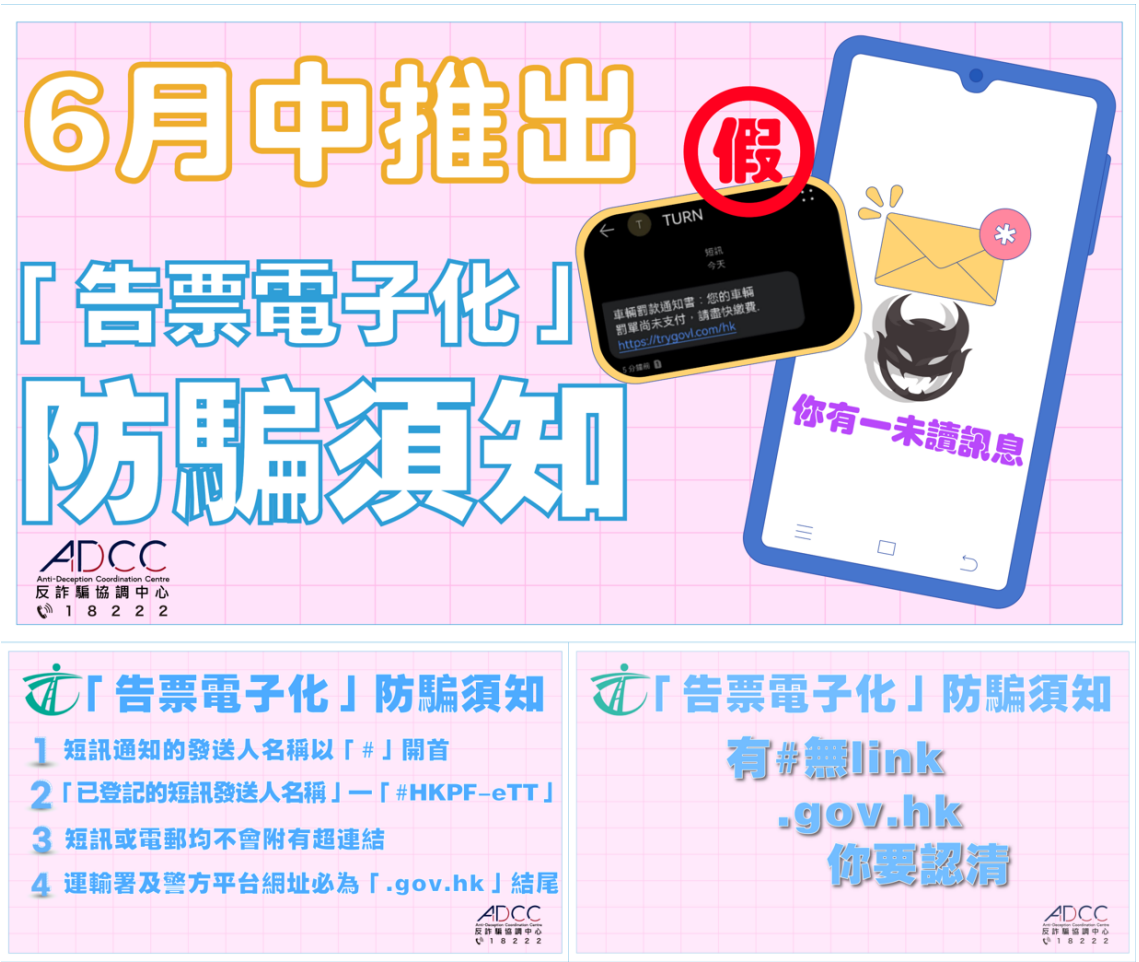
中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

25th June 2025

2025 Q2 Hong Kong Police Force's Anti-Fraud Information

(1) Anti-Scam Notes for Electronic Fixed Penalty Tickets



Beware of Phishing SMSs

The Police are implementing the electronic traffic fixed penalty tickets (FPTs) scheme, in which FPTs will be sent via SMS or email, in mid-June. The Police will then introduce a new thematic portal and mobile application, allowing vehicle owners and drivers to verify and review their electronic FPTs, and pay penalties online via electronic means (such as credit card and Faster Payment System).

中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

Please pay attention to the anti-scam notes below to safeguard yourselves from phishing SMSs:

(1) SMS Sender Registration Scheme – "#"

- The Police have participated in the "SMS Sender Registration Scheme" launched by the Office of the Communications Authority. The Sender ID for SMSs used to issue tickets in the future will have the prefix "#".
- The Registered SMS Sender ID is "#HKPF-eTT".

(2) No hyperlinks embedded

- There will be no hyperlinks embedded in FPTs sent via SMS or email.

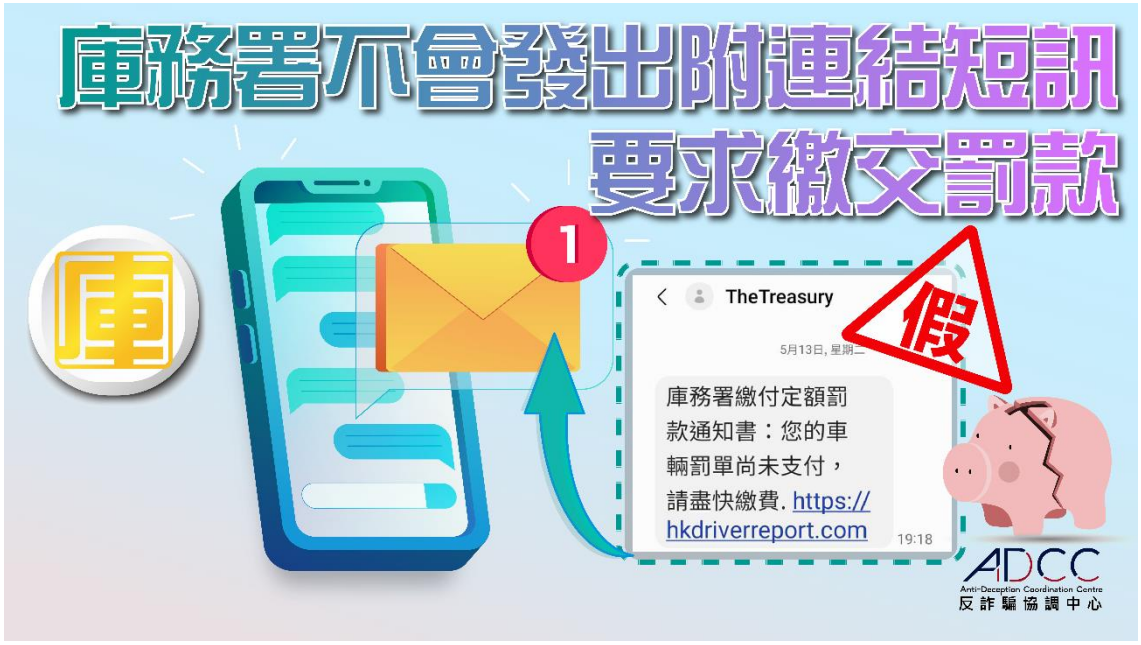
(3) URL domain – ".gov.hk"

- The URL domain of the Police's eTraffic Ticket Platform (www.etrafficticket.gov.hk) is .gov.hk, the same as those of other government departments.
- E.g. the official website of the Hong Kong Police Force (HKPF) is www.police.gov.hk; and that of the Transport Department is www.td.gov.hk.

Notes:

- Do not hastily click on hyperlinks embedded in any emails or SMSs.
- Do not disclose your personal information or account details to anyone before verifying their identities.
- If in doubt, please call the "Anti-Scam Helpline 18222" to contact the Anti-Deception Coordination Centre of the HKPF.

(2) Fraudulent SMSs Purportedly from Treasury Demand Penalty Payments



Defrauding Tricks

Scammers, posing as the Treasury, sent phishing SMSs to members of the public and asked recipients to click on an attached hyperlink to pay a fixed penalty. The Treasury emphasised that it had no connection with such SMSs and reminded the public that it would not ask them to settle payments by sending them SMSs with embedded hyperlinks.

Police Advice

- Do not log on to any websites or download any attachments by hastily clicking on hyperlinks embedded in suspicious SMSs, emails or web pages;
- Do not input your personal information, credit card details, 3-digit security codes (CVC/CVV) and one-time passwords into unknown applications or websites;
- Enter suspicious URLs on “Scameter” of CyberDefender or “Scameter+”, the mobile application of “Scameter”, for security check in addition to seeking verification from relevant organisations;
- Remind your relatives and friends to stay vigilant against deception;
- If in doubt, please call the “Anti-Scam Helpline 18222” for enquiries.

中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

BOCHK Cyber Security Information

- Ensure the website is genuine and reliable before inputting any information or conducting transaction.
- Verify the details of transaction request carefully, in order to confirm these are actually referring to the intended transaction.
- To safeguard your online banking security, you should access Internet Banking through the Bank's official website. Please do not log in Internet Banking through hyperlinks in any email, SMS, QR code, search engine, social networking platform or any third-party website or mobile application not authorised by the Bank.

Bank of China (Hong Kong) Limited