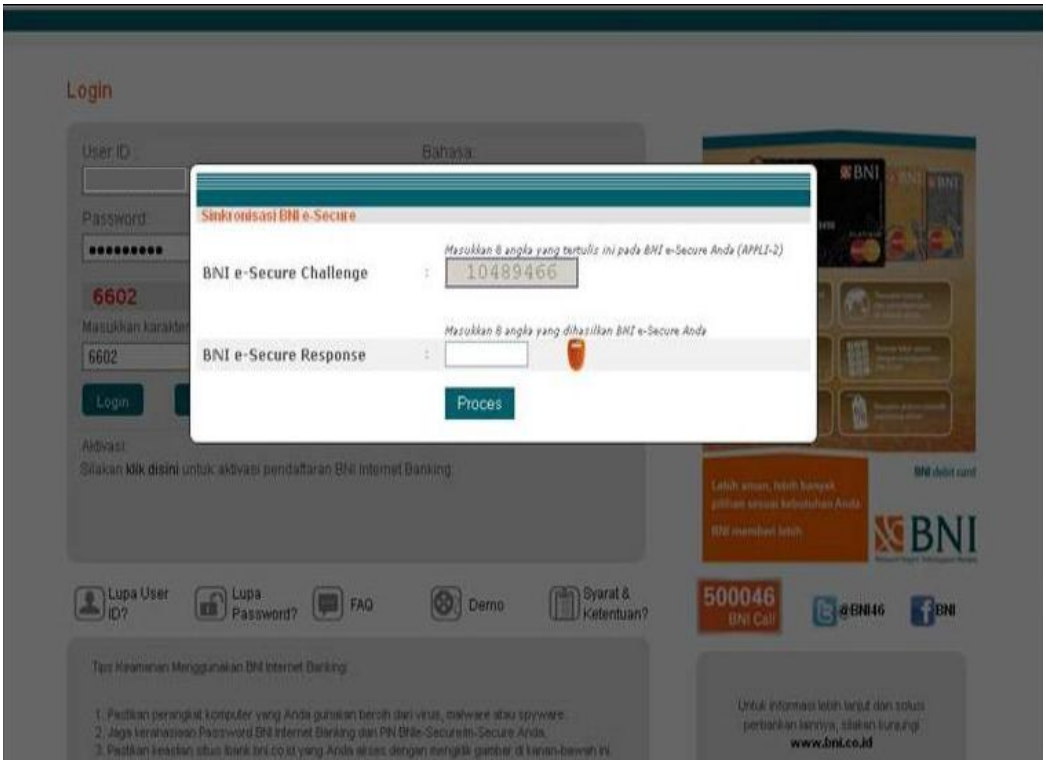
Tips to transact securely at BNI Internet Banking

- Make sure to access the BNI Internet Banking through the official address of the BNI website in www.bni.co.id and click the login button, or directly to the login page BNI Internet Banking in https://ibank.bni.co.id or from bookmark/favorite menu on your browser.

- **Make sure you are using the computer that is free from malware, virus / worm. trojan or spyware. Avoid accessing the BNI Internet Banking from an Internet cafe or from a network / computer that can not be sure they're safe. Avoid opening email attachments from unknown senders or download unauthorized content or access to adult sites that have the potential to transmit malware, virus / worm, trojan or spyware to your computer device or tablet / smartphone.**
- BNI e-Secure / m-Secure is only used for financial transactions or in data changes activity. BNI never asked to synchronize e-Secure BNI / m-Secure on-screen of BNI Internet Banking.
- The figure below is an example of fraud called token synchronization that asks you to input your BNI e-Secure / m-Secure. If you find it, **STOP TRANSACTION** and immediately contact BNI Call at 1500046.



- In order to anticipate similar case but in other forms of malware, simply **STOP TRANSACTION** if you are asked to enter the BNI e-Secure / m-Secure PIN in unusual way during transacting at BNI Internet Banking and immediately contact BNI Call at 1500046.
- Beware of unscrupulous fraud attempts on behalf of a bank officer / BNI clerk by telephone, fax or e-mail asking for personal information, including login password, PIN of BNI Internet Banking e-Secure / m-Secure, and One Time Password (OTP) sent to SMS/E-mail, because BNI officials will not request such questions.
- Beware of fake emails on behalf of BNI for log in activity in BNI Internet Banking.

  Below is the sample of *Phising* email because BNI Internet Banking URL who given & BNI Call contact is different from the official owned by BNI.

From: BNI Internet Banking [mailto:alertzmessage@bni.co.id]
Sent: 15 Mei 2017 11:20
To:
Subject: Message Alert!

Dear Customer,

Your message is available to view through BNI Internet Banking.

To view your secured messages Log into Internet Banking and use the message channel: https://ibank.bni.co.id/auth/login<http://djeserve.ga/proo/1/login.htm>

Alternatively, If you have any queries, please contact us on 150046.

Thank you for Banking with us!

  Immediately delete the email or do not click on the suspected URL and do not enter your User ID & Password on suspicious URL.
- Keep User ID, passwords and PIN of BNI Internet Banking e-Secure / m-secure safely and initiate the replacement of BNI Internet Banking password periodically with a unique combination of letters and numbers, and hard to be guessed by unauthorized party.
- Do not use / enter your User ID and Password BNI Internet Banking on websites and mobile applications in addition to the official application PT Bank Negara Indonesia, Tbk.
- Avoid record / save your Password BNI Internet Banking on any media that may be seen by others.
- Use the virtual keyboard facility when typing your password to avoid criminal attempts of information stealing (keylogger).
- During the transfer transaction, make sure that the appropriate name and account number belong to the recipient has been shown.
- Make sure that you have logged out when you leave your computer even if only for a moment.
- If you find any unusual behavior when accessing BNI Internet Banking web pages, or transactions suddenly cut off, or if you feel that your User ID and PIN are not secrets anymore, then stop your transaction immediately and contact BNI Call at 1500046.