The ABC's you should know

1 April 2022

Phishing and other Scams

Don't be an April Fool

SARS

Members of the public are randomly emailed with false "spoofed" emails made to look as if these emails were sent from SARS, but are in fact fraudulent emails aimed at enticing unsuspecting taxpayers to part with personal information such as bank account details. Examples include emails that appear to be from returns@sars.co.za or refunds@sars.co.za indicating that taxpayers are eligible to receive tax refunds. These emails contain links to false forms and fake websites made to look like the "real thing", but with the aim of fooling people into entering personal information such as bank account details which the criminals then extract and use fraudulently.

Please note these are scams and SARS taxpayers should take note of the following:

- Do not open or respond to emails from unknown sources.
- Beware of emails that ask for personal, tax, banking and eFiling details (login credentials, passwords, pins, credit / debit card information, etc.).
- SARS will never request your banking details in any communication that you receive via post, email, or SMS. However, for the purpose of telephonic engagement and authentication purposes, SARS will verify your personal details. Importantly, SARS will not send you any hyperlinks to other websites – even those of banks.
- Beware of false SMSs.
- SARS does not send *.htm or *.html attachments.
- SARS will never ask for your credit card details.

Other Scams

Phishing has evolved and now has several variations that use similar techniques: **Vishing scams** happen over the phone, voice email, or VoIP (voice over Internet Protocol) calls. **Smishing scams** happen through SMS (text) messages. **Pharming scams** happen when malicious code is installed on your computer to redirect you to fake websites.

Recently we have become aware of **Vishing scams** where you receive a call from what appears to be your bank or some other service provider, for example your cell phone service provider, and the caller appears to have all your personal information. They can read your ID number and your address to you and are very pleasant and helpful. They move through various "security checks" with you and then indicate that

they need another level of verification and tell you that you will receive a PIN that you should read out to them. WARNING! A PIN is a **PERSONAL** Identification Number that is initiated by something **you** do, not a representative of any of these organisations. At this point you should be alerted and end the call without giving the PIN.

Often personal information has been stolen or hacked or sold and the thieves have everything except this one piece of information and that is why they are calling. You should NEVER read a PIN to anyone over the phone.

Be alert and sceptical and do not take phone calls at face value. You can always go into the branch or call the call centre to verify or make any changes that need to be done. That way you are in control.

What to do

If you receive any correspondence that appears to be from SARS, you may forward it to ABC as we are able to check on eFiling if it is correct and in most cases as your Tax Practitioners, we would have received the same communication.

If you receive any other form of communication that makes you feel suspicious follow this principle:

If it smells like a rat, it probably is a rat!

Respond with caution. Go back to the route of communication that you always use with the service provider. Phone them or email them on numbers or addresses that you have used before or that appear on their websites.