中国工商银行股份有限公司 新加坡分行
INDUSTRIAL AND COMMERCIAL BANK OF CHINA LIMITED SINGAPORE BRANCH

NOTICE ON PHONE, SMS AND EMAIL SCAMS

How do scams work?
Scams may come in through a phone call, SMS or email **pretending** to come from a **valid or official source**. These scams may persuade you to do any of the following:-
(1) Disclose confidential information (*e.g.* username, account number, password / OTP / PIN);
(2) Call a designated number or click on malicious links / attachments; and
(3) Perform unwanted transactions.

Please note that ICBCSG will never request you to perform any of the above via phone call, SMS or email.

If you fall victim, the scammer may be able to steal your confidential information, install malware on your device to steal such information, and even transfer funds out of your account.

What should you do when you receive a suspicious phone call, SMS or email?
The golden advice is to **check first** and **do not respond**.

If you receive a suspicious phone call, SMS or email, we recommend that you call our official phone line to verify. Hotline: (65) 63695588.

What can you do to better protect yourself from scams?
(1) Do not disclose your confidential information to anyone.

(2) Do not respond to any suspicious phone call, SMS or email. Always check back with ICBCSG by calling our official phone line and/or accessing our official website.

(3) Select strong password / PIN by taking note of the following:-
(a) Choose at least 6 digits / alphanumeric characters;
(b) Do not use guessable information such as birthdates, telephone numbers or other personal information;
(c) Do not recycle the same password / PIN used for other platforms;
(d) Do not disclose to anyone;
(e) Do not store on browser or record down anywhere; and
(f) Change password / PIN on a regular basis, and especially if there is reason to suspect that the same has been compromised.

(4) Adopt additional safe practices as follows:-
(a) When accessing a bank's website, ensure that the address changes from 'http://' to 'https://' and, where possible, an extended validation certificate; A security icon that looks like a lock or key appears when authentication and encryption is expected;
(b) Do not allow anyone to have access to your security token or generated OTP;
(c) Do not divulge the serial number of the security token to anyone;
(d) Conduct frequent checks on your account (e.g. balance, transactions) and to notify us of any discrepancy;
(e) Update us of any change in mobile number or loss of mobile device;
(f) Install / update operating systems, reputable / reliable anti-virus, anti-spyware and firewall software that guard against viruses, spywares and malwares on a regular basis;
(g) Use encryption technology to protect confidential information;
(h) Back up critical data on a regular basis;
(i) Always log out of all online sessions and clear all browser caches;
(j) Do not install/run software/programs of unverified origin;
(k) Do not open email attachments from strangers.
(l) Do not disclose personal, financial or credit card information to little-known or suspect websites;
(m) Delete junk or chain emails;
(n) Do not use file/printer sharing; and
(o) Always use your own/personal device (*e.g.* mobile, laptop, computer).