VERSI BAHASA INDONESIA

Informasi Keamanan Transaksi Danamon CashConnect

Pastikan Anda selalu menjaga keamanan transaksi Anda melalui Danamon CashConnect, dengan memperhatikan dan melaksanakan petunjuk berikut sebelum Anda melakukan transaksi.

1. Bertransaksi yang Aman melalui Danamon CashConnect

Definisi yang perlu Anda ketahui:

Password atau Kata Sandi adalah kode rahasia yang diperlukan Nasabah untuk mengakses Danamon CashConnect, password ini merupakan kombinasi huruf besar, huruf kecil dan angka dengan panjang minimum 8 karakter.

Token adalah perangkat yang digunakan sebagai sarana otentifikasi bagi Bank Danamon yang menghasilkan Kode Rahasia Token yang diperlukan agar Nasabah dapat menggunakan Danamon CashConnect dan melakukan Transaksi Finansial dan Transaksi Non-Finansial lainnya seperti pengaturan menu, pengaturan hak akses rekening dan sebagainya melalui Danamon CashConnect.

PIN Token adalah nomor identifikasi yang diperlukan agar Nasabah dapat mengaktifkan Danamon Token milik Nasabah untuk Danamon CashConnect.

Token Response adalah Kode Rahasia Token yang diperlukan agar Nasabah dapat menggunakan Danamon CashConnect.

Langkah-langkah pencegahan:

a) Umum

- Selalu gunakan komputer pribadi untuk melakukan transaksi melalui Danamon CashConnect.
- Jangan melakukan transaksi Danamon CashConnect menggunakan *wifi*.
- Jangan mengklik *link* yang terdapat di *e-mail* atau link yang berasal dari situs lain dan jangan menjawab *e-mail* yang meminta identitas Danamon CashConnect Anda.
- Gunakan email resmi / email pribadi dan nomor handphone pribadi Anda sendiri untuk registrasi User dan notifikasi.
- User ID, Password, Token dan PIN Token Anda bersifat rahasia.

b) Password, Token dan PIN Token

- Jangan bagikan Password atau PIN Token Anda kepada siapapun.
- Ganti Password dan PIN Token Anda secara berkala.
- Jangan menuliskan dan menyimpan Password, Token dan PIN Token Anda di komputer atau tempat manapun yang dapat terlihat oleh orang lain.
- Buatlah Password dengan kombinasi minimal 8 karakter huruf (huruf kapital dan huruf kecil) atau angka yang mudah untuk Anda ingat, namun tidak mudah diterka orang lain.
- Jangan buat Password atau PIN Token dengan menggunakan nomor urut, misalnya: ‘123456’
- Jangan buat Password atau PIN Token dengan menggunakan nomor/ huruf yang berulang, misalnya: ‘888888’
- Jangan membuat Password atau PIN Token dengan menggunakan tanggal lahir, nomor telepon, atau kode lain yang mudah diterka oleh orang lain.
- Waspadai penipuan yang mengatakan dari petugas Bank Danamon untuk meminta data

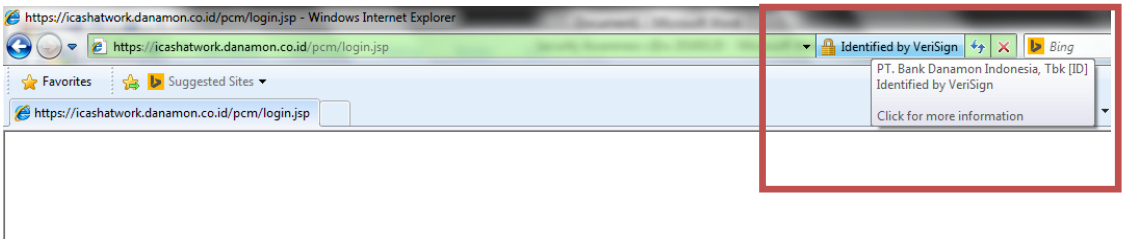
Password dan/atau PIN Token Anda. Petugas Bank Danamon tidak akan pernah menanyakan data Password dan/atau PIN Token Anda.

- Jangan meminjamkan, memindahtangankan Token serta memberitahukan PIN *Token* Anda kepada orang lain.

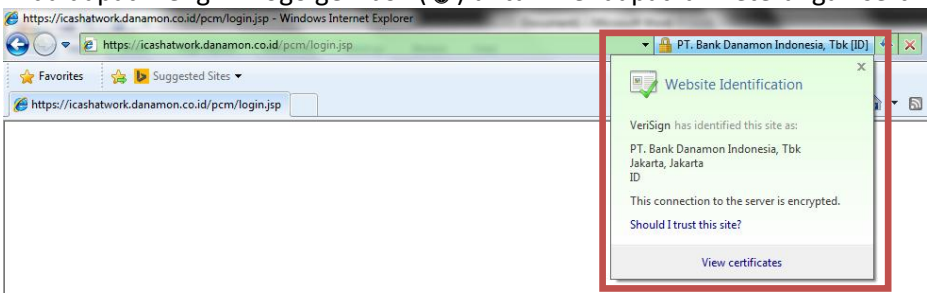
c) Verifikasi Alamat Situs & Aktivitas Transaksi

- Pastikan Anda mengunjungi situs resmi Danamon CashConnect di https://cashatwork.danamon.co.id/ dan pada browser terdapat Logo Kunci atau penanda sertifikasi SSL yang mengindikasikan bahwa situs yang diakses dienkripsi menggunakan SSL. Jika Anda tidak melihat Logo Kunci atau penanda sertifikasi SSL, segera tinggalkan situs tersebut.

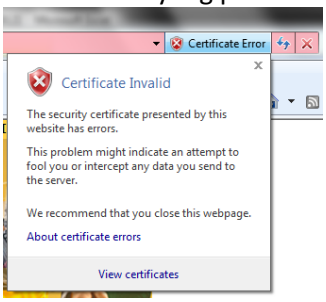
  Contoh Sertifikasi SSL pada browser Internet Explorer:



  Anda dapat mengklik logo gembok (🔒) untuk mendapatkan keterangan sertifikasi:



  Contoh Situs yang perlu Anda curigai sebagai situs tidak resmi:



- Hentikan seluruh aktivitas dan segera tutup situs jika situs menunjukkan hal-hal berikut ini:
  - *There is a problem with this website security certificate*
  - *Certificate Error*
  - *Untrusted Certificate*
  - *This Connection is Untrusted*
  - *Run by (Unknown)*
- Cek riwayat transaksi Anda secara berkala untuk mengidentifikasi transaksi yang tidak sah. Jika terdapat kejanggalan, segera hubungi Help Desk Danamon CashConnect.

- Pada saat melakukan transaksi transfer, pastikan bahwa nama dan nomor rekening tujuan penerima transfer adalah benar.
- Pastikan Anda *log out* setelah melakukan transaksi di Danamon CashConnect.
- Permintaan pengisian Kode Token hanya pada layar konfirmasi transaksi Finansial maupun Non Finansial. Jika ada permintaan untuk mengisi Kode Token selain untuk transaksi, segera *logout* dan laporkan ke Help Desk Danamon CashConnect.

2. Phishing

Definisi yang perlu Anda ketahui:

Phishing adalah cara yang tidak bertanggung jawab untuk mendapatkan informasi pengguna *internet banking* (misalnya: User ID, Password, PIN Token, Kode Token, ataupun informasi lainnya) baik secara langsung maupun tidak langsung.

Contoh Phishing:

- Dengan mengirimkan *link* pada email atau SMS atau media lainnya yang akan menuntun Nasabah ke situs yang mirip seperti situs Danamon CashConnect dengan tujuan mendapatkan data pribadi seperti *User ID* dan *Password* secara tidak sah.
- Berpura-pura menjadi petugas Bank Danamon dan/atau menawarkan hadiah untuk menanyakan data pribadi Nasabah seperti *User ID* dan *Password*.
- Menuntun Nasabah membuat akun Danamon CashConnect, dimana *User ID* dan *Password* Nasabah kemudian dimintakan oleh pihak yang tidak bertanggung jawab.

Hal ini kemudian akan dimanfaatkan oleh pihak yang tidak bertanggung jawab untuk mengakses akun dan melakukan penipuan/transaksi menggunakan akun Nasabah.

Langkah-langkah pencegahan:

- Kenali dan mengakses langsung situs resmi Danamon CashConnect https://cashatwork.danamon.co.id/
- Untuk menghindari kesalahan penulisan alamat situs Danamon CashConnect, simpan alamat situs pada menu *favorites* atau *bookmarks*. Selanjutnya jika Anda ingin mengakses Danamon CashConnect, cukup memilih dari menu favorites atau bookmarks
- Jangan menjawab *e-mail* ataupun pembicaraan melalui *chatting* yang menanyakan informasi pribadi atau data keuangan Anda.
- Jangan merespon dan hapus segera *e-mail* dari pengirim yang tidak dikenal.
- Jangan mengklik link yang meminta Anda untuk mengakses Danamon CashConnect dan/atau memperbaharui data pribadi Anda
- Jangan masukkan informasi sensitif yang dapat membantu memberikan akses ke rekening Anda meskipun situs terlihat sah.

3. Lindungi Komputer Anda dari Virus/Worm, Trojan, Spyware, Spam, dan Malware

Definisi yang perlu Anda ketahui:

Virus/Worm dan trojan, adalah program yang dapat merusak Sistem Operasi, Aplikasi dan data dari komputer yang terinfeksi.

Spyware, adalah sejenis program yang bertujuan untuk merusak mencuri data dan informasi pribadi dari komputer yang terinfeksi.

Spam, adalah email yang tidak diinginkan oleh pengguna fasilitas komputer dalam bentuk surat elektronik (*e-mail*) yang umumnya berisi promo, informasi palsu, atau phishing; sehingga mengakibatkan ketidaknyamanan bagi para pengguna web.

Firewall, adalah sistem yang tugasnya adalah melindungi komputer atau jaringan dari akses komputer lain yang tidak memiliki hak untuk mengakses komputer atau jaringan Anda.

Malware (malicious software), adalah program atau perangkat lunak yang dibuat untuk dapat menyusup atau merusak sistem komputer, yang dapat mengalihkan data yang diinput Nasabah untuk kepentingan pihak yang tidak bertanggung jawab, yang dapat mengakibatkan kerugian finansial bagi Nasabah.

Langkah-langkah pencegahan:

- Instal dan perbarui program *anti-virus* dan *anti-spyware* Anda.
- Gunakan *firewall* pada komputer Anda dan pastikan *firewall* Anda berfungsi.
- Backup komputer Anda secara berkala. Hal ini adalah salah satu cara yang dapat Anda lakukan untuk mengatasi kehilangan data/file penting yang terkena virus.
- Jangan menjawab atau meneruskan *e-mail spam* dari pengirim tidak dikenal, dan segera hapus jika Anda mendapatkannya.
- Jangan mengakses situs dan/atau mengunduh materi yang mencurigakan.
- Jika Anda menemukan proses yang tidak biasa di sistem Danamon CashConnect, jangan input User ID, Password Nomor Seri Token, PIN Token dan/atau Kode Token Anda, antara lain dengan permintaan sinkronisasi token dan kasus lainnya.

ENGLISH VERSION

Danamon CashConnect Transaction Security Information

Please ensure the security of your Danamon CashConnect transactions by understanding and performing the following guidelines before you make a transaction.

1. Securely Doing Transaction through Danamon CashConnect

Definitions you need to know:

Password is a secret code that is needed by Customer to access Danamon CashConnect, this password can be a combination of capital letters, small letters and numbers with minimum of 8 characters length.

Token is a device that is used as a means of authentication for Bank Danamon that can generate the required Token Secret Code so that customers can use Danamon CashConnect and can do a Financial Transactions and Non-Financial Transactions such as the settings menus, setting permissions, and so on through Danamon CashConnect.

Token PIN is an identification number that is necessary for a Customer to activate Danamon Token for Danamon CashConnect.

Token Response is a secret Token Code required by Customers to use Danamon CashConnect.

Preventive steps:

a) General

- Always use a personal computer to initiate transactions through Danamon CashConnect.
- Do not use wifi in doing Danamon CashConnect transactions.
- Do not click on links contained in emails or links from other sites and do not respond to emails requesting your Danamon CashConnect ID
- Use your formal email/ private email and your private handphone number for User and notification registration
- Your User ID, Password, Token and PIN Token is confidential.

b) Password, Token and PIN Token

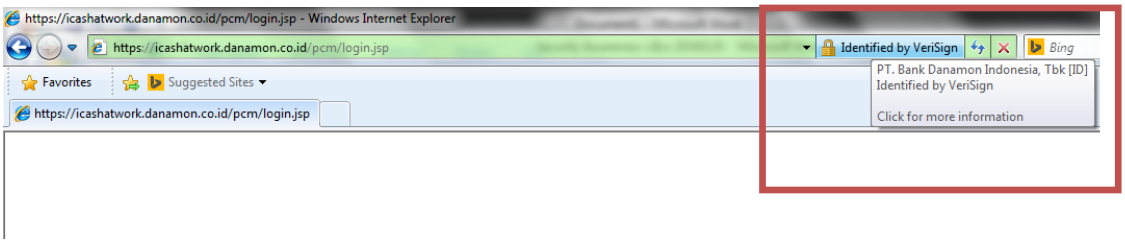
- Do not share your Password or PIN Token to anyone.
- Change your Password and PIN Token on a regular basis.
- Do not write and keep your Password, Token, and PIN Token on your computer or any place that is easily identified by others.
- Create a password combination using minimum of 8 characters alphabet (case sensitive) and number that is easy for you to remember but difficult for other to guess.
- Do not create Password or PIN Token using sequence number, e.g. : '123456'.
- Do not create Password or PIN Token using repetitive number, e.g. : '888888'.
- Do not create Password or PIN Token using your birth date, phone number or other number that is predictable.
- Beware of scams who introduced themselves as the Bank Danamon officer to request your Password and/or PIN Token. Bank Danamon officer will not ask for your Passwor and/or Token PIN data.

- Do not lend or transfer Danamon Token, and inform your Token PIN to others.

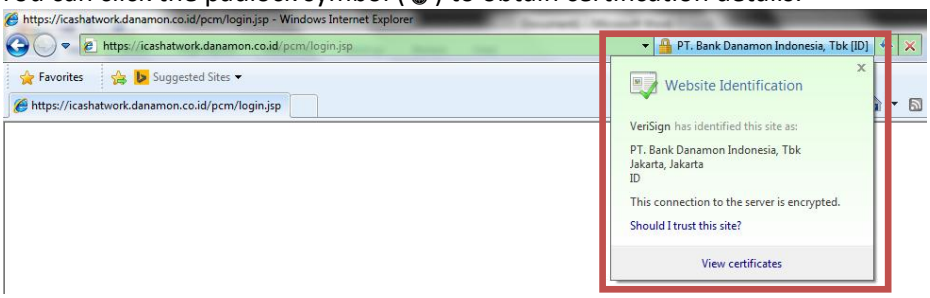
c) Site Address Verification & Transaction Activation

- Make sure you visit Danamon CashConnect official site at https://cashatwork.danamon.co.id/ and the browser indicates padlock logo or SSL certification marker indicating that the site is encrypted using SSL. If you do not see the padlock logo or marker SSL certification, immediately leave the site.

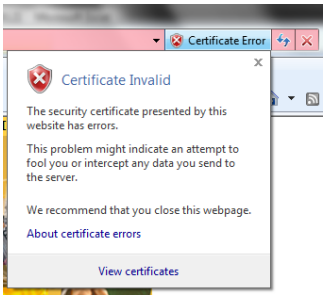
  Example of SSL Certification in Internet Explorer browser:



  You can click the padlock symbol (🔒) to obtain certification details:



  The example of websites you need to suspect as illegal website:



- Stop all activity and close the page immediately if the website shows the following:

  - There is a problem with this website security certificate
  - Certificate Error
  - Untrusted Certificate
  - This Connection is Untrusted
  - Run by (Unknown)

- Check your transaction history regularly to identify unauthorized transactions. If there is any discrepancy, contact the Danamon CashConnect Help Desk immediately
- During doing a transfer transaction, make sure that the name and the account number of the transfer recipient is correct.
- Make sure you log out when you finish doing transactions on Danamon CashConnect
- Request for Token Code only happens during Financial or Non Financial Transaction confirmation screen. If there is a request to fill Token Code in addition to the transactions, logout immediately and report to the Danamon CashConnect Help Desk.

2. Phishing

Definitions you need to know:

Phishing is an irresponsible way to get informations from internet banking users (e.g: User ID, Password, PIN Token, Token Code or other informations) either directly or indirectly

Phishing Example:

- By sending a link in an email or SMS or other means that will lead customers to a site that looks like Danamon CashConnect site with the purpose of illegally obtaining personal information such as User ID and Password.
- Pretend to be a Bank Danamon officer and/or offer a gift to ask for personal data such as User ID and Password.
- Lead the Customer to create Danamon CashConnect account, from which the User ID and Password then requested by the irresponsible party.

This will then be used by the irresponsible person to access the accounts and commit fraud/transactions using customer's account.

Preventive Measures:

- Identify and directly access the Danamon CashConnect official site https://cashatwork.danamon.co.id/
- To avoid Danamon CashConnect website address typing errors, save it into favorites or bookmarks. Later, if you want to access Danamon CashConnect, please choose it from the favorites or bookmarks menu.
- Do not answer emails or conversations via chat that ask for personal information or financial data from you.
- Do not respond and immediately delete emails from unknown senders.
- Do not click on a link that requests you to access Danamon CashConnect and/or update your personal data.
- Do not enter sensitive information that can help provide access to your account even if the site looks legitimate.

3. Protect Your Computer from Viruses/Worms, Trojans, Spywares, Spams and Malware

Definitions you need to know:

Virus/Worm and Trojan is a program that may damage operating systems, applications and data from an infected computer.

Spyware is a type of program that aims to destroy data and steal personal information from infected computers.

Spam is an unsolicited electronic mail (email) which generally contains promo, fake information, or phishing; resulting in inconvenience to the users.
Firewall, is a system whose job it is to protect your computer or network from other computers that do not have the right to access your computer or network.

Malware (malicious software) is a program or software that is created to infiltrate or damage computer system, that can divert data entered by Customer for the interest of irresponsibility party, therefore can cause financial loss for the Customer.

Preventive Measures:

- Install and update your anti-virus and anti-spyware programs.
- Use *firewall* on your computer and make sure your *firewall* is functioning.
- Backup your computer on a regular basis. This is one way that you can do to overcome the loss of data/ important files by viruses.
- Do not reply to or forward a spam email from unknown senders, and immediately delete it if you receive it.
- Do not access the website and/or downloading of suspicious material.
- If you see unusual steps in Danamon CashConnect, do not enter your User ID, Password, Token serial number, PIN Token, and/or Token Code, such as token synchronization request and other cases.