NMB BANK LIMITED

What is phishing?
Phishing happens when fraudsters send you an email claiming to be from a legitimate organization, an example being your Bank. The aim of these emails is to mislead you into disclosing sensitive information relating to your banking relationship. The emails may request you to click on an embedded link which will lead you to a fake website or clicking on an email attachment.

Some requests may request you to disclose your card details and or PIN. Some may request that you provide your account number and some may ask for you to reveal your online banking details. Once you have supplied this information the fraudsters are able to access and transact on your accounts.

Note
As a Bank, we would never ask you to divulge such information. This is done to protect you from such nefarious activities.

How to protect yourself
You can help to protect yourself from these fraudsters by being vigilant and doing the following;

- Treat any email that requests for your banking details with suspicion.
- Always verify requests that come through email by calling your account manager or branch.
- Always check the sending email address to see if it is different from the know Bank email addresses.
- Do not open attachments sent through email coming from sources you do not know or do not trust.
- Do not click on links that claim will point you to our websites. Rather, type in the addresses of our websites manually (www.nmbz.co.zw or https://www.nmbdirect.co.zw)
- Ensure you have an antivirus program installed on your computer and that it is always up-to-date.

What to do if you suspect you have been compromised
If for some reason you believe you have been compromised, you should perform the following actions;

- Advise your account manager or your branch immediately so that your account can be monitored.
- Check your account for any suspicious transactions and report any that you may find immediately.

Sample Phishing emails

Below are sample phishing emails with fake email addresses. These should assist you to identify how the fraudsters work.

From: NMB Bank Limited [mailto:snafuu191@solcon.nl]
Sent: Monday, April 27, 2015 8:20 AM
Subject: Your Secure Mail Notice

Dear Valued Client,

We notice a system charged error on your account so we suspended your account and Internet banking transaction profile.

To clear the system error and unlock your account **Click here**

NMB Bank Limited.

From: NMB Bank Limited <onlineservice@nmbdirect.co.zw>
Date: Thu, 30 Dec 2010 12:27:35 +0200
Subject: Important Security Notification
To:
Dear Account Holder,

NMB Bank is committed to maintaining a safe environment for its community of our personal and business customers.
To protect the security of your account, NMB Bank Employs some of the best advanced security systems in the world and our anti-fraud teams regularly screen the system for unusual activity.

In accordance with NMB Internet Banking user Agreement and to ensure that your account has not been compromised, access to your account was limited.

Your Account Access will remain limited until this issue has been resolved. In order to secure your account and quickly restore full access, we may require some specific information from you for the following
reason:

We encourage you to login and access your full information here with the link below.

For Personal Internet Banking, Click here
https://www.nmbdirect.co.zw/personal/ to continue with the verification process.
For Corporate Internet Banking, Click here
https://www.nmbdirect.co.zw/corporate/ to continue with the verification process.

Failure to verify your account details may lead to account disconnection

Thank you.

Information Technology Department
NMB Bank Limited