恒生銀行
HANG SENG BANK

Hang Seng HSBCnet Security

May 2016

Security

The Bank aims to provide you with a robust, reliable and secure online environment in which to do business. We seek to achieve this through the adoption of proven best practice IT policies and procedures, and the dedication of expert resources to their implementation and monitoring. We employ industry-standard solutions to authenticate your identity when you log on, to ensure that your data is transmitted securely and reliably, and that the customer data we hold is protected. We have back-up and contingency plans to ensure interruptions to the service, for whatever reason, are minimized. Drawing on our considerable experience as providers of secure electronic banking systems, we also operate a control and support structure designed to ensure that we address all aspects of the risks faced in providing transactional banking online.

Hang Seng HSBCnet security features

- Robust authentication processes
- Protection against key-logging and ‘denial-of-service’ attacks
- Two-factor authentication using one-time password generating Security Devices or smart cards
- Encrypted sessions between customer and the Hang Seng Bank (TLS)
- Protection of sensitive information in transit and storage to ensure confidentiality of customer data
- Industry-standard security mechanisms to protect the infrastructure
- Regular independent reviews of system’s security
- Robust and regularly reviewed information security policies covering systems and installation development and management
- Comprehensive contingency and back-up arrangements
- 24/7 security monitoring and centralised incident management team
- Audit trails for administrative and transactional activities

Hang Seng HSBCnet security features

When considering the security of an internet product, Hang Seng Bank has identified three key areas of interest:

- How does the product authenticate my identity to ensure that only an authorised user can obtain access, and therefore, ensure that transactions I perform can be uniquely identified (non-repudiation)?
- How secure is the data transmission between the Bank and myself?
- How secure is my confidential business data?

Authentication

Security credentials and two-factor authentication

Hang Seng HSBCnet aims to authenticate Users logging onto the system based on a set of the credentials, each designed to combat various aspects of the risks faced when authenticating identity over the internet. Hang Seng HSBCnet authenticates a user's identity in a number of ways, each designed to match the risks associated with the service or function being accessed to an appropriate level of security. These methods include traditional usernames and passwords, supplemented by the use of an additional credential we call a 'Memorable Question' that provides protection against denial of service attacks, and two-factor authentication using smart cards and one-time-password generating Security Devices.

Higher risk services and functions are protected by two-factor authentication (in the case of Security Devices at logon level). Two-factor authentication represents a significant enhancement to traditional password based security as it is based upon not only something you know – in this case a PIN number – but also something you must physically possess. A potential attacker must obtain the physical second factor – the Security Device or smart card – and the PIN that protects it before being able to compromise a User's account, eliminating many of the pervasive risks that arise from the distributed nature of the internet.

Authentication

Unauthorized access attempts

If someone tries to access your Hang Seng HSBCnet user account without the proper credentials, the system will lock the account after a number of unsuccessful attempts. However, in order to mitigate the risk of someone maliciously locking your Hang Seng HSBCnet account, the Bank has implemented denial-of-service protection. This aims to ensure that someone who knows only a username is unable to lock that User's account simply by entering incorrect values when challenged.

Encrypted sessions using TLS

Security sensitive data (e.g. password) is masked on-screen when input. When being transmitted to the Bank from customer's browser, the transmission of data is encrypted (via TLS-Transport Layer Security). On reaching Hang Seng, this data is encrypted within the databases. Even Hang Seng HSBCnet administrators do not have access to this information.

If someone obtained my credentials and was able to access the system, how could I determine whether that had occurred?

There are facilities within the Hang Seng HSBCnet application that you can use to review activities performed by a specific username.

- When you log in, your main landing page will indicate the last time this account logged in
- Any business or administrative activities performed by the user account can be viewed by the 'activity query' facility

Security of data transmissions

Both the transmission of security details and all online administrative or transactional activities between you the User and Hang Seng HSBCnet are encrypted using the TLS protocol.

Basic encryption involves the transmission of data from one party to another. The sender encodes the data by scrambling it, then sends it on. The receiver must unscramble the data with the correct ‘decoder’ in order to read and use it.

The effectiveness of encryption is measured in terms of how complex the key used is. The more complex the key, the longer it would take for someone without the correct decoder to break the code. TLS is an industry-standard protocol to secure internet communications between Web browsers and the Bank. The Bank currently supports TLS 1.0,1.1 and 1.2.

Data confidentiality and integrity

Hang Seng Bank employs security industry best practices to protect customer and personal data. Our data privacy statement is presented to each User for agreement at the time of registration and details the protection that Users are afforded.

In addition, no User's information is written to disc or stored on internet-facing Web servers. The Web servers are separated physically from the back office databases that hold the transaction data. Therefore, no customer transaction information is kept on the Web servers.

Sensitive data such as passwords are stored in encrypted databases using a hardware security module.

Functional features

Described below are some of the functional features built into Hang Seng HSBCnet to enable you to more easily control the use of the system.

Access levels

Hang Seng HSBCnet provides two access levels for customer staff. System Administrators can perform general administrative tasks such as the set up and entitlement of users to Hang Seng HSBCnet tools, ordering of smart cards and Security Devices and the suspension or deletion of Users. End users have no access to administrative functions. Either type of User can be allocated transactional functionality, but the system is flexible enough to allow for the complete segregation of administrative and transactional functions.

User access control

The Access Control tool allows your designated Hang Seng HSBCnet System Administrators to determine individual user access rights and entitlements, down to account level viewing and payment authorization limits. The number of users required to authorise a payment can be set, as well as the combinations of User levels for differing values of payments. You can establish a system that requires authorization for payments over a certain value from a separate country or at head office. This enables complete control of access and authorization while allowing payments to be processed efficiently.

Functional features

Dual authorisation control

All critical administrative and business functions in Hang Seng HSBCnet can be controlled on a dual authorisation basis (one user submits a transaction/request; another is required to authorise it). However, the application provides the flexibility for the customer to define whether they require dual authorisation). In normal operating circumstances we would, however, strongly recommend that the dual control option is selected.

Activity log tools (audit trail)

Key administrative and transactional events are logged by Hang Seng HSBCnet and available for viewing online via the activity query log tools. An audit trail is provided allowing for retrospective internal control and financial auditing of System's activity.

Session time-outs

Hang Seng HSBCnet enforces idle (inactivity) session timeouts. If a session remains inactive for a set period of time, the session will be terminated and the user will be required to log back into the application. Moreover, the pages the user has viewed during the session expire to prevent it from being stored in the browser, where they could be accessed later by another user.

Security do’s and don’ts

You are responsible for your own systems and for your communications with the Bank and must implement the following to protect yourself, including:

Security credentials

Users must keep their password, memorable answer, security answers and smart card or Security Device PINs secure and secret at all times, and ensure no unauthorized use is made or attempted to be made of these credentials. In particular:

- Never write, record or reveal these credentials to anyone else;
- Promptly destroy any advice of credentials from the Bank or other parties;
- Avoid passwords, PINs or memorable question and answer combinations that may be easy for others to guess;
- Never record passwords, memorable answers, security answers or smart card/Security Device PINs on any software which can store it automatically (for example, any computer screen prompts or ‘save password’ features or the like on an internet browser);
- Ensure that Users are not overlooked by anyone or monitored by closed circuit TV while logging on to Hang Seng HSBCnet;
- Change PINs as soon as they are received, and both passwords and PINs on a regular basis going forward. Don’t alternate between passwords;
- Never disclose your security credentials to any of Our staff or internally within your organization. You should be cautious of any correspondence or communication purporting to originate from the Bank or from any third party requesting the disclosure of your passwords, security credentials of users, or any account details.

Security do’s and don’ts

System compatibility

You must ensure that you have compatible hardware and software in order to access the system. Minimum technical requirements are detailed in the Hang Seng HSBCnet customer guides.

Security standards

You must review your internal security measures on a regular basis to ensure protection remains up to date and in line with regulatory and industry best practice guidance. In particular, this includes but is not limited to the following:

- The encryption technology used or required to be used by the Bank in relation to the system is compliant with the local law where the system is being accessed.
- You shall use and maintain spam filters, desktop firewalls, and real-time anti-virus software. These tools should be updated and used to scan Your computers at intervals commensurate to the receipt of updates;
- You shall install security updates and application patches to operating systems and all applications as they become available; and
- Do not use public Internet access points to access Hang Seng HSBCnet or your accounts or personal information. If these access points must be used then a VPN (Virtual Private Network) must be employed.

Security do's and don'ts

System access

To prevent unauthorized access to the system you must ensure that:

- Users log off the Hang Seng HSBCnet after use and do not allow access to these terminals whilst logged on to Hang Seng HSBCnet;
- Users log off Hang Seng HSBCnet correctly, following the specified logout process instead of just closing the browser window.
- You must never provide any information over the phone when the caller's identity has not been confirmed. It is your responsibility to collect the details and verify the caller's identity through an independent means either by contacting the Bank via published lines or through a known contact. You will never be requested by the Bank to provide any password information.
- You notify the Bank immediately of any unauthorized or suspected access or use to the system (including to credentials) or any unauthorized, unknown or suspected transaction, Communication or Instruction.
- You remove access rights and notify the Bank immediately of any actual or suspected impropriety on the part of any User in connection with the services or where a User is no longer authorised to use the system (due to leaving employment of otherwise).
- You comply with all reasonable requests from the Bank, the police or other regulatory authorities in identifying actual or potential breaches of security.

Security do’s and don’ts

User suspension

The system permits System Administrators to suspend other Users.

This feature is intended for situations where a User is required to be temporarily disabled from using the system, such as during a holiday absence. It is not intended for use in a situation where material security concerns exist about a User’s behavior.

In such a case, the System Administrator should immediately delete the User from the system and revoke the User’s smart card/Security Device (if held).

If suspension is the only option available (for instance, because the User needs to be disabled urgently and no other System Administrator is available to approve the deletion), it should be undertaken in conjunction with other protective measures, such as the retrieval of the User’s smart card/Security Device. If in doubt, please call the Bank for assistance. Users need to be in ‘Active’ or ‘Approved’ status before they can be suspended. Once a User has been suspended, it is important that no further maintenance is undertaken on that User’s profile or access rights prior to their eventual reactivation or deletion.

Maintaining a secure Hang Seng HSBCnet Mobile experience

In addition to your obligation to comply with the general Hang Seng HSBCnet Security Procedures, you must ensure you also comply with the additional security requirements* relating to Hang Seng HSBCnet Mobile on your mobile device, including the following:

- Do not store your Hang Seng HSBCnet user or profile details on your mobile phone
- Ensure your mobile device is updated with the latest anti-virus and anti-spyware software
- Avoid sharing your mobile device with others
- Avoid using other mobile devices not on the approved list to access Hang Seng HSBCnet Mobile
- Do not leave your mobile phone unattended after logging on to Hang Seng HSBCnet Mobile
- For greater peace of mind, click the “Logout” button when you are finished with Hang Seng HSBCnet Mobile
- To prevent unauthorized access to your mobile device, enable its automatic passcode lock feature
- Use the default browser originally provided with your mobile device
- Avoid using an “unlocked” mobile device or a device with any unauthorized modifications when using Hang Seng HSBCnet Mobile
- Avoid installing applications on your mobile device from unknown sources
- When connecting to a wireless network using your mobile device, use only trusted networks or service providers and enable additional security protection, such as Wi-Fi Protected Access (WPA), if possible.

*For full details of your security obligations in using Hang Seng HSBCnet Mobile, please refer to the Hang Seng HSBCnet Security Procedures