NTRF
NATIONAL TERTIARY RETIREMENT FUND

The Hidden Cyber Risks

Two-Pot Retirement System

South Africa's Two-Pot Retirement system came into effect on 01 September 2024, and while its financial and social impacts have been widely discussed, it's important to highlight associated security issues.

Why does this system increase cyber risks?

The new system involves access to your cash pot, whilst you are still in employment. This means that you can access the money in this Pot without your employer having to verify that you are employed by them. The Two-Pot Retirement system will result in large amounts of money being taken out of the system once members claim their savings withdrawals.

Members may therefore face requests to update banking details, or to click on a link to withdraw money, etc. This situation attracts cybercriminals and fraudsters, as the potential rewards are significant, when millions of people are eligible to access their savings at the same time. For this reason, the National Tertiary Retirement Fund ("NTRF") has decided that your cash pot withdrawals can only be paid into the bank account that your employer uses to make your salary payments into.

IMPORTANTLY:
The NTRF will receive your bank account details directly from your employer. We encourage you not to provide your bank account details to anyone claiming to be from the NTRF, and do not click on any links you receive in an SMS or email to withdraw your savings pot money. Savings pot withdrawals can only be made by logging onto your Momentum Retirement Fund Administrators ("MRA") online profile.

Please be aware of scammers trying to trick you into revealing or changing sensitive personal information. For example, a cybercriminal could pretend to be a pension fund administrator and send a phishing email asking you to click a link to update your details. Any such communication is not from the NTRF.

Is this a one-time risk? No. This increased risk isn't just a one-time event. Over time, the value of your saving pot will grow, making it even more attractive to cybercriminals. Since these accounts are meant for long-term savings, fraudulent activities could go unnoticed for a long time, giving criminals more time to steal funds or cover their tracks.

How to avoid a scam

1. Install an app on your mobile phone that identifies a caller, e.g. TrueCaller.

2. Never click on a link in a message requesting you to confirm a withdrawal.

3. Don’t give your personal or financial information in response to a request that you didn’t make. Never, ever, give anyone your PIN number.

4. If you get an email or text message from someone who claims to be from the NTRF regarding a withdrawal, it’s still best not to click on any links. Instead, contact the NTRF using the website or a phone number that you know is trustworthy.

5. The Fund will not approach you to make a withdrawal – only you can initiate it on the MRA portal. Anyone who pressures you to withdraw or give them your personal information is a scammer.