Mercantile Bank
The Business Bank inspired by entrepreneurs

IMPORTANT NOTICE:

Your attention is drawn to the Conditions of Use and Disclaimer as it appears on this website under the links "Terms and Conditions" and "Disclaimer" which should be read with the following:

BE AWARE AND VIGILANT OF INTERNET SCAMS

You will often get some pretty strange emails asking us to 'click here', send personal information including passwords or claim a great big prize we've won. As exciting as it might sound to win a big prize for a competition you have not entered, this might cost you more. Unfortunately, the Internet holds many risks to the security of your personal information and money. Some of these are:

Phishing is the attempt to acquire sensitive information by masquerading as a trustworthy entity in an electronic communication.

Pharming: Pharming seeks to obtain personal or private (usually financial related) information through domain spoofing.

Smishing: In computing, SMISHING is a form of criminal activity using social engineering techniques similar to phishing.

Webpage spoofing: In this attack, a legitimate webpage such as a bank's site is reproduced in "look and feel" on another server under control of the attacker.

More details about these and other risks appear: under the heading: **IMPORTANT SECURITY INFORMATION FOR ELECTRONIC BANKING**

PLEASE BE vigilant before opening or responding to emails with unknown sources or look suspicious.

Below are just a few tips to be savvier;

- Do not open or respond to emails from unknown sources;
- Read emails that appear to be from us asking for personal details with suspicion, as a bank would never ask for personal information via email;
- Never provide your personal details, for example, your PIN or account details to unknown persons or sources whose identities cannot be rightfully verified;

- Do not follow any links or open attachments in emails that direct you to our internet banking website. Always enter our website address (www.mercantile.co.za) in the address bar to connect to our Internet banking site;
- Do not create shortcuts on your desktop to Internet Banking. Malicious software could redirect the shortcut to a fake site;
- Avoid using public terminals (such as Internet cafes) for Internet banking;
- Do not open other websites while logged into internet banking, only have a single browser window open;
- When accessing Internet banking, check for the padlock icon and https at the beginning of the banking sites URL in your browsers address bar;
- Beware of supposedly confirmatory e-mails from almost identical e-mail addresses, such as .com instead of .co.za, or addresses that differ from the genuine one by perhaps one letter that can be easily missed;
- Instruct staff with the responsibility of accessing Internet banking to scrutinize invoices for irregularities and escalating suspicions;
- Secure your smart phone enabling the lock screen and security function.
- Where possible don't save any sensitive personal information and bank account details on your electronic devices;
- Think before you download apps to your mobile or tablet devices;
- Download and install the security software;
- Disable any wireless connection settings (e.g. Bluetooth, Wi-Fi and NFC) when you're not using it.

The use of internet banking is entirely at your risk Mercantile does not accept any responsibility for the risk or loss resulting from the use of internet banking