# SECURITY INFORMATION

If you suspect that there has been any unauthorised access to your account(s) online, or that any online transaction has taken place which is not initiated by you, please contact us at +65 60289800.

## HOW TO IDENTIFY A SCAM?

- You receive an email, SMS or phone call claiming to be from HL Bank Singapore (“HLBS”), asking you to provide personal financial / security information or your One-Time Password (“OTP”).

- You receive emails or SMS containing a URL internet link which will lead you to a fraudulent unsecured login site.

- You receive emails requesting you to open attachments or free software that may contain malicious software like viruses, spyware and trojans that are designed to steal your personal data.

- Pop-up advertisements asking for personal or financial information are likely fraudulent, so it's better to just close them.

## HLBS SECURITY

HLBS has incorporated the following security features:

- Up to 256-bit encryption with 128-bit minimum enabled by EV SSL certificate to secure online transactions.

- 8-16 character alphanumeric passwords for all HLB Connect customers.

- Temporary ID for registration or reset with HLB Connect. OTP will be used as an additional method to identify that it is you who is authorising the session / transaction in HLB Connect. OTP will be auto-triggered to your registered mobile number to authenticate certain online transactions, settings, registration and reset.

- HLB Connect will automatically log off if there is no activity performed after a while.

- Your HLB Connect account will be deactivated (dormant) if you do not login for 3 months.

## IDENTIFYING FRAUD

### PHISHING

**Protecting You from Phishing Scams**

Online fraud such as phishing scams have been rampant around the world causing undue financial losses and distress that can be avoided with proper education and care. At HLBS, we make it a priority to protect you, our valued customers from such threats. With your online security in mind, we hope to equip you below with practical tips on how you can prevent you from being a victim.

**What is Phishing?**

Phishing is an automated form of social engineering used by fraudsters to deceive one to give away sensitive information. The initial phishing email is designed to entice the recipient to open the email and click on the link provided. The fraudsters use multiple methods to do this including enticing subject lines, forging the address of the sender, using genuine looking images and text and disguising the links within the email.

MALWARE ALERT

There has been news reporting on “Dyreza” banking malware on banking websites. Learn more and take the necessary precaution when banking online.

**1.0 What is Malware?**

Malware is short for Malicious Software. Commonly known malwares may include viruses, worms and trojan horses. Malware is any kind of hazardous software that is installed on your electronic device without your knowledge or consent.

**2.0 How does the “Zeus” malware work on infected computer or mobile/tablet devices?**

Once the device is infected with malware, the fraudster is able to inject modified fake content or pages while you are accessing a legitimate online banking website via your Internet browser. The fake page will request your smartphone operating system (OS) and mobile number.

IMPORTANT NOTE:
The bank will never request your smartphone operating system and mobile number on the website for any reason related to your HLB Connect access.

**3.0 How does malware infect your computer, smartphones or tablet device**

3.1 From an email with Website URL hyperlinks or attachments:

Opening an email attachment or clicking on a hyperlink may contain and allow the malware to be installed into your PC, smartphone or tablet devices.

When receiving an email with a hyperlink or an attachment, and if the email was not expected or from someone you don't know, delete it. If the email is from an organization or someone you know and you’re not expecting it or requested for it, be cautious too; do not click on the given hyperlink or open the attachment as instructed, contact the sender to verify beforehand.

3.2 From mobile SMS or MMS with a website URL or attachments: Same as above emails with hyperlinks or attachments.

3.3 From instant mobile or web messaging with website URL or attachments: Same as above emails with hyperlinks or attachments. Examples of instant messaging are WhatsApp, Twitter and Line.

3.4 Accepting without reading: A user accepts what is prompted on the screen without reading the prompt or understanding what it's asking. For example: while browsing a webpage, an Internet advertisement or window appears that says your computer is infected with a virus or malware; you have won a prize; asking to complete a survey or that a unique plug-in is required. Without fully understanding what it is you're getting, you accept the prompt that will install malware.

3.5 Downloading applications (apps) from a website: Only download programs from reputable websites and with a valid digital signature. If you are unsure, leave the site and research the website and the software you are being asked to install. If it is OK, you can always come back to the site and install it.

Files that don't have a digital signature or were downloaded from an unknown source should always be treated as dangerous.

3.6 Not updating your operating system, web browser or application to the latest version: Running a web browser, application or operating system that is not up-to-date with the latest updates can be a big security risk and can be a way your computer becomes infected.

Some of the updates from your computer, smartphone/mobile, tablet device manufacturer, web-browser or application provider (e.g. Microsoft, Apple, Blackberry, Samsung, LG, Adobe, Google, Mozilla etc), include security updates. Make sure you install them and have the latest updates to minimize the risk of malware infections.

3.7 No antivirus scanner: It's highly recommended that you have some form of antivirus on your computer, smartphone/mobile or tablet devices to help scan and clean any infections currently on your device and to help prevent any future threats.

## 4.0 How to protect yourself from malware?

4.1 Never click on an unknown website link or open an attachment sent via email, SMS, Twitter, WhatsApp or other popular text/instant communication applications, especially when the content is related to financial matters.

4.2 Be a smart surfer when browsing websites that are new to you. Be mindful of any pop-up window that request for your personal information or prompts you to use a certain program.

4.3 Be very selective of the files or programs that you would like to download, always double-check the genuity of the website and the source, even if it comes from your friends.

4.4 Keep your operating system, internet browser, applications and firewall up to date.

4.5 Install robust anti-virus, anti-spyware and firewall software on your computer and all other devices, configure it to update automatically at regular intervals.

4.6 Run full system scans periodically to remove any new found virus or malware, do not forget to reset your password and clear all browser caches, history and cookies before you login to your online banking again.

**5.0 IMPORTANT REMINDER when you're assessing HLB Connect online banking:**

5.1 Do not respond to any form of pop-up screen, window, web pages asking for your personal info.

5.2 Notify the Bank immediately when you come across any suspicious or unusual web pages asking for personal information when you are about to login to HLB Connect.

5.3 You are advised not to proceed with your online banking transactions until your computer or device has been checked and disinfected.

## OTHER COMMON INTERNET SCAMS

### Password Cracking

Password cracking is a common way to retrieve a password by repeatedly trying to guess for the password. The most common method of password cracking is guessing and dictionary attacks.

### Keystroke Logging

Keystroke logging or more commonly known as 'keylogging' is a way of obtaining passwords or information by capturing what the user types. It is a diagnostic tool that comes in the form of software or hardware (i.e. a program or inserted in to the keyboard).

**Login Spoofing**

Login spoofing is a way of obtaining a user's username and password. The user is presented with the bank's Login page to prompt for the username and password. When the username and password are entered, the information is then passed to the attacker.

**Shoulder Surfing**

Shoulder surfing as it suggests, is a way of obtaining a user's username and password by peeping.

**Spyware**

Spyware is computer software that is often installed onto the PC without the user's knowledge and usually takes place during a user's download of free software, games or subscribing to free online services from the Internet. Once installed, it does not only monitor the user's surfing activity but is also capable of retrieving any personal and sensitive information that is being transmitted on the Internet before being sent in the background to interested parties.

**Trojan Horse**

A Trojan horse is a type of malware (malicious software) that allows unauthorized access by the attacker to the user's computer and more often for the purpose of data theft (e.g. personal information, bank account numbers and password). It can be spread through opening an email attachment from an unknown source or a visit to an unknown website.

**Mule Scam**

As the result of responding to spam email or job recruitment that offers opportunities to make easy money, a person could fall for a mule scam. This person is known as a "money transfer agent" or "money mule" whereby a mule's bank account is used to receive stolen money from phishing victims and such an account can also act as a transit prior to the funds being sent abroad, later to be withdrawn by the fraudsters.

**Telephone Tapping**

Telephone tapping is the unauthorized monitoring of telephone and Internet conversations and/or key tone by a third party. Phone Tapping is possible on a public switched telephone network and can be difficult to detect. To minimize the risk, consider disabling your mobile phone's Bluetooth connection to prevent any unauthorized access to the signal sent to and from your phone.

## YOUR ROLE

Con artists today have taken to all sorts of methods to try and trick unsuspecting victims. Their goal is to get the account holder's private information for fraudulent uses.

We've put together a guide to show you how to do your banking safely online:

**Vigilance Is The Key**
when it comes to your online safety. Visit www.singcert.org.sg to find out the latest Internet threats.

**Shred or Securely Store**
your printed statements.

**Sharing Is Not Always Caring**
Never share information such as your username, password, NRIC number etc. via emails or pop-up windows and phone calls.

**Don't Click**
links in emails, SMSes, or pop-ups. Always type the web address yourself.

**Make It Complicated**
Create your password using a combination of alphabets and numbers. Make sure you never write your password down and that it's changed regularly.

**Check & Monitor**
your transaction records as often as you can! This way you will notice if there is anything suspicious.

**Keep It At Home**
Never use a public computer or an unsecured wireless network ("WIFI") when performing online transactions.

**Disable The Auto-complete & Auto-save Function**
for usernames and passwords.

**Don't Keep Your Cache**
After every online session, clear your internet cache. Usually this button is under the Internet Options section of your internet browser.

**Look Out For The Padlock On Your Browser**
when visiting websites that require you to share your security information. Make sure it's there as the icon indicates that the website uses a secure connection.

**If You Doubt It, Junk It**

No matter how legitimate it may seem, never respond to unsolicited emails.

**Invest A Little**

In your computer security. Set up a personal firewall, anti-spy, and anti-virus software. Make sure it’s updated regularly!

**“Use of same device to receive the One Time Password (“OTP), access Internet Banking, and perform on-line banking transactions**

For your convenience, you will be able to receive the OTP, access Internet Banking, and perform on-line banking transactions on your device. Please note however that you will need to keep your device secure at all times (both in terms of physical care as well as preventing software viruses/hacks) to prevent any loss to or unauthorised transactions on your account.”