
Invicta
HOLDINGS LIMITED

Invicta
HOLDINGS LIMITED

# PHISHING SCAM RISK

Phishing is when fraudsters send you unsolicited emails, in which they claim to be from a reliable organisation, like a bank or an email service provider.

**How it works:**

- You receive an email request to update or confirm your details by clicking on a link or an icon
- Once you click on it, a fake website is launched
- On the website, you are asked to share your account details, username or password for online banking, email account, cellphone number or bank card details
- Any details you provide on the fake website are captured by the fraudsters and used to defraud you

**How to identify it:**

- There's usually a sense of urgency in the email, followed by a threat (like the suspension of your bank account)
- You need to respond quickly, not giving you time to think things through or ask someone for advice
- The email says you have been a victim of fraud, or due to receive funds, and you need to login to your accounts by clicking on a the link to report the incident and cancel your bank card, or give permission to accept the sum of money
- You're asked to supply your personal and account details via a hyperlink, attachment or icon, provided in the email

# CHANGE OF BANKING DETAILS SCAM

This is when fraudsters attempt to steal funds by posing as one of your suppliers, or someone you're meant to pay, and asking you to update their bank account details.

**How it works**

- You receive an email, letter or fax supposedly from a recognised supplier
- You are informed of a change in bank account details and asked to update your records accordingly
- But these 'new' bank account details are false
- So, your monthly payment is paid to the scammer instead of your supplier

**How to identify it**

- The request doesn't come from your usual 'contact' or point of contact at the supplier
- The request for change of bank details wasn't made via official correspondence or using the contact details that you have in your database
- In some instances, fraudsters may spoof the e-mail address of the supplier or falsify the e-mail address to look like that of the supplier

- If you ever receive such a request, confirm it with a contact you trust before changing any bank account details

**What you can do:**

- If you receive a suspicious email containing links, please forward it to info@invictaholdings.co.za for shutdown