



July 2026

Important Security Alert: Beware of Spoofed Emails and Phishing Attempts

Dear Supplier,

We would like to alert you to an attempted spoofing and phishing incident where criminals tried to impersonate Sibanye-Stillwater to mislead suppliers and potentially facilitate fraudulent activity.

In a recent example, an email address using the domain **sibanyestilwater.co.za** was used to contact suppliers. Please note the subtle differences: the domain contains only one "L" in "stilwater" and uses **.co.za** instead of Sibanye-Stillwater's legitimate **.com** domain.

These types of attacks are designed to look convincing and may appear to come from a trusted person or organisation. Criminals often rely on small changes in email addresses, urgent wording, or requests for payment or sensitive information to trick recipients into acting quickly without checking.

Tell-tale signs and common red flags

- **Slight changes in the email domain:** Watch for missing letters, extra letters, swapped characters, numbers replacing letters, or domains that look almost correct.
- **Unexpected domain endings:** Be cautious if an email uses a different ending than expected, such as **.co.za** instead of **.com**.
- **Urgent or pressured requests:** Messages that push you to act immediately, bypass normal processes, or keep the request confidential, should be treated with caution.
- **Payment or banking changes:** Any request to change banking details, payment instructions, invoice details, or supplier information must be independently verified.
- **Unusual wording or tone:** Be alert to wording, phrasing, or tone that differs from previous communications. However, remember that AI can make fraudulent emails appear polished, reducing obvious warning signs such as poor grammar or spelling mistakes.
- **Unexpected attachments or links:** Do not open attachments or click links if the email is unexpected, suspicious, or asks you to enter login details or confidential information.
- **Changed reply-to address:** Check whether replies are directed to a different or unfamiliar email address.
- **Requests for confidential information:** Be suspicious of any request for passwords, login credentials, banking information, tax details, supplier documents, or personal information.
- **Unusual timing:** Emails sent outside normal business hours, especially with urgent instructions, should be carefully reviewed.
- **Too good to be true or out-of-process requests:** Be cautious of unexpected opportunities, refunds, tenders, or payment arrangements that do not follow normal business channels.





July 2026

What to do if something looks suspicious

- **Do not respond to any RFQ, spot bid, tender, or related request received via email.** All legitimate events and requests are exclusively available on the **Coupa System** and must be viewed and submitted only through the **Coupa Supplier Portal**.
- **Do not click links or open attachments** until the email has been verified.
- **Do not respond directly** to the suspicious email or use contact details provided in that email.
- **Contact your known Sibanye-Stillwater contact** using trusted contact details that you have used before.
- **Confirm any payment, banking, or supplier-detail changes** through an independent and trusted communication channel.
- **Report any suspicious emails to:**
 - ictservicedesk@sibanyestillwater.com
 - suppliers@sibanyestillwater.com
 - suppliercommunication@sibanyestillwater.com
- **If you are unsure, stop and check:** Do not click, do not rush, step back and evaluate the message before taking any action.

Important reminders:

Sibanye-Stillwater will not ask suppliers to bypass normal verification processes or make urgent changes to banking or payment details without proper confirmation through official channels.

Any public events advertised will appear solely on the **Sibanye-Stillwater website** and the **Coupa Supplier Portal Public Events page**: [Available tenders - Sibanye-Stillwater](#).

Please note:

*This communication is directed to our **SA Region** suppliers and contractors and does not impact the other international regions*

Your vigilance is an important part of preventing fraud. When in doubt, please pause and verify.

