- The fraudsters may use your information to submit inflated tax returns to generate a refund which SARS assigns to you. This may result in your tax status being changed resulting in you falling into a higher income tax bracket with a higher tax liability. It can also result in you being subject to a criminal investigation by SARS
- The information you provide to the fraudsters may also be used to register you as a taxpayer with SARS through which false tax returns are submitted to generate refunds from SARS which will impact, often to your disadvantage, your tax status
- Outside of the SARS environment, the fraudsters can use your information for other financial transactions such as obtaining loans or buying items on credit - for which you will be liable.
- The fraudsters can also use the information to open bank accounts using your information to channel money obtained through fraud to themselves. This may be a form of money laundering which can result in you becoming a subject of a criminal investigation. Note that in some instances, fraudsters can ask you to open a bank account on their behalf and to hand over access to the account to them; or them may ask you to allow them to use your account to receive money which they will have you to withdraw for them - allowing you to keep some of the money deposited into your account. Apart from this making you liable to criminal investigation, this additional income may also alter your tax status with SARS, resulting in you having to pay more tax.

This is what you need to do to protect yourself and your personal and business information

- Always use common sense - if you are uneasy about a communication received, treat it as suspicious and do not respond to it
- SARS officials will not ask you for information, such as ID numbers, tax numbers, etc, which are already in SARS's possession. Neither will SARS ask you for your banking details and bank account access details such as PIN numbers or for your eFiling password. Such information should not be provided to anyone over the phone or via email
- If a person contacts you claiming to be from SARS, ask them for their contact details - email address (which must be in this format - nameofperson@sars.gov.za and office telephone numbers. Ask the caller to send you an email using their SARS email address. Contact SARS using contact numbers provided on the SARS website (www.sars.gov.za) and ask to speak to the person who called you.
- If you receive an email which claims to be from SARS, check the email address - it must end with ....@sars.gov.za
- Do not contact persons offering their services on social media platform where they ask you contact them via WhatsApp direct message (DM) or phone only. Should you have any tax related enquires contact SARS directly or make use of a registered tax practitioner
- Do not open any email, sms or messaging links which you cannot confirm originated from SARS
- Ensure the phone and computer which you use to contact SARS and to access your eFiling profile has suitable anti-virus software.
- Ensure you have a strong eFiling password (alpha-numeric with a minimum of eight characters) which is safeguarded. It should not be shared and must be changed regularly.
- Activate the One-Time-Pin (OTP) security feature on your eFiling profile
- Do not use the same passwords on different platforms (eg Facebook, Banking, etc)
- Do not share your password and username
- Do not save your username and password in the browser used to access your efiling profile.
- Access your efiling profile regularly to check if access to it has not been disrupted in any way.
- Avoid accessing your eFiling profile on public wifi hotspots.
- You must log-off completely after accessing your eFiling profile

It is your responsibility to safeguard your personal information.

Should you receive a suspicious email, and not open any links in it and forward it to phishing@sars.gov.za

To report any suspicious activities related to your SARS profile, or if you are aware of anyone offering services to obtain illegal tax refunds or to use bank accounts to receive tax refunds, you should report that to the SARS Fraud and Anti-Corruption Hotline -- **0800-00-2870**