Beware of Cryptocurrency Scam

Now a days, fraudsters are conning people using fake link promising huge returns on Cryptocurrency investment. These frauds have recently been more prominent through Social Media platforms like Instagram, Telegram and Facebook etc.

Modus Operandi

- **Scammers hack social media accounts of user and then misuse these accounts for malicious and fraudulent activities**

How Social Media Account is hacked ?

Method 1

- ⇒ **Scammer sends message with a link to user offering fee to promote a product/service on social media platform**
- ⇒ **When the user clicks on the link, social media account gets hacked**
- ⇒ **Scammer immediately takes control of the user's social media account, changes the account password & also the details of the registered email id in the social media account**

Method 2

- ⇒ **Once the crypto scammer takes control of user's social media account, sends messages to the friends of the victim through his contact list**
- ⇒ **Lures victim's friend / contacts by sharing fake stories & examples on huge return after crypto investment**
- ⇒ **Asks for changing the email address that is linked to social media account with scammer's email address as an initial step for crypto investment**
- ⇒ **As soon as the victim changes the email address, victim's account is hacked by scammer**

Method 3

- ⇒ **Scammer uses Virtual Private Network (VPN) to hack social media account of target user**

- **After hacking user's account, scammer posts lucrative messages - like fake crypto return on investment, fake pictures of Bank Statements showing receipt of huge return of money on investment, details of advantages of cryptocurrency investment and few links for investing money - to defraud more people**
- **People in the friend / contact list of the user get convinced easily and transfer money to the given Bank Account of Scammer**
- **Once the money gets transferred, scammer disappears and deletes all messages / traces**

Best Practices to avoid such scam

- ✗ **Avoid clicking random links / posts displayed on social media promising high return on investment using cryptocurrency especially Bitcoin**
- ✗ **Avoid interacting with random accounts discussing cryptocurrency**
- ✗ **Don't trust people who promise quick return in the crypto investments**
- ✗ **Do not change your e-mail account linked with social media account at the behest of any person. If anyone entices to do so, he/she may be scammer**
- ✓ **Scammers often use stolen photos to make their accounts look legitimate. If any posts from your known contacts seems suspicious or uncertain, verify the authenticity of that post by making direct contact with that person**
- ✓ **Enable Two Factor Authentication (2FA) on social media account and set up a strong password with uppercase, lowercase, numbers & special characters**

यूको बैंक (भारत सरकार का उपक्रम) UCO BANK (A Govt. of India Undertaking)

सम्मान आपके विश्वास का Honours Your Trust