

Cyber Crime Information – 145

To: All members
From: cyberdost@mha.gov.in

Jan 14th, 2022

Subject: Cybercriminals hacking WhatsApp accounts to defraud citizens

Respected Sir / Madam,

Threat Summary

WhatsApp has become an integral part of our lives, it has more than 50 crore users in India. WhatsApp installation requires a six-digit verification code that is sent on your phone via SMS or call. The OTP is stolen using SMS, call, SMS forwarder or Remote Access app, etc. Both methods of activation (SMS and call) are innovatively misused by fraudsters to take-over WhatsApp accounts. Various cybercrimes are perpetrated using Social Engineering over call or SMS.



Fig 01. WhatsApp registration

Modus Operandi

1. Call based WhatsApp account take over: OTP over call

- Victim gets a call from an unknown number (fraudster) on a prevalent topic (Vaccine Feedback, WhatsApp support, a Survey etc.)
- Simultaneously, fraudster initiates WhatsApp registration process for the target number.
- Call based WhatsApp activation option is selected and victim is asked to merge the call stating some made-up reason.
- Victim merges the call, which is a verification call from WhatsApp that has OTP.
- Fraudster enters the OTP and activates the account and the victim gets logged off.

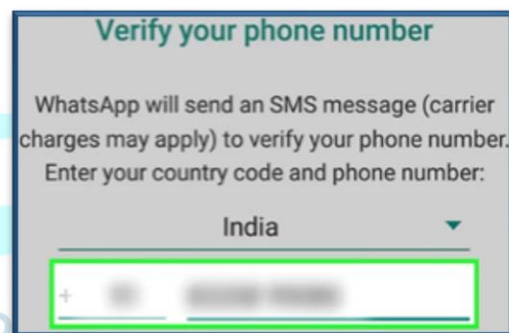


Fig 02. Phone no. verification

2. SMS based take over

Victim is called and asked for OTP stating random reasons. Unaware victim shares OTP which is WhatsApp activation OTP and this account gets compromised.

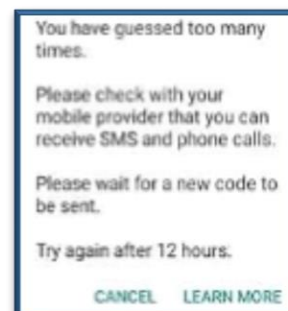


Fig 03. Freezing re-registration

Disclaimer: This advisory is provided "as is" for informational purposes only. The I4C(MHA) does not provide any warranties of any kind regarding any information contained herein. The I4C does not endorse any commercial product or service referenced in this Advisory or otherwise.

Fraudsters then exhaust the limit of entering OTP so the WhatsApp account is frozen for some time (typically 12-24 hours) for registration on any other device. This means, victim's account is taken over by Cybercriminals for that duration.

3. Fraudsters perpetrate following cybercrimes using hacked WhatsApp account

- i. **Financial Fraud:** Message all groups and contacts, e.g., "I am hospitalized; I need money. Please transfer to my account..."
- ii. **Extortion:** Blackmailing using personal information & pictures.
- iii. **Defamation:** Posting status/messages that may defame victims.
- iv. **Connected Account compromise:** WhatsApp based activation service can be opted and used.

[WhatsApp payment cannot be used, as SIM is mandatory for registration of UPI service.]

[WhatsApp is end-to-end encrypted and messages are stored on users' device, so cybercriminals hacking a WhatsApp account using other devices can't read the past conversations of victims.]

Suggestions

- Two-Factor Authentication may be turned on in WhatsApp to secure the account, and WhatsApp users may restrict who can view their profile photo.
- Relatives and friends may be contacted to avoid responding to any request for money & other messages.
- Complaints to be submitted to WhatsApp support via email and WhatsApp customer care.
- Report any such incidents on the cybercrime.gov.in portal and follow [@CyberDost](https://twitter.com/CyberDost) on Twitter to know more about safety tips.

Indian Cyber Crime Coordination Centre

Regards,

Threat Analytical Unit (TAU)
Indian Cyber Crime Coordination Centre
CIS Division, MHA
011-23438207