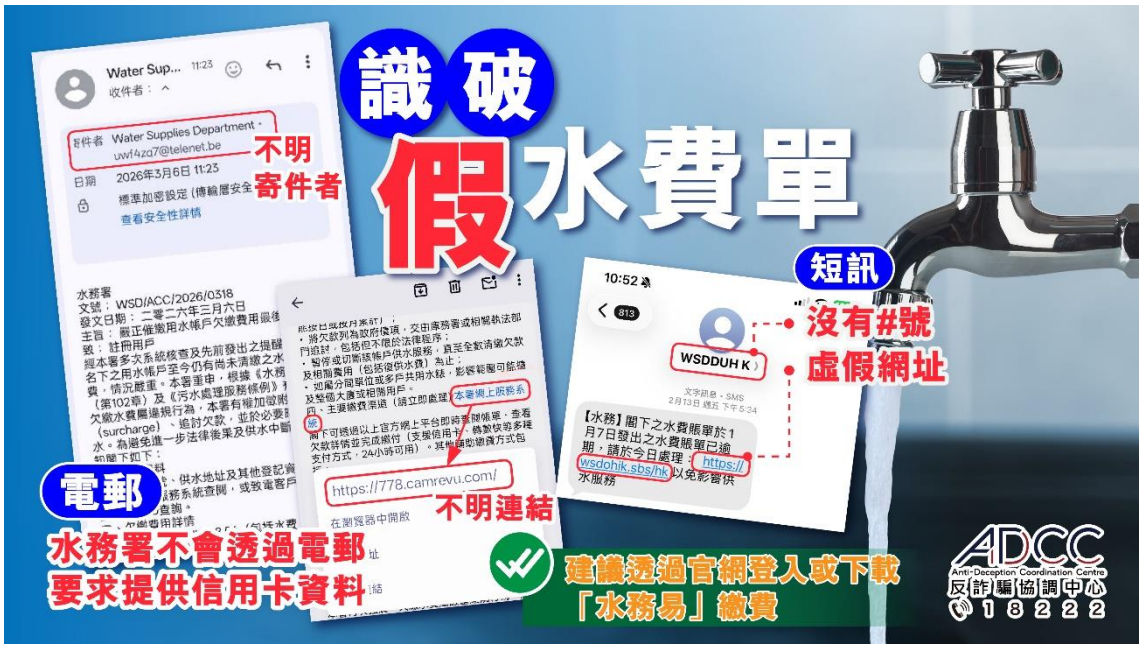
中國銀行(香港)有限公司
BANK OF CHINA (HONG KONG) LIMITED

22nd April 2026

Beware of scams involving fake water bills and counterfeit insurance service deduction notice

Based on the information from the Hong Kong Police Force, following are some antifraud tips for scams involving fake water bills and counterfeit insurance service deduction notice. Please stay alert and vigilant.

Five Dodgy Features of Fake SMSs/Emails about Water Bills Names with "WSD" or "GOV" Don't Imply Authenticity



Fake water bills/demand notes appear continuously. New victims include company directors. The Hong Kong Police Force urges the public to stay vigilant. Sender names with "WSD" or "GOV" do not imply authenticity. Remember the following three points:

- The SMS sender ID of the Water Supplies Department (WSD) must have prefix "#" (#WSD and #WSD eWater);
- The WSD will never lead its customers to other websites or ask them for their credit card information through the hyperlinks in emails or SMSs.
- All WSD's emails to customers about electronic bills are sent by customer_services@wsd.gov.hk or ccbs_no_reply@ccbs.wsd.gov.hk.

Five Characteristics of Fake Water Bills

1. Characteristics of SMS or email senders (The dodgiest)

Scammers imitate WSD's sender names, using those with "WSD", "GOV", etc. For example:

- WSDDUHK
- WSDGT HK
- WSDPP HK

The sender IDs of fake SMSs do not have prefix "#", while those of official SMSs must have it (e.g. #WSD and #WSD eWater) to prove that the senders have joined the SMS Sender Registration Scheme.

The email addresses are fake (The WSD uses customer_services@wsd.gov.hk or ccbs_no_reply@ccbs.wsd.gov.hk only).

2. Minimal amounts seeming to be reasonable

Only claim that a few to tens of Hong Kong dollars are overdue (e.g., HK$18.54, HK$28.26), and because the amount is relatively small, it is easy to make people drop their guard and click on the links.

3. Offensive wording

Offensive wording such as "overdue water bill", "supply shuts down soon" and "fine" to pressure victims into clicking on links.

4. Characteristics of URLs

The URL of WSD's official website is www.wsd.gov.hk, so scammers use fake URLs similar to the official one. For example:

- wsdgov[.]com
- wsd.govi[.]qpon/hk

5. Request Payment

Scammers will ask people to fill in their credit card information and enter verification codes on suspicious websites.

A Recent Case

A company director checked emails, then found a suspicious one with subject "WSD Customer Service" claiming that a water charge of HK$18.54 had been overdue. Having no suspicions, he clicked on a link in the email, visited a website posing as WSD's one and entered credit card information. His bank informed him soon that around HK$23,000 had been deducted from his account. He discovered this irregularity, then made a report to the police immediately.

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

Digital Payment Platform or its Insurance Partner Company Fake Deduction Scams! Man Transferred HK$150,000 in a Hurry

Recently, there were a number of scams involving scammers posing as digital payment platform or its insurance partner company! The scammers claimed that victims had "accidentally" ticked or automatically activated insurance service on their digital payment apps. They said that free trials had been offered at first, but such service was about to expire or would be upgraded to paid service soon. If the victims did not cancel the service, fees would be automatically deducted from their accounts every month, or one-off payments of thousands of dollars would be deducted!

Some scammers even fabricated insurance policies to make the scams more realistic. Following instructions in a hurry, someone was cheated out of almost HK$150,000.

Defrauding Tricks

- Scammers send phishing SMSs, make phone calls or send messages on instant messaging software, claiming that they are staff members from digital payment platform or its insurance partner company. Being able to mention information such as names or phone numbers correctly, they claim that fees for insurance service will be deducted soon and that autopay will be arranged if such service is not cancelled in time.
- Ask victims to call another "cancellation helpline" or send instant message to another number.
- Provide fraudulent URLs to ask victims for personal information, bank account numbers, OTPs, etc.; or show counterfeit insurance policies, threatening to "lock accounts or deduct credits if complete information is not provided".
- Lure victims to transfer money to designated accounts on the pretext of "handling fee", "verification fee", "unlocking fee", etc.

Real Case One

A man received an unsolicited phone call. Mentioning the victim's name correctly, the caller claimed that they were a digital payment platform staff member and that he had "accidentally" ticked to activate insurance service when opening his account. The service was on a free trial at first, but had been upgraded to paid service, so a premium of HK$40,000 would be automatically deducted from his bank account every year!

Upon hearing this message, the victim was frightened and called another "cancellation helpline" according to instructions. Claiming that they were an insurance company staff

member, the scammer lured him to visit a fraudulent website to fill in personal information, bank account numbers, credit card information, etc. The scammer even said that if he did not want the deduction, he must submit complete banking information for verification, otherwise their system would lock his bank accounts immediately!

Being extremely anxious, the victim made a transfer in a hurry, so was cheated out of almost HK$150,000. He only knew that the whole process was just a scam after making a report to the police.

Real Case Two

A victim received a phone call whose caller claimed that they were an insurance company staff member. The caller said that an insurance policy of the victim was about to expire and asked if the victim wanted to renew it. The victim said that such policy had never been bought, and then the caller changed their tune immediately, saying that they would help the victim make a cancellation to avoid the deduction.

By luring the victim to log on to a fraudulent website, the fake staff member asked the victim to transfer a "verification fee" of over HK$30,000, and promised that it would be refunded in full later in the day. The victim became more and more suspicious of the transfer after making it, so made a report to the police, but the amount had been lost.

Police Advice

- Do not call phone numbers in SMSs or click on unknown hyperlinks;
- Do not share your screen with strangers;
- Do not hastily click on hyperlinks, download mobile applications, log on to any suspicious websites or download any attachments;
- You may enter suspicious phone numbers, URLs or transferees' account numbers on "Scameter" of CyberDefender or "Scameter+", the mobile application of "Scameter", for security check in addition to seeking verification from relevant organisations;
- If in doubt, please call the "Anti-Scam Helpline 18222" for enquiries.

For more cases of fraudulent SMS scams, please visit the "Compilation of Fraudulent SMSs" webpage of The Anti-Deception Coordination Centre:
https://www.adcc.gov.hk/en-hk/alerts-detail/alerts-1980544509240999938.html