Beware of Parcel Delivery Scam:

Safeguard Your Data from Deceptive Tactics

Now a days, individuals awaiting parcels are defrauded by fraudsters through social engineering tactics.

Modus Operandi of the Scam

⇒ Individual / citizen who is expecting courier / parcel, contacts a courier helpline number found through search engine.

⇒ Fraudster, with the guise of a courier service agent, cunningly gains the individual's trust and convinces to share the order number and tracking code under false pretenses.

⇒ By creating a sense of urgency, fraudster pressurizes the individual to quickly update the delivery address to receive the parcel promptly.

⇒ Fraudster then instructs the individual to download 'AnyDesk' App - a remote access tool & persuades for sharing the unique address code displayed within the App.

⇒ After that, using deceptive techniques, fraudster coerces the individual into accepting App permissions and security warning notifications for gaining control of the device remotely.

⇒ The fraudster sends a Google Form link to the individual through text message, asks to fill up the personal details & also encourages the individual for paying a small amount as "address verification charge" using debit or credit card.

⇒ During the payment process, the individual's personal information and card details are captured. Armed with this data and remote access to the victim's device, fraudster initiates unauthorized transactions and reads OTPs received during transactions, causing financial loss to the victim.

Best Practices to Avoid such Scam

✗ Avoid searching Customer Care or Helpline number on search engine because fraudster may display misleading information/ads under spoofed / fake website to lure individuals.

✓ Always refer the official website or App of the organization to find legitimate Customer Care or Helpline number related information.

✗ Do not download any unknown App and never carry out financial transaction on unknown / random website or at the behest of any stranger.

✗ Never share sensitive personal / financial information, such as card details, financial credentials, OTP, PIN, UPI PIN with anyone or in any random forms / websites / social media platforms etc.

✓ Carefully review App permissions, notifications, security warnings etc. Do not grant unnecessary permissions to App which allow remote access.

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

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

CISO OFFICE

Security Advisory 106 Dated: 24.07.2023