30 November 2023 | Important Notice

Suspension of Screen Capture and Recording Functions on Android Devices to Protect Customers from Malware Scams

Livi Bank Limited ('livi' or 'livi bank') wishes to alert customers and the general public to beware of malware scams. In response to recent malware scams noted in the market in which fraudsters deceive users into installing malicious mobile applications onto their mobile devices for obtaining users' e-banking login credentials, livi has suspended the screen capture and recording features on livi mobile application via any Android devices for Personal and Business banking customers in order to protect account security.

Personal and Business banking customers who would like to obtain the transaction record can head to the 'Transaction History' tab at the bottom of the app and select the specific transaction record made during the past year to view the transaction details. If customers want to download the transaction record, click the 'Download Transaction Advice' button on the transaction details page. A message 'Saved Successfully' will pop up once the advice is saved to the mobile device's album.

Customers and members of the general public are advised not to install any unverified mobile application. Customers should also refrain from clicking any hyperlinks from suspicious SMS messages, emails or websites, provide any personal information or conduct any transactions via unverified channels. If customers are unsure whether a website is legitimate, please call the Hong Kong Police Force Anti-Deception Coordination Centre's Anti-Scam Helpline 18222 for assistance.

Anyone who may have disclosed personal information to or conducted transactions through any fraudulent websites or mobile applications should immediately report the case to the Hong Kong Police Force and contact livi Customer Service Hotline (852) 2929 2998 or livicare@livibank.com.

Livi Bank Limited
28/F Oxford House, Taikoo Place
Quarry Bay, Hong Kong

livi bank also reminds customers to stay alert for possible scams:

- Do not click on links from suspicious SMS messages, email, attachments, websites, social media pages/posts or unknown sources. In case of doubt, please immediately stop browsing and do not input any data. Please close the windows and delete the mobile applications;
- Only download and install mobile applications provided by trusted and verified developers from official mobile application stores;
- Evaluate permissions requested from mobile applications carefully before installation and when prompted. Do not install the mobile application or immediately delete it if suspicious permission rights are required;
- Do not jailbreak or root your mobile devices;
- Install updates and patches for the mobile app, operating systems and browsers regularly from official channels. Do not download software and applications from any untrusted sources.

livi bank will update the fraud alerts on livi's website from time to time. For details, please visit https://www.livibank.com/important-notices.html. For more security tips about our e-banking services, please visit https://www.livibank.com/security-tips.html.

Livi Bank Limited
28/F Oxford House, Taikoo Place
Quarry Bay, Hong Kong