Discovery
Corporate and
Employee Benefits

Two-Pot Withdrawals: How to Avoid Being Scammed

Two-pot withdrawals: How to avoid being scammed

AS OF 1 SEPTEMBER, YOU ARE ABLE TO WITHDRAW FROM THE SAVINGS COMPONENT OF YOUR RETIREMENT FUND. BECAUSE THE TWO-POT SYSTEM IS STILL NEW, IT IS VULNERABLE TO SCAMMERS AND FRAUDSTERS.

They may try to steal your personal information so they can withdraw money from your savings component. Follow these tips to avoid being a victim.

Never open or answer emails from unknown sources. Check the email address and make sure that it is the same one your employer or retirement fund normally uses to communicate with you.

Beware of emails, SMSes and WhatsApps that ask for personal, tax, banking and SARS eFiling details. This information includes login credentials, passwords, one-time pins, tax numbers and bank account details. SARS, the retirement fund and your employer will never ask you to confirm information over email, SMS or WhatsApp.

Never submit your details on hyperlinks sent by email, SMS or WhatsApp. Learn the verification process that your company or retirement fund uses to access your account.

Do not open any .htm or .html attachment sent by email. Criminals use these attachments to redirect you to a malicious website that mimics the sign-up pages of your bank or retirement fund to steal your information.

Trust your instinct. A legitimate representative of your retirement fund will never ask you to share sensitive information that can be used to authenticate you. They will also never ask you or rush you to withdraw. If it doesn't 'feel right', then it may be a scam.

Make sure that your data and digital profiles are protected from criminals. Use strong passwords, enable two-factor authentication and make sure that communication is legitimate by checking it against previous communication from the company or retirement fund.

What to do if you become aware of a scam

- Tell your employer immediately about any suspicious activity. Give them the numbers and email addresses that were used in the attempt.
- Contact your fund administrator, using the contact details your employer has given you, to make sure that your profile has not been compromised.

Additional source: SARS