Beware of Fraudulent SMSs Purportedly Sent from foodpanda and Keeta

Defrauding Tricks

Scammers randomly send phishing SMSs, claiming "Your order has been confirmed and HK$XXX has been deducted", along with a suspicious phone number to lure recipients into calling for enquiries. After calling the number, victims are connected to scammers who pose as foodpanda or Keeta customer service. The scammers instruct victims to transfer "guarantee money" to designated accounts, claiming to help them cancel the orders. Once they have received the money, the scammers can no longer be reached.

[Important Reminder] Messages from senders with the same name will be automatically dropped into the same inbox by mobile phones. Taking advantage of this loophole, scammers sent phishing messages under the name of foodpanda or Keeta, so that the fraudulent messages would be displayed alongside the genuine ones, making it hard for members of the public to distinguish between genuine and fraudulent messages. Scammers would also commit fraud by sending phishing SMSs with ordinary phone numbers.

Case example

A victim received a phishing SMS purportedly sent from foodpanda. Having mistakenly believed it, they called its "customer service". The scammer claimed that guarantee money was required to cancel the order and tricked the victim into transferring HK$ 4,300 to a designated account. The victim subsequently realised that they had fallen prey to a scam when failing to contact the bogus customer service officer.

Our Advice

- Do not rashly call phone numbers in SMSs. If in doubt, you should contact customer service via the applications of foodpanda or Keeta;
- Even if strangers who send you messages are able to tell your personal information, it does not necessarily mean that they are genuine staff. Scammers can obtain the personal information of the public by unlawful means;
- Do not believe the scammers' identities simply by the phone numbers they provide. You are advised to verify their identities by making enquiries to relevant organisations;
- Do not log on to any suspicious websites or download any attachments by hastily clicking on hyperlinks embedded in emails, SMSs or web pages;
- You may enter suspicious information on "Scameter" of CyberDefender or "Scameter+", the mobile application of "Scameter", for security check in addition to seeking verification from relevant organisations;
- If in doubt, please call the "Anti-Scam Helpline 18222" for assistance.