FMLIT Publicity Materials for Q4 2023 – Fraudulent Investment and Wealth Management Channels for Deception

Caution! Caution! Caution!

Instant messaging groups

國海金探通 VIP 專員, 情深即是晚風, 港股財經 171 揭秘老仙股, 宏楊學院, 聚沙成塔股友交流 77, 財經佈局交流群

Fraudulent apps

USDT - Metatrader5, Exscion, Bitstorage, DIFX, 富達, 金沙娛樂城, HR=HL-Semplice, Narkasa, Moderna, 澳門巴黎人 II

Unknown hyperlinks

gjrapp[.]com	bitstorageep[.]com/h5
h5.tokshop56[.]com	bika/wealthred[.]com
www.xhgj693[.]com/Public.login.do	app.xinsgcbhvg[.]com
app.jcvkgedf[.]com/	zicoleo.com[.]h5
app.gtydgfh[.]com	app.csasea[.]cc
cjvipaa68[.]com	narkasaep[.]com
cjvipyy123[.]com	m.965825[.]vip
singapore4d[.]online	hlhrapp[.]com
dasator[.]com/h5	www.modernas[.]ltd
www.bsproex[.]com	www.ahaosheng[.]com/appff
hlhr-stock[.]com/	zhonghuat[.]com
app.jcvkgedf[.]com	web389[.]vip
xinpujing668[.]xyz	balirenxgvip88[.]com
www.proexu[.]pro/mobile	w.btforexm[.]com/h5
h5.actrade[.]vip	web389[.]vip/
www.proexu[.]pro/mobile	app.ethicn[.]com/home
h1hrapp[.]com	mexczx[.]cn
6rld2.scafyhm[.]com/tucm4	vrcoin[.]cloud
galaxy-11[.]top	www.siqwejja[.]com

Our Advice

- Do not connect to any websites or download any attachments by clicking on hyperlinks embedded in suspicious SMS messages, emails or web pages at will;
- You are advised to make investment through registered investment institutions;
- You may check out the public register of licensed persons and registered institutions on the website of the Securities and Futures Commission (SFC);
- You may enter suspicious phone numbers, web addresses or transferee's account numbers on "Scameter" or "Scameter+", the mobile app of "Scameter", for security check;
- Remind your relatives and friends to stay vigilant against deception;
- If in doubt, please call the "Anti-Scam Helpline 18222" for enquiries.

FMLIT Publicity Materials for Q4 2023 – Beware of Celebrity

Investment Scam

Defrauding Tricks

Recently, it has come to the Police's attention that certain fake investment advertisements and websites, carrying photos of such high-ranking officials and celebrities as the Chief Executive and Financial Secretary, lure the public to click on the advertisements and direct them to suspicious transaction platforms. The authorities concerned have solemnly clarified that the advertisements and remarks are all fictitious. The Police is taking follow-up action and conducting investigation on the incident.

Our Advice

- When you see reports or advertisements on celebrities making successful investment, verify their authenticity. Do not click on the reports, advertisements or embedded links;
- Do not input your credit card details, online banking account information or digital keys of e-wallets into unknown websites or applications;
- Check for spelling mistakes, invalid links or faulty grammar which are typical for fake investment websites;

- It is probably a scam if the so-called “investment company” collects investment capital through personal bank account or e-wallet;
- If in doubt, call the “Anti-Scam Helpline 18222” for enquiries.

FMLIT Publicity Materials for Q4 2023 – WhatsApp Hijacking

What is WhatsApp Hijacking?

1. Obtaining verification code by deceit

Posing as the victim's family or friends, scammers send victims messages asking them to relay the verification code of social media apps. Using the victim's phone number to open a new account on instant messaging apps, scammers hijack the victim's account.

2. Rob account

The scammers used the victim's phone number to log in to his WhatsApp account, thereby robbing the victim's account.

3. Obtaining game point cards by deceit

After successfully taking over the control of the victim's account, scammers send messages to his/her family and friends, asking them to buy game point cards and send the game point card serial number to the scammers.

Anti-scam advice

- Activate two-factor authentication for instant messaging apps
- To keep your account secure, do not give the social media verification code of your instant messaging apps to anyone
- If anyone you know asks you, through social media, to buy game point cards for them or transfer money, verify his/her identity first
- When in doubt, call Anti-scam Helpline 18222

https://youtu.be/hRNn2DRfHYA

FMLIT Publicity Materials for Q4 2023 – Online Account Hijacking

What is Online Account Hijacking?

Instances of account hijacking date back to 2014. During this time, the instant messaging software LINE had a system vulnerability that exposed users' accounts to hackers. These hackers were then able to deceive the victim's family and friends in their contact list into purchasing prepaid cards. The situation continued until around 2016, when the vulnerability was eventually resolved. In 2017, scammers began hijacking users' WhatsApp accounts to trick people into purchasing prepaid cards using similar deception methods. Later, WhatsApp introduced the "two-step verification" (now known as "two-factor authentication") feature. This feature has gradually improved the situation and made it harder for scammers to hijack accounts.

In August 2023, a new account hijacking method involving phishing messages emerged and later transformed into "search engine optimisation poisoning" attacks—these attacks primarily target WhatsApp accounts, with a few cases involving Telegram and other online platforms.

Trick 1: Phishing text messages

- Scammers send phishing text messages with links to fake websites
- The fake websites obtain the user's phone number and request the platform to issue a registration code to the user
- Scammers then get the registration code from the user
- Scammers then use another device to log into the user's account Scammers exploit excuses like bank transfers and loans to defraud users' family and friends

Trick 2: Search engine optimisation poisoning attack

- Scammers create fake WhatsApp web login page
- Scammers advertise using the keyword "WhatsApp" on search engines
- When users enter the keyword "WhatsApp" in a search engine, the fake website will appear as the top ad
- When users click on the top ad, they are taken to the fake website, where they scan a malicious QR code, allowing scammers to obtain their connection information
- Scammers simultaneously log into users' accounts through the online version of WhatsApp to deceive the users' family and friends for money

Online account intrusions can have different causes. For instance, one may forget to log out of web-based messaging software after using a public computer, use malicious multi-account login tools, or have their electronic devices compromised by malicious software.

Scammers often use the excuse that online bank transfers exceed the limit and request contacts in the address book to help transfer money. They promise to repay the amount the following day, and the requested amount can vary from thousands to tens of thousands of dollars. Occasionally, there are also requests for large transfers.

Tips for avoiding online account hijacking:

Enable two-factor authentication

Regularly review the devices linked to your account and log out any unknown connected devices

Avoid disclosing passwords and verification codes casually or scanning QR codes without verifying

Set a strong password for your voicemail to prevent theft of voice one-time password

Avoid connecting to public Wi-Fi or logging into online accounts on public computers

Bookmark frequently used websites instead of relying solely on search engines for trustworthy results

Beware of any abnormalities in text messages and websites, such as misspelled domains or a mixture of traditional and simplified Chinese characters

If you receive a message from family or friend requesting help with bank transfers or remittances, always call to verify their identity and relevant request

If in doubt, use Scameter to assess for URLs, payment accounts, etc., or call 18222 for enquiries