

## Bjb Quickcash Portal Security Guidance

Bjb quickcash portal optimally designed to deliver security protections for bjb quickcash agents. However anyone using internet communication are susceptible to threats, some of the common threats and security guidance as follow :


- a. Always concerned over the bjb quickcash portal security system when accessing it;
- b. Please be assure to keep your password confidential at all time, password is one of the main security access to bjb quickcash portal;
- c. Only enter bjb Quickcash Portal in a place that you think is safe, accessing bjb quickcash portal on public area is not recommended;
- d. Do not leave your browser in logon position.

Possible bjb Quickcash Portal internet communication threats and tips securing yourself are as follow :

### a. Phishing

Phishing is a method of fraudulent actions through internet connection to gain access of valuable personal data details such as credit card number, bank account, usernames and password, PIN etc. To lure the unsuspecting victims, phisher masqueraded as a trustworthy entity such as popular social web sites, auction sites, banks, online payment processors or IT Administrators and send emails containing links to websites that are infected with malware. Phisher will direct victims to enter personal data (such as user ID and Password) at a fake website which are almost identical to the legitimate one. Once your personal valuable data/details have been accessed, phisher then record the data and use it to commit fraud crimes such as identity theft and bank fraud.

Security Guidance :

- If you receive an email that demand you to change your bjb quickcash portal Identity, please do not respond the demand until you verify it by accessing <https://qcportal.bankbjb.co.id>;
- In any circumstances you feel that your user ID and password are no longer confidential, please immediately change your password by accessing **the Administration-Change Password** menu;
- Before you enter bjb Quickcash Portal please ensure that there is a lock/key () sign on the left top corner of the home page as an indication of SSL 128 bit data transmission encryption between bjb quickcash portal and your browser.

### b. KeyLogger

Keylogger is a device (hardware) or a computer program (software) that log all keystrokes that are generated from your keyboard. The keystrokes are secretly logged without you knowing it and are saved into a log or text notes. Keylogger are used to steal confidential information such as online

banking passwords, username, password, account number, etc. The scammer usually embed the keylogger tools earlier to be able to record all of your keyboard activity.

#### Security Guidance :

- Use an onscreen keyboard when inputting confidential data such as user id, password and account numbers. Some operating system have already provide an onscreen keyboard program (Microsoft Windows XP : Click Start Menu select Program > Accessories > Accessibility > On-Screen Keyboard);
- Be sure to always use the latest Antivirus program, the latest antivirus program usually can detect presence of a keyloggers program as a virus;
- Use an anti-keylogger program if possible.

#### c. Virus / Worm

A computer virus is a malware program that when executed, replicates by inserting copies of itself into other computer programs, data files, boot sector, etc without the knowledge of the user.

A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. Although computer worm does not cause a much damage as a computer virus, but computer worm can be used to carry dangerous attachments.

#### Common symptom of virus/worm infected computer are :

- Computer runs slower than normal computer performance.
- File duplication automatically occur without any command.
- Computer keeps restarting itself.
- Hard drive is not accessible.
- Computer slows down and stop responding “hang”
- Disappearance of computer fundamental functions.
- Data loss.

#### Security Guidance :

- Always update your software or operating system patches from its manufacture official sources;
- Always buy and install original computer programs and applications;
- Install antivirus software from a trusted manufacture that could real-time scan your computer and periodically always update the antivirus;
- Another media of virus dispersion is through email. Please use your email wisely and be aware when founding/opening suspicious email from unknown sender;
- Always scan email attachment before opening it;

- Most operating system has a personal firewall program included on, we recommend you to install and use it to provide protections for your computer;
- Downloading or installing any application programs from an unknown source in the internet is not recommended;
- Scanning is highly recommended before opening any files from other source (Floppy disk, CD, DVD, Flash Disk, USB Drive, etc).

#### d. Spyware

Spyware is malicious software that scammers try to install on your computer. Spyware program allow people/scammers to spy on what you are doing on your computer, it could spy on the website you visit, files you use and other detail information. Spyware usually enter you computer from content that are downloaded from internet or by installing certain application from websites.

Common symptom of spyware infected computer are :

- Computer performance suddenly runs slower than usual, especially when connected to internet;
- Essential tools and program stop working when opening specific web pages;
- Your home page web address, mouse pointer, or search program changes unexpectedly;
- Excessive popup windows and you are not able to stop or close it and often direct you to a particular web site.

Security Guidance :

Generally, Security tips has the same security issue with Virus/worm, but there are more additional tips :

- Beware of web sites that demand you to install a certain applications/programs;
- Pay a special attention and consider about the reviews given (whether it's a spyware or not) before using or installing a free application;
- General security guidance are also applied.