集友銀行
Chiyu Banking Corporation Ltd.

June 2024

Chiyu Bank Reminds Customers of Online Security and Precautions Against Phone and Online Scams

Dear Valued Customer,

Chiyu Banking Corporation Limited (the "Bank") reminds customers to remain vigilant at all times and beware of mobile device malware scams to protect their own interests.

To mitigate the risk of fraudsters using different pretexts to trick customers into installing malicious applications on their mobile devices, thereby invading or controlling customers' mobile devices through malicious applications to conduct unauthorized transactions. Therefore, the Bank has updated the security protection of the Mobile Banking Application.

Following the upgrade, if the Bank identifies potential risks on your device, which may include:

- Applications that enable relevant “Accessibility” features[1].
- A suspicious application downloaded from unofficial channels which is installed on your mobile device.

In such cases, in order to protect the security of your account, our Mobile Banking Application will be closed and will redirect to the notification page of our website.

To continue using the bank mobile application, the Bank recommends disabling the accessibility features or removing suspicious applications on the mobile device.

We urge customers to stay alert and guard against being deceived:

- Do not click on unknown text messages, emails, attachments, web pages, social media content or links from unknown sources. If in doubt, please stop the operation immediately;

- Only download and install applications provided by trusted and verified developers from officially recognized App stores, and keep the device configured correctly (for example, do not allow the installation of applications from unknown sources, etc.);

集友銀行
Chiyu Banking Corporation Ltd.

- Carefully evaluate the permissions requested by applications before installation. Do not grant permissions lightly, especially those that could give third-party Apps complete control over your device or share your screen. Do not install the mobile application if suspicious permission rights are requested;

- Avoid modifying your mobile devices with Jailbreak or Root;

- Beware of the “Phishing” fraudsters sending out emails or SMS purportedly from our Bank, and request you to click on the embedded hyperlinks in the emails or SMS messages and enter your account details, passwords, personal information, credit card numbers/security code etc;

- Avoid logging into Internet/Mobile Banking or providing any sensitive personal information through hyperlinks or QR Code embedded in any third-party website, mobile Apps, emails or SMS;

- The Bank will not notify customers of any irregularities or suspension of their bank or credit card accounts, and request customers to input their personal information or contact bank staff for identity verification through any pre-recorded voice messages, e-mails, SMS or instant messaging Apps. Customers are also reminded not to rely solely on the incoming call display, e-mail address, SMS, website address or message content to identify the caller/sender.

- Customers who are suspicious about the identities of the callers should end the conversation right away, or request for the callers’ contact numbers and names, etc. for verification and should not disclose their personal information during the process;

- Please change your password regularly and set a strong password, avoid selecting the same password that you have used for accessing other web services. Meanwhile, please keep your password, ATM card and security device(s) properly. Do not write or save the password on any of the devices or anything which is usually kept with these devices. To protect your PIN, please cover the keypad with your hand while you enter. If you notice any suspicious device, please do not use.

- If customers would like to verify any phone calls, e-mails, SMS or website addresses purporting to be from the Bank, they should call the Bank's Customer Service Hotline at (852) 2232 3625 (press "8" after selecting language) or visit any of our branches for enquiry. Customers who may have disclosed their password or personal information to any suspicious person, should immediately change password, contact the Bank or directly contact the Hong Kong Police Force;

- To protect customers' online banking security, customers are requested to log in to online banking through the Bank's official website (www.chiyubank.com).. Do not log into the Internet Banking through any hyperlinks embedded in e-mails from unknown sources;

- Customers should pay attention to their responsibilities regarding the security issues of electronic banking services and comply with the relevant security measures specified by the Bank from time to time to protect customers. If the customer fails to take the safety precautions recommended by the Bank, the customer shall bear the risk of any loss suffered or incurred.

- If customers do not wish the Bank to use their personal data or provide it to any third party for the purpose of direct marketing, they may exercise their opt-out right by calling our Customer Service Hotline or visiting any of our branches.

For details of the security information of our electronic banking services, please visit our website www.chiyubank.com. If you have any inquiries, please call our customer service hotline: (852) 2232 3625.

Remarks:

[1] Accessibility features such as text-to-speech enhances user interface and makes it easier for users with disabilities to use a mobile device. However, fraudsters are using these settings to control devices remotely to steal sensitive information.

Chiyu Banking Corporation Limited