JOINT ADVISORY BY THE CYBER SECURITY AGENCY OF SINGAPORE
AND
SINGAPORE POLICE FORCE

PROTECTING YOURSELF AGAINST MALWARE SCAMS DURING THE FESTIVE SEASON

Cybercriminals may advertise attractive deals leveraging festive-related content to trick users into downloading malicious applications or providing confidential information. Members of the public are advised to stay vigilant against such festive-themed malware scams.

What are Festive-Themed Malware Scams?

2 It is common for cybercriminals to distribute malicious software, or malware through advertisements on festive-related offers such as attractive holiday deals, food products, electronic appliances, event / concert tickets, electronic gift cards etc. They may do so by impersonating legitimate entities and placing advertisements on social media platforms to trick unsuspecting victims into downloading and installing malicious apps to gain remote access to their devices.

3 The modus operandi of festive-themed malware scams may take the following forms:

- Cybercriminals will advertise attractive festive offers and promotions through email, text messages or social media platforms such as Facebook, Instagram, etc.

- When you click on the links found in emails or messages (SMSes,WhatsApp etc) and download the malicious software, your device may be compromised once installed.

- Once the malware has been installed, cybercriminals may be able to perform various activities such as keylogging, reading your messages, accessing your screen and camera remotely and stealing your personal details, including Internet banking account details. In some cases, malicious apps disguised as legitimate apps may also request to perform monetary transactions such as payments for deposits or booking fees to enjoy the festive offers.

4 Members of the public are advised to stay extra vigilant during this period and take active steps to protect yourself against malware scams.

- **ADD Security Features and Settings to Secure your Personal Devices**

    - Add anti-virus/anti-malware apps to your device to enhance protection against malware and conduct regular scanning to remove any known malware. You can find more information here.

    - Update your devices' operating systems and apps promptly to be protected by the latest security patches.

    - Disable "Install Unknown App" or "Unknown Sources" in your phone settings.

    - Do not download suspicious software/apps from messenger apps, third party websites, or emails.

- **CHECK the Source and Permissions Granted for the App**

    - Check that you are only downloading apps from official app stores (i.e. Google Play Store and Apple App Store).

    - Exercise caution when granting permissions for apps you downloaded, in particular "accessibility" permissions which can allow scammers to control the device remotely.

    - Check the developer information, number of downloads and user reviews to ensure it is a reputable and legitimate app.

- **CHECK the Authenticity of the Advertisements/Emails/Messages**

    - Always verify the authenticity of these advertisements with the organisations through their official sources. Report the advertisements / online deals to the respective social media platforms if you suspect them to be fraudulent.

    - Always be wary of suspicious emails/messages and verify with the organisations through their official sources before clicking any links or downloading any attachments, especially if the email/message comes from an unfamiliar sender. Report the email/message to the service provider if you suspect it to be malicious.

- **CHECK that you are Using Secure Methods to Make Online Purchases / Transactions**

    - Check that you are not making online purchases or accessing sensitive information when using public Wi-Fi networks.

    - Check that you are using secure websites when shopping online or performing online transactions. Verify the authenticity of these websites by checking the Secure Sockets Layer (SSL) certificate through the lock icon on your browser's URL bar. You are advised to avoid websites that do not support HTTPS.

    - Check that you are using secure payment methods such as credit cards or trusted digital wallets. You are advised to avoid using unconventional payment methods such as gift cards and cryptocurrency.

- **CHECK that you have Secured Your Online Accounts**

    - Passphrases are passwords, but longer and made up of a string of words. To create a strong passphrase, you may refer to our advisory here. Change your password if you suspect that your account has been compromised.

    - Enable Multi-Factor Authentication (MFA) or Two-Factor Authentication (2FA) for your online accounts, whenever possible, to provide an additional layer of security for your online accounts. For more information on MFA, you may refer to our advisory here.

- **TELL Authorities, Family, and Friends about Scams**

    - Pause to check and call a family member or friend for advice. If unsure, call the Anti-Scam Helpline at 1800-722-6688.

    - Report any fraudulent transactions to your bank immediately.

What to do if you suspect that your mobile device has been compromised

5 Members of the public are advised to adopt the following measures if you believe that a malicious mobile app has been downloaded onto your mobile device:

a. Disconnect your device from the Internet by disabling Wi-Fi and mobile data or set your device to “flight mode”.

b. Check for any suspicious apps installed on your device by going to your device’s settings. Uninstall any app that you suspect to be malicious.

c. Install a reputable anti-virus app from your device’s official app store and use it to scan for any malicious mobile app.

d. Check your bank accounts, SingPass, CPF account, etc. for any unauthorised transactions. As a precaution, it is advisable to change your passwords to prevent unauthorised access.

e. Regularly monitor your accounts for any unusual or unauthorised activity.

f. If there are unauthorised transactions, report them to the relevant authorities, and lodge a report with the Police and SingCERT.

g. Should you face difficulties removing the malicious app, do consider performing a data backup and “factory reset” on your device.