

## SECURITY ALERT TO THE CUSTOMERS AND GENERAL PUBLIC

It has been appearing in news that customers of various Banks have been tricked into parting with personal information like password, account nos., etc by replying to fake/ misleading emails (popularly known as Phishing) apparently emanating from Bank's e-mail id. The e-mail states that the customer's account has been chosen for verification purposes or similar reasons and customers were being requested to update sensitive account information like user-id, password, Transaction password, Debit card number etc. by clicking on the link provided in the e-mail or by visiting a web site.

It has been found that the hyperlink provided in the email was directing the customers to a web page hosted in an upcountry based web server, deceptively similar to the Bank's home page. Once the information is submitted by the customer, he/she is redirected to the Bank's original web site.

In this regard the customers are advised to take note of the following:

Indian Bank does not request the account information of the customers in any form. Please do not provide personal information like user-id, login passwords, transaction passwords, pin number, cvv number, Debit card or credit card number etc to any entity in response to email / oral/ SMS or any other form of request.

If you receive any email claiming to be from Indian Bank requesting to update sensitive account information, please forward the email to [indbank@vsnl.com](mailto:indbank@vsnl.com) or [ebanking@indianbank.co.in](mailto:ebanking@indianbank.co.in)

If you have revealed any sensitive account information as indicated above, please change the passwords or pin number immediately.

Do not click on any link to access our web site. Always type <http://www.indianbank.in> or <https://www.indbank.net> in the browser address field to access the web site/ netbanking page of Indian Bank.

View any mail request for financial information or personal data with suspicion.

Contact the Bank and confirm before acting on such e-mails.

Periodically verify the transaction history of your account for correctness.

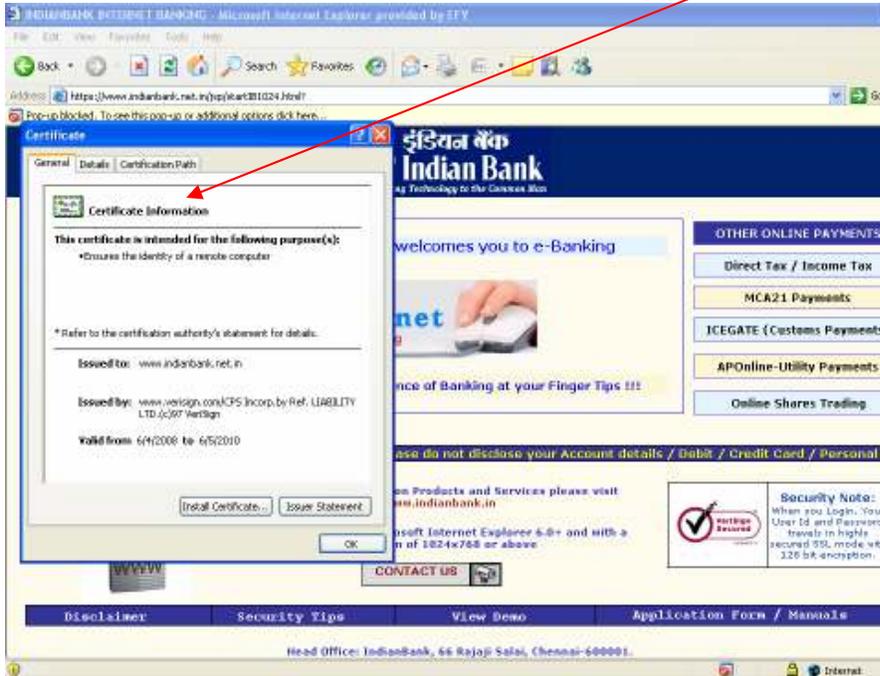
Look for the correct URL address and also the SSL (Secure Socket Layer) lock sign at the bottom of the browser of Internet Banking site of Indian Bank as given below.



When the mouse cursor is kept near the Lock, the display will be like this:



When the user double clicks on the lock symbol, the following screen is displayed.



Please ensure that the latest version of browser is installed and phishing filter is enabled in the browser.

Please follow the above guidelines for safe Net banking / ATM services.