Subject: Fake SMSs related to unpaid Electricity Bill to dupe citizens

Threat Summary

Smishing - Cybercriminals send text messages pretending to be from trusted sources to get targets to click on links that install malware or steal personal & banking details.

It has been observed that Cyber fraudsters have started duping people in the name of unpaid electricity bill. The fraud campaign is being aggressively spread using SMSs. Users tend to be less skeptical of text messages, so smishing is often lucrative to attackers looking for credentials, banking information, or private data.

Fig. 01 – Cyber frauds using fake SMSs

Modus Operandi

- Fraudster sends text messages (SMSs) to the target phone numbers stating "Your Electricity Power will be disconnected tonight at 9:30 pm because your previous month bill was not updated. Please immediately contact with our electricity officer 9898XXXXXX".
- Once the victim makes contact with the given fraudster's number, then the fraudster tries to convince victim to share the bank account details for the purposes of verifying previous payments.
- Spammers use caller ID Spoofing to make it appear the text is from a trusted or local source.

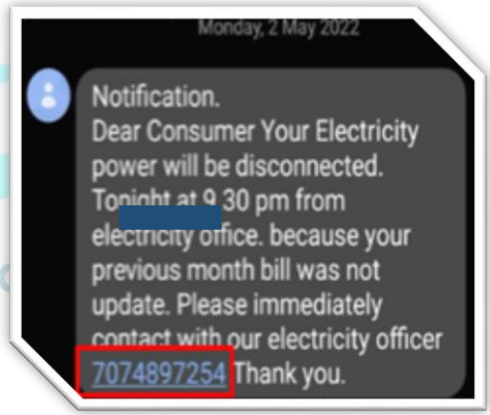

Fig. 02 – Smishing SMSs

- The fraudster also asks victim to install remote access application like Anydesk, Team viewer, etc.
- Once the victim shares all the information and follows the instructions given by the fraudster, the victim's bank account is under the fraudster's control to make fraudulent transactions

Suggestions

- Avoid sharing your phone number unless you know the person or organization well.
- Spammers use caller ID Spoofing to make it appear the text is from a trusted or local source.
- Avoid downloading software from unofficial sources. Remove non-essential applications.
- Avoid providing personal or financial information in response to the unsolicited text or at a website linked to the message.
- Avoid clicking on links in suspicious text; they could install malware on your device or take you to a site that does the same.
- Report any such incidents on the ***cybercrime.gov.in*** portal and follow ***@CyberDost*** on Twitter, YouTube, Facebook, Instagram, Public, Koo and LinkedIn to know more about safety tips.

Regards,

Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207