Beware of Fraudsters: Smart Tips for Consumers

1. Smart Tips Against Phishing SMS and Emails

In accordance with the HKMA's supervisory requirements, banks will not send SMS or email messages with embedded hyperlinks directing customers to their websites or mobile applications to carry out transactions. Nor will they ask customers to provide sensitive personal information, including login passwords and OTPs, via hyperlinks.

If you receive SMS or email messages with embedded hyperlinks requesting you to input internet banking login credentials, these messages should not originate from banks. You should think twice before clicking any hyperlinks purportedly sent by banks. If you find the hyperlinks (or attachments) in the SMS or email messages suspicious, do not click the hyperlinks (or open the attachments). You should always access Internet banking by entering the bank's website address directly, or using a bookmark or an Internet banking mobile application (app).

In case of any queries, bank customers can contact the relevant bank to verify the SMS or email authenticity via other channels (e.g. bank's customer service hotline).

Internet banking login credentials, including usernames, login passwords and one-time passwords (OTPs), are as important in the digital world as the keys to their houses are in the physical one, and should be properly safeguarded.

2. Sample Phishing Emails Purportedly from Banks

Five Common Characteristics:

1. The name of the addressee is not specified (i.e. an undisclosed recipient).
2. The name and email address of the sender may be exactly the same as the genuine information of the related bank.
3. The email usually appears as an important notification from the bank (e.g. "Notification for a huge amount of fund transfer in the customer's account" or "Request the customer to activate a new security function, otherwise, a specific banking service (such as fund transfer service) will be suspended"). The customer will be requested to click the hyperlink or open an attachment in the email.
4. The email normally carries a hyperlink which looks like a genuine website address of the bank. However, when mouse-over the hyperlink, you will notice that the actual hyperlink embedded is another URL.
5. Grammatical mistakes or typos may be found in the email.

Friendly Reminder:

If in doubt about the email, check out the bank's customer service hotline via its official channels (e.g. website, letters or promotional materials), even if a phone number is shown in the email.

Hackers may add some security tips at the bottom of the phishing email to make it look more genuine.

3. Smart Tips Against Credit Card Scams

There are credit card scams happening from time to time, with evolving modus operandi and different deceptive tactics used by fraudsters. Remember to stay vigilant and safeguard your card information to avoid falling prey to credit card scams. As a smart credit card user, you should pay attention to the following tips:

- Take due care and precautions in safeguarding your credit cards, card data and relevant authentication factors (e.g. one-time password, mobile device, etc.).
- Do not disclose to third parties your credit card information, including card number, expiration date, security code (usually printed on the back of the card next to the signature box) and one-time password.
- Verify the genuineness of merchants and websites (e.g. enquire the risk levels / alerts through "Scameter" of the Hong Kong Police Force) before providing personal and credit card information to authorise transactions, and stay vigilant to any suspicious calls, SMS or emails (e.g. phishing messages are often purported to be sent by reliable companies, merchants or banks with very similar text and brand logos, and often embed with hyperlinks to bogus websites luring cardholders to provide credit card and sensitive personal information).
- Check the details of the SMS one-time password carefully, including the relevant transaction information (including type of transaction, name of merchant, transaction amount and currency, etc.), and be cautious of using AutoFill feature of smartphone. Never input the one-time password and proceed with the transaction without verifying the transaction details in the SMS. Once the card information (including the one-time password) is inputted, the transaction may not be cancelled and the customer may be liable for the transaction.
- After you have bound a credit card to a contactless mobile payment service (e.g. Apple Pay, Google Pay), the bank will send a binding notification to the mobile number you have registered with the bank, specifying the contactless mobile payment service to which the credit card has been bound. You should check the notification and notify the card issuing bank immediately in case you have not given such binding instruction. Once the binding is made successfully, one-time passwords may not be needed for the subsequent transactions.
- Always pay attention to communication messages (such as e-mails, SMS, etc.) sent from banks. Check credit card transaction records from time to time and verify your monthly statements. Report to your card issuing bank immediately if there are any suspicious or unauthorised transactions identified, regardless of the amount involved.

- Report to your card issuing bank and the Police immediately if you lose your credit card, suspect your card or card information has been stolen, or suspect your card has been bound to a suspicious mobile device.

If you do not use or safeguard your credit cards and card information properly, fraudsters may exploit such opportunity to commit frauds (e.g. steal your cards to conduct unauthorised credit card transactions), causing financial losses to you. In short, remember to safeguard your card and card information to avoid falling prey to credit card scams.

4. Smart Tips Against Bogus Phone Calls and SMS Messages

Whenever receiving calls, SMS messages, emails, letters or communications through any other channels that claim to be from banks, even though your account is said to be at stake, transactions are said to have been conducted using your credit card or no matter how interested you are in the products being promoted, you should be cautious and:

- Authenticate the identity of the caller or sender;
- Avoid simply relying on the incoming call display to establish the true identity of the caller or directly calling the bank hotline numbers provided in the messages and following the given instructions; and
- Do not provide sensitive personal information easily, in order to safeguard your own interests.

The HKMA or banks do not ask for any sensitive personal information (including login passwords or one-time passwords) through phone calls, emails or SMS messages. Nor do they notify anyone of account irregularities through pre-recorded voice messages. You can check the relevant banks' hotline numbers on their respective official websites or on the back of your ATM/credit cards. You can also find the list of retail banks' hotlines for authenticating the identity of the callers claiming to be bank representatives on the Hong Kong Association of Banks' website. After calling the bank's hotline for authentication, the most prudent way for the customer to continue the process is to contact such bank's representative using the phone number obtained from the bank.

5. Authenticating the Callers and Bank Hotline Numbers

You can check the relevant banks' hotline numbers on their respective official websites or on the back of your ATM/credit cards. You can also find the list of retail banks' hotlines for authenticating the identity of callers claiming to be bank representatives on the Hong Kong Association of Banks' website.

6. FAQs on Fraud Cases

A. Do I need to pay financial insurance or transfer fees for money transfer from Hong Kong to elsewhere?

According to Article 112 of the Basic Law, "No foreign exchange control policies shall be applied in the Hong Kong Special Administrative Region. The Hong Kong dollar shall be freely convertible. Markets for foreign exchange, gold, securities, futures and the like shall continue. The Government of the Hong Kong Special Administrative Region shall safeguard the free flow of capital within, into and out of the Region." It means that there is no restriction on money transfer in Hong Kong and the HKMA does not impose charges of any kind on money transfer.

B. Can you verify if I need to deposit an advance fee into a designated bank account before I can get the lottery money which I was told to have won?

We suspect that you have encountered a fraud case. The HKMA is the banking regulator in Hong Kong and we have no relationship with any kind of lottery activity.

In addition, according to Article 112 of the Basic Law, "No foreign exchange control policies shall be applied in the Hong Kong Special Administrative Region. The Hong Kong dollar shall be freely convertible. Markets for foreign exchange, gold, securities, futures and the like shall continue. The Government of the Hong Kong Special Administrative Region shall safeguard the free flow of capital within, into and out of the Region." It means that there is no restriction on transfer of money in Hong Kong and the government does not demand for any kind of charges on money transfer.

If you suspect that fraudulent activities are involved, you may wish to report the case to the local police station or the Commercial Crime Bureau of the Hong Kong Police Force direct.

C. What should I do if I received suspected fraudulent bank e-mails or phone calls, or came across suspected fraudulent bank websites?

If you receive any suspicious messages or identify any suspicious websites that purport to be related to banks, please contact the bank concerned and the police (either a local police station or the Commercial Crime Bureau) to report your case.

“Click the Links, Fall for Scams!” (30-second video) – Transcript

Video Link: https://www.youtube.com/watch?v=T1vEFnbiWh4

Scammer:	Download the app to verify your information or you will face detention
Superimposed text:	...Download the app to verify your information, or you will face detention...
University student:	What?
Voice-over:	Think there’s a misunderstanding?
Mother:	Why not find a part-time job?
Son:	Mom! Look at this job!
Voice-over:	Think you've found a dream job?
Superimposed text:	...Great jobs available. Provide personal information to facilitate salary payment...
Middle-aged woman:	Sure-win investment group with insider tips and recommendations?
Superimposed text:	…Sure-win investment group, open your account now…
Voice-over:	Think sure-win investment options are just lying around? One click on the wrong link can bring disaster
Superimposed text:	Please click the link to download the app and provide your personal information, ID number, bank account login name and password

	http://xxbank.vip/
Voice-over:	Be cautious of fake links or you will regret it for life
Son:	My money and personal information!
Voice-over:	Click the links fall for scams
Superimposed text:	Click the links Fall for scams

“Three Anti-Scam Tactics” - Vintage Cantonese Anti-Scam Video (1):

Fighting off impersonation of law enforcement officers

Video Link: https://www.youtube.com/watch?v=4dLS5soS0fI&t=2s

English	
Superimposed text:	Vintage Cantonese Anti-Scam Video (1)
Leading actress:	Who’s calling?
Scammer:	I am a law enforcement officer. You have committed an offence!
Leading actress:	How could I have committed any offence? Don't wrong me
Scammer:	You know it well whether you have committed an offence or not I have issued an arrest warrant against you
Leading actress:	What?
Scammer:	Cooperate and give me your bank account number and password Otherwise, you will be sent to prison
Leading actress:	No way! My...my... My account number is...
Male host of TV promotional video:	Scammers have many tricks; believe them and you'll be in a fix
Leading actress:	Humph! Needless to say This person must be a scammer
Leading actress:	Let me apply the "Three Anti-Scam Tactics"

Superimposed text:	Three Anti-Scam Tactics
Leading actress:	Keep Calm
Superimposed text:	Keep Calm Keep calm, don't panic
Leading actress:	Give Nothing
Superimposed text:	Give Nothing Give no personal data or money
Leading actress:	Verify and Seek Help
Superimposed text:	Verify and Seek Help Verify the caller's identity and seek help from others
Scammer:	You have your tactics, but I have an arrest warrant I am only following instructions on this Hurry up and hand over your money and bank account password
Leading actress:	Ha! Law enforcement officers will not request for account information Your arrest warrant is fake I have discerned your hoax
Leading actress:	Watch this!
Scammer:	Argh...
Superimposed text:	The End
Leading actress:	No matter how old the trick is, there are always people who fall for it Remember the "Three Anti-Scam Tactics" Scammers will no longer be rampant

Superimposed text:	Remember the "Three Anti-Scam Tactics"! Scammers can no longer play tricks!
Leading actress:	In addition, the HKMA has launched the "Money Safe" service Just like a safe, it adds an extra layer of protection for deposits
Superimposed text:	Money Safe
Leading actress:	Contact your bank for details now
Superimposed text:	(Hong Kong Monetary Authority Logo)

“Three Anti-Scam Tactics” - Vintage Cantonese Anti-Scam Video (2):

Break the Deepfake Technology

Video Link: https://www.youtube.com/watch?v=VJvrWYZBvBw&t=5s

English	
Superimposed text:	Vintage Cantonese Anti-Scam Video (2)
Superimposed text:	Three months ago
Son:	I am leaving for the capital for business Father, take good care of yourself!
Father:	Be careful and stay safe
Fake Son:	Father! Save me!
Father:	Why are you so scared?
Fake Son:	I was robbed by bandits on the way to the capital I lost all my goods and money, and I could not deliver the goods on time I need to compensate the clients for their losses! Transfer money to the account which I’ve just sent you immediately!
Father:	For my son’s sake, I had no choice but to…
Master:	Hold on What is fake looks real while what is real looks fake Sir Let me share with you the "Three Anti-Scam Tactics"!
Superimposed text:	Three Anti-Scam Tactics
Master:	Tactic One Keep Calm

Superimposed text:	Keep Calm Keep calm, don't panic
Master:	Tactic Two Give Nothing
Superimposed text:	Give Nothing Give no personal data or money
Master:	Tactic Three Verify and Seek Help
Superimposed text:	Verify and Seek Help Verify the caller's identity and seek help from others
Master:	Sir, remember these words
Father:	Your uncle is an official working in the capital Why not reach out to him for help?
Fake Son:	Uncle is overwhelmed with responsibilities and not available!
Father:	Humph! Uncle has already retired and returned home! You evil monster! How dare you impersonate my beloved son using “deepfake”!
Superimposed text:	Goodbye
Master:	No matter how old the trick is, there are always people who fall for it Remember the "Three Anti-Scam Tactics" Scammers will no longer be rampant
Superimposed text:	Remember the "Three Anti-Scam Tactics"! Scammers can no longer play tricks!
Master:	In addition, the HKMA has launched the "Money Safe" service

Superimposed text:	Money Safe
Master:	Just like a treasure box, it adds an extra layer of protection for deposits Contact your bank for details now
Superimposed text:	(Hong Kong Monetary Authority Logo)