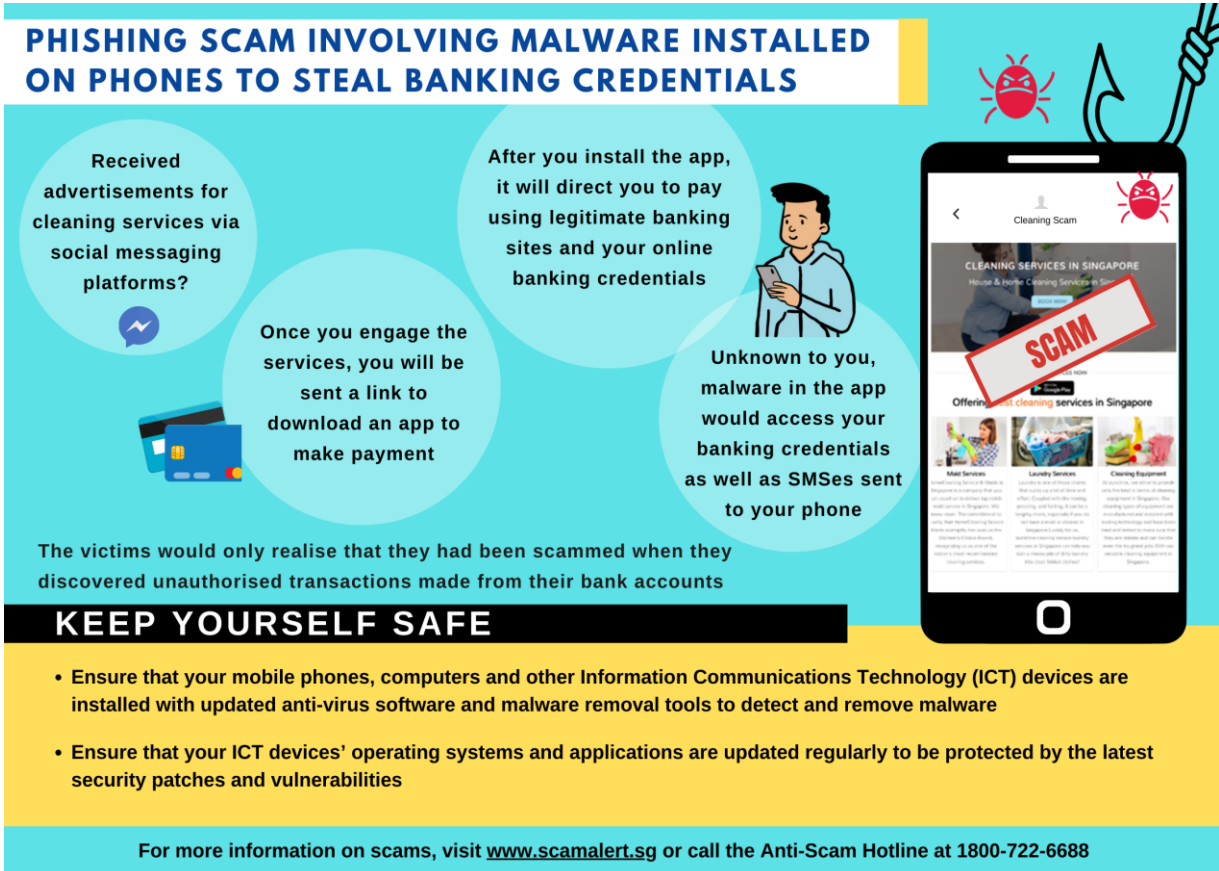


POLICE ADVISORY FOR PARENTS/GUARDIANS

Dear Parents/Guardians,

In this edition of our Police advisory, we would like to highlight a new phishing scam variant involving malware being installed on victims' phones to steal their banking credentials.

2. In this variant, the victims would receive advertisements for cleaning services via social media platforms and a link would be sent to the victims who show interest in engaging their cleaning services.
3. The scammers would then tell the victims to make payments by downloading an app which contains the malware and directing the victims to make payment for the services via legitimate banking sites using their online banking credentials.
4. Unbeknownst to the victims, the app that was installed with the malware would allow the scammers to access the banking credentials and SMSes that are sent to the victims' phones. Victims will only realise that they had been scammed when they discover unauthorised transactions made from their bank accounts.



PHISHING SCAM INVOLVING MALWARE INSTALLED ON PHONES TO STEAL BANKING CREDENTIALS

Received advertisements for cleaning services via social messaging platforms?

Once you engage the services, you will be sent a link to download an app to make payment

After you install the app, it will direct you to pay using legitimate banking sites and your online banking credentials

Unknown to you, malware in the app would access your banking credentials as well as SMSes sent to your phone

The victims would only realise that they had been scammed when they discovered unauthorised transactions made from their bank accounts

KEEP YOURSELF SAFE

- Ensure that your mobile phones, computers and other Information Communications Technology (ICT) devices are installed with updated anti-virus software and malware removal tools to detect and remove malware
- Ensure that your ICT devices' operating systems and applications are updated regularly to be protected by the latest security patches and vulnerabilities

For more information on scams, visit www.scamalert.sg or call the Anti-Scam Hotline at 1800-722-6688



**SINGAPORE
POLICE FORCE**
SAFEGUARDING EVERY DAY

5. **How to protect yourself from such scams:**

- **Ensure** that your mobile phones, computers, and other Information Communications Technology (ICT) devices are installed with updated anti-virus software and malware removal tools to detect and remove malwares.
- **Ensure** that your ICT devices' operating systems and applications are updated regularly to be protected by the latest security patches and vulnerabilities.
- **Avoid** downloading suspicious apps with few ratings or dubious reviews. Perform a search online to verify the authenticity of the app you are downloading.

6. To stay updated with the latest crime information, alerts and advisories, do sign up for Singapore Police Force's Community Watch Scheme.

7. Visit <https://www.police.gov.sg/Join-SPF/Volunteer-Schemes/Community-Watch-Scheme> > or scan the QR code.

Yours faithfully,

**SUPT LEE HAN SHENG
COMMANDING OFFICER
BEDOK NEIGHBOURHOOD POLICE CENTRE
BEDOK DIVISION
SINGAPORE POLICE FORCE**

Sign up now!

