FMLIT Publicity Materials for Q3 2023 – Phishing related Scams

What is phishing attack?

Hackers send phishing emails or text messages impersonating organisations such as the government, banks, online payment service providers, online retailers or business partners, with links or QR codes directing to phishing websites which look like the genuine websites of relevant organisations, tricking the recipients into inputting login passwords, personal information, credit card details, etc.

Hackers may also attach links, QR codes or files in the messages, if the recipients click on the links or open attachments indiscriminately, their devices may be infected by malware.

Impersonating financial institutions/ e-payment platforms

- Hackers impersonate financial institutions, such as banks, and send phishing text messages to the victims, claiming irregularities detected or updates on the payment instructions, and request users to process or confirm.
- They lured the victims into visiting a fraudulent website and providing their mobile numbers and one-time-password.
- The hackers then hijack the accounts by using another mobile and transfer funds out.
- There are also some hackers who gather personal information via various channels (e.g. system loophole, dark web), then impersonate bank staff to make calls and request the users to provide “PIN” and “one-time-password” to update their e-payment accounts, otherwise their accounts will be frozen.

As scammers are able to state the personal information of the call recipients, they are easily trusted by the victims. After getting the above information, the scammers will then hijack the accounts and drain their deposits.

Security Tips

- Do not click on the hyperlinks in suspicious emails or messages.
- Do not log into websites that are not verified.
- Pay extra attention if the websites ask for personal or credit card details.
- Check if the scammer has made any purchases with your accounts.
- If the affected account has access to your bank details, contact your bank immediately.
- Update your computer's antivirus software, and run a scan.
- If you suspect that you have fallen prey to a scam, save relevant emails or messages and report the case to the police.

Crime Alert Video (From Cyberdefender.hk)

Youtube Link: https://www.youtube.com/watch?v=tP0mr1mcSKs

Stay Alert: 2023 Consumption Voucher Scheme 2nd Instalment - List of designated telephone numbers for contacting registrants

Recently, members of the public have received scam calls with 8-digit local phone number, purporting to be made from the Consumption Voucher Scheme (CVS) Secretariat or contractors. The caller claimed that the recipients were disqualified from 2023 CVS 2nd Instalment and asked for their personal information.

The registration for 2023 CVS 2nd Instalment closed on Tuesday (27 June). The Government will conduct eligibility check for all registrants. In the course of checking, the CVS Secretariat and its contractors will perform verification and contact registrants. The public are reminded to pay particular attention to the following:

- the calls will not be recorded messages;
- the SMS messages will not provide any hyperlinks;
- no personal information will be obtained from the registrants directly; and
- the Government or its contractors will only use the following designated telephone numbers to call or send SMS messages:

（I）Calling the registrants

	Designated telephone number
Consumption Voucher Scheme Secretariat	3852 7500 or 2241 9400
Contractor appointed by the Government to conduct checks on the registrant's eligibility Deloitte Touche Tohmatsu	2852 1009

（II）Sending SMS to the registrants

	Designated telephone number
Consumption Voucher Scheme Secretariat	852-6059 1120 or 852-2241 9400
Contractor appointed by the Government to conduct checks on the registrant's eligibility Deloitte Touche Tohmatsu	852-5567 3873
Contractor appointed by the Government to process/ check forms SPS UK&I Limited Toppan Forms (Hong Kong) Ltd.	852-6115 1226 34849 852-6522 4964

All registrants will be notified of their checking results by SMS messages issued through the specified telephone number (852 6059 1120). Members of the public can also enquire about their checking results through the interactive voice response system of hotline 18 5000.

Our Advice

- Stay alert and do not believe calls purportedly made by the CVS Secretariat. If the callers ask for your personal or financial information under various pretexts, contact the Secretariat to verify their identities;
- If you have doubts about the authenticity of the calls or SMS, you may call the CVS hotline at 18 5000 to make enquiry.
- Do not disclose your personal information to callers, including your HKID card numbers, stored value facility account, bank account numbers and passwords.

- Remind your relatives and friends, especially the elderly at home, to stay alert against deception;
- If in doubt, please call the “Anti-Scam Helpline 18222” for enquiries.

For the list of designated telephone numbers for contacting registrants, please visit: https://www.consumptionvoucher.gov.hk/en/information_list.html

Beware of Scam Calls Purportedly from China Internet Illegal Information Reporting Centre

Defrauding Tricks

Recently, members of the public have reported to the Police about receiving scam calls made in the form of pre-recorded message or by a real person. Posing as staff of the **China Internet Illegal Information Reporting Centre** (CIIRC), the scammers spoke fluent Putonghua or Cantonese and claimed that the recipients' identity had been stolen for registration of WeChat accounts to publish messages selling counterfeit medicines and luring people to engage in fraudulent events in Southeast Asian countries. The scammers would also ask the recipients to report to the Mainland law enforcement agencies for clarification and then forward the call to another scammer impersonating Mainland law enforcement officer, who alleged that the recipients had committed money laundering offences and requested their personal information, bank account number and password. They were even asked to remit money as guarantee or handling charges.

Our Advice

- Stay vigilant when receiving phone calls pruportedly from the CIIRC;
- Do not believe strangers or disclose your personal information, bank account number and password;
- Even if the strangers are able to tell your personal information or send you legal documents with your photo, it does not necessarily mean that they are genuine law enforcement officer**s.** Scammers can obtain the personal information of the public by unlawful means;
- If the callers claim themselves as officers of law enforcement agencies or government organizations, stay alert and contact corresponding offices to verify their identities;
- Remind your relatives and friends to stay vigilant against deception;
- If in doubt, please call the “Anti-Scam Helpline 18222” for enquiries.

Phishing SMS Messages Purportedly from HKPF

Defrauding Tricks

Recently, scammers impersonating Hong Kong Police Force sent fraudulent phishing SMS messages to the public, claiming that deception cases have been detected and an amount of defrauded money worth HK$80 million has been recovered. The recipients are tricked into clicking on the embedded malicious hyperlink which directs them to a fraudulent website.

As the recipients enter the fraudulent website, the scammers might ask them to input personal or bank account details, or intrude their mobile operating system to steal important data through malware.

Please note that Hong Kong Police Force will not ask members of the public to click on any URL links through SMS messages.

Our Advice

- Do not connect to any suspicious websites or install any mobile applications by clicking on hyperlinks embedded in SMS messages, emails or websites;
- Do not input your personal information, credit card details, bank account details, 3-digit security codes or one-time password into unknown websites or applications;
- Please contact the officer in charge of case or divisional police station for progress of cases;
- Remind your relatives and friends to stay vigilant against deception;
- If in doubt, please call the “Anti-Scam Helpline 18222” for enquiries.

Beware of Scam Calls Purportedly from Security Bureau

Defrauding Tricks

Recently, members of the public have received scam calls with 8-digit local phone number, purporting to be made from the Security Bureau. Posing as the Bureau's staff, the caller claimed that the recipients had published messages containing photos and videos of Russo-Ukrainian War as well as appeals to donate money on social media platforms with telephone numbers registered in the Mainland, suspected of having violated Mainland laws. The scammers who speak fluent Putonghua then asked the recipients to provide their personal information or proceed to the Security Bureau office to verify their identity in person. Some scammers were able to tell the recipients' name during the calls.

Our Advice

- Do not identify the callers' identity simply by the name of organisation, phone number, fax number or staff number provided by the callers;
- Stay vigilant and verify the identity of the callers when receiving any suspicious phone call;
- Do not disclose to callers such personal information as your ID card number, bank account number and password;
- Remind your relatives and friends to stay alert against deception;
- If in doubt, please call the "Anti-Scam Helpline 18222" for enquiries.

Phishing Scam Involving Fraudulent Scameter

Defrauding Tricks

Recently, there are scammers sending phishing SMS messages to the public and claiming that an amount of fraudulent funds worth more than HK$50 million have been recovered. The recipients are tricked into clicking on a link that leads to a phishing website. They will then be asked to install a bogus version of the anti-scam app “Scameter+” and input their mobile phone number and password.

Our Advice

Please note that the app “Scameter+” does not collect users’ personal information or require login. As soon as the recipients install the app and set up an account, the scammers might pose as officials from the mainland and ask them to deposit money into designated accounts as handling charge to retrieve the money lost.

There is no individual website for “Scameter”. You can use it for free on the homepage of CyberDefender (https://cyberdefender.hk/en-us/). You can also download the app by

entering “防騙視伏 App” or “Scameter+” from the official app stores or by clicking on the following links:

Apple “App Store”
Android “Google Play”
Huawei “App Gallery”

To know more, visit https://cyberdefender.hk/en-us/scameter/