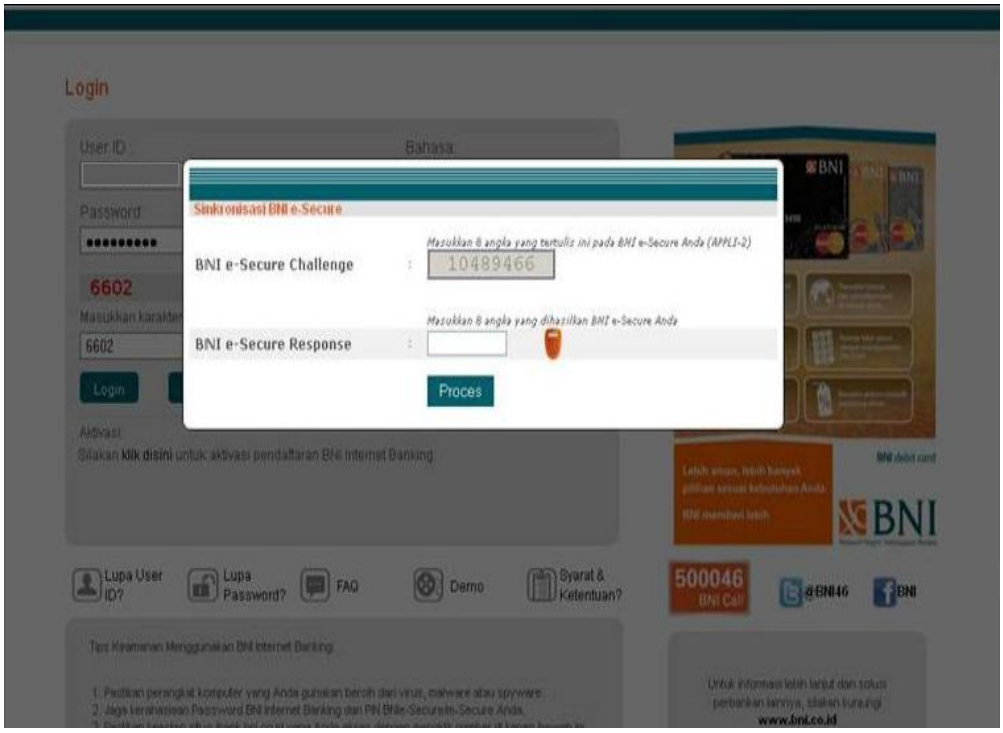
Tips Transaksi Aman di BNI Internet Banking

- Pastikan Anda mengakses BNI Internet Banking melalui alamat resmi situs BNI di **www.bni.co.id** dan klik tombol login, atau langsung ke halaman login BNI Internet Banking di **https://ibank.bni.co.id** atau dari menu bookmark/favourite di browser Anda.

- **Pastikan komputer yang Anda gunakan bersih dari malware, virus/worm. trojan atau spyware. Hindari untuk mengakses BNI Internet Banking dari warnet atau jaringan/komputer yang tidak dapat dipastikan keamanannya. Hindari membuka attachment email dari pengirim yang tidak dikenal atau download content tidak resmi maupun akses ke situs-situs dewasa yang berpotensi untuk menularkan malware, virus/worm, trojan atau spyware ke perangkat computer maupun tablet/smartphone Anda.**
- BNI e-Secure/m-Secure hanya digunakan untuk aktivitas transaksi finansial atau perubahan data. BNI tidak pernah meminta melakukan sinkronisasi BNI e-Secure/m-Secure di layar BNI Internet Banking Nasabah.
- Gambar dibawah merupakan contoh tindak penipuan yang disebut **sinkronisasi token** yang meminta Anda untuk menginput BNI e-Secure/m-Secure Anda. Jika Anda menemukan hal ini, **STOP / HENTIKAN TRANSAKSI** dan segera hubungi **BNI Call di 1500046.**



- Untuk mengantisipasi kasus serupa namun dalam bentuk malware lainnya, **STOP/HENTIKAN** transaksi apabila Anda diminta menginput PIN BNI e-Secure/m-Secure di luar kebiasaan bertransaksi dengan BNI Internet Banking dan segera hubungi **BNI Call di 1500046**.
- Waspadai upaya penipuan dari oknum yang mengatasnamakan petugas bank/petugas BNI melalui telepon, fax atau email yang menanyakan data pribadi termasuk *password* Internet Banking , PIN BNI e-Secure/m-Secure, dan *One Time Password* (OTP) yang terkirim via SMS/E-mail, Karena petugas BNI tidak akan meminta atau menanyakan hal tersebut.
- Waspadai email-email yang mengatasnamakan BNI untuk aktivitas *Log In* BNI Internet Banking.

  Berikut contoh email yang terindikasi *Phising* dikarenakan URL BNI Internet Banking yang diberikan & nomor BNI Call berbeda dengan yang resmi dimiliki 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!

  Segera hapus email tersebut atau hindari untuk melakukan klik URL yang dicurigai tersebut serta jangan pernah memasukkan data User ID dan Password pada URL yang mencurigakan tersebut.
- Jaga kerahasiaan User ID, *password* BNI Internet Banking dan PIN BNI e-Secure/m-Secure Anda dan lakukan penggantian *password* BNI Internet Banking Anda secara berkala dengan kombinasi huruf dan angka yang unik serta sulit ditebak oleh pihak lain yang tidak berwenang.
- Tidak menggunakan/memasukkan User ID dan Password BNI Internet Banking pada website dan aplikasi mobile selain aplikasi resmi PT Bank Negara Indonesia, Tbk.
- Hindari mencatatkan/menyimpan Password BNI Internet Banking pada media apapun yang memungkinkan diketahui orang lain.
- Gunakanlah fasilitas *virtual keyboard* saat mengetikkan *password* anda untuk menghindari tindak kejahatan pencurian informasi (*keylogger*).
- Pada saat melakukan transaksi transfer, pastikan bahwa nama dan nomor rekening tujuan penerima telah sesuai.
- Pastikan bahwa Anda telah *logout* saat meninggalkan komputer Anda meskipun hanya sesaat.
- Apabila Anda menemukan hal yang tidak biasa saat mengakses halaman web BNI Internet Banking, atau transaksi tiba-tiba terputus, atau apabila Anda merasa bahwa User ID dan PIN Anda sudah tidak rahasia lagi, segera hentikan transaksi Anda dan segera hubungi BNI Call di 1500046.