# BUSINESSES ALERT:

## Beware of Change-of-Banking-Details Scam

Businesses need to stay alert as scammers are using increasingly clever tactics to deceive them, especially during payment transactions. It's crucial to double-check supplier details thoroughly before making payments to minimise the risk of falling victim to scams like the change-of-banking-details scheme.

## HOW SCAMMERS OPERATE:

- Your company receives correspondence purportedly from a supplier, indicating altered banking details.
- You're urged to update your records accordingly and direct future payments to the new account.
- However, the provided account information is fraudulent, diverting payments to the scammers instead of your legitimate supplier.

## PROTECT YOURSELF WITH THESE 4 STEPS:

### 1 SCRUTINISE EMAILS:

- Watch out for minor discrepancies in email addresses or domain names, which scammers often exploit.
- Pay attention to subtle alterations, such as misspelled domains or domain suffixes (for example, .com instead of .co.za).

### 2 VERIFY SUPPLIER IDENTITY:

- Maintain direct communication with trusted contacts within your supplier network.
- Exercise caution when receiving requests from unfamiliar sources claiming to represent suppliers.

### 3 INDEPENDENTLY VERIFY REQUESTS:

- Always authenticate any change-of-banking-details requests through separate channels.
- Avoid responding directly to the email or contact provided in the suspicious correspondence.

### 4 SAFEGUARD INFORMATION:

- Protect sensitive company data and refrain from disclosing it to unverified parties.
- Consider alternative methods for sharing banking details with trusted contacts, such as secure communication channels.

## WHAT TO DO IF SUSPICIOUS:

- Immediately report suspicious activity to your bank's fraud department.
- Forward the questionable email as an attachment to the designated fraud email address provided by your bank.
- Promptly delete the suspicious correspondence after reporting.

## REMEMBER:

Your bank will never solicit your card details via email or SMS. Stay vigilant and report any suspicious activity promptly to safeguard your business from financial scams.