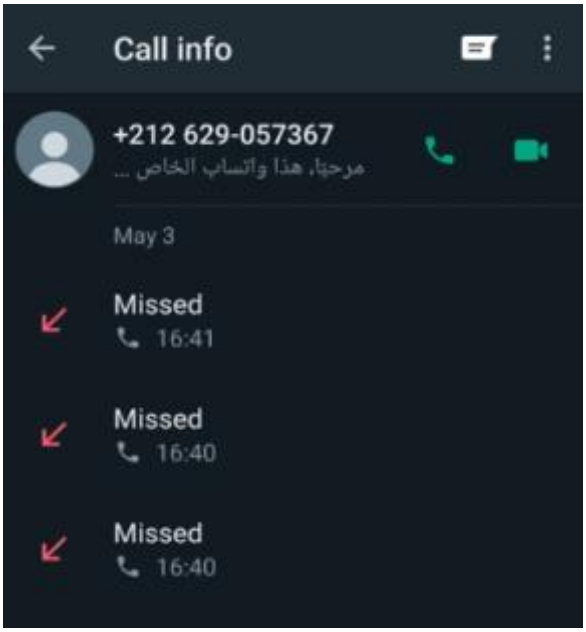
WhatsApp Scams

1. Introduction:

Scammers on WhatsApp are quite active to commit frauds and threat the users through numerous swindles. It may commence with miss calls on WhatsApp, message offering any job / business opportunity or video call/weblink to follow. All such acts aim to menace the victim and lead them to severe situations, costing them huge amount of money.

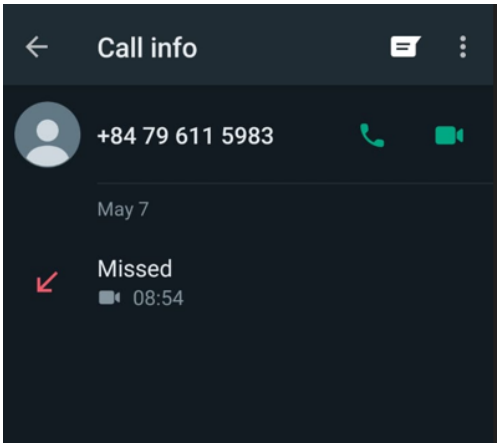
2. Types of WhatsApp Scams:

a. Missed calls: The hackers try to approach by giving one/two ring WhatsApp missed calls to the users. Being a missed call, you may ignore it but it's very dangerous. The hackers are using code scripted bots to find the active users and then target them for various cyber threats. Mostly, such numbers start with +254, +84, +63, +1(218) and others. These are country codes and belong to Si, Vietnam, Kenya, Ethiopia and Malaysia origin.

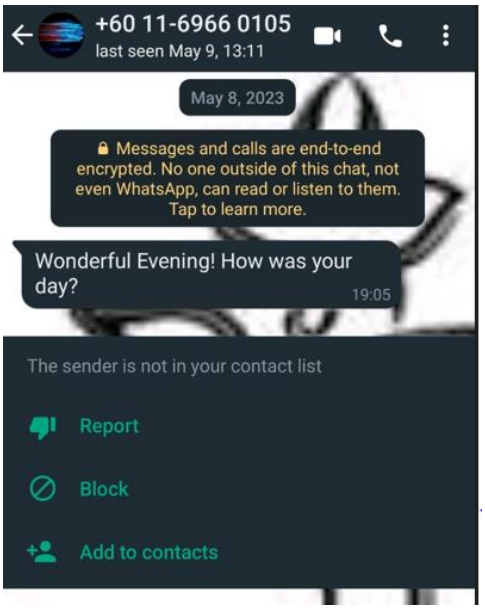


b. **Job Offers:** Hackers even try to approach the users by offering them jobs. It could be a part time/full time job offer with handsome pay offers. Such jobs are generally offered from non-business WhatsApp accounts having no profile picture or anonymous or irrelevant picture.

c. **Video Calls:** Some people also witnessed WhatsApp video calls from unknown numbers. These were basically “sextortion based nude video calls'' which were then used to threaten the user. In this, hackers blackmail the user and ask for money in return.

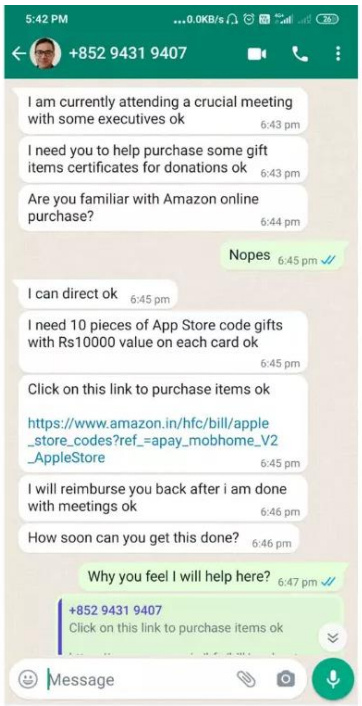


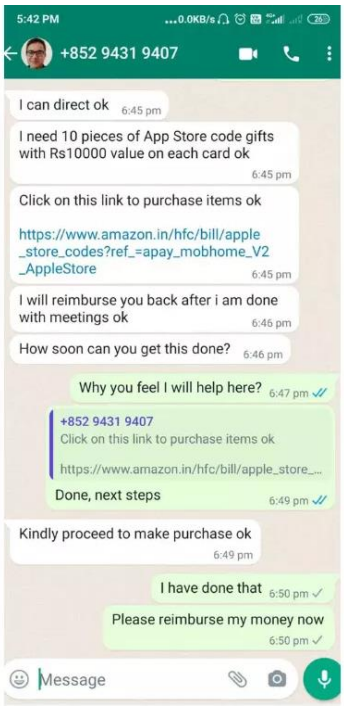
d. **Investment Plans:** Numerous users also reported that they have received messages from different numbers, where the sender claims himself/herself to be a trading expert and guarantees profit making trading calls/suggestions to the user. They provide some unauthorized android applications (not available on Google Play Store) through which the user can invest and exponentially increase their trading profits. In the initial phase, they provide some penny profits to gain user faith and when he invests big amounts, the hackers just terminate their contact numbers and go off.

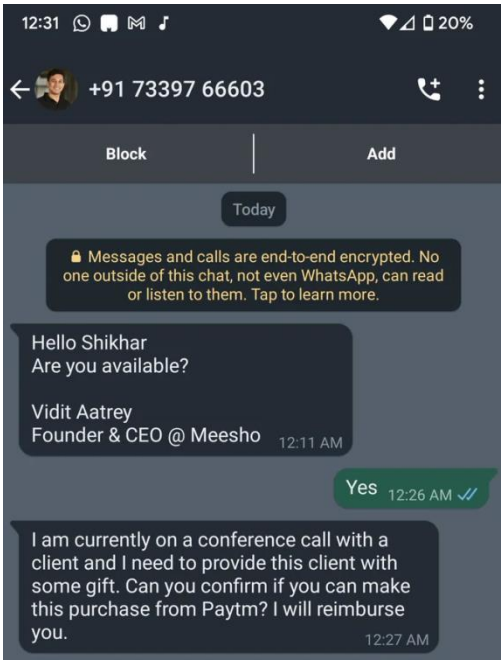


e. **Impersonation (CEO/Officer Scam):** Scammer contacts the victim and pretends as CEOs/Senior Officers of their organizations. They usually target the officials from top management like CFO, COO, CTO, etc. and high rank officers from Police and government bodies. As per the reports, the fraudsters get personal information of the personnel they are pretending to be, by surfing their social media profiles and publicly available information and create similar profiles. Initially, they indicate their occupancy at some important business

meeting or some issues with their previous phone number in order to convince the victim of their authenticity. They usually share web links and ask for some sensitive information or showcase immediate need for payment to be made and assure them for the reimbursement of the funds.







f. **Hijacking: -** Another type of scam, where scammers take unauthorized access to the victim's WhatsApp account. The scam is strategized with the mobile carrier’s automatic call forwarding service and MMI code. Initially, the scammers identify the victim's phone number and do relevant social engineering about the person.

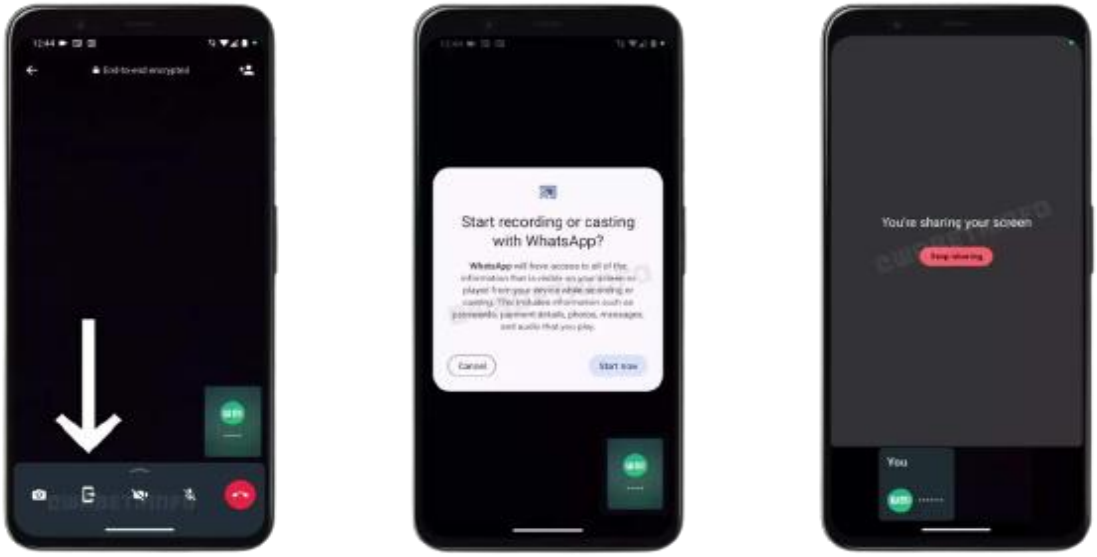
   The hacker initiates a call to the target victim and persuades to enter a number within an MMI code in the instructed format, i.e., "67<10 digit number>" or "405<10 digit number>." Once entered, it will enable the call forwarding feature on the victim's phone when the user's number is busy or engaged and calls to the victim's phone will be forwarded to the scammer's phone.

   In the background, the scammer initiates the WhatsApp registration for the victim's number on his own mobile phone and opts to send the OTP via phone call. Because the victim's phone line is occupied, the OTP call gets redirected to the scammer's phone and grants them complete access to the victim's WhatsApp account.

   The scammers now rush to execute frauds like impersonate and request money from victim’s contacts, share web links to invest in cryptocurrency or can lead towards any criminal activity.

g. **Screen share:** Recently, WhatsApp released its latest feature, i.e., Screen Share”, in which users can share their mobile screen with another person on call. In the past, numerous frauds were witnessed where scammers get victim’s screen access fraudulently and commit

illicit activities. Cases of scams committed unauthorized access are registered in vast numbers. Scammers impersonate themselves as officials from banks, financial institutions, government bodies, etc. On successfully convincing the victim to share the screen, the scammers surreptitiously install malicious app/software to get their sensitive information like bank details, passwords and even the access to their banking services.



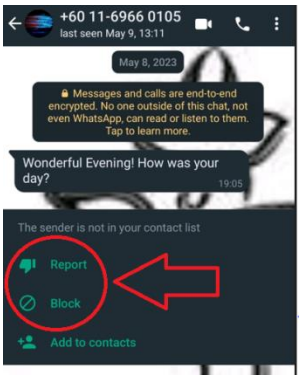
3. **Some use cases:**

a. **WhatsApp Audio Leak Case**: - WhatsApp is being questioned for the app's microphone usage, not just for international scam calls. This came to light after a Twitter engineer reported that WhatsApp was using his Pixel phone's microphone while he was sleeping. In response, WhatsApp pointed finger at Android, claiming that a bug is causing misattribution on the privacy dashboard. As per the official

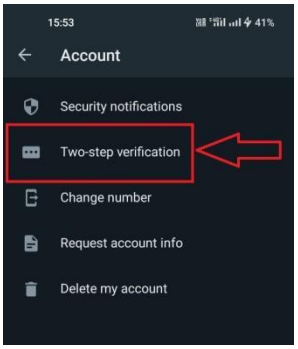
statement, “We believe this is a bug on Android that misattributes information in their Privacy Dashboard and have asked Google to investigate and remediate.”

b. **IT guy loses 42 lakhs: -** A software engineer working with an IT company in Gurgaon fell victim to a scam where he was deceived of approximately Rs. 42 lakh, according to police. The scammers lured him with promises of substantial earnings by simply liking certain videos. The incident unfolded when he received a message on WhatsApp. The message claimed that he could earn additional income by engaging in a part-time job involving liking videos on the popular video sharing platform.

4. **Do’s & Don’ts:**
   a. **Do not reply: -** First of all, don’t respond to such suspicious messages claiming to offer jobs/financial benefits.
   b. Don’t trust in doubt: If anyone impersonates, asks for OTP or asks to execute any task like dialing any code or clicking on any link, never follow them.
   c. **Don’t answer: -** If you receive any such video/audio WhatsApp call which seems to be suspicious, never answer it.
   d. **Report & block: -** Don’t just ignore it, immediately report & block such suspicious numbers on WhatsApp. It will help to fasten the process of identifying such fraudulent numbers.



e. **Activate 2FA:-** Most importantly, enable the Two Factor Authentication on your WhatsApp account. It will enable an additional layer of security on your WhatsApp account. This feature can be found under the account tab of settings menu.



5. Conclusion:

The officials associated with messaging app “Whatsapp” are already been informed for this data breaching act. As numerous government bodies and ministry officials are already working on it, official communications are sent to the concerned authorities for the same. As a precautionary measure, unknown communications on WhatsApp without verifying their authenticity should be avoided. Still, any appropriate solution to such problems is not yet recognized. Our team of expert professionals has identified the above mentioned steps “Do’s and Don’ts” to prevent the users from these WhatsApp threats.