





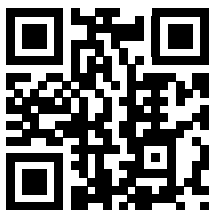


USCryptoCop FIELD CARD

First 24-Hour Cryptocurrency Response

-  **RESPONSE:** Stop payments, isolate victim, check for remote access tools
-  **DATA:** Collect ALL TXIDs, wallets, timestamps, screenshots
-  **DISRUPTION:** Notify exchanges immediately and request freeze
-  **INTEL:** Trace funds, identify exchanges, detect reuse patterns






Scan for Step-by-Step Victim Checklist








USCryptoCop XRPD-Enhanced Investigation Guide

CRITICAL TRANSACTION DATA





-  Collect ALL TXIDs (victims often send multiple transactions)
-  Confirm if payments increased over time
-  Capture wallet addresses (sending and receiving)
-  Document crypto type, network, timestamps, and amounts
-  Preserve transaction screenshots

TXID: A unique ID used to locate and track a transaction on the blockchain.





REMOTE ACCESS / DEVICE COMPROMISE

-  Ask if suspect accessed victim device
-  Identify remote software (AnyDesk, TeamViewer)
-  Determine if suspect controlled transactions





FUNDING SOURCE TRACEBACK

-  Identify how victim obtained crypto (bank, card, ATM)
-  Collect bank transaction records
-  Capture exchange purchase confirmations
-  Document ATM receipts and locations




COMMUNICATION & WEBSITE FORENSICS

-  Preserve texts, emails, WhatsApp, Telegram
-  Capture FULL URLs of scam sites
-  Screenshot dashboards, balances, withdrawal errors
-  Document usernames, phone numbers, profile links




VICTIM TIMELINE

-  Initial contact method and date
-  Manipulation tactics used
-  Transaction sequence and escalation
-  Point of fraud realization





RECOVERY WINDOW

-  0–24 hours: highest chance of disruption
-  24–72 hours: funds begin layering
-  72+ hours: funds dispersed or mixed





DISRUPTION ACTIONS

-  Notify exchanges with TXIDs immediately
-  Request account freezes and preservation
-  File IC3 and local reports

INVESTIGATIVE ACTIONS

-  Trace transactions via blockchain explorers
-  Identify exchange off-ramps (KYC)
-  Look for wallet reuse and clustering
-  Compare against known scam infrastructure

SCAM TYPE CLASSIFICATION

-  Investment / Pig Butchering
-  Romance Scam
-  Tech Support Scam
-  Impersonation

INTELLIGENCE FLAGGING



Identify reused wallets



Identify reused domains



Flag repeat scripts/messages



Link to other potential victims

Officer Directive: Provide victims with the USCryptoCop Step-by-Step Victim Checklist at www.uscryptocop.com