FMLIT Publicity Materials for Q1 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

Phishing SMS – CMHK (偽冒中國移動香港釣魚式短訊)

Defrauding Tricks

Recently, there are scammers impersonating staff from China Mobile Hong Kong Company Limited (CMHK) and sending fraudulent phishing SMS messages with an unknown link under the name of "CMHKnotice" to the public. The messages claim that the status of the recipients' CMHK mobile number is abnormal and the service will be suspended. The recipients are lured into clicking on the link to a fraudulent CMHK website which may seek to obtain their personal information and credit card details.

Our Advice

- Stay alert and do not connect to any suspicious websites via hyperlinks embedded in emails or SMS messages;
- Do not click on any links or open any attachments embedded in suspicious SMS messages;
- Do not input personal information, credit card details or security codes to unknown applications or websites;
- Remind your relatives and friends to stay vigilant against deception;
- If in doubt, please call the CMHK Customer Service hotline 12580 for verification or the "Anti-Scam Helpline 18222" for enquiries.

Phishing Email– IRD　(偽冒稅務局釣魚式電郵)

Defrauding Tricks

Recently, there are scammers impersonating staff from the Inland Revenue Department and sending fraudulent emails titled “HK-Refund-Online-Confirmation” to the public. The emails provide a hyperlink to another website which may seek to obtain the recipients’ personal particulars and credit card information.

Our Advice

- Do not connect to any suspicious websites via hyperlinks embedded in emails;
- Do not click on any links or open any attachments embedded in suspicious emails;
- Do not input credit card details or security codes to unknown applications or websites;
- Check out the notice issued by the Inland Revenue Department;
- If in doubt, please call the “Anti-Scam Helpline 18222” for enquiries.

Phishing SMS – SFHK

Defrauding Tricks

Recently, members of the public have received phishing SMS messages purporting to be from SF Express (Hong Kong) Limited (SFHK), claiming that the recipients' express parcels are undeliverable. Members of the public are lured into clicking on the embedded link which will direct them to a fraudulent SFHK website where they are asked to provide their personal information or credit card details.

Our Advice

- Do not connect to any suspicious websites via hyperlinks embedded in SMS messages;
- SFHK states that it would never ask for sensitive personal information, such as identity document numbers, bank account numbers and PIN codes or credit card numbers etc. through phone calls, emails, SMS messages or hyperlinks when contacting customers for delivery. Members of the public may check out the notice on the **SFHK website**, or contact its service hotline at (852) 2730 0273 (Hong Kong) or (853) 2873 7373 (Macau) for enquiries.
- Remind your relatives and friends to stay vigilant against deception;
- If in doubt, please call the "Anti-Scam Helpline 18222" for enquiries.