



A VERY IMPORTANT SECURITY MESSAGE FOR ALL ISINET CUSTOMERS

National Bank of Vanuatu advises that hoax emails are again in circulation.

The Bank is aware of an attempt by **Online Criminals** to establish a look-alike *IsiNet* website designed to obtain your login details.

This is a common strategy employed by criminals against bank customers, all over the world. NBV is not a special case.

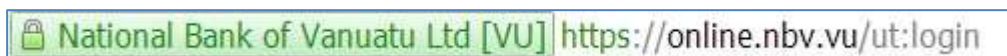
IsiNet employs all international-standard security features for Internet Banking. However, it is not possible for the Bank to prevent you being tricked into providing your login details to Online Criminals.

NBV will **never** send unsolicited emails containing web links, asking you to click on them. If you receive a message like this, *it is fraudulent and has not been sent by NBV.*

Never click on any links contained in these emails and ignore their instructions.

It is **very important** that you adhere to the following practices when accessing *IsiNet*:-

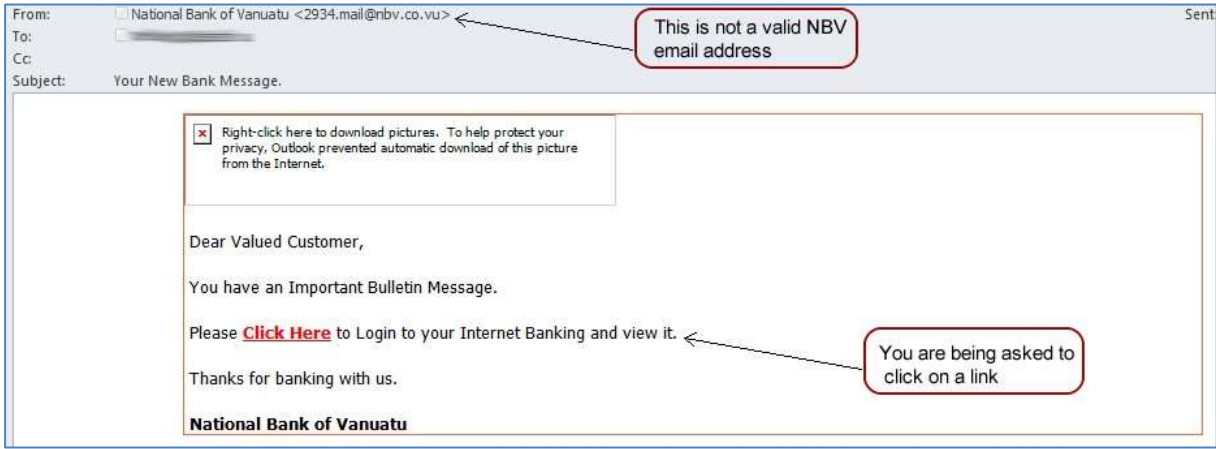
- 1) You should only access *IsiNet* from the button provided on the NBV Website.
- 2) From the *IsiNet* login screen, you should always look to see if the security certificate information is in the top of the screen (left or right side, depending on the Internet browser you use), and the web address must be 'https://online.nbv.vu/ut:login' :-



- 3) You can click on this security indicator to see that it is a valid certificate, as per below:-



Example of a fraudulent email and fraudulent IsiNet:-



If you clicked on the link in the fraudulent email, you would see the following (slightly different depending on the browser you use):-



For further information, please phone the Bank on +678 22201.