Beware of

WhatsApp Hacking Scam

Nowadays, individuals are falling victim to hackers who compromise their WhatsApp accounts and use them to solicit money from their contacts.

यूको बैंक UCO BANK

Modus Operandi

- Hacker posing as a technical support representative gains the trust of user by providing convincing information using technical jargon & offering a solution to dummy/reported issues.
- Convinces the victim to provide sensitive information or follow their instructions such as dialing specific codes which are used for call / message forwarding or performing certain tasks / actions to resolve the problem.
- By tricking the victim into providing confidential codes, the scammer gains access to the victim's WhatsApp account. They attempt to link the victim's account to their own device by obtaining the verification code, which is typically sent via SMS forwarding.
- With access to the victim's WhatsApp account, the scammer now impersonates the victim and sends fraudulent messages to their contacts for urgent need of money , requests financial assistance etc. The contacts, believing the messages are genuine, may be more likely to comply with the hacker's demands.
- The scammer may continue using the compromised account for further fraudulent activities, such as spreading malicious links, soliciting money from additional contacts, or engaging in identity theft.

Best Practices

- ✓ **Ignore such OTP if not requested by you or generated without your consent.**
- ✓ **Enable two-step authentication feature that adds an extra layer of security to your WhatsApp account to prevent the unauthorized access & misuse**
- ✓ **If you suspect that your WhatsApp account has been hacked, immediately reset the WhatsApp account and log-in again with the newly generated OTP to lock out the hackers and regain control of your account**

- ☒ **Do not trust unknown callers & never perform user prompted actions like clicking random links, dialing codes, downloading unknown Apps etc. at the behest of any stranger**
- ☒ **Avoid sharing sensitive / personal information like Bank Credentials, Card Details, CVV, PIN, OTP, App-code, Aadhaar & PAN Number etc. with anyone**
- ☒ **Never grant unnecessary permissions to Apps which allow remote access or may forward incoming SMSs to unknown mobile number**

Report Cyber fraud Incident to **https://www.cybercrime.gov.in**
or **Call 1930** for assistance

यूको बैंक (भारत सरकार का उपक्रम) UCO BANK (A Govt. of India Undertaking)
सम्मान आपके विश्वास का Honours Your Trust

CISO OFFICE

Security Advisory105 dated 13.06.2023