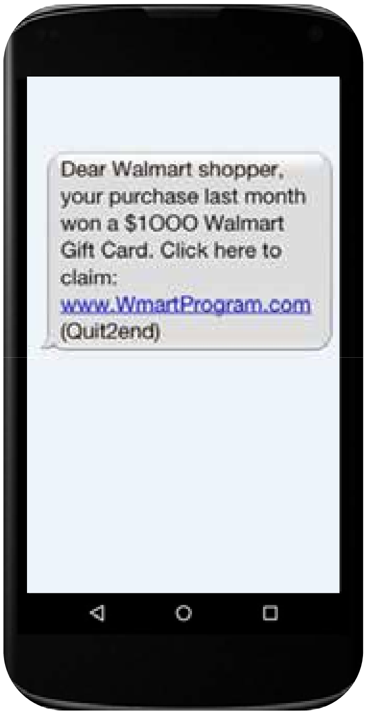
NCIS CYBER DIRECTORATE

SMiShing: An Emerging Threat to Mobile Device Users

While phishing remains the most common attack method used amongst malicious cyber actors, ‘SMiShing’ or ‘SMS Phishing’ is an emerging threat to mobile device users.

SMiShing is a phishing message sent via short message service (SMS) text, rather than email. SMiShing texts are typically sent with a purpose of collecting personally identifiable information (PII) from the victim, or to deliver malware to the victim’s smartphone for follow-on cyber operations. While crafting malicious text messages, cyber actors commonly pose as a legitimate service or organization and request the victim to reply with sensitive information or click on a malicious link within the text message. Victim phone numbers are commonly acquired through previously compromised information or databases available on the dark web. Phone numbers acquired can be used in mass phishing campaigns or in targeted text messages, tailored to a specific victim or group.



Dear Walmart shopper, your purchase last month won a $1000 Walmart Gift Card. Click here to claim: www.WmartProgram.com (Quit2end)

Cyber actors are increasingly targeting mobile devices to obtain sensitive information from victims. Malicious cyber actors appear to be more aggressively targeting mobile devices by targeting installed applications used for entertainment, communications, data storage, Global Positioning System (GPS) services, and other daily activities.

- The increasing use of automated text messages by organizations for notifications such as appointment confirmations or delivery notifications presents further opportunities for malicious cyber actors to craft realistic SMiShing texts.
- Malware threats to a smartphone may include ransomware, spyware, or adware, and if successfully downloaded on the victim’s mobile device, could allow a malicious cyber actor to access personal data, contact information, banking credentials, or locational data.

Phishing via text message can be difficult to detect and often successful. Many times, there are no indications visible to the victim to alert them of a possible compromise. When falling victim to mass SMiShing, opening and replying to a malicious text message can alert cyber actors that the targeted phone number is still active, and initiate further targeting. Protecting PII and avoiding clicking on links or replying to messages from unknown senders will reduce the risk of potential threats from malicious SMS texts.