

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.