Mercantile Bank
The Business Bank inspired by entrepreneurs

INTERNET BANKING SECUTIRY TIPS

Call **0860119923,** We are listening

01

PHISHING

Phishing is a psychological attack used by cyber criminals to trick you into giving up information or taking action. Phishing originally described email attacks that would steal your online username, password, and any other message-based attack.

These attacks begin with a cyber criminal sending a message pretending to be from someone or something you know, such as a friend, your bank or a well-known store. They will not only use emails, but will also use other methods, such as instant messaging or social media posts.

SAFETY TIPS

- Do not click on links or icons in unsolicited emails.
- Do not reply to these emails. Delete them immediately.
- Do not believe the content of unsolicited emails blindly. f you are worried about what is alleged, use your own contact details to contact the sender to confirm.
- Don't send emails that contain personal information, such as your card number and expiry date.
- Install a spam blocker on your email system. This will ensure that fraudsters find it difficult to send you phishing emails.
- Keep your operating system, browser, and antivirus software up to date on your personal computer/laptop or cell phone, as they include important security enhancements to help detect phishing sites and malware.
- Should you realise that you have responded to a phishing mail, change your internet banking credentials immediately and advise your bank.

02

VISHING

Vishing is when a fraudster phones a victim posing as a bank official or service provider, and uses social engineering skills to manipulate them into disclosing confidential information, while at the same time leading them to believe that they are speaking to the bank or service provider. This information is then used to defraud the victim.

TIPS

- Be conscious of the fact that criminals can mask their telephone numbers to appear as though it is a legitimate individual or company that is making the phone call.
- Never share personal and confidential information with strangers over the phone.
- Also note that Banks will never ask you to confirm your confidential information over the phone.
- If you are uncertain ask for the person's information and call your bank or relationship banker to verify.

03

PHARMING

Pharming seeks to obtain personal or private, usually financial-related information, through mimicking the Mercantile website, through what techies call a "spoofed domain".

TIPS

- Check that the domain name as https in front of the bank's URL.
- Also look out for the lock on the left (it must be closed).
- Log onto your bank's website by typing in the web address yourself, instead of accessing it via Google search, as it might lead you to a spoofed site.
- Do not use web links that are saved under your Favourites, and never access

04

SMISHING

Smishing, short for SMS Phishing, is where criminals send an SMS, often purporting to be from your bank, requesting personal or financial information such as your account or PIN number. Criminals are aware that people are spending more and more time on their smartphones, but also know that users are often using their smartphones on-the-go, or when in a hurry, and may be less likely to scrutinise and deliberate SMS's with suspicious links. Clicking on these suspicious links may install malware onto your phone, or could take you to a spoof website where you will be asked to enter personal or confidential information.

TIPS

- Do not click on links or icons in unsolicited SMS's.
- Do not reply to these SMS's. Delete them immediately.
- Do not believe the content of unsolicited SMS's blindly. If you are worried about what is alleged, use your own contact details to contact the sender to confirm.

05

MALWARE

Clicking on an unsolicited link or icon could also result in a victim's computer being infected with malware (malicious software). The malware used in internet banking fraud is software designed to gather and send sensitive information to a predetermined destination, under control of the criminal. You could be tricked into infecting your computer with malware through clicking on a link or an attachment in an email, as well as through accessing a fake website purporting to sell you software to fight malware. Criminals deploy malware designed to harvest banking credentials. These malicious programs relay the keys typed to the criminals who then decipher bank-related usernames and passwords. The compromised information is then used to access the victim's online banking profile unlawfully, and should there be funds available, these are transferred into the criminals account.

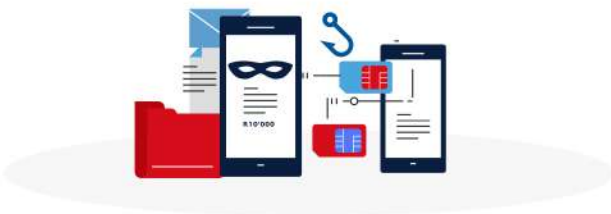
TIPS

- Ensure that the device you use for internet or mobile banking has the latest version of antivirus and antispyware software installed from a reputable vendor.
- Do not do your banking on a public or unfamiliar computer found at libraries, internet cafes and hotels.
- Avoid using WiFi hotspots, and ensure your own wireless network is encrypted before performing any banking transactions on your private computer. Prevent illegal software from being downloaded on your computer by creating administrative rights.
- Beware of fake anti-virus software that is offered at no charge, as it could contain malware.
- Do not use unknown devices, such as USB flash drives on your system, as they may transfer malware unknowingly.
- Avoid downloading pirated software as it may contain malware.
- Remember to log off immediately when you have finished banking.
- Install a personal firewall on your PC.

06

SWIM SWOPS

Through fraudulent SIM swops, criminals can take control of their victim's mobile number, enabling them to receive SMS's sent by the bank to the client. These include Transaction Verification Codes (TVC), Random Verification Number (RVN), PINs, or One Time Passwords (OTPs). Using these codes, together with compromised login credentials, criminals can change, add beneficiaries, and transfer money out of the victim's account.
Criminals are also known to port their victim's cellphone number fraudulently before doing a fraudulent SIM swop. Mobile Number Portability (MNP) gives mobile phone users the ability to move to another mobile network and still retain their mobile number (MSISDN). In this scenario, the victim's SIM card is deactivated and the criminal receives communication for the new SIM card issued by the second mobile network operator, enabling them to receive a victim's Transaction Verification Codes (TVC), Random Verification Number (RVN,) PIN or One Time Passwords (OTPs).



TIPS

- Be suspicious if you receive lots of spam email or SMS messages. It could indicate that your computer or cell phone has been infected.
- Memorise your PIN and passwords and never write them down or share them, not even with a bank official.
- Make sure your PIN and passwords cannot be seen when you enter them.
- If you think your PIN and/or password has been compromised, change it immediately either online or at your nearest branch.
- Choose an unusual PIN and password that are hard to guess and change them often.
- For your security, you only have three attempts to enter your PIN and password correctly before you are denied access to your services.

CELLPHONE BANKING

The mobility of your cellphone allows you to bank at any time from practically anywhere. It is a safe way of doing your banking as it relies on encrypted SMS messages or secure WAP connections. WAP uses similar security as that used by Internet Banking. It is therefore important to make sure that your cellphone is locked at all times and that the latest software is downloaded to ensure your safety.

IMPORTANT NOTES

- Memorise your PIN; never write it down or share it with anyone.
- Make sure no one can see you entering your PIN.
- Choose an unusual PIN that is hard to guess, and change it often.
- Remember, for your own security you are required to re-enter your PIN before each transaction.
- If you think your PIN has been compromised, visit your nearest branch and change it immediately.
- Protect your phone content and personal information by using a PIN or password to access your phone. Do not leave your phone unlocked.
- Do not respond to competition SMS's or MMS's.
- If you receive a phone call requesting personal information, do not respond and end the call.
- If you use a smartphone, install an up-to-date anti-virus application to your cellphone. Most banks provide this free of charge to thier customers.

INFORMATION COURTESY OF

sabric

Making South African banking safe, secure and fraud free

GET IN TOUCH

W www.mercantile.co.za

Mercantile Bank
The Business Bank inspired by entrepreneurs