METROPOLITAN

Protect yourself against fraudsters and scammers

- Avoid sharing or exposing your personal or policy information. Carefully throw away or shred any old policy documents, letters or statements. Scammers have even resorted to going through bins to find discarded policy documents. To keep all confidential information secure and private, opt to receive your policy documents electronically via email or downloaded straight to your phone on our WhatsApp channel.
- Keep track of any changes made to your policy. Metropolitan will always notify you when we change your details. Check your emails and SMSs notifying you of updates on your contact or banking details and contact us if it isn't you transacting with us.
- Monitor your claims to verify your claim submissions. Contact your financial adviser or our call centre on 0860 724 724 if you've been notified of a claim you're unaware of or did not initiate.

Red flags to watch out for

-Emails asking for personal details (ID, passwords, pins)
-Emails from public domains or poor grammar/spelling
-Suspicious links or attachments in messages
-Generic greetings like "Dear Customer"
-URLs that don't match the company's official domain (metropolitan.co.za)

Phishing
Phishing is a type of online scam where fraudsters trick you into sharing personal or financial information by pretending to be a trusted source, like your bank or a well-known company.

Types of phishing scams

Deceptive phishing
You get a credible-looking email from a bank or other reputable institution asking you to confirm personal information either by responding to the email or following a link. No bank will ever ask you to disclose sensitive information through an email, SMS or digital link.

Link manipulation and smishing
Crafty and often difficult to spot. You get a link and click on it, thinking it's taking you to a specific website, but you land on the phisher's malicious site. Always be wary of emails prompting you to click on links or attachments.

Spear phishing
Unlike traditional email phishing, where one email is sent to numerous random users, spear phishing is more targeted. Fraudsters study their victims' online habits then customise their messages accordingly. When you open the email, the source and content look legitimate, and the next thing you know, you've been scammed.

Vishing
Vishing is phishing done through a phone call. The aim is to trick you into handing over confidential information to the caller, who usually claims to be representing a legitimate institution such as your bank.

Website spoofing or forgery
Criminals create a replica of a genuine website, with the aim of collecting confidential information from users in order to defraud them. Always check to see if the URL is correct and matches the website. Preferably type the URL yourself rather than follow a link.

Tips to stay safe online

- Never share **personal or financial** info with unverified sources.
- Avoid clicking **unknown links** – hover to preview before opening.
- Don't deposit money into **personal accounts** – always verify payment details.
- Be sceptical of "**get rich quick**" offers.
- Don't feel pressured to make **decisions** immediately.
- Use **strong passwords** and multi-factor authentication.
- Limit the **personal information** you share online or on social media.
- Change your **passwords** regularly and avoid reusing them.

Already been scammed?

Take action immediately

- Contact us at info@metropolitan.co.za
- Report fake social accounts impersonating Metropolitan.
- Notify the South African Police Services (SAPS)
- Report identity theft to South African Fraud Prevention Service (SAFPS)
- Alert your bank, insurers, and other financial providers
- Change all passwords (email, social, banking, etc.)
- Run a full device malware/virus scan
- Inform credit rating agencies to secure your credit record
- Call the SAFPS helpline at +27 (0)11 867 2234

If you need to confirm the authenticity of a transaction, contact us directly.
Speak to your certified Metropolitan Financial Adviser.

Call: 0860 724 724
Email: info@metropolitan.co.za

Stay alert. Stay informed. Stay protected with Metropolitan. **Together we can**

Together we can

www.metropolitan.co.za