momentum
METROPOLITAN

Momentum Metropolitan urges you to protect yourself from scams

Your security is a high priority for us, especially as we are seeing an unprecedented increase in fraudulent activity. Scammers are getting very clever in deceiving people, but we can defeat them together if we are extra vigilant, aware, and cautious.

We've listed below a few of the common scams our experts have identified.

Financial scams

Scammers pretend to be from reputable companies. They either create fake social media or WhatsApp posts and profiles to convince you to share your personal or financial information – often with promises of exorbitant or unrealistic financial returns or large sums of money for little or no effort on your part.

The profiles often impersonate real employees or use a real company's name or logo. Always think twice before handing over or depositing money or providing your information to the suspected scammer, as it can be used to access your bank account, make fraudulent purchases, or steal your identity. Once you've deposited your money into the bank account nominated by the perpetrator, you'll likely never hear from them again.

Employment scams

Legitimate employers will never promise work in exchange for an up-front fee or favours. There's also no good reason for you to send them your bank account details prior to securing a job.

Do not go for interviews in unsafe places. Reputable companies will interview you at their offices or a registered employment agency, or via an online call (in the age of COVID). Never agree to meet someone at a private home or apartment for an interview.

Romance scams

Beware of individuals you meet through social media sites or apps, especially if they promise romance before you've met in person. These scammers play on your emotions to defraud you out of your money. They tend to be experts at creating fake profiles. Recently set up profiles or pages with very little information, friends or timeline of existence must be treated as suspicious.

Requests for travel money to meet you, cash gifts or money to help them out of a personal crisis should have you running in the opposite direction, immediately. Not being able to 'meet' them on a video call or to speak on the phone should also be a red flag, especially if they always cancel at the last minute.

Tips to stay safe online

- **Don't share personal or financial information** – Don't share details of your financial circumstances or any other personal information prior to verifying that the information was requested by an authorised representative of a financial services provider. Legitimate companies will not call, email, SMS, or WhatsApp to ask for your personal information.
- **Learn to identify possible scammers, phishing emails, and malicious websites** – We've noted a recent trend where scammers may change one letter in a legitimate email address or use fake websites, or fake social media accounts and WhatsApp profiles to defraud you. Their objective is purely to access your personal accounts, such as email accounts, bank- and other financial accounts.

- **Know who you are transacting with** – Momentum or Metropolitan employees will never ask you to deposit money into differently named or personal bank accounts or to make payments via WhatsApp. If you receive a call or email from someone claiming to be from Momentum Metropolitan, first contact us directly to verify that the adviser, employee, investment, or added-value offer is real.
- **Never deposit money into personal bank accounts** – Always check that lump sum payments, any money or premiums are going directly to the company and not to individuals or personal bank accounts.
- **Be careful what you share -** Beware of unsuspected attempts to get your personal information, like filling out application forms, answering phone surveys or responding to social media quizzes. Don't fill out every field on your social media profile such as your phone number, home address or company details – including these details significantly increases the chance of identity theft.
- **Stranger danger** – Beware of direct messages or friend requests from people you don't recognise or can associate with known friends of yours.
- **Get rich schemes are just that, schemes** - Beware of unrealistic promises of low repayment loans and high financial returns over a short period of time. If an offer looks suspicious or too good to be true, it usually is.
- **Don't be pressured in deciding on the spot** - Offers that are time sensitive or urgent are usually scams. Legitimate organisations will give you time to make an informed decision, so don't be pressured into making decisions immediately.
- **Interception of e-mails is increasing** - When someone clicks on a phishing link, a link that looks identical to the legitimate address, the criminal can gain access to your email account, upload malware to your machine or take over your machine. Tip: Hover over the link with your mouse (but don't click on it) to confirm the email address or website is legitimate. It is highly recommended to change your email account settings to enable multi-factor authentication.
- **Constantly review and improve the strength of your passwords** - Password123 is not a good password! And DO NOT use the same password for all your online activity. Create complicated passwords, consisting of capital letters, numerical numbers and special characters that are not easy to decipher and remember to change them often.
- **If anything feels wrong, stop, and check what you are doing -** Check every detail and every spelling, contact the company directly to check if it is them that you are doing business with. Especially check bank deposit details and never hand over cash or deposit money into an individual's account. A moment to check or one phone call can save you from being caught out.

What should you do if you suspect you are being or have been scammed?

- If you are unsure about the legitimacy of an offer or would like to verify any Momentum Metropolitan employee, rather contact info@mmltd.co.za
- If you come across a social media account impersonating a Momentum Metropolitan employee, report it to info@mmltd.co.za or send us a private message on Twitter, Facebook, LinkedIn, or Instagram.
- If you have already sent them money, you unfortunately have very little chance of recovering your money.
- Report and lay a charge with the South African Police Services.
- Where identity theft is suspected, the matter must be reported to the South Fraud Prevention Services on https://www.safps.org.za/Home/About