

To Raise Awareness against Phishing Risks:

Protect your Personal Digital Keys; Beware of Fraudulent Links!



1. Internet Banking login credentials, including Internet Banking number, usernames, login passwords and one-time passwords (OTPs), are as important in the digital world as your physical keys for home, which should be properly safeguarded.
2. BOCHK will not send SMS or email messages with embedded hyperlinks, QR codes or attachments directing customers to the Bank's website or mobile applications to carry out transactions. Nor will the Bank ask you to provide any sensitive personal information, including login passwords and OTPs, via hyperlinks, or contact you via telephone voice messages.
3. If you receive any suspicious SMS or email messages with embedded hyperlinks purportedly to be from BOCHK requesting you to input any personal information, you should be vigilant and think twice. In case of doubt, please contact BOCHK Customer Service Hotline at (852) 3988 2388.
4. Do not download any mobile applications from unreliable sources. You should download BOCHK Mobile Banking and BoC Pay mobile application from official application stores or BOCHK official website.