Cyber Fraud Awareness:

Recognize.. Prevent.. Protect

KYC Fraud

⇒ Scammers impersonate as Bank officials or government representatives, target customers through deceptive text messages or calls to lure into providing personal / sensitive / financial information under the false pretext of updating KYC details.

⇒ Never share personal / sensitive / financial information over unsolicited calls or messages.

⇒ Verify the authenticity of requests through official channels and always cross-check and confirm the KYC status by directly communicating with your Home Branch.

Lottery Fraud

⇒ Victims receive Fake notifications claiming they've won a lottery, but they need to pay fees or provide personal details to claim the prize, resulting in financial loss.

⇒ Do not trust unexpected messages from unknown sender & avoid clicking on unknown link.

⇒ Do not pay any advance fees or provide personal / sensitive / financial information for claiming unexpected prize / reward / lottery/ free gift etc.

Loan Fraud

⇒ Fraudster create unscrupulous Loan Apps offering easy & instant loans without checking credit history / scores. Upon downloading the app, users are prompted to grant multiple permissions, including remote access. By obtaining full control of the user's device, fraudsters can carry out fraudulent activities.

⇒ Exercise caution if the lender appears more interested in obtaining personal or sensitive information rather than checking credit scores.

⇒ Check the authenticity of any App before downloading & do not allow unnecessary permissions to Apps which allow remote access.

⇒ Always apply loan from RBI approved Banking & Financial Companies / Institutions.

Electricity Bill Scam

⇒ Fraudster sends fake message threatening disconnection of services due to unpaid bills. Messages may also contain fake contact number of electricity officer.

⇒ Do not trust such type of messages.

⇒ Never call-back on the given number.

⇒ Always refer Customer Care or Helpline number provided in original electricity bill & pay bills from authorised / official website / App.

Digital Arrest Fraud

⇒ Cybercriminals posing as police officials have been alleging unsuspecting individuals in fictitious money-laundering cases, manipulating and extorting money by threatening individuals with fake cases and interrogation.

Cybercrime Helpline No. 1930

Customer Care Fraud

⇒ Scammers manipulate search engine results to display fake customer care numbers. When users search for helpline numbers of legitimate companies or organizations, they may end up contacting these fraudulent numbers and unknowingly share sensitive information.

⇒ Avoid searching for customer care or helpline numbers on search engines. Instead, rely on official websites or apps of the company or organization for authenticated customer care contact details.

Card Fraud

⇒ Fraudster posing as Bank representative, may call & ask for sharing Card Number, Expiry Date, CVV, PIN, OTP etc. under false pretext or fabricated scenarios.

⇒ Be cautious of unexpected calls requesting such information and always verify the caller identity through official channels.

⇒ Never share sensitive / financial information like card number, expiry date, CVV, PIN, OTP or Financial credentials with anyone.

UPI Fraud

⇒ Fraudsters masquerade as legitimate entities or known individuals, enticing users with attractive schemes, refunds, offers, or urgent messages. They persuade users to make fund transfers or payments to unknown UPI IDs or disclose sensitive UPI credentials such as UPI ID, PIN, OTP, etc., enabling them to carry out fraudulent transactions.

⇒ Avoid sharing UPI ID, PIN, or OTP with anyone under any circumstances.

⇒ Enter UPI PIN / scan QR code ONLY to make payment, not for receiving money.

⇒ Never approve payment / fund transfer request from unknown UPI ID.

Task Based Job Fraud

⇒ Scammers approach individuals, enticing them with lucrative work-from-home opportunities promising substantial earnings with minimal effort. Victims are convinced to invest initially, but end up losing significant amounts of money due to subsequent demands for higher payments.

⇒ Do not trust or respond to unsolicited messages on social media or instant messaging platforms like Telegram, WhatsApp etc., which promise easy money in exchange for completing online tasks.

⇒ Avoid engaging in user prompted tasks or actions at the behest of any stranger.

⇒ Always verify legitimacy of job offers or investment opportunities etc. from official & trusted sources.

⇒ Rely on authentic job portals, official websites, or apps for genuine job-related information and opportunities.

⇒ Be wary of unsolicited calls claiming legal issues or urgent threats, especially if they demand immediate action or money transfer.

⇒ If threatened with legal action, verify with the relevant authorities, ask for the Official notice & directly communicate with the local police station before complying with any instructions or transferring funds.

⇒ Always ask for the Official notice, other necessary details etc. & directly communicate with the local police station for verification / clarification.

⇒ Refrain from sharing personal, financial, or Aadhaar card details over the phone unless you can confirm the legitimacy of the call.

⇒ Always remember, real police authorities don't question individuals digitally. Official discussions happen through legitimate or formal channels, not through random online intimidation or coercion.

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

Security Advisory 117
Dated 16.02.2024

यूको बैंक (भारत सरकार का उपक्रम) UCO BANK (A Govt. of India Undertaking)
सम्मान आपके विश्वास का Honours Your Trust
CISO OFFICE
1800-103-0123 (Toll Free) 8334001234 7666399400 Follow us on