Important Notes for Bright Smart Customers on Personal Identification Number (“PIN”) Security

Please read the following precautions before using Bright Smart Internet Securities/Futures Trading Service:

A. PIN Management

1. Do not disclose your PIN to anyone including any joint account holder(s). In addition, do not send your PIN via email and never use the same PIN to access other services.
2. Call Bright Smart immediately of any actual or suspected unauthorised use of your PIN and confirm your notification to Bright Smart in writing.
3. Do not, under any circumstances, disclose your PIN to anyone who claims to represent Bright Smart or who claims to be an employee of Bright Smart or other authorised person or the police. It is not necessary for anyone to know your PIN. Bright Smart will never ask you for your PIN by email, phone, or any other method.
4. Disable options on your browser to avoid storing or retaining your PIN on your personal computer.
5. Change your PIN immediately when using Bright Smart Internet Securities/Futures Trading Service for the first time and destroy any documents containing PIN information.
6. Do not use your HKID Card number, passport number, telephone number, date of birth, driving licence number, or any popular number sequences (such as 987654 or 123456) in your PIN. Avoid using the same digit more than twice (such as 111111 or 222222).
7. Do not write down your PIN - memorise it.
8. Be alert to your surroundings before conducting any transactions. Make sure no one sees your PIN and cover the keypad when you enter your PIN on any device, such as a personal computer, an ATM, or other self-service terminal.
9. For security reasons, change your PIN regularly.
10. Change your PIN immediately if you suspect that you have been deceived by a fraudulent website or email. For example, if you fail to log in to a service website after inputting your correct PIN, with or without any alert messages.

B. Personal Computer and Email Protection

1. Take precautions against hackers, viruses, spyware, and any other malicious software when sending and receiving email, opening email attachments, visiting and disclosing personal / financial information to unknown websites, and downloading files or programmes from websites.
2. Increase your protection with proper firewalls, anti-virus software, and anti-spyware software, and update them with security patches or newer versions on a regular basis. Use such protection measures to scan your PC from time to time to strengthen the security of your personal computer.

3. Upgrade browsers and application software to support 128-bit SSL encryption or a higher encryption standard.
4. Remove file and printer sharing options on your personal computer, especially when you have Internet access via cable modem, broadband connection, wireless connection, or other similar set-up.
5. Do not use software or programme(s) from untrustworthy sources.
6. Do not click URLs or hyperlinks embedded in any email to access our website.
7. Limit the number of people who can use your personal computer and set your own password for your personal computer if it has this facility.
8. Disable your browser's "AutoComplete" function. On some browsers, this function remembers the data you input previously. Refer to your browser's "Help" function if necessary.

C. Accessing Bright Smart Internet Securities/Futures Trading Service

1. Keep your Bright Smart Internet Securities/Futures Trading Service account number confidential at all times and do not send account information via email.
2. Make sure that all other browsers are closed before logging in to Bright Smart Internet Securities/Futures Trading Service.
3. Input Bright Smart Internet Securities/Futures Trading Service or Bright Smart's website into the address bar of a web browser directly.
4. Only access Bright Smart Internet Securities/Futures Trading Service through www.bsgroup.com.hk.
5. Every time you log in to Bright Smart Internet Securities/Futures Trading Service, please verify your last login date and time, displayed underneath "Welcome! [Your Name]" on the first page.
6. Do not click a hyperlink in an email, search engine, or any untrusted source to log in to Bright Smart Internet Securities/Futures Trading Service.
7. Confirm the authenticity of Bright Smart's website by comparing the URL and Bright Smart's name in its digital certificate. A security icon resembling a lock or key appears when authentication and encryption are activated.
8. Always log out and then clear the browser cache after each trading session.
9. Do not leave your personal computer unattended while using Bright Smart Internet Securities/Futures Trading Service.
10. Do not use / install any software or programme to access Bright Smart Internet Securities/Futures Trading Service.
11. Access Bright Smart Internet Securities/Futures Trading Service with browsers recommended by Bright Smart.
12. Do not use public computers to access Bright Smart Internet Securities/Futures Trading Service.
13. Check your balance and transaction history regularly. Notify Bright Smart immediately if you discover any errors or unauthorised transactions.
14. Regular review and follow security tips issued by Bright Smart.

15. Contact Bright Smart for confirmation immediately whenever a website claiming to originate from Bright Smart looks suspicious to you.

D. Other Notes

1. Check your statement(s) regularly and inform Bright Smart immediately if you find any suspicious or unusual transactions.
2. Keep your statements and other important documents in a safe place. If you want to discard any documents that contain your personal information, destroy them first.
3. Under no circumstances shall Bright Smart, by way of email, ask for your personal information, such as your password, HKID Card number, date of birth, credit card number, credit card expiry date, etc. In addition, we will not ask you to access Bright Smart's website by clicking hyperlinks attached to any email.
4. Check the website's privacy policy statement and statement on security safeguards before providing personal data to the website.