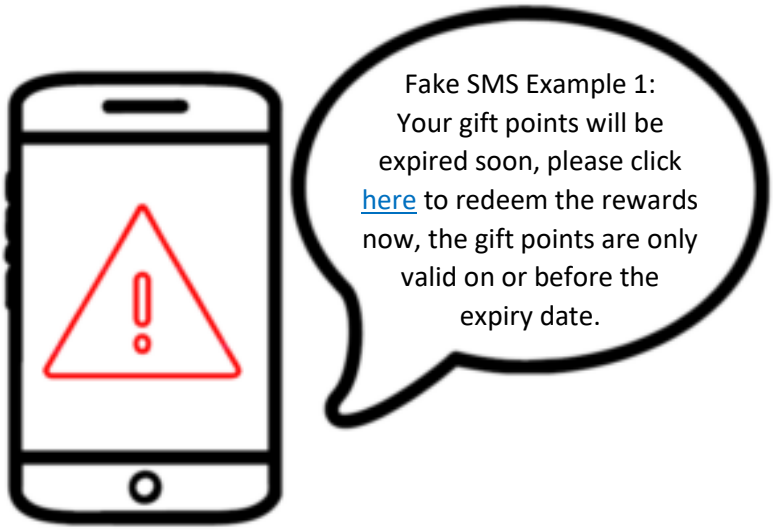
We strive to provide you with a **more secure credit card experience** and to **enhance your security awareness**.

Strengthen the security of your credit card by binding it to Apple Pay via the Wallet App.

1) PrimeCredit will send you an authentication SMS, then reply “1” for confirmation.
2) Enter the One Time Password (OTP) and follow the instructions in order to complete the process.

Watch out for the latest examples of phishing scams!

Fraudsters may send fraud messages purporting to be from government departments or other companies to lure you to click on the embedded link. Your related personal information and credit card details will be stolen once you provided these in the fraudulent website. Always stay vigilant to protect yourself and beware of scams!



Anti-Fraud Tips

1) Never click on any links in suspicious messages to log in to any websites or to download files.
2) Never reveal your personal information, credit card details (including credit card number, expiration date, 3-digit security codes) and One Time Password (OTP) to any untrusted contact or unknown websites or apps.
3) Do not use the keyboard auto-populate function to input SMS OTP. Immediately contact us if you receive an SMS OTP/confirmation SMS which is not initiated by you. You can check relevant Customer Service Hotline numbers on our websites or on the back of your credit card.
4) Verify the authenticity of the messages by contacting the relevant institutions through official channels (e.g. official hotline or website).
5) PrimeCredit will not request you to provide any sensitive personal information (including login password or OTP) via phone calls, emails or SMS and also will not notify you of credit card account irregularities via pre-recorded voice messages.
6) Take due care in safeguarding your credit card, credit card details and relevant authentication factors such as OTP, mobile device, etc.
7) You should provide an updated contact details to us promptly if there are any changes of your contact information.
8) Contact us immediately if you detect any unauthorized credit card transactions.
9) If you suspect you have been tricked by phishing emails, SMS or fraudulent websites and you have disclosed sensitive information such as any personal data and OTP, you should immediately contact our Customer Service Hotline.
10) If you fail to take due care, you will be liable for any unauthorized credit card transactions due to negligence such as not duly protecting your credit card, credit card details and OTP or ignoring pre- and post-credit card transaction notifications from us.