Danamon

A member of MUFG, a global financial group

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.

Danamon

A member of MUFG, a global financial group

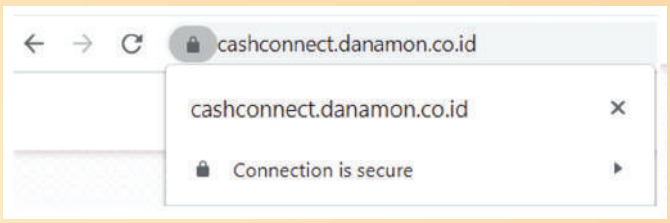
b. Password, Token and PIN Token

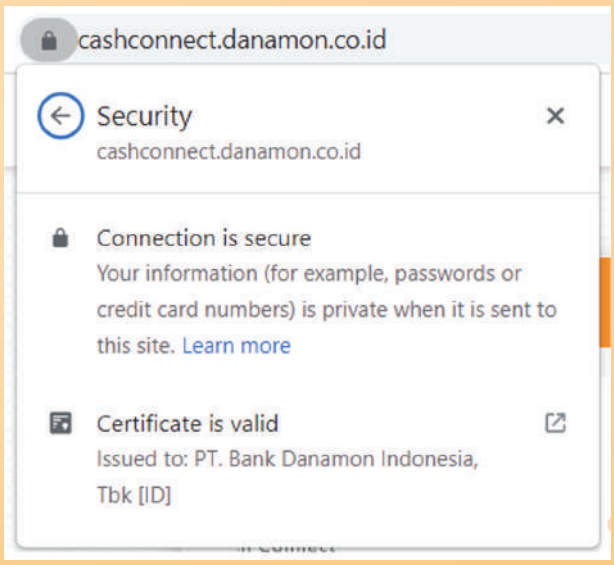
- Do not share your Password or PIN Token to anyone.
- Change your Password and PIN Token on a regular basis.
- Do not write and keep your Password, Token, and PIN Token on your computer or any place that is easily identified by others.
- Create a password combination using minimum of 8 characters alphabet (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://cashconnect.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 Google Chrome & Internet Explorer browser:

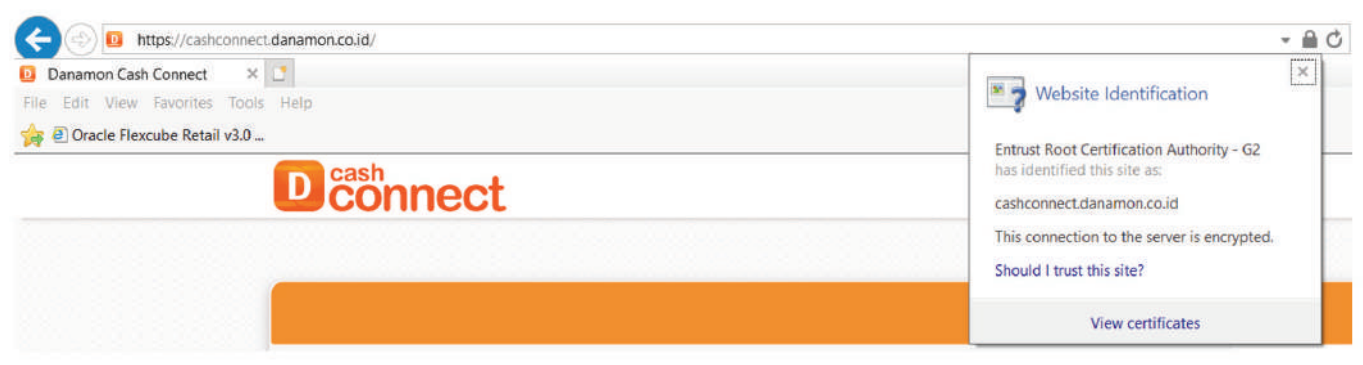




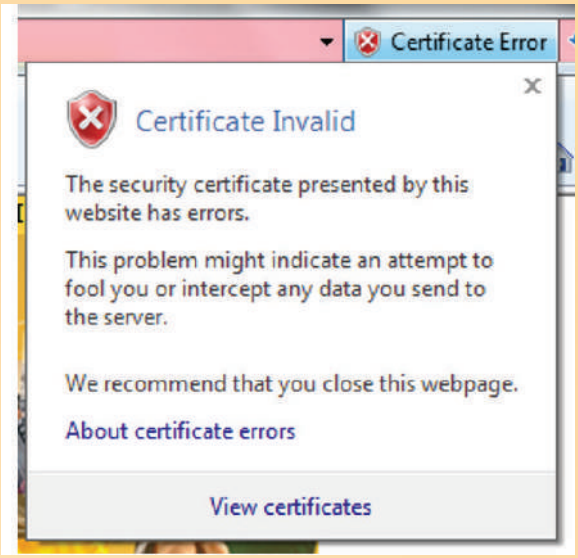
Danamon

A member of MUFG, a global financial group

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.

Danamon

A member of MUFG, a global financial group

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://cashconnect.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.

Danamon

A member of MUFG, a global financial group

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.

Danamon

A member of MUFG, a global financial group

For further inquiries, please do not hesitate to contact Bank Danamon through these channels:

***Hello* Danamon**

Call : **1-500-090** then enter 152 (for Trade Finance) or 153 (forCash Management)

Chat : WhatsApp Danamon **0858-1-1-500-090** and then type 7 (Chat with Hello Danamon)

Email : hellodanamon@danamon.co.id

Or through

TB Service

Chat : WhatsApp Danamon **0858-1-1-500-090** then type 6 (Business Solution)

Email : tb.servicetrade@danamon.co.id (for Trade Finance) or tb.servicecash@danamon.co.id (for Cash Management)