GOVERNMENT OF MEGHALAYA

PRESS RELEASE

Press Release issued by the Spl. Superintendent of Police (CID), Meghalaya

SEXTORTION: What to do if you have fallen victim to such cyber-attack.

- Block the person immediately. Do not save his/her contact number in your phone
- Silence unknown callers in WhatsApp
- You may anticipate numerous threatening calls from unknown mobile numbers/virtual mobile numbers posing as Police, Advocates and Judges after the incident demanding money in order to stop circulation of the video content
- Do not panic
- Do not make any payment
- Report the matter to Helpline no. 1930 or cybercrime.gov.in
- Immediately, inform/warn your contacts by uploading Status/Stories in your Social Media accounts regarding the incident

Cybercriminals are fraudulently posing as Senior Government officials of CBI, IB, INTERPOL, I4C, DOT, TRAI and State Police Department of Maharashtra, thereafter serve notices and file fake charges against innocent individuals in various ways (eg:- informing an individual that some mobile numbers are registered in their name and committing illegal activities like advertising fraud investments, harassing other individuals through messages, browsing and watching pornographic content, etc. and that cases has been registered with Mumbai Police) coercing innocent individuals to divulge personal information through Skype and respond to the notice served to them within 24 hours failing which they will be arrested and dealt seriously in the Court of Law. Of late, many citizens have fallen victim to such type of crime and most of the individuals end up paying hefty amount of money to fraudsters for case settlement.

[06/03, 19:44] Mr Chyne:

- In WhatsApp impersonation scam, the perpetrator creates WhatsApp account using the identity of higher ranking officials by putting their names and DP.

- The particulars, official designation and contact information (such as name, designation, picture, mobile no., etc.) of the superior(s) and target(s) are usually obtained from the public domain or official website of an Organization.
- Starts masquerading as the Superior of a particular organization and initiate chats with the selected target (usually a subordinate rank) asking their favour to send money urgently on the pretext that he is occupied in an official meeting.

Do's & Dont's

- Intimate the official concerned directly/indirectly and verify the same before making any payment.
- Do not save the number in your phone.
- Activate “Silence unknown callers” in WhatsApp.
- Report the matter in Helpline No. 1930 or cybercrime.gov.in