Indian Cyber Crime Coordination Centre

EMERGING CYBER CRIMES IN INDIA: A Concise Compilation

(August, 2021)

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)

Modernization Division
BUREAU OF POLICE RESEARCH AND DEVELOPMENT
Ministry of Home Affairs, Government of India

Emerging Cyber Crimes in India:
A Concise Compilation

National Cyber Crime Research & Innovation Centre (NCR&IC)

Modernization Division
Bureau of Police Research & Development
New Delhi

Disclaimer

- This document is not a substitute for existing manuals available in the States/UTs. It is only a guide for awareness purpose. In case of any conflict, local manual/practice may prevail.
- BPR&D does not promote any tool/software of a particular vendor. All the tools and software mentioned in this manual are for illustration purpose only.
- Wherever any Image/graphics/flowchart is taken from other sources, the same has been duly acknowledged.

वरुण सिंधु कुल कौमुदी, भा.पु.से.
महानदिशक
VSK Kaumudi, IPS
Director General
Tel. : 91-11-26781312 (O)
Fax : 91-11-26781315
Email : dg@bprd.nic.in

पुलिस अनुसंधन एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037
Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

MESSAGE

The setting up of the National Cyber Crime Research & Innovation Centre (NCR&IC) at the BPR&D Hqrs.and its branch, the National Cyber Crime Research, Innovation and Capacity Building, at the CDTI, Hyderabad, has been a major technological milestone in the cyber research and training capabilities of the BPR&D. The NCR&IC, as part of the umbrella scheme of the Indian Cyber Crime Coordination Centre (14C), MHA, has been striving countinuously to strengthen and augment the capacity of Law Enforcement Agencies (LEAs) in their efforts of Cyber Crime prevention and investigation.

I am happy that NCR&IC professionals have come up with the following four booklets to address the urgent need for awareness related to Cyber Crimes, keeping in mind the skill set required by the police officers in the investigation of Cyber Crimes:

- Emerging Cyber Crimes in India - A Concise Compilation
- First Responder Handbook - Computer System Acquisition
- SOP on Investigative Process/Methodologies for Cryptocurrency related Cyber Crimes
- Manual on Social Media Intelligence (SOCMINT) for LEAs

The above manuals/SOPs are result of the sincere efforts of Dr. Karuna Sagar, IPS, IG (Modernization), Sh. B. Shanker Jaiswal, IPS, DIG (Mod), Dr. M. M. Gosal, SSO (T) and NCR&IC professionals/experts, namely, Dr. Pankaj Choudhary, Sh. Gourav Chaurasia, Sh. M. Krishna Chaitanya and Sh. Farhan Sumbul, BPR&D. I record my deep appreciation for their hard work.

I believe, these booklets will guide the police officers in understanding the Cyber Crimes of various categories, including the modus operandi of cyber criminals, Data Acquisition in different scenarios, Methodology for Investigating Cryptocurrency and Social Media Platform, etc.

(V. S. K. Kaumudi)

Place: New Delhi

नीरज सिन्हा, भा.पु.से.
अपर महानिदेशक

Neeraj Sinha, IPS
Additional Director General

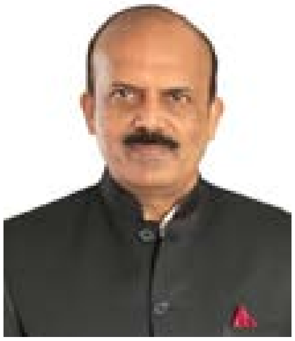
Tel.: + 91 11 26781341 • Fax: 91 11 26782201
Email: adg@bprd.nic.in • Website: www.bprd.nic.in

सत्यमेव जयते

पुलिस अनुसंधान एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग–8, महिपालपुर,
नई दिल्ली–110037

Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

MESSAGE



Technology is often value neutral. It can be used effectively by friends and foes alike. On occasions, the rapid strides by technology, especially in the domain of cyber-space, threatens to outpace the skills of inadequately trained professionals, especially at the cutting edge.

BPR&D, with its motto of 'Promoting Good Standards and Practices', has often bridged the information gap for the LEAs, with its thoughtful seminars and publications. It gives me great pleasure that the National Cyber Research & Innovation Centre (NCR&IC) professionals are putting together 04 significant compilations, including 'Emerging Cyber Crimes in India – A Concise Compilation'; 'First Responder Handbook – Computer System Acquisition'; 'SOP on Investigative Process/Methodologies for Crypto-currency related Cyber Crimes'; and 'Manual on Social Media Intelligence (SOCMINT) for the LEAs'.

The team of the Modernization Division of the BPR&D, led by Dr. Karuna Sagar, IPS, IG, Shri B S Jaiswal, IPS, DIG, Dr. Manjunath M Gosal, SSO (T), Dr. Sarabjit kaur, Dr. Pankaj Choudhary, Sh. Gourav Chaurasia, Sh. M. Krishna Chaitanya and Sh. Farhan Sumbul, are deserving of our appreciation for the publications.

I trust the Investigating Officers, particularly at the cutting edge, would find these compilations useful in their day to day professional lives.

(Neeraj Sinha)

Place: New Delhi.

डॉ. करुणा सागर, भा.पु.से.
महानिरिक्षक/निदेशक (आधुनिकीकरण)
Dr. Karuna Sagar, IPS
Inspector General/Director (Modernisation)

Tel. : 91-11-26782023
91-11-26782030 (F)
Email : igmod@bprd.nic.in

पुलिस अनुसंधन एवम् विकास ब्यूरो
गृह मंत्रालय, भारत सरकार
राष्ट्रीय राजमार्ग-8, महिपालपुर,
नई दिल्ली-110037
Bureau of Police Research & Development
Ministry of Home Affairs, Govt. of India
National Highway-8, Mahipalpur,
New Delhi-110037

EXECUTIVE SUMMARY

There are many disturbing things happening in cyber space. Cyber crime refers to all the activities done with criminal intent in cyber space. These could be either the criminal activities in the conventional sense or could be activities, newly evolved with the growth of the new medium. Because of the anonymous nature of the Internet, it is possible to engage into a variety of criminal activities with immunity and people with intelligence, have been grossly misusing this aspect of the Internet to indulge in criminal activities in cyber space. The field of Cyber crime is just emerging and new forms of criminal activities in cyber space are coming to the forefront with the passing of each new day.

There is always a need for concise booklets on emerging trends in cyber crimes to help investigators in our police forces. In this endeavour, the present booklet is a brief compilation of sample cases encompassing various categories of cyber crimes like cyber extortion, social engineering frauds and most importantly dark net frauds. Each sample case also includes the modus operandi. This may be of great help for cyber crime investigators.

There are a total of 06 categories of cyber crimes being covered in this booklet which are cyber extortion, identity theft, internet banking frauds, social engineering frauds, cryptocurrency frauds and darknet frauds. Each category includes a brief introduction to the readers of the way in which cyber criminals commit these crimes. The sample cases mentioned in the booklet are taken from reliable news sources and the links of each source are duly acknowledged in each section.

The contribution of Sh. Farhan Sumbul, Content Developer, NCR&IC is significant in preparing this booklet for the benefit of the LEAs.

18.8.2021

(Dr. Karuna Sagar)

Place: New Delhi

Table of Content

List of Abbreviations

LEA	Law Enforcement Agencies
RBI	Reserve Bank of India
PII	Personally Identifiable Information
UDID	Unique Device Identifier
IMEI	International Mobile Equipment Identity
ATM	Automated Teller Machine
CRPF	Central Reserve Police Force
OTP	One Time Password
QR	Quick Response
TOR	The Onion Router
I2P	Invisible Internet Project

1. Introduction

With the advent of high-speed internet and mobile technologies, the cyber crime graph is rapidly increasing in our country. In an offline world, people can be advised to refrain from going to lonely places where robbers can snatch the valuables and run away easily. But in the case of the digital world, things are very different so much so that a well-educated gentleman can also become the victim of cyber crime.

Every day the news watchers do observe new cases of cyber crimes being reported. Few cases have demanded LEAs to do deep-diving into the cyber world, liaison with cyber and digital experts to nab the culprits.

The fundamental idea behind compiling this booklet is to provide LEAs with a glance at emerging cyber crimes in India. The booklet shall also try to present the Modus Operandi of each mentioned case so that those investigation officers who might have not come across similar incidents may also get an overview of the crimes. For the larger benefit of its readers, few emerging cybercrimes being reported outside India are also included.

This booklet comprises various verticals of cyber crimes like cyber extortion, Internet Banking frauds, Cryptocurrency frauds, Darknet frauds and Social Network frauds to name a few.

All the cases compiled in this booklet have been taken from reliable news sources, social media and government publications.

Since cyber crimes are increasing every day and criminals keep employing new modus operandi, it has been planned that this booklet will be released incrementally.

The first volume of Emerging Cyber crimes in India: A Concise Compilation is in your hands.

2. Cyber Extortion

Cyber extortion is a digital form of blackmailing. So, the cyber criminals do not do real-life kidnapping for demanding ransom money but they employ various new and innovative tricks to threaten potential victims through online mediums. In some cases, extortionists may tell to a victim that they have got hold of his private information and demand ransom money for not sharing it publicly.

According to a research paper "Cyber extortion can take many forms. It can be very lucrative, netting attackers millions of dollars annually. A typical cyber-attack may result in a demand for thousands of U.S. dollars. Furthermore, payment does not guarantee that further attacks will not occur, whether the attacks continue from the same cyber extortionists or a different group attacks". [1]

Sample Case 1: According to a recent report published in Indian Express, India is among the top 10 sextortion mail source countries. Sextortion is a type of phishing crime where the criminals send emails to the victims demanding money by claiming to have private photos or videos of an individual.

Image Source:https://www.alamy.com/stock-photo-background-concept-wordcloud-illustration-of-cyberextortion-glowing-86398574.html

[1] Source URL: https://www.iup.edu/WorkArea/DownloadAsset.aspx?id=170745#:~:-text=Cyber%2 extortion%20is%20a%20 crime,avert%20or%20stop%20the%20attack.&tex-t=When%20many%2 people%20think%20of,pictures%20or%20even%20 plain%20 bullying.

Modus Operandi:

1. Criminals send emails to vulnerable persons. They claim that they have accessed the compromised photographs or videos of the victims.
2. Victims get afraid and try to negotiate with the criminals without informing anyone.
3. Criminals demand ransom and continue to exploit.

News Source: The Indian Express

1. https://indianexpress.com/article/technology/tech-news-technology/india-top-10-sextortion-country-how-to-protect-from-cyber-attack-6380192/

Sample Case 2: During the past few months, many suicides have been reported in Telangana for which the reason is said to be the blackmailing of young men and women by the app-based (PowerBank, Tesla Power Bank) loan providers. The fraud was so massive that Telangana Police hired data analysts to track down the web of fraudsters from across the state.

Alarmingly, Telangana Police reported that 1.40 Crore money lending transactions were reported involving Rs 21,000 Crores. Police also apprised the RBI working group and sought appropriate intervention to regulate the malicious money lending apps.

Modus Operandi:

1. People in need of money trying to find out loan providers by searching several mobile apps claiming to be trusted loan providers in quick and easy steps. Such apps also promise less paperwork, low-interest rates and low processing fee etc.
2. People get attracted to such apps without realizing that such apps are never regulated by government financial controllers.
3. When people start failing loan repayment deadlines then app administrators start exploiting and threatening them for dire consequences etc.
4. It has been revealed through investigations, that the cheated money was siphoned off through bank accounts of shell companies, by way of crypto currency to foreign country.

News Source: The Hindu

1. https://www.thehindu.com/news/cities/Hyderabad/police-interact-with-rbi-officials-on-loan-app-fraud/article33762148.ece
2. https://www.thehindu.com/news/national/telangana/financial-experts-roped-in-to-decode-21000-cr-transaction/article33495082.ece

Sample Case 3: Cyber security researchers in the UK have found that high net worth individuals are being targeted for sextortion crimes through their LinkedIn profiles. According to news reports published in international media, cyber criminals gather information of individual’s profile, their career details and salaries etc. They establish an online relationship on LinkedIn with a married person and then threaten to reveal the details of the affairs with their partners. They demand ransom amounts in a popular cryptocurrency called Bitcoin.

There are reports that cyber-criminals are even threatening to kill the potential victims if they fail to pay the ransom money. This new type of threat is called the Hitman campaign in the UK.

Researchers analyzed bitcoin wallets related to sextortion ransom scams and found that cyber-criminals minted 540 USD per individual.

The sextortion cases are rapidly surging in India and targeting of working youth and business men’s having social media potential profiles. The gangs involved in sextortion are operating from Bharatpur, Alwar and Mewat region etc. The cyber criminals work in coordination with Jamtara gang. The social media users are laid into the trap of attractive and indecent social media profiles. Once, the contact is established with user and the chat starts, the target is intended to have online intimate scenes, which are recorded. Thereafter, the victim is extorted the money under the threat of releasing the intimate videos on social media channels. An inter state sectortion gang has been recently arrested by Alwar and Bharatpur Police. The detailed analysis of mobile phones and bank details, have led to inter linkage with many FIRs of online sextortion cases in different states.

Image Source: Independent

Modus Operandi:

1. The cyber-criminals gang go around hunting for the potential victims of sextortion using the LinkedIn profile.
2. Since people have the habit of posting a lot of personal and professional details on LinkedIn which is a popular online platform for working professionals around the globe, it becomes very easy for stalkers to gather the necessary information to target the individuals.

3. Once they can breach the password of victim’s social profiles, their crime becomes easier.

4. Extortionists, even if they do not have anything, pose to the potential victims as if they have got some intimate content of their personal lives.

5. Extortionists are also gauging the salary of individuals and demanding the ransom money accordingly, many a time, even on cryptocurrency.

News Source: Independent

1. https://www.independent.co.uk/life-style/gadgets-and-tech/news/linkedin-cyber-crime-gang-sextortion-email-scam-pornography-digital-shadows-a8789926.html

3. Identity Theft

Cyber criminals become impostors on online platforms by stealing personal information generally called Personally Identifiable Information (PII) and commit cyber crimes. Identity theft frauds can be related to digital payment frauds, insurance claims frauds, and online employment frauds among others. There are various types of identity theft like Biometric Identity Theft, Mail Identity Theft, Unemployment Identity Theft and Tax Identity Theft etc.

In this section, news reports of few emerging crimes are collected for the general reference of LEAs.

Image Source:https://www.fraud-magazine.com/article.aspx?id=4295009331

Sample Case 1: According to a news report that appeared in NDTV and The Indian Express on 4th February 2021, an Italian surveillance company built and distributed a fake version of the WhatsApp app for iOS users. As per the reports published in online news portals, the surveillance company built this fake app to target select individuals by tricking them to install few configuration files into their mobile phones to steal data.

Modus Operandi:

1. One Italian firm Cy4Gate developed a fake version of WhatsApp for iOS users.
2. Victims got lured to it as the branding and graphic details looked very legitimate for normal users.
3. Upon installing the fake version of the app, hackers installed few configuration files into the mobile phones of victims and leaked information like Unique Device Identifier (UDID) and International Mobile Equipment Identity (IMEI) numbers.

   Contact List, Personal files and Images etc.

News Source: NDTV, The Indian Express

1. https://gadgets.ndtv.com/apps/news/whatsapp-iphone-fake-version-hack-users-cy4gate-italian-spyware-motherboard-citizen-lab-report-2362841
2. https://indianexpress.com/article/technology/tech-news-technology/whatsapp-fake-version-iphone-italian-spyware-company-specific-targets-7174516/

Sample Case 2: On January 15, 2021, an Indian journalist appeared on Twitter to announce that she had been a victim of a very strange, unique and well-orchestrated phishing attack. The fraudsters disguised as the recruiters belonging to the world's best university conducted online interviews, sent offer letters and continued to keep the journalist in limbo for many months.

Image Source:https://www.endnowfoundation.org/detect_job_frauds.php

Modus Operandi:

1. People pretending to be the officials of reputed institutions send emails to the victims with job offers.
2. Fraudsters use email ids with slight and unnoticeable variations of the authentic email ids.
3. The language of email and every other thing appears to be real for the victims.
4. Fraudsters even conduct online interviews and extend fake job offers without the victim realizing that he/she has been duped.

News Source: Twitter

Sample Case 3: Recently Mumbai Police busted a racket of criminals who created fake mobile apps disguised as Prime Minister Loan schemes and duped thousands of people across the country. They created the apps named – Pradhan Mantri Yojna Loan, PM Loan Yojna, PMYL Loan, and Sarvottam Finance Loan Service etc. These apps promised loans with very low-interest rates.

Modus Operandi:

1. Cyber criminals create unauthorized mobile apps disguised as government-backed service providers.
2. Thousands of people fail to verify the authenticity of such apps.
3. People get lured to attractive fake credit schemes and charge processing fees etc.

News Source: Hindustan Times

1. https://www.hindustantimes.com/cities/mumbai-news/mumbai-cyber-police-bust-major-online-racket-that-duped-250k-people-nationwide-101614022710802.html

Sample Case 4: Computer Weekly reported that their investigation revealed schools, smalls businesses and charities received threatening demands for hundreds and thousands of pounds for using the apparently free Flickr photographs from the internet unintentionally. A German photographer Marco Verch put thousands of apparently free-to-use images on the internet and people started using it without being aware that they were actually falling prey to a copyright scam.

Modus Operandi:

1. A photographer publishes tens of thousands of copyright images on the internet belonging to Flickr.
2. Common users download them without even realising that they violate any license agreements.
3. The photographer uses his software and third-party enforcement services to identify people who apparently have violated the copyright rules.
4. The people who downloaded those images unknowingly become a target of fines and legal penalties.

News Source: Computer Weekly

1. https://www.computerweekly.com/news/252493452/Top-10-Investigations-and-National-Security-Stories-of-2020

Sample Case 5: An US intelligence agency has reported that there has been an increase in cyber crime activities during COVID19 involving unemployment insurance claims by impersonating and phishing means. The criminals are obtaining the stolen identity using a variety of techniques like data breaches, cold-calling victims, phishing attacks, from social media and public websites etc. Individuals are targeted by the cyber criminals impersonating the victims and using the victim's stolen identities to make online insurance claims.

Modus Operandi:

1. Cyber criminals use the stolen personal information of potential victims and make fake unemployment insurance claims.

2. Victim individuals come to know about the fraud once they themselves go to claim the unemployment insurance or when their employer sends them notices about such claims despite being employed.

News Source:

1. https://www.fbi.gov/contact-us/field-offices/elpaso/news/press-releases/fbi-el-paso-sees surge-in-fraudulent-unemployment-insurance-claims-filed-using-stolen-identities

4. Internet Banking/ATM/Debit Card Frauds

Internet or Digital banking related frauds have become very common in cyberspace. Fraudsters always employ new modus operandi to cheat common people and steal their hard-earned money from their bank accounts. This section, it is attempted to present some unique types of cyber crimes pertaining to digital banking.

Sample Case 1: In January 2021, Bangalore police registered a strange case where fraudsters used a blocked debit card and withdrew a huge sum. The complainant told police that he had only Rs 19 balance and yet criminals could run away with more than seven lakh rupees.

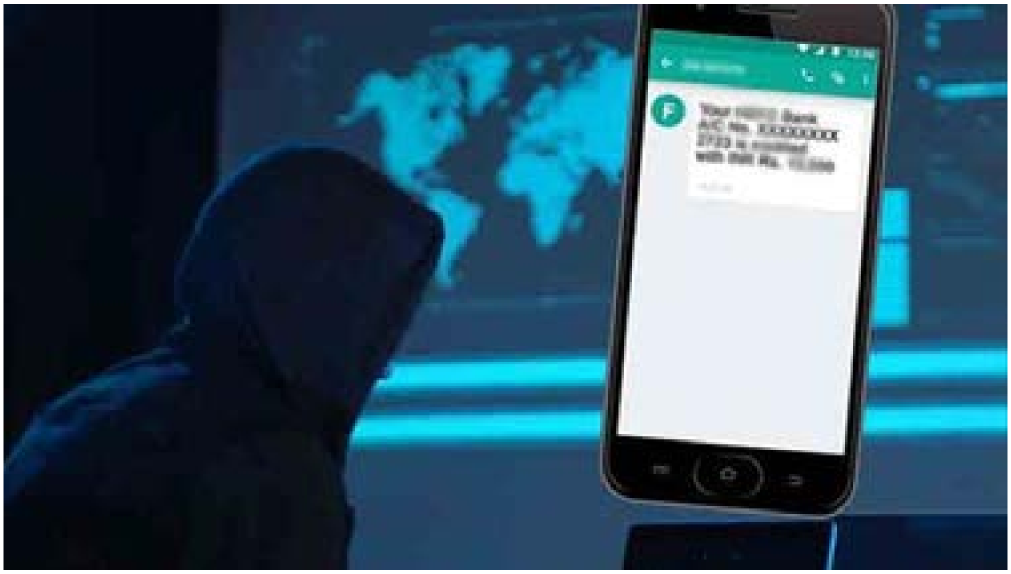


Image Source:https://cutt.ly/McKERBl

Modus Operandi:

1. Criminals used a blocked debit card of a customer who had only Rs 19 in account balance.
2. Somehow, they succeeded in duping the bank itself by withdrawing more than seven lakh rupees by using the blocked debit card.
3. It is suspected by Police that there must be some bug in the backend of the Banking software which let this fraudulent transaction take place.

News Source: Times of India

1. https://timesofindia.indiatimes.com/city/bengaluru/miscreants-withdraw-7l-using-blocked-debit-card/articleshow/79746485.cms

Sample Case 2: Karnataka Police arrested a 25 years old young man in Nov 2020 on the charges of hacking several private and government websites and stealing money online. The arrested person is also accused of stealing Rs 11 crore from the e-procurement portal of the Karnataka government.

According to media reports, the police has charged him for being involved in the purchase of Ganja on the dark web by making payments via bitcoins.

Modus Operandi:

1. The accused hacked many private and government websites to steal data.
2. The accused create mirror websites to deceive the people and collected information on credit and debit cards used by them.
3. Mirror sites are the exact replicas of original websites. This is used by cyber criminals to deceive people by disguising the fake website as the real ones and when people enter some important information into the fake website considering it real, the hackers steal the information from there.

News Source: Times of India, The Indian Express

1. https://timesofindia.indiatimes.com/city/bengaluru/bengaluru-youth-who-hacked-games-government-websites-lands-in-net/articleshow/79294416.cms
2. https://indianexpress.com/article/cities/bangalore/bengaluru-25-year-old-govt-portal-hacker-sent-to-13-day-ccb-custody-7085208/

Sample Case 3: On March 21, Pune Police nabbed a gang of fraudsters from multiple locations, allegedly involved in stealing bank data and selling it for hard cash. The group with the help of hackers targeted active private bank accounts which were lying idle but were full of cash. Such bank accounts belonged to various government schemes and funds belonging to Corporate Social Responsibility Funds. According to police and mentioned in media reports the group wanted to hack the user IDs and Passwords of such bank account with huge sum and sell it further to another group of cyber-criminals. The police also suspect the role of bank employees behind this fraud.

Modus Operandi:

1. A group of fraudsters identified the active and inactive bank accounts with a huge sum of money.
2. They took screenshots of such bank accounts with the possible help received from bank employees.
3. They planned to sell the bank account data to a group of hackers and divert the money to other accounts.

News Source: Pune Mirror

1. https://punemirror.indiatimes.com/pune/crime/11-held-for-bank-data-theft/articleshow/81556410.cms

5. Social Engineering Frauds

Social Engineering frauds are related to cyber crimes happening on social network websites. According to Kaspersky, “Social engineering is a manipulation technique that exploits human error to gain private information, access, or valuables.”

Image Source: https://usa.kaspersky.com/resource-center/definitions/what-is-social-engineering

Sample Case 1: In November 2020, news reports appeared that enemy state actors were trying to dupe CRPF jawans by cloning their Facebook profiles. Responding to the threat CRPF issued a guideline called “Manual on Social Media Cloning” to educate the jawans about the pitfalls of careless usage of Facebook.

Modus Operandi:

1. Enemy state actors try to know the exact locations of CRPF men.
2. They create clone Facebook accounts in the name of their family members or relatives and send SOS messages asking for locations etc.

News Source: Hindustan Times

1. https://www.hindustantimes.com/india-news/crpf-warns-jawans-of-facebook-profile-cloning-to-extract-confidential-information/story-KFzePLjuI17NWAGfN8YYaN.html

Sample Case 2: In January 2021, Mumbai police arrested a highly educated engineer on the charges of cheating 22000 woman customers through his online shopping website.

Modus Operandi:

1. The accused created a website for online shopping where he disguised for selling women clothes.
2. He projected low prices for clothes and did not allow the Cash on Delivery option for customers. So, people paid online while making orders.

3. Finally, the accused did not send them the ordered items and kept the money with himself.
4. Since the customers paid small amounts only, they did not care if the order was not delivered.

News Source: NDTV

1. https://www.ndtv.com/india-news/engineer-turned-clothes-merchant-arrested-for-cheating-over-22-000-women-2354635

Sample Case 3: In November Mumbai Police registered a case against a teenager who hacked into the network of a coffee shop chain and converted the money into gift cards for his friends.

Modus Operandi:

1. A teenager hacks the network of a coffee shop chain.
2. He transfers money into gift cards.
3. He shares the gift cards with his friends and eventually, the money is being stolen from the online network of coffee shop chains.

News Source: NDTV

1. https://www.ndtv.com/india-news/mumbai-teen-detained-for-cyber-crime-at-coffee-shop-chain-2331295

Sample Case 4: In Dec 2020 Vishakhapatnam Police registered a case from a trader that he has duped Rs 51 Lakhs by cyber criminals. The victim used to run a departmental store and wanted to place bulk orders online. Incidentally, he landed on a fake website and contacted the phone number given in that. The victim placed his procurement order and was asked to pay Rs 15 Lakh in one account and Rs 36 Lakh in another account. After making the payments the victim kept waiting for his orders to arrive and it never happened.

Modus Operandi:

1. A victim does online browsing for the procurement for his departmental shop.
2. He lands on a fake website.
3. The victim places the order and makes a huge sum of payments.
4. The victim is duped by the money.

News Source: Times of India

1. https://timesofindia.indiatimes.com/city/visakhapatnam/cybercrime-trader-duped-of-rs-51-lakh-in-vizianagaram/articleshow/79828096.cms

Sample Case 5: In September 2020, a team of Mumbai Police arrested a cyber-criminal from Gujarat who had stored objectionable photos belonging to more than 700 teenage girls.

Modus Operandi:

1. The criminal allegedly created fake Instagram accounts using a female name.
2. He used to trap young and teenage girls by befriending them and collected photographs from them.
3. He later used those photographs to blackmail the girls.

News Source: NDTV

1. https://www.ndtv.com/india-news/cyber-crime-20-year-old-cyberstalker-arrested-for-blackmailing-teen-pre-teen-girls-objectional-images-found-2292609

Sample Case 6: According to the news reports published in Aug 2020, Maharashtra Police registered a complaint from a nursery owner that he was duped of Rs 1.5 Lakh by a cyber-criminal through a payment gateway platform.

Modus Operandi:

1. Cyber-criminal posed as potential customers sent a QR Code to the victim.
2. Once the victim scanned the QR Code an amount was debited from his account.
3. The criminal further called the victim and told him that he wished to return the money by asking to send the OTP he had received.
4. Upon sharing the OTP the victim has further duped the sum totalling 1.5 Lakh rupees.

News Source: NDTV

1. https://www.ndtv.com/cities/online-fraud-customer-dupes-nursery-owner-of-rs1-5-lakh-while-paying-for-plants-2283033

6. Cryptocurrency Frauds

A cryptocurrency is a new form of Blockchain-based virtual currencies. In many countries including the US the exchange of cryptocurrencies are legal and people have started buying and selling goods and services using cryptocurrencies. Bitcoin and Ethereum are some of the popular cryptocurrencies in circulation over Blockchain networks.

Image Source:https://www.pandasecurity.com/en/mediacenter/security/cryptocurrency-fraud/

Cyber criminals have started doing fraudulent activities using crypto currencies. In this section, we are giving some glimpses of such modern frauds happening in other countries.

Sample Case 1: In the US it has been reported that digital frauds involving cryptocurrencies are on a rise. Criminals have started deceiving people in the name of investments in cryptocurrencies. Many are running crypto currency Ponzi schemes and promises people of incredibly high returns.

Modus Operandi 1:

1. When someone sees the value of crypto currency go up and decides to invest for high returns, he approaches an online trader.
2. The trader asks the investor to buy some amount of cryptocurrency using cash and he also takes a commission for doing that.
3. After some time the investor wants to encash the profits and asks the trader to do so. The trader asks for more out-of-pocket commission and even goes out of contact.

Modus Operandi 2:

1. In some other scenarios, the trader contacts a potential victim and offers attractive investment schemes.
2. The investor falls prey to the fake promises and hands over his cryptocurrency coins to the cyber criminal through the online medium suggested by him.
3. By doing so the investor unknowingly transfers his coins not into a legal trading account but the criminal's wallet.

Modus Operandi 3:

1. The investor comes to know about some incredibly high return investment schemes using cryptocurrencies. In actuality, such offers are Ponzi schemes.
2. The trader who is an expert and clever cyber criminal make the potential victim invest coins.
3. To continue the exploitation for a longer period, the trader gives some partial pay-outs also and in addition asks for more investments and loans.
4. After some longer period, the investor ends up losing all money.

News Source: Federal Bureau of Investigation

1. https://www.fbi.gov/contact-us/field-offices/portland/news/press-releases/oregon-fbi-tech-tuesday-building-a-digital-defense-against-crypto-investment-scams

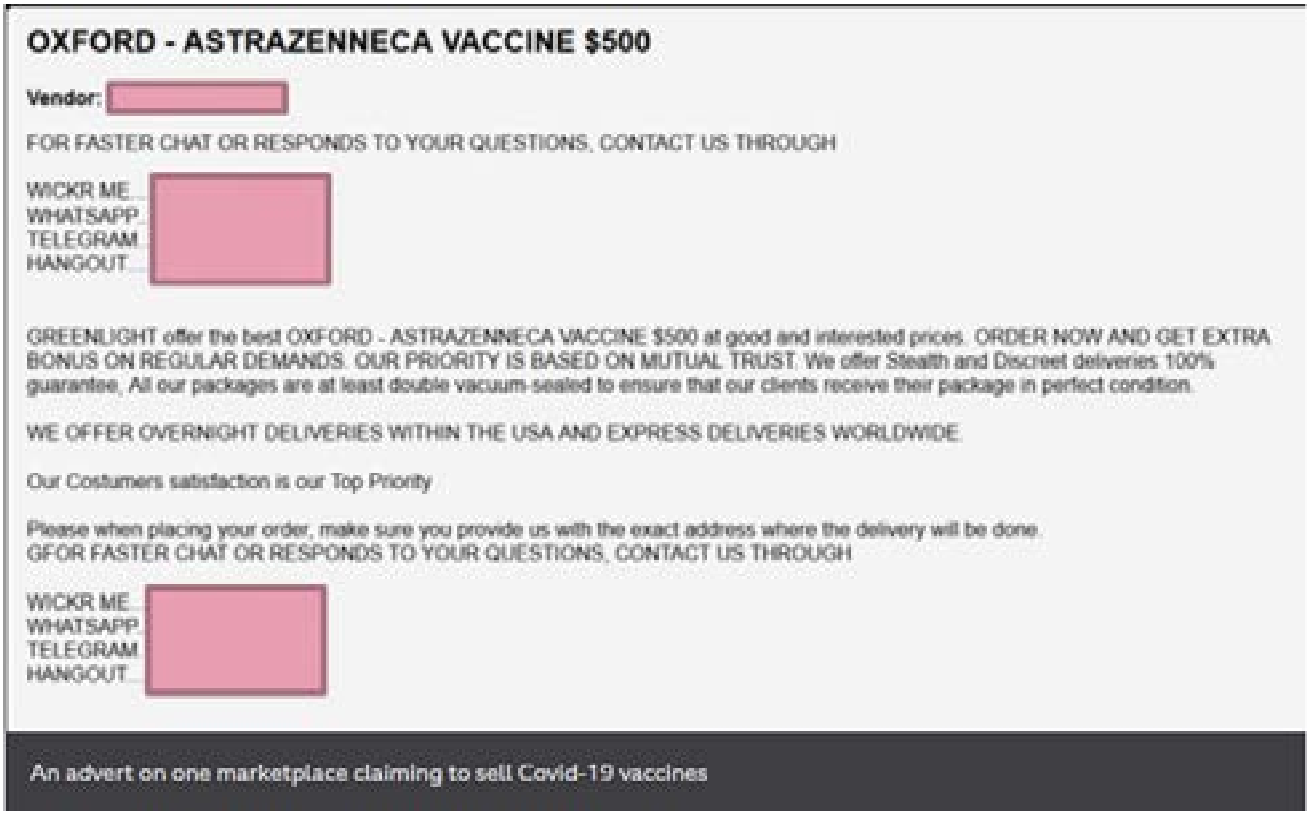
7. Dark Net Frauds

Internet content put in Darknet are encrypted so that it cannot be accessed via traditional search engines. In other words, certain websites cannot be accessed via common internet browser tools like Chrome, Mozilla or Microsoft Edge etc. One has to use specific browsing tools like TOR to reach those websites. Darknet is hidden from the common public's access for the simple reason that cyber criminals want to do their illicit cyber activities while in hiding. Drugs, counterfeit money, stolen credit card and personal data and anonymous SIM cards are sold and bought on Darknet websites.

In this section fraud related to cyber crime happening over the darknet is mentioned.

Image Source: https://indianexpress.com/article/world/largest-illegal-darknet-marketplace-darkmarket-taken-offline-7143638/

Sample Case 1: According to international news organisations COVID-19 vaccines and negative test reports are being sold on Darknet in Western countries. Darknet is also known as the dark web and people access it through specific browsers like TOR and I2P. Darknet is used for doing illicit trade and many other forms of cyber crimes.



OXFORD - ASTRAZENNECA VACCINE $500

Vendor: [redacted]

FOR FASTER CHAT OR RESPONDS TO YOUR QUESTIONS, CONTACT US THROUGH

WICKR ME
WHATSAPP
TELEGRAM
HANGOUT [redacted]

GREENLIGHT offer the best OXFORD - ASTRAZENNECA VACCINE $500 at good and interested prices. ORDER NOW AND GET EXTRA BONUS ON REGULAR DEMANDS. OUR PRIORITY IS BASED ON MUTUAL TRUST. We offer Stealth and Discreet deliveries 100% guarantee, All our packages are at least double vacuum-sealed to ensure that our clients receive their package in perfect condition.

WE OFFER OVERNIGHT DELIVERIES WITHIN THE USA AND EXPRESS DELIVERIES WORLDWIDE.

Our Costumers satisfaction is our Top Priority

Please when placing your order, make sure you provide us with the exact address where the delivery will be done.
GFOR FASTER CHAT OR RESPONDS TO YOUR QUESTIONS, CONTACT US THROUGH

WICKR ME
WHATSAPP
TELEGRAM
HANGOUT [redacted]

An advert on one marketplace claiming to sell Covid-19 vaccines

Image Source: BBC

Modus Operandi:

1. Cyber criminals are selling COVID-19 vaccines on Darknet and are offering next day delivery. Doses of AstraZeneca, Sputnik, Sinopharm and Johnson & Johnson are being sold at prices ranging from USD 500 to USD 750.
2. Seller of these vaccines is reported to be coming from countries like the US, UK, Spain, Germany, France and Russia.
3. Fake vaccination certificates are also on sale for USD 150 on the darknet.
4. Fake covid negative test reports are also being sold with the offers like one negative report is offered free upon purchase of two negative reports.
5. Many sellers are taking Bitcoin instead of cash from the buyers.

News Source: BBC

1. https://www.bbc.com/news/technology-56489574

8. Final Comments

All the information provided in this booklet is expected to create awareness among LEAs about the various kinds of new cyber crimes taking place in India and outside. The next volume of this booklet will be a fresh compilation of emerging cyber crimes. All the feedback and comments may be forwarded to NCRIC, Mod Division, BPR&D, New Delhi.

officialBPRDIndia

BPRDIndia

Bureau of Police Research & Development India

bprdIndia

www.bprd.nic.in

Cyberdost

www.cybercrime.gov.in

Indian Cyber Crime Coordination Centre

NATIONAL CYBER CRIME RESEARCH & INNOVATION CENTRE (NCR&IC)

BUREAU OF POLICE RESEARCH AND DEVELOPMENT

Ministry of Home Affairs, Government of India
NH-8, Mahipalpur, New Delhi-110037