Common online banking scams

Phishing

- Victims are tricked to into disclosing their bank account log-in details, PIN and OTPs to scammers impersonating bank services
- Led to open attachments, follow links to fraud websites, fill out forms with personal information
- SMS, email and social media ads are common channels for such attacks
- Attackers capitalise on heightened emotions, urgency or trust, to exploit human error

SMS OTP diversion

- Cybercriminals gain unauthorised access to the systems of overseas telcos; use them to modify the location data of victims' mobile phones
- They were then able to divert, to overseas telcos, the SMS OTPs sent by Singapore banks to their customers
- Having separately obtained their victims' card details, attackers make fraudulent online card payment transactions that are authenticated via the diverted SMS OTPs

Malware infection

- If a victim downloads a document with a virus or clicks on a malicious link, they unknowingly allow a harmful software to exploit personal information on their computers
- Malware infections often monitor for online banking sessions and attempt to inject their own transaction in the web browser, or swap the beneficiary account before the transaction is sent to the banking server

Compiled by BT