Joint Advisory on Protecting Yourself from Malicious QR Codes

The Cyber Security Agency of Singapore (CSA) and the Singapore Police Force (SPF) would like to remind the public of the dangers of malicious Quick Response (QR) codes and the measures individuals can take to protect themselves.

A QR code is an array of black and white squares arranged in a unique pattern that stores information. They can be easily processed by digital devices with QR readers. While QR codes typically store URLs, they can also store email addresses, phone numbers, calendar data and geolocation data. QR codes are now commonly deployed by businesses to facilitate digital payments.

Due to its convenience, the use of QR codes is becoming increasingly prevalent. It is thus crucial for individuals to be aware of the potential threats and to adopt protective measures.

QR codes are not inherently dangerous, but threat actors with malicious intentions could make use of QR codes to trick unsuspecting individuals into scanning these codes and exposing themselves to various threats.

Common Types of Attacks Involving QR Codes and related Applications

Phishing
Malicious QR codes are used to redirect unsuspecting individuals to phishing websites masquerading as legitimate ones to steal sensitive information such as login credentials, credit card numbers or other personal data.

QR Code Swaps
Legitimate QR codes displayed at businesses are altered or tampered with to trick individuals into directing payment to the threat actor's bank account instead of the intended recipient.

Malware Distribution/Infection
Malicious QR codes are embedded with links that when scanned and accessed, download, and install malware onto the individual's device, potentially leading to unauthorised access, data breaches or other malicious activities.

Malicious Advertisements in QR Code Scanner Applications
During the use of QR code scanner applications, victims may come across advertisement banners suggesting for the creation of an account. Assuming that it is part of the service that they had scanned for, victims click on the advertisement and are directed to a phishing site requesting for personal information and banking credentials. Members of the public are advised to remain vigilant especially when using a third-party QR code scanning application. (Refer to Annex A for screenshots)

How You Can Protect Yourself from Malicious QR Codes

Individuals should adopt the following (non-exhaustive) precautionary measures:

Be Vigilant
Avoid scanning codes received via unsolicited text or WhatsApp messages, emails, social media messaging platforms or from unknown entities.

Check QR Codes Prior to Scanning

Before scanning QR codes, carefully examine them for any signs of tampering or irregularities. Avoid scanning QR codes if it appears to have been pasted over the original code or if there are design inconsistencies. If unsure, always verify with representatives from the organisation which provided the QR code.

Check the Destination Link Before Accessing the Website

After scanning the QR code, carefully inspect the website address to ensure that it is the intended URL. Check for misspelt domains, extra characters, or unfamiliar addresses. If the URL appears suspicious, do not access the website.

Verify Recipients of Digital Payments Through QR Codes

When scanning QR codes to perform digital payments, review the transaction details displayed on the payment application carefully before confirming the payment. Ensure that the amount, recipient name and other information are accurate. If unsure, always verify with representatives from organisation.

Regularly Update Your Devices' Software

Regularly update your devices' operating system and applications to ensure that they contain the latest security patches and updates. This will reduce the risk of unpatched vulnerabilities being exploited when malicious QR codes are inadvertently scanned.

Refrain From Downloading Applications From QR Codes

Refrain from downloading applications from third-party websites that the QR code links to. Mobile applications should only be downloaded from official sources such as Google Play Store or the Apple App Store.

Be Wary of Attractive Offers

If the QR code leads to a website that solicits for personal information in exchange for attractive offers or handouts, extra vigilance should be taken. When an offer is too good to be true, it probably is.

Report Cybersecurity Incidents

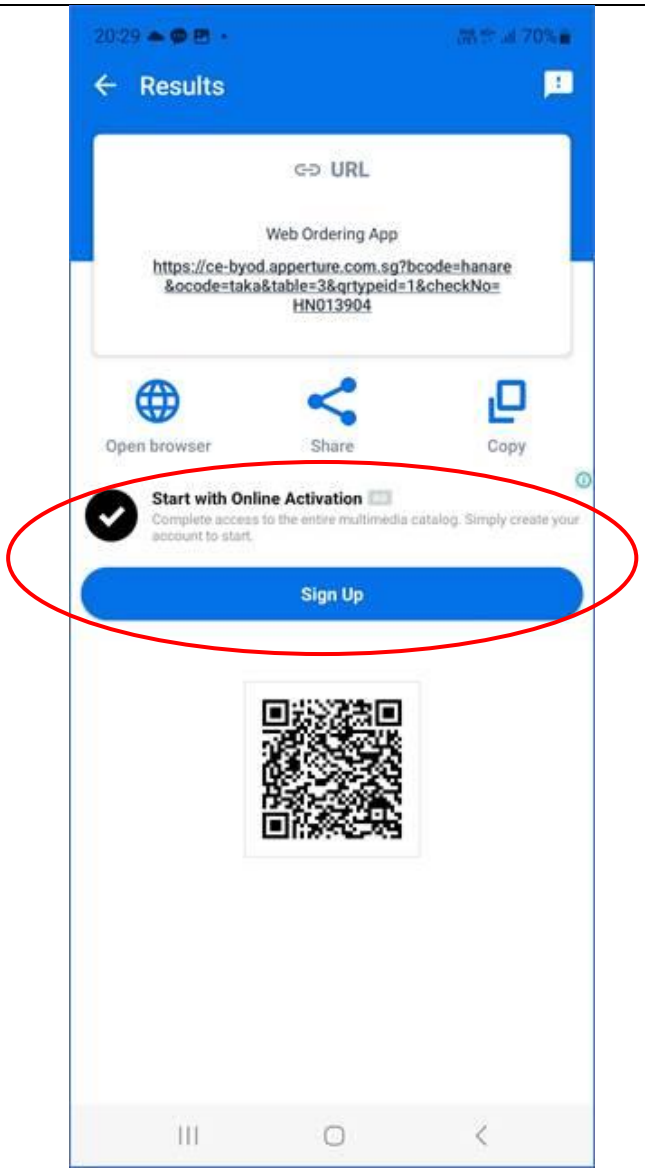
If you suspect that you have been a victim of a cybersecurity incident, report the incident to SingCERT through our incident reporting form at https://go.gov.sg/singcert-incident-reporting-form.

For more information on scams, members of the public can visit https://www.scamalert.sg or call the Anti-Scam Helpline at 1800-722-6688.

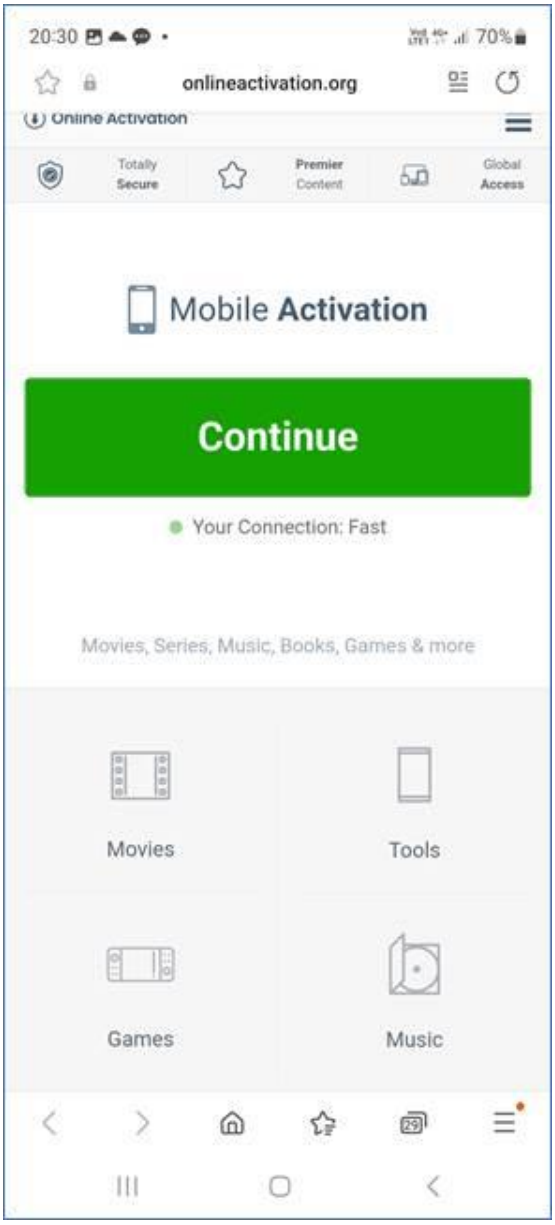
References

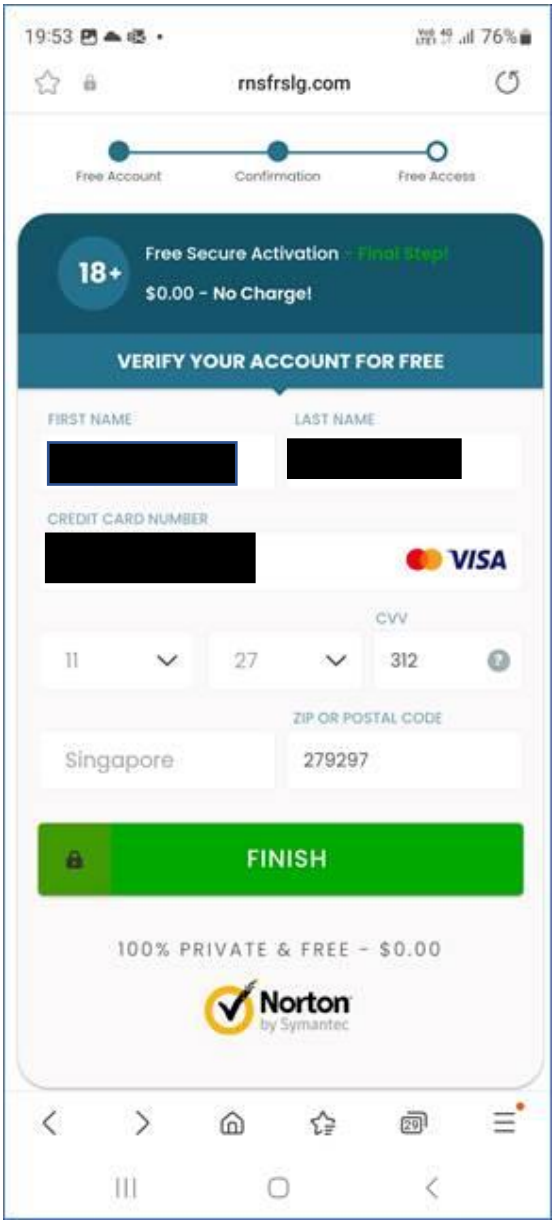
https://www.bleepingcomputer.com/news/security/fbi-warns-of-malicious-qr-codes-used-to-steal-your-money
https://www.einfochips.com/blog/exploring-qr-codes-how-they-work-and-risks-of-phishing-attacks/
https://www.isaca.org/resources/news-and-trends/newsletters/atisaca/2021/volume-18/qr-code-security-challenges#:~:text=Revealing%20the%20user's%20location%E2%80%94Malicious,spear%20phishing%20and%20other%20attacks.
https://www.techopedia.com/the-dangers-of-qr-codes/2/34413

Annex A

Advertisement Banner Within QR Code Scanner Application that Prompts Victims to Create an Account


Phishing Website Requesting for Victims' Credit / Debit Card Details





Issued by:

CSA SINGAPORE

SINGAPORE POLICE FORCE
SAFEGUARDING EVERY DAY