KASTELO

SECURING YOUR ACCOUNT

Kastelo is committed to ensuring the financial security of our clients. Hence, we've employed advanced technologies aimed at safeguarding your personal and financial information, but it remains your responsibility to be vigilant and take the necessary precautions. We have compiled a few tips to help you stay safe and avoid the most common scams, such as phishing attacks, account takeovers and other malicious activities:

1. THE OFFICIAL KASTELO WEBSITE

- Always ensure that you are interacting with www.kastelo.co.za. Fraudsters often create websites that look nearly identical to the original sites but may have small spelling differences (e.g., kastell0.co.za or kast5lo.co.za). Before entering your sensitive information, double-check the URL to confirm you are on the actual Kastelo platform.
- Consider bookmarking the official website to avoid navigating to fraudulent sites.

2. PHISHING

- Phishing is a common scam in which fraudsters deceive you into disclosing personal information, such as usernames, passwords, or financial information.
- Always check the sender's email address. Kastelo will only communicate using email addresses that finish with @kastelo.co.za or @kastelo.com
  If you receive an email from another domain, it might be a phishing effort.
- Do not click on or follow links or download files from unexpected emails, especially if they promise speedy results or immediate action.
- Offers that appear too good to be true frequently are. If you are promised unusually large sums of money or receive urgent requests, double-check their validity before taking any action.

3. MALWARE AND IDENTITY THEFT

- Identity theft can occur if someone gets hold of your Personal Information and impersonates you on the web.
- Malware can give fraudsters access to your devices and accounts. To avoid this:
  - Frequently action security updates on all your devices;
  - Use reputable antivirus software;
  - Avoid downloading attachments or software from unverified sources;
  - Protect your identification documents and report any loss or theft immediately.

4. PHONE, SMS, AND INSTANT MESSAGING SCAMS

- Kastelo will never ask for sensitive information such as your password, OTPs, or 2FA codes over the phone, via SMS, or through messaging apps.
- If in doubt, hang up and contact Kastelo directly using the official contact details provided on our Website.

5. PASSWORD

- Your password is your first line of defence. Use a unique password with at least 8 characters, mixing upper and lowercase letters, numbers, and special symbols. A password manager can help you create and store strong passwords securely. Never reuse passwords across different websites. Keep your online ID or password private. Never write these details down or share them with anyone, not even with a Kastelo employee.

- Ensure to regularly update your passwords to enhance security.

6. KEEP AN EYE ON YOUR ACCOUNT

- Regularly review your Kastelo Account for any unusual transactions. If something seems out of the ordinary, contact info@kastelo.co.za immediately for assistance.

- Never leave your device unattended after you have entered your Kastelo Profile password. Always log off or sign out at the end of a session.

7. COMPROMISED KASTELO ACCOUNT

If you believe that your Kastelo Account has been compromised, contact info@kastelo.co.za immediately. Kastelo cannot be held responsible for losses due to unauthorised transactions, but will assist in resolving the issue if appropriate.

8. STAY UP TO DATE

Make it a habit to stay informed about the latest scams and how to protect your assets. By following these tips and staying alert, you can ensure your personal and financial information remains secure with us.