How to Secure Transaction

For your transaction security, please pay attention to the following things:

USER ID, PASSWORD, MPIN, TOKEN

1. Change your J NET BUSINESS & J MOBILE Password regularly with a combination that is unique and difficult for other people to guess.
2. Do not give your password or PIN to other parties, including bank officers.
3. Avoid saving J NET BUSINESS & J MOBILE passwords on your computer/laptop, smartphone and computer.
4. Never send sensitive information via email. Please be aware that J Trust Bank will not request sensitive information via email or other unsecured electronic channel..
5. Always pay attention to transaction notifications sent by the Bank and check carefully transaction value carried out

COMPUTER/LAPTOP, SMARTPHONE/TABLET DEVICES

1. Use a trusted personal computer and network to access J NET BUSINESS & J MOBILE services. It is best to avoid using public computers, for example in internet cafes, and/or untrusted networks, for example wifi access points provided by cafes or shops in shopping centers.
2. Always update the version of the web browser or application that you use for transactions via J NET BUSINESS & J MOBILE.
3. Ensure that the computer/laptop used is safe from key logger devices.
4. Be careful when downloading files that contain viruses or malware because they can steal personal data.
5. Log off completely from the device used to make transactions via J NET BUSINESS & J MOBILE.

NETWORK/ NETWORK

Do not use public Wi-Fi access when making transactions via J NET BUSINESS & J MOBILE. Wireless networks that are publicly available can also be used by criminals to steal information from cellphones, which included banking information.

SAFE ZONE

Use the official application specially issued by J Trust Bank by downloading the J MOBILE application directly from the application store or by accessing the official J Trust Bank website. Or to make sure you are in a safe zone, start with the correct URL, such as 'https'. You can also see the padlock image in the bottom right corner of the monitor screen which shows whether the website you are entering is safe or not.

VERIFICATION

Before carrying out any transaction, first make sure that you are accessing J Trust Bank. Verify information such as number that can be contacted and a clear address if an error occurs. Also check with the bank by telephone about the account number you are intended, starting from the website address to the valid account number.

UPDATE

Keep updating the mobile banking application, update the latest version manually or by activating the auto-update function. Always use the latest version of the application on J MOBILE services.

OTHER

1. Several things that need to be considered regarding the security of transactions via J NET BUSINESS & J MOBILE are as follows:

a. Phishing

Phishing is a method of fraud carried out by certain parties by creating a fake website that is very similar to the Bank's official website with the aim of obtaining confidential customer information such as User ID and Password which can be used to harm the Customer. Security against phishing can be done in several ways as follows:

1. Make sure you access J NET and J NET BUSSINESS via the official site address at https://jnet.jtrustbank.co.id/eb-personel (for Individual customers) and http://jnetbusiness.jtrustbank.co.id/eb-business (for Corporate customers) or use the link available on the website www. jtrustbank.co.id, Always double-check the spelling of the website name, so there are no typos, including the use of symbols.
2. Make a short cut or save the J TRUST NET Individual site address in your browser (bookmark) so that you can use the short cut and bookmark to minimize typing errors in J TRUST NET Individual website addresses.
3. Be alert to fraudulent attempts from individuals acting in the name of J Trust Bank officers via telephone, fax or email asking for personal data including PIN. J Trust Bank Officers will not request or ask for your password or PIN number.
4. Never enter your User ID and Password on a web page that opens automatically (pop up) and/or from suspicious links such as from digital advertisements/banners on websites.

b. Virus

Viruses are computer software created with specific purposes to damage the operating system, applications and data on the infected computer. Viruses can spread through many media such as email, CDs, removable storage, programs downloaded from the internet, networks, and also from unsafe website pages. Some examples of the impact of a virus infection are that the computer device becomes unstable and often 'hangs' (freezes), data is deleted, and some application programs become unable to function properly. Protection against viruses can be done in several ways as follows:

1. Use the latest anti-virus to prevent your computer from being infected with viruses, malware, spyware or other forms of applications that can be detrimental.
2. Be careful downloading email attachments because they can contain viruses that can steal sensitive data. Scan the attachment first using your anti-virus software before opening it.
3. Be careful when downloading and/or installing software.
4. Be careful when connecting removable storage devices to your computer device. Scan the removable storage using anti-virus software first before opening its contents.
5. Avoid accessing and/or downloading files from untrusted web addresses.

c. Spyware

Spyware is computer software that is created to retrieve important/personal information such as credit card numbers, User ID and PIN/Password, account numbers, email addresses, etc. from infected computer devices and will send this information to certain locations for the benefit of third parties. who is irresponsible. Spyware can be installed via email attachments, programs installed from unsafe sources/websites. Viruses can also be programmed to spread spyware. The way Spyware works tends to be difficult to detect so it is easier to collect the information that the creator/spreader wants. Security against spyware is the same as security against viruses.

2. To confirm the details of the security certificate and website address https://jnet.jtrustbank.co.id/eb-personel (for Individual customers) and http://jnetbusiness.jtrustbank.co.id/eb-business (for Individual customers Corporate) select View Certificate in the green bar/security icon next to the web address in the browser you are using. If a warning message appears regarding the certificate when accessing J NET and J NET BUSINESS, please do not access the website or double-check the website name you have typed.
3. Make sure your Internet browser has a padlock/key image indicating that the page you are currently accessing is encrypted using Security Socket Layer (SSL). If you do not see the lock/key image, please log out.
4. Never register for J TRUST NET Individual to get a prize or for any reason at the request of someone over the phone or by other means. Register for J Trust Bank Electronic Banking services officially only through the Branch Office or J Trust Bank Electronic Banking Portal.
5. If there is a notification from J Trust Bank regarding activity on your account while you have never done this, immediately follow up by visiting the nearest J Trust Bank Branch Office or J Trust Bank call center.
6. Confirm with J Trust Bank via the J Trust call center "Ask J" on 1500615 if there is a suspicious request.
7. Stop transaction activities if you feel there is something odd/unusual about the computer/laptop or smartphone/tablet or web page/application that is being accessed.