गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

सत्यमेव जयते

Indian
Cyber
Crime
Coordination
Centre

CYBER DIGEST

PREPARED BY
INDIAN CYBER CRIME COORDINATION CENTRE

MINISTRY OF HOME AFFAIRS

22nd December 2023

FOR MORE INFO

Helpline 1930 WWW.CYBERCRIME.GOV.IN *Follow: @cyberdost*

National

S. No.	News	Source
1.	Cybercrime police nabbed accused duping 3.65 lacs from senior citizen by changing sim card	Face 2 News
2.	A cybercriminal arrested by Delhi police for duping 900 families on pretext of providing them information about their missing kids	News Nine
3.	BKC Police Recovers Stolen ₹9.84 Lakh In Cyber Fraud Case	Free Press Journal
4.	In Bengaluru, crooks hack man's phone with automated call, siphon off Rs 39,000	Times of India
5.	How present banking system identify online fraudsters and retrieve money	Study Cafe
6.	77-year-old Pune man cheated of Rs 42 lakh on pretext of investment in forex, commodities markets	Indian Express
7.	Beware of bumper offers on Christmas, the link that looks like the real thing may be a scam	Divya Himachal
8.	Avoid online holiday shopping scams with these tips	WF TV
9.	Scam Watch: Fake calls from telecom dept threaten users with mobile number disconnections	News Checker

International

S. No.	News	Source
1.	What is a romance scam? What is catfishing?	Deseret News
2.	Hackers Exploiting Old MS Excel Vulnerability to Spread Agent Tesla Malware	The Hacker News

National

Cybercrime police nabbed accused duping 3.65 lacs from senior citizen by changing sim card

In a major breakthrough under the leadership of Sh. Ketan Bansal, IPS, SP-Cyber, UT, Chandigarh, under close guidanceof Sh. A Venkatesh, DSP/Cyber Crime& IT UT, Chandigarh and supervision of Inspector Sh. Ranjit SinghSHO Police Station-Cyber Crime, Sec.17, Chandigarh, one (1) accused has been arrested inCase FIR No. 128 dated 18.12.2023 U/S 419, 420, 120B IPC PS Cyber Crime, Sector 17 UT, Chandigarh in which the accused fraudulently made alleged transactions of amounting Rs. 3,65,900/- by changing victim's SIM card and taking unauthorized access of his PNB Net Banking.

Police said, the present case has been registered on the complaint of Sh. Ram Dhani S/o Shitu R/o Village Maloya Chandigarh in which he allegedly reported that he is a senior citizen and retired from PWD department Chandigarh. He has a Punjab National Bank Account in which he received his retirement fund. But his retirement pension has not come into effect yet. For this he requested to his well-known Grocery shopkeeper and his son at Maloya from where he used to purchase grocery items. He does know their names.

The shopkeeper's son told him that he would help him to start his retirement pension and asked him for papers, Bank passbook and mobile phone, which was handed over to him. Further he told him that he would have to come, when he called, he would get it done. After some time, he returned his bank passbook and mobile phone. Next day, he was found that his mobile SIM number was not working due to which he issued a duplicate SIM card of above number. After few days, he needed of money and went to Punjab National Bank where he has come to know that someone has made fraudulent transaction of Rs. 3,65,900/-.

The shopkeeper's son told him that he would help him to start his retirement pension and asked him for papers, Bank passbook and mobile phone, which was handed over to him. Further he told him that he would have to come, when he called, he would get it done. After some time, he returned his bank passbook and mobile phone. Next day, he was found that his mobile SIM number was not working due to which he issued a duplicate SIM card of above number. After few days, he needed of money and went to Punjab National Bank where he has come to know that someone has made fraudulent transaction of Rs. 3,65,900/-.

During investigation, a team was constituted headed by SI Gurmeet Singh, Ct. Vinod Kumar, Const. Pardeep Kumar & Ct Amit Kumar. Furtheron the basis of technical support and secret information, on 18.12.2023, a raid was conducted at Maloya Chandigarh from where arrest of accused Rakesh Yadav S/o Lal Bahadur Yadav R/o #22 Village Maloya Chandigarh (House-cum-Grocery Shop) have been made from Maloya Chandigarh in the above case.

Delhi police has arrested a cybercriminal for allegedly duping 900 families on the pretext of providing them with information related to their missing children.

The Delhi police has arrested a cybercriminal for allegedly duping at least 900 families on the pretext of providing them with information related to their missing children. The accused, identified as Shyam Sundar Chauhan who hails from Uttar Pradesh's Mau district, was arrested by a cyber-unit of Delhi police.

Explained: Modus operandi of cybercriminal

Chauhan used to get in touch with the families of missing children over a phone call and demand money in exchange for information. Chauhan managed to get the details of missing children and their families from the government portal ZIPNet (Zonal Integrated Police Network) and several other platforms.

According to a senior police officer, Chauhan used to receive money from the victims, ranging between Rs 2,000 and Rs 40,000, through the QR code of his UPI account.

Case filed against Chauhan

"Recently, a girl went missing from Delhi's Wazirabad area. Her family filed a missing complaint at a nearby police station and uploaded the necessary information on ZIPNet and other platforms. A few days later, Chauhan contacted the family of the missing girl and demanded Rs 8,000 in exchange for the information. Chauhan sent a QR code on the WhatsApp handle of one of the family members of the missing girl to receive money," a police officer said.

Based on the complaint, a case was filed under relevant Sections and several teams were formed to arrest Chauhan. During the interrogation, Chauhan confessed to having scammed more than 900 families so far.

“Shyam Sundar Chauhan has a degree of Bachelor of Computer Application (BCA),” the officer added.

Delhi: Man arrested for duping 900 families on pretext of providing them information related to missing children

The Delhi police has arrested a cybercriminal for allegedly duping at least 900 families on the pretext of providing them with information related to their missing children.

BKC Police Recovers Stolen ₹9.84 Lakh In Cyber Fraud Case

The BKC Police has successfully recovered the entire sum of ₹9.84 lakh lost by a victim in a cyber fraud incident, following his prompt complaint. The complainant, Debayan Dipankar Das (34), reported the matter to the police and cyber crime authorities immediately after the incident, providing crucial information that led to the swift registration of an FIR. Consequently, the police promptly blocked the bank account where the misappropriated funds had been transferred.

According to police sources, Das received a message on his mobile between July 4 and July 5, offering a part-time job. The message included a contact number, and upon reaching out, Das was briefed on the task. The perpetrator enticed Das with promises of substantial returns upon task completion.

Subsequently, the accused gradually siphoned ₹9.84 lakh from Das under the guise of a prepaid task, failing to deliver anything in return. Realizing he had fallen victim to fraud, Das promptly reported the incident to the police.

In response, the police initiated a swift investigation, leading to the immediate freezing of the implicated bank account. A police official confirmed that the account had been effectively blocked. With the cooperation of the complainant, who completed the necessary procedures in court, the entire stolen amount was successfully recovered.

In Bengaluru, crooks hack man's phone with automated call, siphon off Rs 39,000

A man who attended an automated phone call, purportedly from Swiggy, ended up losing Rs 39,000 from his loan application LazyPay. The victim's mobile phone was flooded with almost 10,000 messages containing OTPs to keep him engaged and prevent him from taking measures to stop the fraud.

Channakeshava KS, sales executive at an automobiles firm, told police he received a call from 080 69673056 around 11.39am on December 18.

On attending the call, he found it to be an automated one. The voice message said: "We have received an order for Rs 5,345 from your Swiggy account, if it is you please press 2, otherwise press 1."

Channakeshava told TOI, "Since I hadn't ordered anything I pressed 1. The next voice message said, 'We have sent an OTP to your mobile number. Kindly enter the OTP to verify your account'. I typed a six-digit OTP on the call. After 30 seconds, the voice message said, 'Your account is verified and it is safe now, thank you'."

Around 12pm, Channakeshava received four OTPs from Swiggy. "I assumed somebody was trying to log into my account. I didn't worry much because unless I give my mobile number and OTP, none would be able to log in," said Channakeshava.

How present banking system identify online fraudsters and retrieve mone

How present banking system identify online fraudsters and retrieve money

The Minister of State Dr Bhagwat Karad in the Ministry of Finance in a written reply to a question raised in Rajya Sabha Sabha said, " How present banking system identify online fraudsters and retrieve money"

Shri Sanjay Raut asked these questions in the Rajya Sabha:

Will the Minister of Finance be pleased to state:

(a) whether it is a fact that the cases of digital frauds committed using cards and internet-based payment methods have nearly been doubled as fraudsters are using new techniques to cheat customers;

(b) if so, the details thereof and Government's reaction thereto;

(c) whether the present banking system is unable to identify the fraudsters and retrieve the money; and

(d) if so, the details of steps taken or proposed to be taken by Government to protect the public money?

The Minister of State replied:

(a) and (b): According to the Reserve Bank of India (RBI), the number of frauds (1 lakh or more) reported by Scheduled Commercial Banks under the categories "Cards/internet – credit cards, cards/internet – debit cards, and cards/internet banking- based on date of reporting" during the financial years 2021-22 and 2022-23 was 3,596 and 6,659, respectively. In the context of the overall expansion of the digital ecosystem, the number of reported frauds is significantly surpassed by an enormous rise in total digital payment transactions during the same period.

(c) and (d): According to the Seventh Schedule to the Indian Constitution, 'police' and 'public order' are state matters, according to the Ministry of Home Affairs. Through their Law Enforcement Agencies (LEAs), states and territories are principally responsible for the prevention, identification, investigation, and prosecution of crimes, including cyber fraud. The Central Government enhances the efforts of state governments by providing recommendations and financial aid through several capacity-building schemes.

The government additionally launched the National Cyber Crime Reporting Portal to allow the public to report all types of cyber crimes, with a special emphasis on cyber crimes against women and children. Cyber crimes reported on this portal are automatically routed to the respective State/UT law enforcement agency for further handling in accordance with the provisions of law.

The Indian Cyber Crime Coordination Centre (I4C) conducts proactive analysis of digital lending apps on a regular basis. On the basis of its analysis and complaints made on the National Cyber Crime Reporting Portal, the I4C team analyzes Apps on numerous parameters and reports suspicious Apps to MeitY for blockage.

Furthermore, the RBI issued instructions to banks regarding limiting customer liabilities in unauthorized/fraudulent electronic transactions in circulars dated July 6, 2017 and December 14, 2017 for Commercial banks and Cooperative banks, respectively, outlining the criteria for determining the customer's limited liability in various types of digital transactions.

Several initiatives have been made by the government, the RBI, and banks to raise awareness about cybercrime, especially financial fraud, and to protect citizens' interests. Among the initiatives taken in this direction are the following:

1. The RBI's "RBI Kehta Hai" campaign and booklet "BE(A)WARE" educate the public on the measures to be taken when conducting financial transactions using digital platforms.

2. The RBI has developed an initiative for conducting electronic-banking awareness and training (eBAAT), which has primarily focused on raising awareness about fraud and risk reduction.

3. In partnership with the RBI's Regulated Entities (REs), a Nationwide Intensive Awareness Programme (NIAP) was implemented, with about 1.63 lakh programmes delivered through various channels.

4. The RBI additionally conducts Financial Literacy Week (FLW), and banks are encouraged to hold special camps through Financial Literacy Centres (FLCs) and rural branches.

5. In collaboration with the National Centre for Financial Education (NCFE), the RBI developed a framework for financial education to be included in school students' education curricula.

6. Dissemination of cybercrime messaging via short message service (SMS), radio compaigns, and public awareness of cybercrime prevention and cyber safety guidelines via the I4C's social media accounts.

77-year-old Pune man cheated of Rs 42 lakh on pretext of investment in forex, commodities markets

The cyber crime wing of the Pune City police launched a probe after a 77-year-old retired manager of a private company was cheated of Rs 42 lakh over a period of a month on the pretext of investment in forex and commodities markets.

The man, a resident of Sahakarnagar, who retired from a private technology firm, registered a complaint at the cyber police station of the Pune City police on Tuesday.

According to the complainant, on August 14, he received a call from a person claiming to be an executive of a company that operates online platforms for trading in forex and commodities.

"The suspects directed the complainant to a fraudulent online page, where he was kept under the impression that he was getting high returns on his investments. Over the period of a month, various people claiming to be representatives of the company called him and asked for more and more money for investment," said an officer from the cyber police station.

After sending Rs 42.45 lakh, the complainant thought of withdrawing some amount but he was told that he would not be able to do so.

"After he was repeatedly denied withdrawals, the complainant realised he has been cheated," said the officer adding that the police have launched a probe into the numbers and accounts used by the suspects.

Beware of bumper offers on Christmas, the link that looks like the real thing may be a scam

There is a flood of offers for online shopping regarding Christmas. Due to big Christmas discounts, people are giving priority to online shopping. Sensing this mood of the people, companies are also giving various types of offers to woo the customers. At some places, discounts of up to 50-70 percent are being offered on the purchase of an item, while at others, loans at zero interest rates are being offered for purchasing expensive electronic items. At the same time, up to 50 percent discount is being given on clothes.

Customers should be extremely careful while clicking on any such bumper offer. Because it is possible that the offer that looks like the original may be a fraudulent link and as soon as you click on it, fraudsters can withdraw the amount from your bank account.

These days, crooks have started using new methods to rob customers. It has become difficult to identify real or fake among these. Many times, to commit fraud, a website is created with the look and design of the real company. As soon as you click on these, all your confidential information reaches the miscreants. Cyber cell has also issued an alert to avoid fraudsters regarding online shopping during the season of Christmas offers. Cyber Cell Shimla SP Rohit Malpani says that before accepting the offer of any company during the festive season of Christmas, definitely check the social media accounts of the company. He said that even after this, if there is any doubt, then definitely visit the nearby branch or showroom of the company and get information about the offers being given for the online market. This will also provide better information about the difference in prices and benefits of online and offline markets.

Avoid online holiday shopping scams with these tips

“Whether it’s fake orders, fake websites, refunds, things like that, 32% of all scams across the entire year reported to us, across the entire nation are under the bucket of online shopping,” said Regional Manager for the BB, Logan Hickle.

The most likely scam you will see is what is called a “look-a-like site,” which steals logos and branding from major storefronts.

“It’s easy nowadays to set up a website to even make it look secure with that little lock symbol,” said Hickle.

hese fake sites look just like the big brands but offer deeper discounts to lure you in. That is why the BBB said you must take a second look before hitting ‘buy.’

“Don’t just click on the link that’s provided to you in the advertisement. Go to the profile, research them, and see if they’re verified, but also look at those comments. Look at their most recent posts, look at those comments,” Hickel said.

Another thing to be wary of is tricky email confirmations for orders you didn’t make. These are phishing attempts.

“You’re going to see that email, it’s going to say they need more information or you need to pay a certain amount of money. You click on the link in the email, which you shouldn’t do, but you go ahead and click on the link in the email and you’re giving over your personal information. You’re giving over credit card information,” he said.

Another red flag that you may be dealing with fraud can be shipping issues.

"Especially if it's a fake order altogether, they're going to call you and they may say, oh, well, you need to pay for insurance. Oh, it's stuck in customs. You need to pay more money. So be careful about that," he said.

One thing the BBB said to do around the holidays is turn on your credit card alerts. If your credit card gets into the wrong hands, then they will also be spending fast and you can move quickly to protect yourself.

Scam Watch: Fake calls from telecom dept threaten users with mobile number disconnections

What if you received a call from the telecom department warning you that your Aadhaar ID was used to register a mobile number which was found to be involved in illegal activities? Panic is the first and the most instinctive response, one that has been skillfully exploited by scamsters out to hoodwink users off their hard earned money.

That is exactly what happened in the case of a Bangalore based techie, who lost Rs 3.7 crores to scamsters posing as telecom department and CBI officials. According to the Whitefield police, the IT professional received an automated call claiming to be from the telecom department, warning that a sim card was registered in the name of the complainant using his Aadhar details and was used for posting illegal advertisements. The call was then transferred to another person posing as an official of the Mumbai police, who said that the complainant had to visit them and the CBI offices in Delhi and Mumbai if he wanted to avoid arrest. This was followed by a call over Skype. Over the video call, a few men dressed in police uniforms, ID cards and even a copy of a fake FIR asked the complainant to transfer money to several accounts so that the money could be audited, reports revealed. The complainant transferred over Rs 3 crore rupees to them before finding out that they were fraudsters.

This is not an isolated incident. 36-year-old media professional Shalini Dogra (name changed) also received one such call while she was at work. "I usually don't entertain calls from numbers I don't recognise. This one said it is from the "telecom dept," so I got curious and pressed 9 as directed. The call was directed to a "customer care number " and the woman on the other end claimed that she was from the customer care of the telecom dept..which is a vague thing to say since they didn't mention ministry etc. I didn't believe it and hung up".

International

Iranian Hackers Using MuddyC2Go in Telecom Espionage Attacks Across Africa

It started with a friend request on Facebook in February. The handsome Army officer stationed abroad liked Alicia Bultez's profile and wanted to be friends. She accepted.

Single for seven years, the 81-year-old Bultez was lonely. She craved companionship.

"The walls just don't talk to you," she said in the living room of the Santaquin home she shares with her aunt and two cousins, where her 10-year-old Pomeranian, Muffin Ann, excitedly scurried around and pictures and a sculpture of Jesus are placed among the Christmas decorations.

Bultez was flattered that a man in his 60s took interest in her. They messaged back and forth, shared their likes and dislikes, talked about their families, exchanged photos. Right up front, they both agreed they would be totally honest with each other. A romance developed over the next few months. They planned to get married when he returned to the States in August.

"I thought wow. I really liked the way he made me feel. I felt loved. After having three divorces, and not feeling loved, to have someone really love me and care about me and want to do things for me, I was all open for it," Bultez said, whose main source of income is Social Security.

Before he returned from overseas, he told her a "portfolio" he was sending home got hung up in customs. He asked her to send $1,500 to a "diplomat" in Philadelphia who was helping him get it through. She rounded up the money and sent it. Then he told her customs needed another $5,000. She withdrew the money from her small life savings and sent it. But it didn't stop there. He asked for $40,000. She told him she'd given all she could.

A check for $95,200 arrived on her doorstep a week or so later. He told her to deposit the money in an IRA at her bank and then send him $40,000. She found out the check bounced when her Latter-day Saint ward Relief Society president insisted they go to the bank together a few days later.

"When they told me that at the bank, I just fell apart," Bultez said, recalling how a teller "just held me and I cried."

It was with the help of her ecclesiastical leaders in The Church of Jesus Christ of Latter-day Saints that Bultez learned she was being scammed. They brought in the police. They told her never to contact the Army officer again, and she hasn't. But it tore her up inside.

"I was in such denial and I was hurt and I was angry and I felt all these emotions," she said as she teared up. "I just put it in the Lord's hands because there's nothing more I could do about it."

Bultez is willing to talk about what happened to her, hoping it will prevent others from scrolling into the same trap.

"It's horrific that people prey on people like that," said Katie Hass, director of the Utah Division of Consumer Protection. "But I applaud her for overcoming whatever shame she felt to share her story so that other people don't fall victim."

Sadly, Bultez's story is a familiar one.

"We do see a lot of romance scams. I think one of the reasons why we see a lot of that, and the surgeon general talked about this, is we have a loneliness epidemic," Hass said, adding it's not only women but men who get pulled into those bogus relationships.

"I think our generation, I'm a generation Xer, we have to take some ownership of the fact that our senior citizens are feeling lonely and they're not as connected. ... We have to recognize that the walls don't talk to them."

Bultez's online romance with the Army officer had all the elements of catfishing, the act of creating a false identity to lure people into relationships. Scammers frequently create bogus profiles on dating or other social networking sites to find their victims. Often, they claim to live far away, maybe saying they're traveling for business or are in the military. That makes it easier to avoid meeting in person — and more plausible when they ask for money to be sent overseas for a medical emergency or unexpected legal fee.

Estimates of how much money people 60 and older lose to cyber fraud each year vary widely. Based on reports to its Internet Crime Complaint Center in 2022, the FBI put the number at $3.1 billion, including 7,166 victims of romance/confidence scams who lost $419 million. Victims ages 30-39 were the largest group reporting fraud, but the greatest dollar loss was incurred by people 60 and older.

In Utah, 741 people over age 60 lost a total of $27.6 million to fraud, according to the report.

A recent AARP study found older Americans lose $28.3 billion annually to all types of financial exploitation, with $20.3 billion being stolen by friends, family and caregivers and $8 billion by strangers.

A Federal Trade Commission report released in October showed older adults continued to report higher individual median dollar losses than younger adults, and the disparity remained particularly large among people 80 and over compared to younger adults.

Hackers Exploiting Old MS Excel Vulnerability to Spread Agent Tesla Malware

Attackers are weaponizing an old Microsoft Office vulnerability as part of phishing campaigns to distribute a strain of malware called Agent Tesla.

The infection chains leverage decoy Excel documents attached in invoice-themed messages to trick potential targets into opening them and activate the exploitation of CVE-2017-11882 (CVSS score: 7.8), a memory corruption vulnerability in Office's Equation Editor that could result in code execution with the privileges of the user.

The findings, which come from Zscaler ThreatLabz, build on prior reports from Fortinet FortiGuard Labs, which detailed a similar phishing campaign that exploited the security flaw to deliver the malware.

"Once a user downloads a malicious attachment and opens it, if their version of Microsoft Excel is vulnerable, the Excel file initiates communication with a malicious destination and proceeds to download additional files without requiring any further user interaction," security researcher Kaivalya Khursale said.

The first payload is an obfuscated Visual Basic Script, which initiates the download of a malicious JPG file that comes embedded with a Base64-encoded DLL file. This steganographic evasion tactic was previously also detailed by McAfee Labs in September 2023.

The concealed DLL is subsequently injected into RegAsm.exe, the Windows Assembly Registration Tool, to launch the final payload. It's worth noting that the executable has also been abused to load Quasar RAT in the past.

Agent Tesla is a .NET-based advanced keylogger and remote access trojan (RAT) that's equipped to harvest sensitive information from compromised hosts. The malware then communicates with a remote server to extract the collected data.

"Threat actors constantly adapt infection methods, making it imperative for organizations to stay updated on evolving cyber threats to safeguard their digital landscape," Khursale said.

The development comes as old security flaws become new attack targets for threat actors. Earlier this week, Imperva revealed that a three-year-old flaw in Oracle WebLogic Server (CVE-2020-14883, CVSS score: 7.2) is being utilized by the 8220 Gang to deliver cryptocurrency miners.

It also coincides with an uptick in DarkGate malware activity after it began to be advertised earlier this year as a malware-as-a-service (MaaS) offering and as a replacement for QakBot following its takedown back in August 2023.

"The technology sector is the most impacted by DarkGate attack campaigns," Zscaler said, citing customer telemetry data.

"Most DarkGate domains are 50 to 60 days old, which may indicate a deliberate approach where threat actors create and rotate domains at specific intervals."

Phishing campaigns have also been discovered targeting the hospitality sector with booking-related email messages to distribute information stealer malware such as RedLine Stealer or Vidar Stealer, according to Sophos.

"They initially contact the target over email that contains nothing but text, but with subject matter a service-oriented business (like a hotel) would want to respond to quickly," researchers Andrew Brandt and Sean Gallagher said.

Only after the target responds to the threat actor's initial email does the threat actor send a followup message linking to what they claim is details about their request or complaint."

Stealers and trojans notwithstanding, phishing attacks have taken the form of bogus Instagram "Copyright Infringement" emails to steal users' two-factor authentication (2FA) backup codes via fraudulent web pages with an aim to bypass account protections, a scheme called Insta-Phish-A-Gram.

"The data attackers retrieve from this kind of phishing attack can be sold underground or used to take over the account," the cybersecurity firm said.

News / Feeds References

National

1. https://www.face2news.com/news/90240-cyber-crime-police-nabbed-accused-duping-365-lacs-from-senior-citizen-by-changing-sim-card.aspx
2. https://www.news9live.com/crime/delhi-man-arrested-for-duping-900-families-on-pretext-of-providing-them-information-related-to-missing-children-2383013
3. https://www.freepressjournal.in/mumbai/mumbai-news-bkc-police-recovers-stolen-984-lakh-in-cyber-fraud-case
4. https://timesofindia.indiatimes.com/city/bengaluru/crooks-hack-mans-phone-with-automated-call-siphon-off-rs-39000/articleshow/106168029.cms
5. https://studycafe.in/how-present-banking-system-identify-online-fraudsters-and-retrieve-money-277172.html
6. https://indianexpress.com/article/cities/pune/man-cheated-of-rs-42-lakh-on-pretext-of-forex-trading-9076804/
7. https://www.divyahimachal.com/2023/12/cyber-crime-beware-of-bumper-offers-on-christmas-the-link-that-looks-like-the-real-thing-may-be-a-scam/
8. https://www.wftv.com/news/local/avoid-online-holiday-shopping-scams-with-these-tips/4HDECJMN7RD6PBGAMWMHJ3GGCU/
9. https://newschecker.in/scam-watch/scam-watch-fake-calls-from-telecom-dept-threaten-users-with-mobile-number-disconnections/

International

1. https://www.deseret.com/u-s-world/2023/12/20/23997770/romance-scam-catfishing-fraud-81-year-old-woman-victim-financial-exploitation
2. https://thehackernews.com/2023/12/hackers-exploiting-old-ms-excel.html

IF YOU ARE A VICTIM OF "ONLNE FINANCIAL FRAUD" IMMEDIATELY CALL ON HELPLINE NUMBER 1930

REGISTER YOUR COMPLAINT AT

HTTPS://WWW.CYBERCRIME.GOV.IN

FOLLOW US ON

CYBER DOST