JOINT NEWS RELEASE BY SINGAPORE POLICE FORCE AND CYBER SECURITY AGENCY OF SINGAPORE

JOINT ADVISORY ON SCAMS TARGETING YEAR-END ONLINE SHOPPING AND FESTIVITIES

With the festive season approaching and travel resuming, the Police and the Cyber Security Agency of Singapore (CSA) would like to advise members of the public (e.g. online shoppers), e-commerce platforms and online merchants to be more cautious of possible online threats such as:

- Fake / phishing website scams
    - Websites that would imitate websites of legitimate brands or companies to trick victims into providing sensitive information such as their login information, One-Time Password (OTP) or credit card details.
- Fake / malicious mobile applications
    - Mobile applications which would imitate legitimate applications for phishing purposes, or have malware embedded within, which could be used to monitor victims' activities or steal their personal data when executed.
- Phishing email / SMS scams
    - Emails or SMSes with links that would direct victims to phishing websites controlled by scammers.
- Impersonation scams
    - Scammers may contact victims through email or direct messaging pretending to be a government official or person you know, with the intention of luring victims to provide them with money or sensitive information (e.g. OTP, credit card details).

- Online purchase scams

    - For buyers: Scammers would pose as sellers on popular e-commerce platforms listing an unusually good deal for a product (e.g. a gadget, concert tickets, etc.). These “sellers” would ask for payment upfront but end up not delivering the item or delivering a different item from what was purchased (e.g. cheap replicas). Some scammers would create too good to be true advertisements to attract victims to click on a link that would direct them to a phishing site.
    - For sellers: Scammers would approach victims (sellers) and express interest in buying the items listed by the victim. After agreeing on the price of the item, scammers would send the victim a URL link on the pretext of facilitating payment/delivery. Upon clicking on the URL, victims would be directed to a spoofed website where they would be asked to key in their bank account and personal details.
- Travel scams
    - Scammers would sell fake vacation packages that at a much cheaper than usual price or offer to sell sold out items at a marked-up price. These items may include fake airplane tickets, hotel bookings, or tickets to attractions. Buyers who were duped into making upfront payments for such packages would find out that the promised packages did not exist or were invalid.
- Job scams
    - Scammers may approach victims and offer attractive compensation for completion of simple taskings via messaging apps, social media, spoofed websites etc. Scammers would instruct the victims to deposit a sum of money before they could start the job, which promised the victim good profit. Some scammers would offer incentives to victims to refer people to join the ‘job’. Victims would realise that they had been scammed when they were unable to withdraw any money.
    - Scammers may use global events such as the World Cup to attract victims. Scammers may also target students who are looking for part-time jobs during the school holidays.

- Loan scams

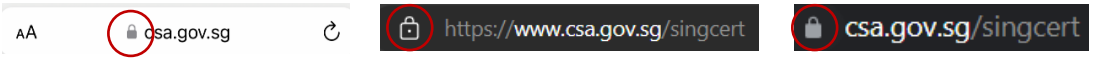
- Scammers would advertise loans on online platforms or through SMS to attract potential victims. The scammers may claim to be staff from a licensed money lender and victims who expressed interest were asked to provide their personal information (e.g. IC number, bank account details). Victims would then be asked to pay a 'fee' before receiving the loan. Victims would realise that they had been scammed when the scammers kept asking for more 'fees' without providing the loan.

Recommendations for Online Shoppers

2 Online shoppers are recommended to take the following steps for a safer online shopping experience:

<u>Ensuring Safety and Legitimacy of Websites / Applications:</u>

- Do not click on the links from promotional emails or SMSes. Instead, visit the official website by typing the web address directly into the address bar of your browser to verify the validity of the promotion.
- Avoid clicking on pop-up ads or opening files or email attachments from unknown senders.
- Verify that the website encrypts all traffic by checking on the presence of the Secure Sockets Layer (SSL) certificate through the "lock" icon (see image below) on your browser's URL bar. Users should avoid websites that do not implement HTTPS.



"lock" icon example

- Only download applications from the official Play Store (Android) and App Store (iOS).
- Download all software and files, including applications and updates, directly from official and verified sources instead of from third-party websites.

- Ensure that your mobile phones, computers and other IT devices are updated regularly with the latest firmware and software versions and install anti-virus applications that can detect and remove malware.
- Buyers can refer to the e-commerce marketplace transaction safety ratings for an overview of the safety features adopted by common e-commerce marketplaces.

Securing Financial Transactions:

- Avoid using public Wi-Fi networks when making online financial transactions.
- Purchase only from authorised sellers or reputable sources, especially for high-value items. If the price is too good to be true, it probably is.
- Opt for buyer protection using in-built options that release payment to the seller only upon delivery. Insist on official payment methods or cash on delivery and avoid making advance payments or direct bank transfers to sellers as this method does not offer any protection.
- Turn on email or SMS alerts for all online credit card transactions or new logins so that you will be notified when a transaction is made.
- Never disclose your personal or Internet banking details and OTP to anyone.

Protecting Online Accounts:

- Use a strong password of at least 12 characters which includes upper case, lower case, numbers and/or special characters.
- Avoid using the same password for all your online accounts.
- Enable Two-Factor Authentication (2FA) for all online accounts and transactions when available.

You may wish to do the following if you believe you have fallen victim to an online scam:

- Report any fraudulent credit/debit card charges or unauthorised transactions to your bank immediately.
- Lodge a police report immediately to receive assistance from the relevant authorities.
- Change your account credentials and use a strong password.

Recommendations for Online Merchants on E-Commerce Platforms

3 Online merchants are recommended to take the following steps to avoid becoming victim of scams:

- If selling on an e-commerce platform, transact within the platform, and where possible, insist on official payment methods or cash-on-delivery.
- Opt to meet up to deliver your item, or use tracked parcels which require proof-of-delivery to monitor your item's location.
- Take pictures of your item before transacting as photographic evidence of the item's condition.

4 Online merchants may wish to do the following if they believe they have fallen victim to an online scam:

- Report the incident to the e-commerce platform to flag the scammer's account.
- Lodge a police report immediately to receive assistance from the relevant authorities.

Recommendations for E-commerce Platforms

5 E-commerce platforms are recommended to take the following steps to ensure a safer shopping experience for your customers:

<u>Securing Your Network and Systems:</u>

- Patch your web servers and software to the latest versions.
- Ensure that your website offers secure online payment service for customers.
- Implement data encryption to protect any data collected from customers and visitors to your website.
- Avoid storing credit card details in your databases.
- Disable public network access to database servers and regularly review the logs of all incoming and outgoing traffic for suspicious activities.
- Implement the principle of least privileges (and access) on user accounts with access to the database server.

- Enforce 2FA for all logins to prevent brute force attacks.

6 E-commerce platforms may wish to do the following if they believe the organisation is a victim of a cyber incident:

- Lodge a police report immediately to receive assistance from the relevant authorities.
- Please contact SingCERT at singcert@csa.gov.sg if you have any enquiries or require any assistance. You may also wish to report any cybersecurity incidents to the SingCERT incident report form at https://go.gov.sg/singcert-incident-reporting-form.
- If you believe your customers' personal data was compromised, report the incident to the Personal Data Protection Commission (PDPC) at https://eservice.pdpc.gov.sg/case/db.
- Contact your affected customers, if any, to take steps to secure their accounts. You may also wish to consider enforcing a password change for all affected accounts
- Engage a reputable cybersecurity vendor to clean up or restore affected systems and recommend appropriate measures to prevent a repeat incident.

7 To find out more on how to protect your website from cyber-attacks, you may wish to refer to SingCERT's advisory at https://www.csa.gov.sg/singcert/Advisories/ad-2022-007. For more information on scams members of the public can visit www.scamalert.sg or call the Anti-Scam Hotline at 1800-722-6688. Join the 'Spot the Signs. Stop the Crimes' campaign at www.scamalert.sg/fight by signing up as an advocate to receive up-to-date messages and share them with your family and friends.

SINGAPORE POLICE FORCE
CYBER SECURITY AGENCY OF SINGAPORE
1 DECEMBER 2022 @ 5.20 PM