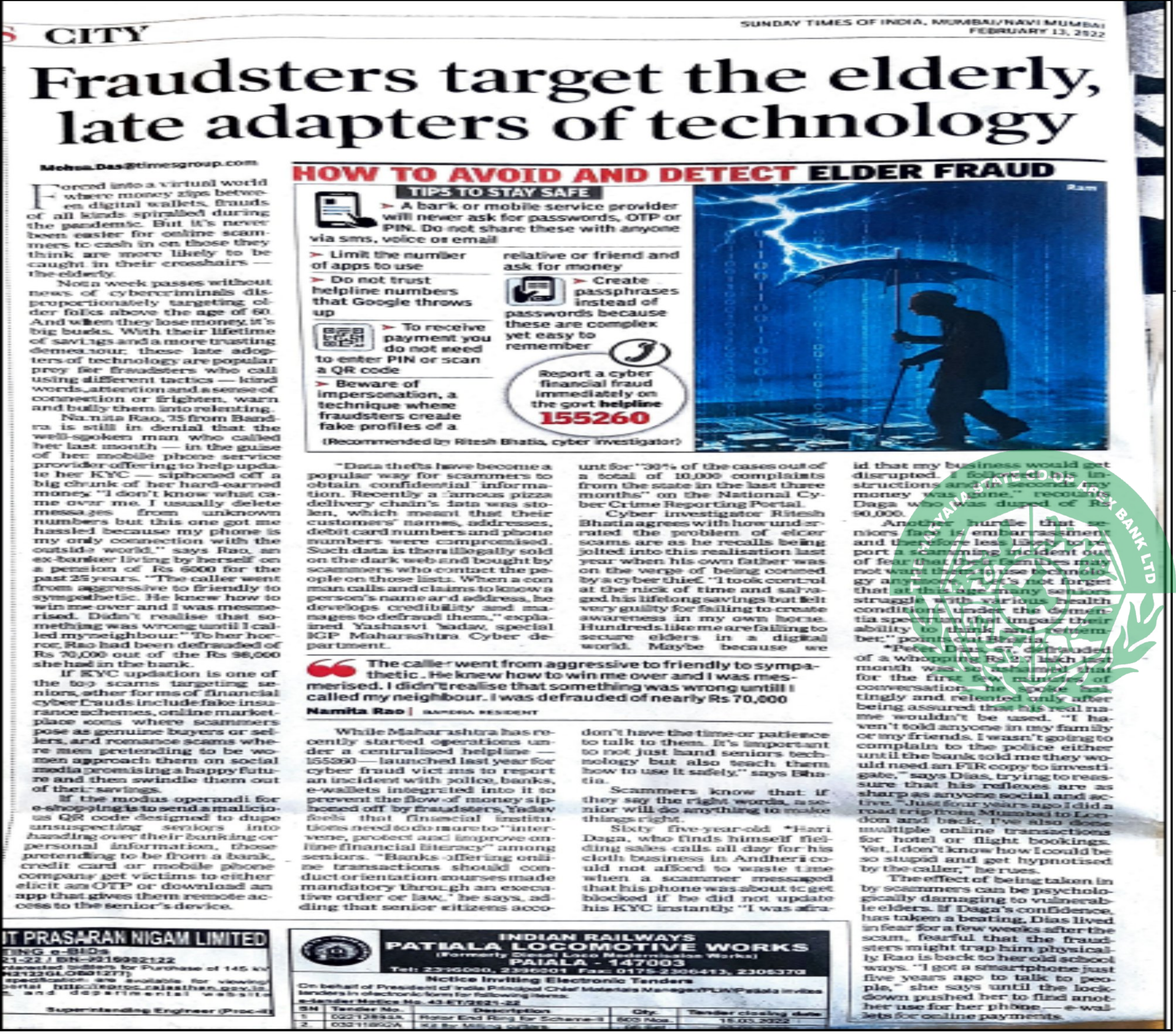
CYBER
SECURITY
dark web
financial institutions
denial of service
cyberspace
anonymous
corporations
servers
internet
wikileaks
backdoor
remote administration tools
SSL
government
trojan
bitcoin
porn
adwares
root
data
spoofing
privacy
data dump
keylogger
antivirus
whitehat
database
blackhat
information technology
cross site scripting
social engineering
hackers
firewall
worms
script kids
malwares
distributed denial of service
defacement
encryption
world wide web
surveillance
stuxnet
warez
access
activism



CITY

SUNDAY TIMES OF INDIA, MUMBAI/NAVI MUMBAI
FEBRUARY 13, 2022

Fraudsters target the elderly, late adapters of technology

Mohan.Das@timesgroup.com

Forced into a virtual world where money zips between digital wallets, frauds of all kinds spiralled during the pandemic. But it's never been easier for online scammers to cash in on those they think are more likely to be caught in their crosshairs — the elderly.

Not a week passes without news of cybercriminals disproportionately targeting older folks above the age of 60. And when they lose money, it's big bucks. With their lifetime of savings and a more trusting demeanour, these late adopters of technology are popular prey for fraudsters who call using different tactics — kind words, attention and a sense of connection or frighten, warn and bully them into relenting.

Namita Rao, 75 from Bandra is still in denial that the well-spoken man who called her last month — in the guise of her mobile phone service provider offering to help update her KYC — siphoned off a big chunk of her hard-earned money. "I don't know what came over me. I usually delete messages from unknown numbers but this one got me hassled because my phone is my only connection with the outside world," says Rao, an ex-banker living by herself on a pension of Rs 6000 for the past 25 years. "The caller went from aggressive to friendly to sympathetic. He knew how to win me over and I was mesmerised. Didn't realise that something was wrong until I called my neighbour." To her horror, Rao had been defrauded of Rs 70,000 out of the Rs 98,000 she had in the bank.

If KYC updation is one of the top scams targeting seniors, other forms of financial cyber frauds include fake insurance schemes, online marketplace cons where scammers pose as genuine buyers or sellers, and romance scams where men pretending to be women approach them on social media promising a happy future and then swindle them out of their savings.

If the modus operandi for e-shopping is to send a malicious QR code designed to dupe unsuspecting seniors into *handing* over their banking or personal information, those pretending to be from a bank, credit card or mobile phone company get victims to either elicit an OTP or download an app that gives them remote access to the senior's device.

HOW TO AVOID AND DETECT ELDER FRAUD

TIPS TO STAY SAFE

- ➤ A bark or mobile service provider will never ask for passwords, OTP or PIN. Do not share these with anyone via sms, voice or email
- ➤ Limit the number of apps to use
- ➤ Do not trust helpline numbers that Google throws up
- ➤ To receive payment you do not need to enter PIN or scan a QR code
- ➤ Beware of impersonation, a technique where fraudsters create fake profiles of a relative or friend and ask for money
- ➤ Create passphrases instead of passwords because these are complex yet easy to remember

Report a cyber financial fraud immediately on the govt **helpline**
155260

(Recommended by Ritesh Bhatia, cyber investigator)

Ram

"Data thefts have become a popular way for scammers to obtain 'confidential' information. Recently a famous pizza delivery chain's data was stolen, which meant that their customers' names, addresses, debit card numbers and phone numbers were compromised. Such data is then illegally sold on the dark web and bought by scammers who contact the people on those lists. When a con man calls and claims to know a person's name and address, he develops credibility and manages to defraud them," explained Yashasvi Yadav, special IGP Maharashtra Cyber department.

While Maharashtra has recently started operations under a centralised helpline — 155260 — launched last year for cyber fraud victims to report an incident with police, banks, e-wallets integrated into it to prevent the flow of money siphoned off by fraudsters, Yadav feels that financial institutions need to do more to "intervene, protect and improve online financial literacy" among seniors. "Banks offering online transactions should conduct orientation courses made mandatory through an executive order or law," he says, adding that senior citizens account for "30% of the cases out of a total of 10,000 complaints from the state in the last three months" on the National Cyber Crime Reporting Portal.

Cyber investigator Ritesh Bhatia agrees with how underrated the problem of elder scams are as he recalls being jolted into this realisation last year when his own father was on the verge of being conned by a cyber thief. "I took control at the nick of time and salvaged his lifelong savings but felt very guilty for failing to create awareness in my own home. Hundreds like me are failing to secure elders in a digital world. Maybe because we don't have the time or patience to talk to them. It's important to not just hand seniors technology but also teach them how to use it safely," says Bhatia.

> "The caller went from aggressive to friendly to sympathetic. He knew how to win me over and I was mesmerised. I didn't realise that something was wrong untill I called my neighbour. I was defrauded of nearly Rs 70,000
>
> **Namita Rao** | BANDRA RESIDENT

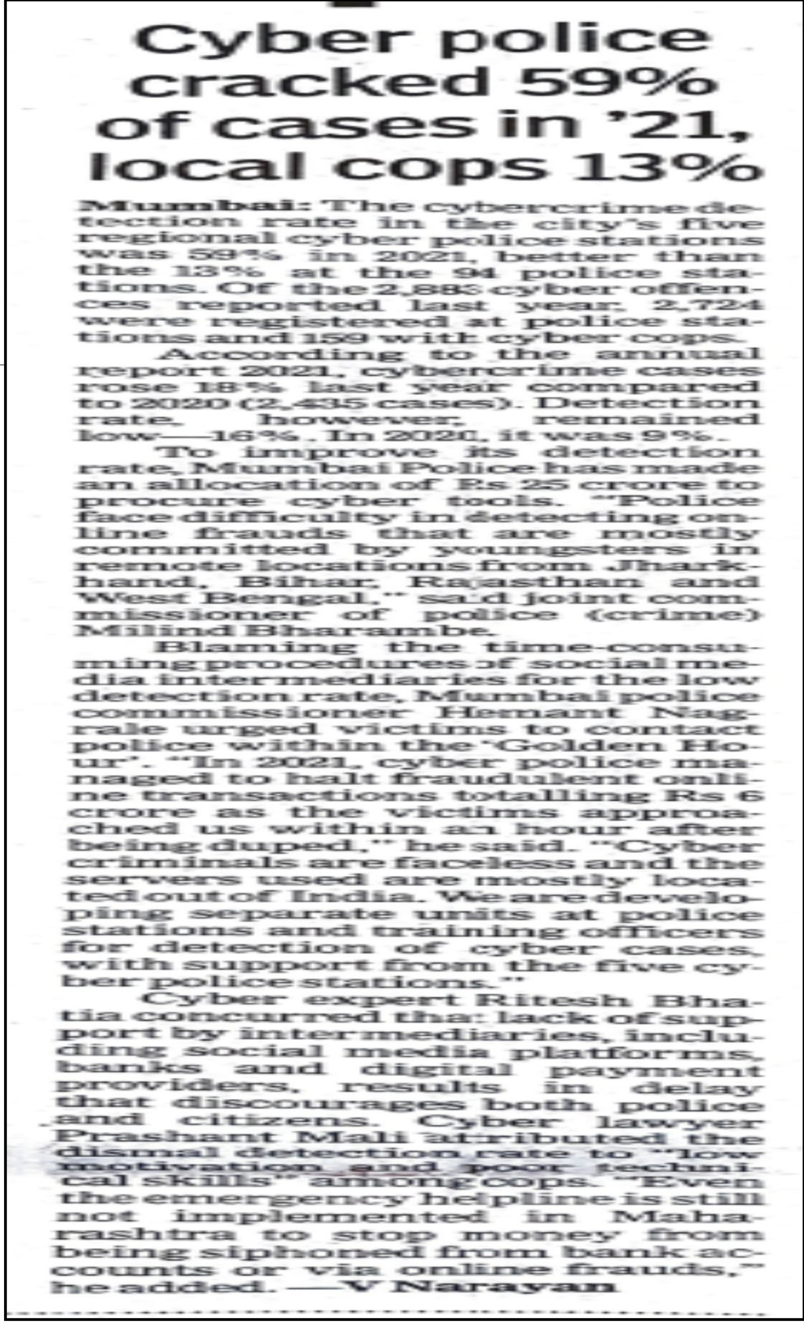
Scammers know that if they say the right words, a senior will do anything to make things right.

Sixty five-year-old *Hari Daga, who finds himself fielding sales calls all day for his cloth business in Andheri could not afford to waste time when a scammer messaged that his phone was about to get blocked if he did not update his KYC instantly. "I was afraid that my business would get disrupted. I followed his instructions and in seconds my money was gone," recounts Daga who was duped of Rs 90,000.

Another hurdle that seniors face is embarrassment and therefore less likely to report a scamming incident out of fear that their families may not want them to use technology anymore. "Let's not forget that at this age many seniors struggle with various health conditions under the dementia spectrum that impair their ability to think and remember," points out Bhatia.

*Peter Dias, 67, defrauded of a whopping Rs 2.7 lakh last month was so ashamed that for the first few minutes of conversation he spoke haltingly and relented only after being assured that his real name wouldn't be used. "I haven't told anyone in my family or my friends. I wasn't going to complain to the police either until the bank told me they would need an FIR copy to investigate," says Dias, trying to reassure that his reflexes are as sharp as anyone social and active. "Just four years ago I did a road trip from Mumbai to London and back. I've also done multiple online transactions for hotel or flight bookings. Yet, I don't know how I could be so stupid and get hypnotised by the caller," he rues.

The effect of being taken in by scammers can be psychologically damaging to vulnerable elders. If Daga's confidence has taken a beating, Dias lived in fear for a few weeks after the scam, fearful that the fraudsters might trap him physically. Rao is back to her old school ways. "I got a smartphone just five years ago to talk to people," she says until the lockdown pushed her to find another use for her phone — e-wallets for online payments.



Cyber police cracked 59% of cases in '21, local cops 13%

Mumbai: The cybercrime detection rate in the city's five regional cyber police stations was 59% in 2021, better than the 13% at the 94 police stations. Of the 2,883 cyber offences reported last year, 2,724 were registered at police stations and 159 with cyber cops.

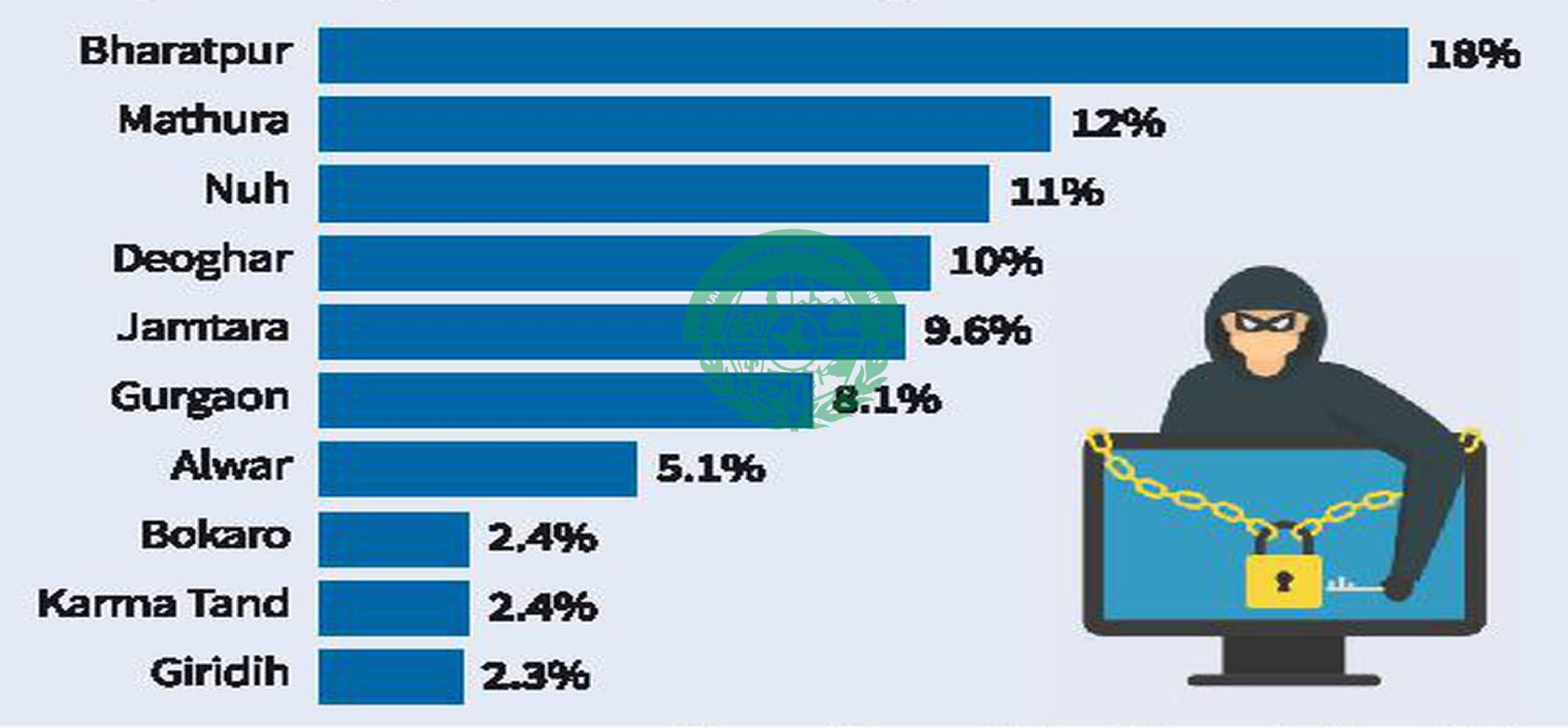
According to the annual report 2021, cybercrime cases rose 18% last year compared to 2020 (2,435 cases). Detection rate, however, remained low—16%. In 2020, it was 9%.

To improve its detection rate, Mumbai Police has made an allocation of Rs 25 crore to procure cyber tools. "Police face difficulty in detecting online frauds that are mostly committed by youngsters in remote locations from Jharkhand, Bihar, Rajasthan and West Bengal," said joint commissioner of police (crime) Milind Bharambe.

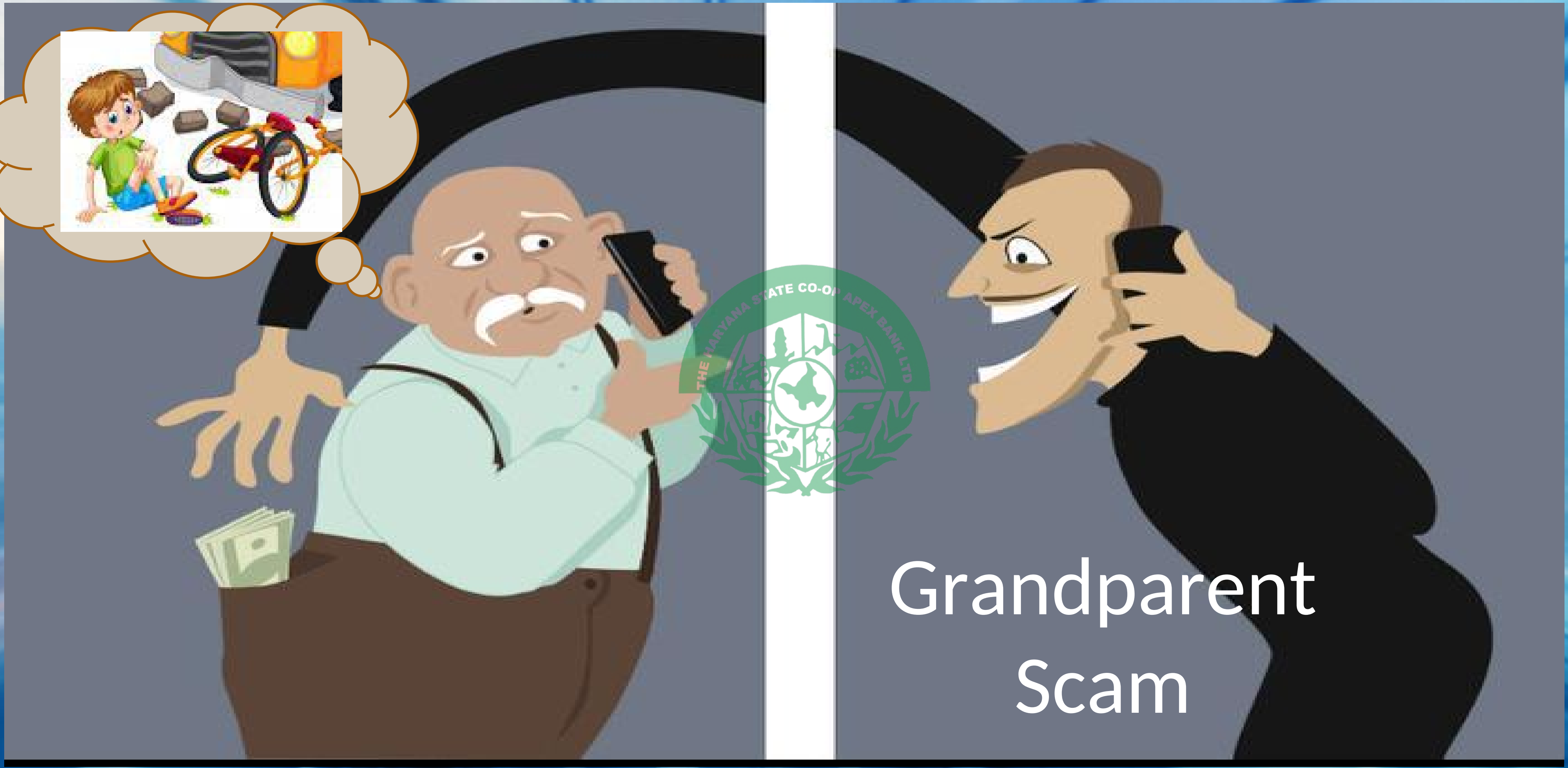
Blaming the time-consuming procedures of social media intermediaries for the low detection rate, Mumbai police commissioner Hemant Nagrale urged victims to contact police within the 'Golden Hour'. "In 2021, cyber police managed to halt fraudulent online transactions totalling Rs 6 crore as the victims approached us within an hour after being duped," he said. "Cyber criminals are faceless and the servers used are mostly located out of India. We are developing separate units at police stations and training officers for detection of cyber cases, with support from the five cyber police stations."

Cyber expert Ritesh Bhatia concurred that lack of support by intermediaries, including social media platforms, banks and digital payment providers, results in delay that discourages both police and citizens. Cyber lawyer Prashant Mali attributed the dismal detection rate to "low motivation and poor technical skills" among cops. "Even the emergency helpline is still not implemented in Maharashtra to stop money from being siphoned from bank accounts or via online frauds," he added. —V Narayan

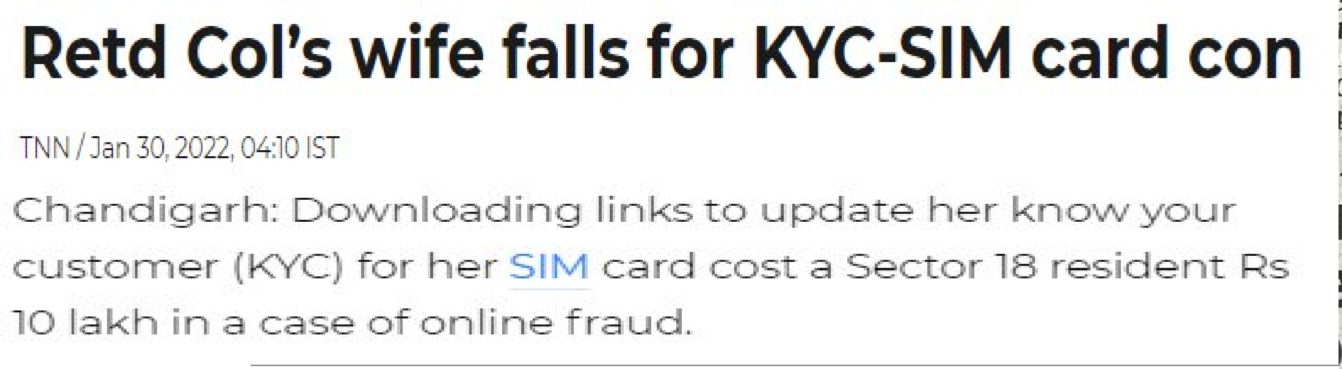
Top 10 cybercrime epicentres



Source: Future Crime Research Foundation



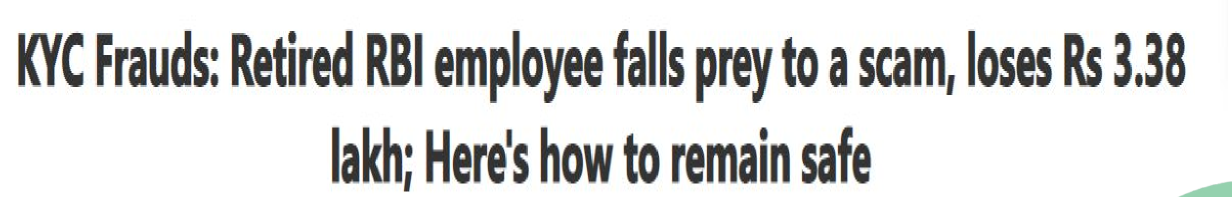
Grandparent Scam



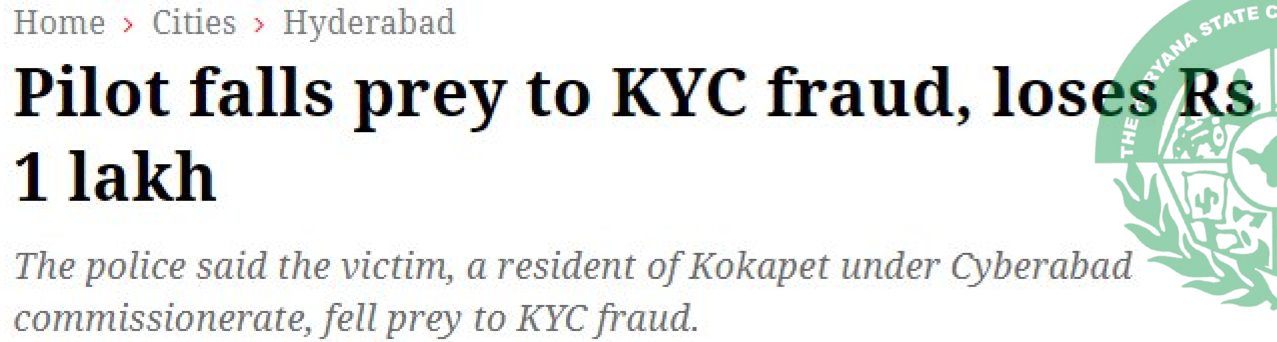
Retd Col's wife falls for KYC-SIM card con

TNN / Jan 30, 2022, 04:10 IST

Chandigarh: Downloading links to update her know your customer (KYC) for her SIM card cost a Sector 18 resident Rs 10 lakh in a case of online fraud.



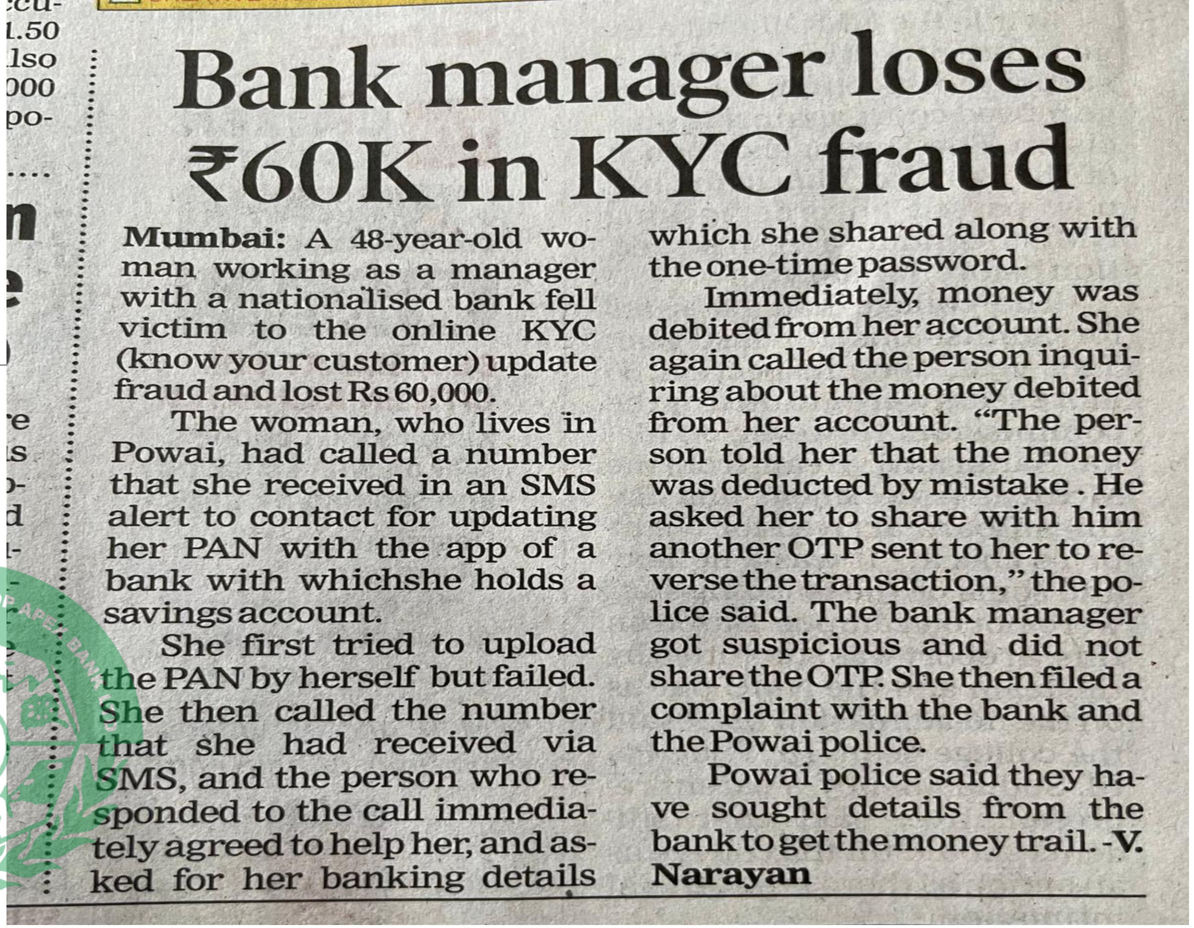
KYC Frauds: Retired RBI employee falls prey to a scam, loses Rs 3.38 lakh; Here's how to remain safe



Home › Cities › Hyderabad

Pilot falls prey to KYC fraud, loses Rs 1 lakh

The police said the victim, a resident of Kokapet under Cyberabad commissionerate, fell prey to KYC fraud.



Bank manager loses ₹60K in KYC fraud

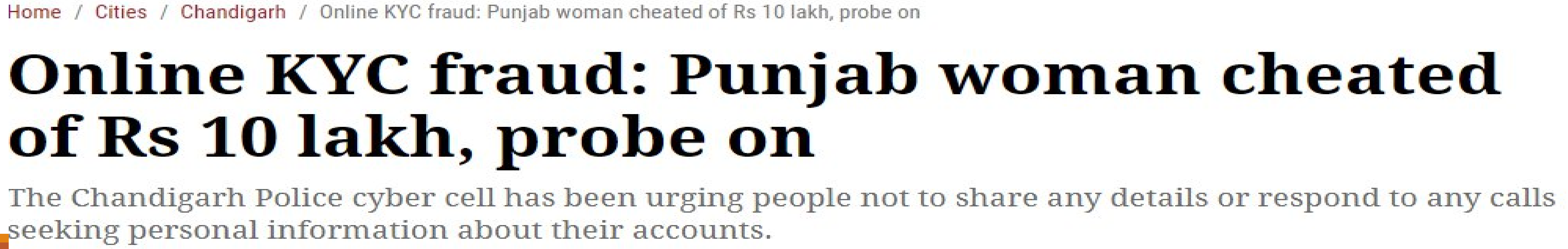
Mumbai: A 48-year-old woman working as a manager with a nationalised bank fell victim to the online KYC (know your customer) update fraud and lost Rs 60,000.

The woman, who lives in Powai, had called a number that she received in an SMS alert to contact for updating her PAN with the app of a bank with whichshe holds a savings account.

She first tried to upload the PAN by herself but failed. She then called the number that she had received via SMS, and the person who responded to the call immediately agreed to help her, and asked for her banking details which she shared along with the one-time password.

Immediately, money was debited from her account. She again called the person inquiring about the money debited from her account. "The person told her that the money was deducted by mistake . He asked her to share with him another OTP sent to her to reverse the transaction," the police said. The bank manager got suspicious and did not share the OTP. She then filed a complaint with the bank and the Powai police.

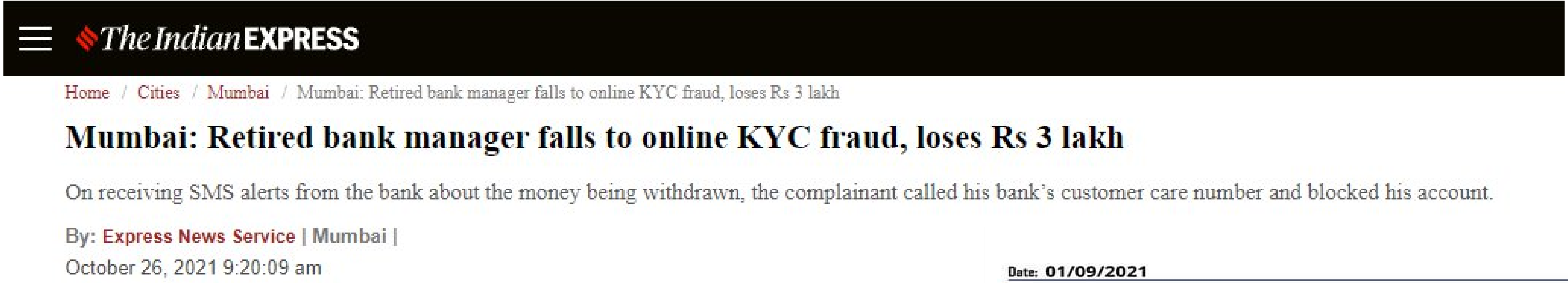
Powai police said they have sought details from the bank to get the money trail. -V. Narayan



Home / Cities / Chandigarh / Online KYC fraud: Punjab woman cheated of Rs 10 lakh, probe on

Online KYC fraud: Punjab woman cheated of Rs 10 lakh, probe on

The Chandigarh Police cyber cell has been urging people not to share any details or respond to any calls seeking personal information about their accounts.



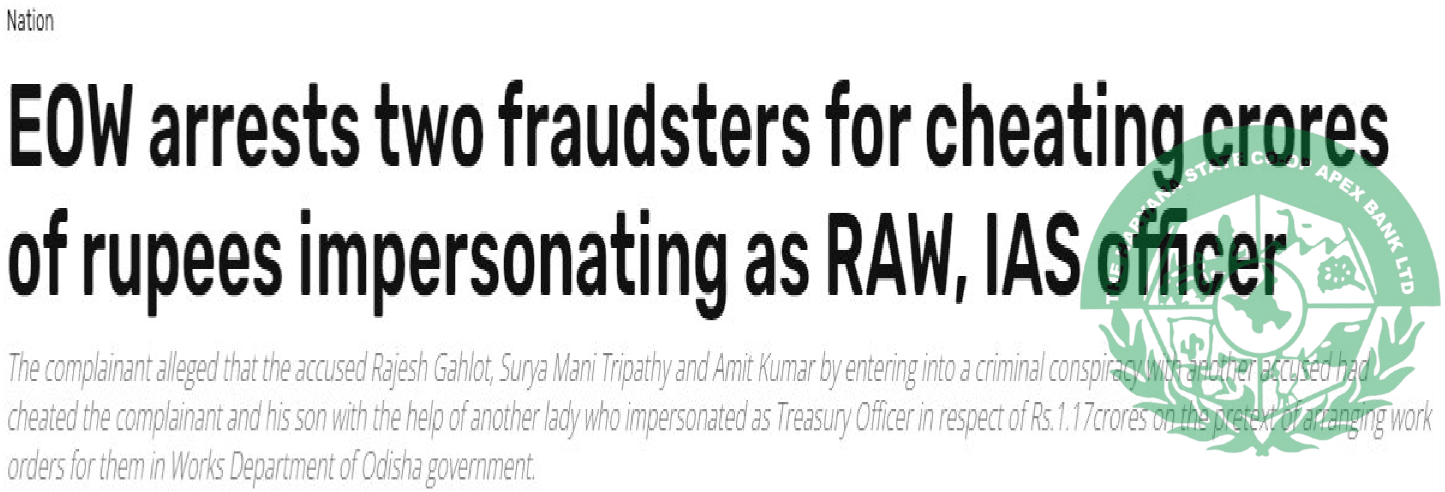
The Indian EXPRESS

Home / Cities / Mumbai / Mumbai: Retired bank manager falls to online KYC fraud, loses Rs 3 lakh

Mumbai: Retired bank manager falls to online KYC fraud, loses Rs 3 lakh

On receiving SMS alerts from the bank about the money being withdrawn, the complainant called his bank's customer care number and blocked his account.

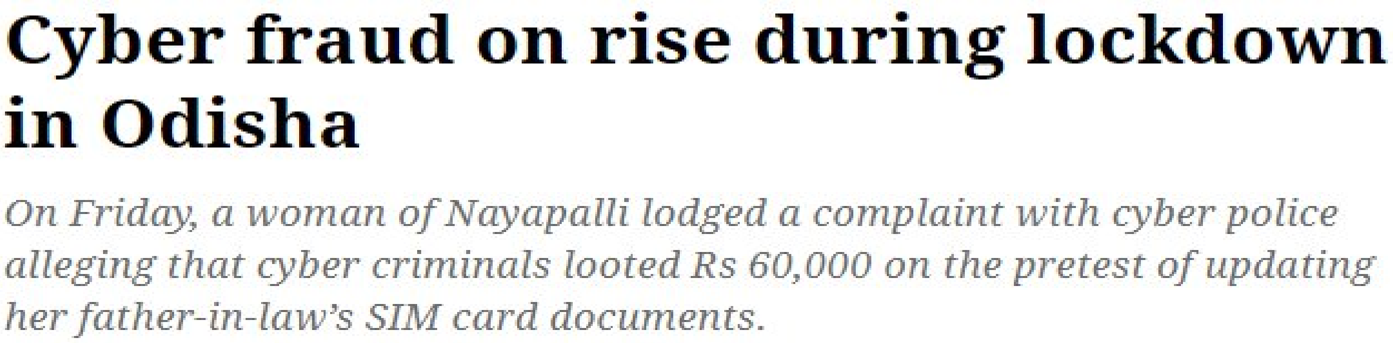
By: Express News Service | Mumbai |
October 26, 2021 9:20:09 am



Nation

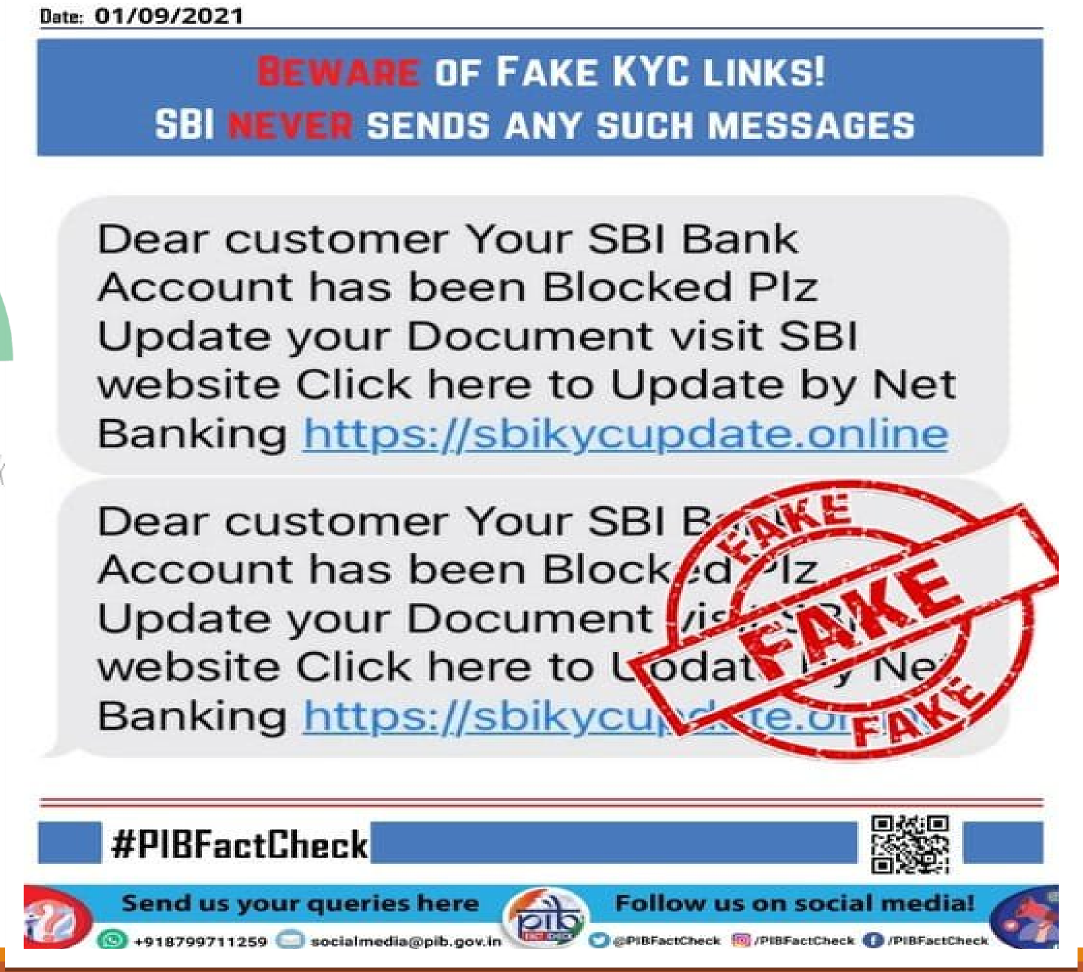
EOW arrests two fraudsters for cheating crores of rupees impersonating as RAW, IAS officer

The complainant alleged that the accused Rajesh Gahlot, Surya Mani Tripathy and Amit Kumar by entering into a criminal conspiracy with another accused had cheated the complainant and his son with the help of another lady who impersonated as Treasury Officer in respect of Rs.1.17crores on the pretext of arranging work orders for them in Works Department of Odisha government.



Cyber fraud on rise during lockdown in Odisha

On Friday, a woman of Nayapalli lodged a complaint with cyber police alleging that cyber criminals looted Rs 60,000 on the pretest of updating her father-in-law's SIM card documents.



Date: 01/09/2021

BEWARE OF FAKE KYC LINKS!
SBI NEVER SENDS ANY SUCH MESSAGES

Dear customer Your SBI Bank Account has been Blocked Plz Update your Document visit SBI website Click here to Update by Net Banking https://sbikycupdate.online

Dear customer Your SBI Bank Account has been Blocked Plz Update your Document visit SBI website Click here to Update by Net Banking https://sbikycupdate.online

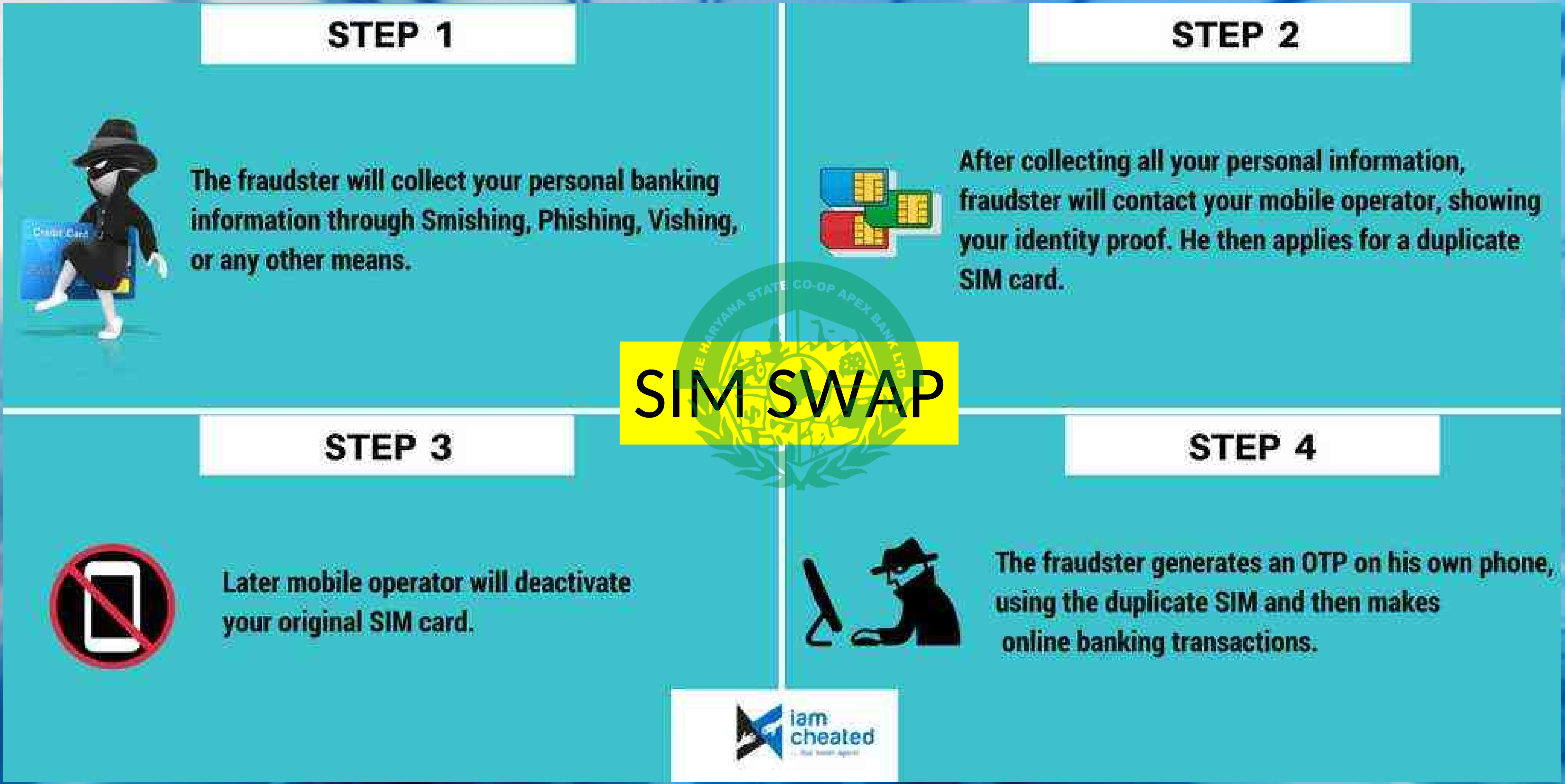
FAKE FAKE FAKE

#PIBFactCheck

Send us your queries here
+918799711259 socialmedia@pib.gov.in

Follow us on social media!
@PIBFactCheck /PIBFactCheck /PIBFactCheck

SIM SWAP



STEP 1

The fraudster will collect your personal banking information through Smishing, Phishing, Vishing, or any other means.

STEP 2

After collecting all your personal information, fraudster will contact your mobile operator, showing your identity proof. He then applies for a duplicate SIM card.

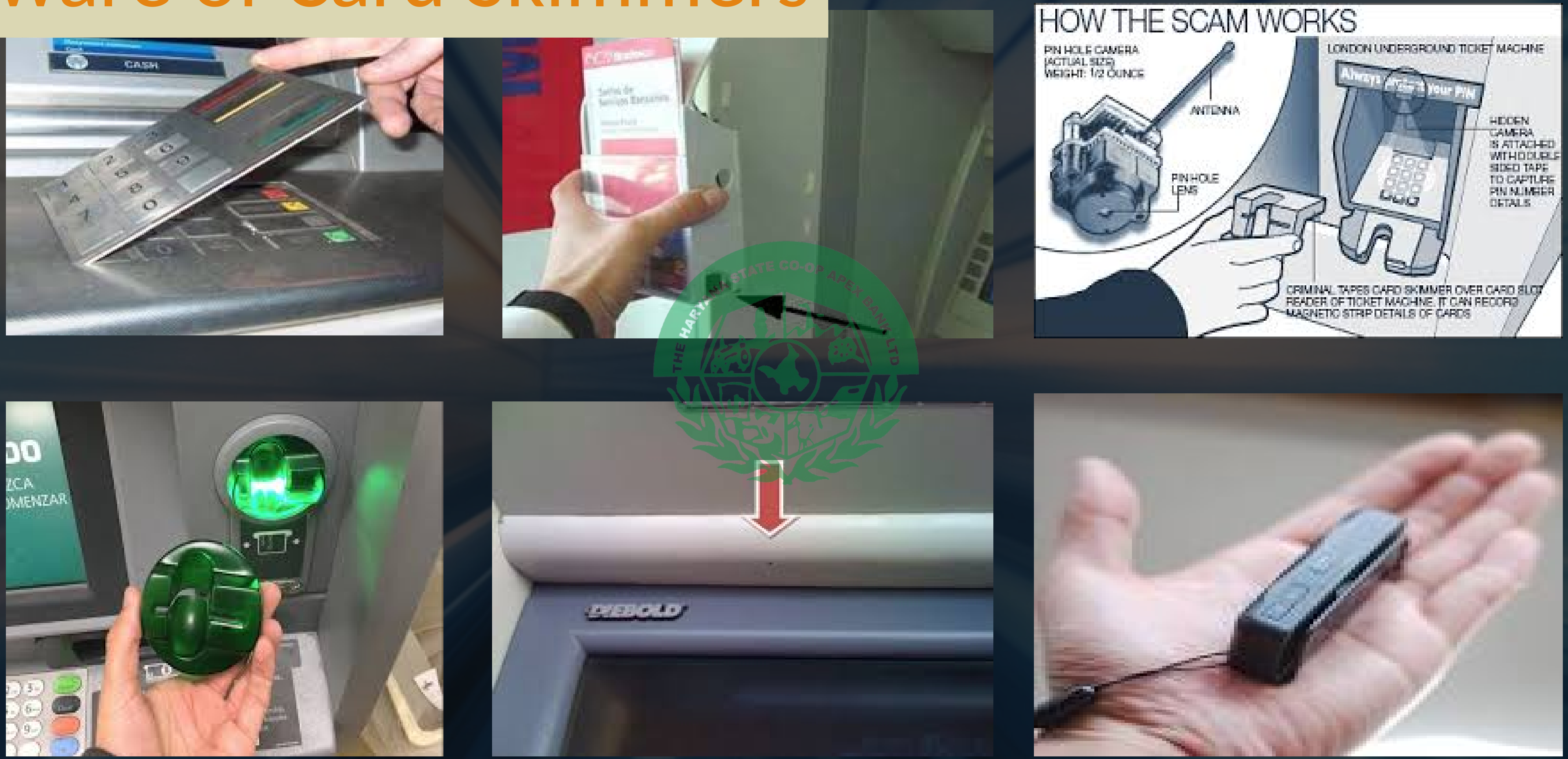
STEP 3

Later mobile operator will deactivate your original SIM card.

STEP 4

The fraudster generates an OTP on his own phone, using the duplicate SIM and then makes online banking transactions.

Beware of Card Skimmers


CASH
HOW THE SCAM WORKS
PIN HOLE CAMERA
(ACTUAL SIZE)
WEIGHT: 1/2 OUNCE
ANTENNA
PIN HOLE LENS
LONDON UNDERGROUND TICKET MACHINE
Always protect your PIN
HIDDEN CAMERA IS ATTACHED WITH DOUBLE SIDED TAPE TO CAPTURE PIN NUMBER DETAILS
CRIMINAL TAPES CARD SKIMMER OVER CARD SLOT READER OF TICKET MACHINE. IT CAN RECORD MAGNETIC STRIP DETAILS OF CARDS
DIEBOLD

SAMPLE CASE

Vijay, the SBI customer and received three SMSes for debits in his savings bank account of Rs.6,000/-. Rs.12,000/- and Rs.22,000/- (total Rs.40,000/-) on 31.12.2024 at 9.00 pm. He came back to home branch on 05-01-2025 and complained about these transactions.

On investigation, it came to know that customer card data was compromised at Urban Co-operative Bank ATM, when Vijay used his card in that ATM for normal cash transaction.

By using compromised data fraudsters created cloned card and done above transactions.

REPORTING & RESOLUTION OF UNAUTHORISED ONLINE BANKING TRANSACTIONS COMPLAINTS

An **unauthorized transaction** is any **transaction** that customer **didn't make** and **didn't permit anyone else to make**.

Un-authorised (Fraudulent) transactions happens due to negligence of :

(A) CUSTOMER

(B) BANK

(C) 3rd PARTY,

i.e. other than the customer and his/her bank

SAMPLE CASE

Vijay, the SBI customer and received three SMSes for debits in his savings bank account of Rs.6,000/-. Rs.12,000/- and Rs.22,000/- (total Rs.40,000/-) on 31-12-2023 at 9.00 pm. On investigation, it came to know that customer card data was **compromised at Urban Co-operative Bank ATM**, when Vijay used his card in that ATM for normal cash transaction. By using compromised data fraudsters created cloned card and done above transactions.

Negligence

SAMPLE CASE

Vijay, the SBI customer and received three SMSes for debits in his savings bank account of Rs.6,000/-. Rs.12,000/- and Rs.22,000/- (total Rs.40,000/-) on 31-12-2024 at 9.00 pm. Mr. Vijay is so busy in casino in GOA, he ignored these messages. He came back to home branch on 05-01-2025 and complained about these transactions. On investigation, it came to know that customer card data was compromised at Urban Co-operative Bank ATM, when Vijay was used his card in that ATM for normal cash transaction. By using compromised data fraudsters created cloned card and done above transactions.

Reporting Time

SAMPLE CASE

Vijay, the SBI customer had received three SMSes for debits in his **savings bank** account of Rs.6,000/-. Rs.12,000/- and Rs.22,000/- (total Rs.40,000/-) on 31-12-2024 at 9.00 pm. Mr. Raja is so busy in casino in GOA, he ignored these messages. He came back to home branch on 05-01-2025 and complained about these transactions. On investigation, it came to know that customer card data was compromised at Urban Co-operative Bank ATM, when Vijay was used his card in that ATM for normal cash transaction. By using compromised data fraudsters created cloned card and done above transactions.

Account Type

What is LIMITED LIABILITY of CUSTOMER ?

NEGLIGENCE	REPORTED ON	CUSTOMER LIABILITY	BANK LIABILITY
CUSTOMER	Up to reporting time	FULL	ZERO
	Once reported, further transactions using same information	ZERO	FULL
BANK	No conditions for reporting time	ZERO	FULL

3rd PARTY	CUSTOMER LIABILITY IS DEPENDS ON REPORTING TIME AND ACCOUNT TYPE		
REPORTING TIME	ACCOUNT TYPE	CUSTOMER LIABILITY	BANK LIABILITY
0 TO 3 Working Days	ALL ACCOUNTS	ZERO	FULL
4 TO 7 Working Days	BSBD/PMJDY	up to 5000/-	>5000/-
	SB/MSME	up to 10000/-	>10000/-
	CA/OD	up to 25000/-	>25000/-
Beyond 7 Working Days	ALL ACCOUNTS	FULL	ZERO

WORKING DAYS AS PER HOME BRANCH

LIABILITY WILL BE CALCULATED PER TRANSACTION, HENCE REPORTING TO BE DONE TRANSACTION WISE

Sample Case

Vijay, the SBI customer had received three SMSes for Rs.6,000/-. Rs.12,000/- and Rs.22,000/- (total Rs.40,000/-) on 31-12-2023 at 9.00 pm.

Mr. Vijay was so busy in casino that he ignored these messages of transactions in his Savings Bank Account.

He came back to home branch on 05-01-2025 and complained about these transactions.

On investigation, it came to know that customer card data was compromised at Urban Co-operative Bank ATM, when Raja was used his card in that ATM for normal cash transaction.

By using compromised data fraudsters created cloned card and done above transactions.

In this case who has to bear/compensate the loss and how much?

(Third Party negligence, Reported in 4-7 days, SB account) : Rs.14000/-

Nil for Rs.6000/- , Rs.2000 for Rs.12000/- and Rs.12000 for Rs.22000/- txn

Who is negligent in this case?

How much amount bank must pay for these transactions

Reporting time of these transaction, in terms of days if no holidays between 31-12-2023 to 04-01-2024?

HOW TO IDENTIFY THE CALLER?

Several apps can help you identify the caller ID on your phone. Some popular options include Truecaller, CallApp, Tellows, Mr. Number and Eyecon all of which offer free versions with various premium features. These apps can also help you block unwanted calls and SMS.

Use Caller ID apps

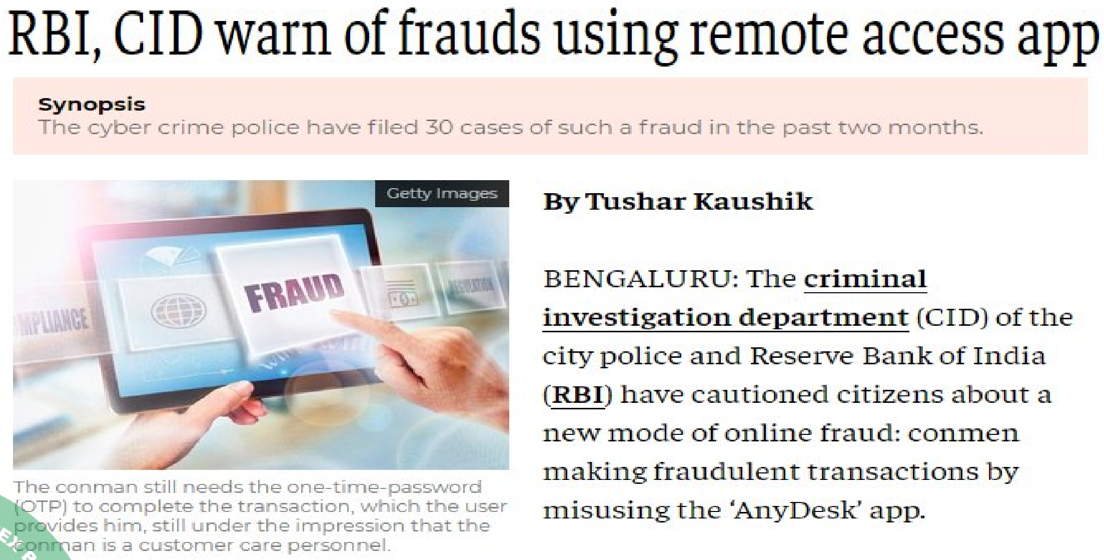
But, don’t trust them blindly.

India among top 3 countries most targeted for phishing: Report

Cyber frauds dupe man of Rs 1.19 lakh

TNN / Updated: Jun 15, 2021, 12:12 IST

JAIPUR: A man was cheated of Rs 1.19 lakh by unknown online conmen on pretext of helping him get a waiver on the annual fees for his credit card. The victim lodged a case of cheating against the unknown accused on Sunday.



RBI, CID warn of frauds using remote access app

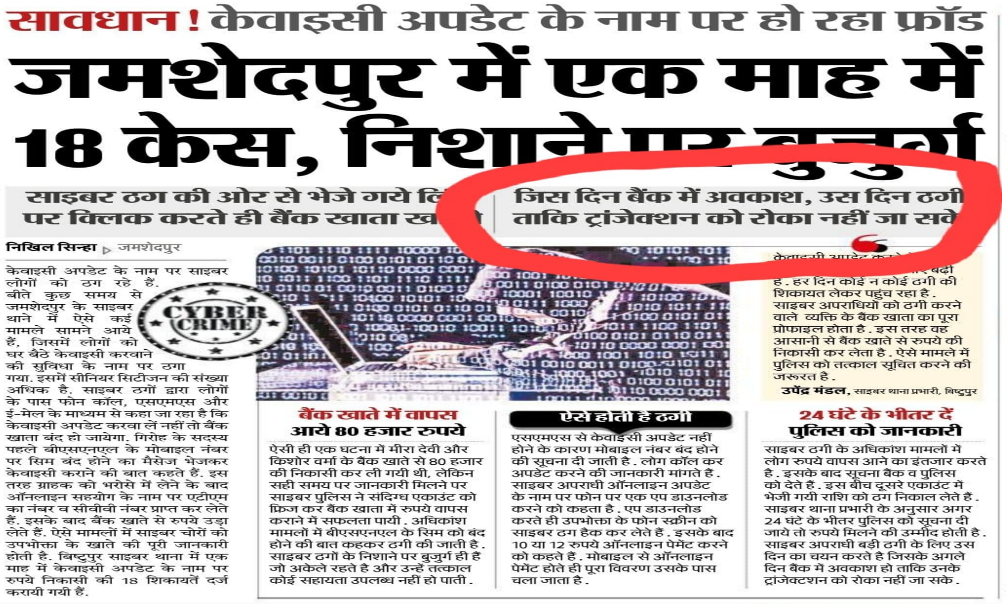
Synopsis
The cyber crime police have filed 30 cases of such a fraud in the past two months.

Getty Images

The conman still needs the one-time-password (OTP) to complete the transaction, which the user provides him, still under the impression that the conman is a customer care personnel.

By Tushar Kaushik

BENGALURU: The criminal investigation department (CID) of the city police and Reserve Bank of India (RBI) have cautioned citizens about a new mode of online fraud: conmen making fraudulent transactions by misusing the 'AnyDesk' app.



CYBER
CRIME

सावधान ! केवाइसी अपडेट के नाम पर हो रहा फ्रॉड

जमशेदपुर में एक माह में 18 केस, निशाने पर बुजुर्ग

साइबर ठग की ओर से भेजे गये लिंक पर क्लिक करते ही बैंक खाता खाली

जिस दिन बैंक में अवकाश, उस दिन ठगी ताकि ट्रांजेक्शन को रोका नहीं जा सके

निखिल सिन्हा ▷ जमशेदपुर

केवाइसी अपडेट के नाम पर साइबर लोगों को ठग रहे हैं. बीते कुछ समय से जमशेदपुर के साइबर थाने में ऐसे कई मामले सामने आये हैं, जिसमें लोगों को घर बैठे केवाइसी करवाने की सुविधा के नाम पर ठगा गया. इसमें सीनियर सिटीजन की संख्या अधिक है. साइबर ठगों द्वारा लोगों के पास फोन कॉल, एसएमएस और ई-मेल के माध्यम से कहा जा रहा है कि केवाइसी अपडेट करवा लें नहीं तो बैंक खाता बंद हो जायेगा. गिरोह के सदस्य पहले बीएसएनएल के मोबाइल नंबर पर सिम बंद होने का मैसेज भेजकर केवाइसी कराने की बात कहते हैं. इस तरह ग्राहक को भरोसे में लेने के बाद ऑनलाइन सहयोग के नाम पर एटीएम का नंबर व सीवीवी नंबर प्राप्त कर लेते हैं. इसके बाद बैंक खाते से रुपये उड़ा लेते हैं. ऐसे मामलों में साइबर चोरों को उपभोक्ता के खाते की पूरी जानकारी होती है. बिष्टुपुर साइबर थाना में एक माह में केवाइसी अपडेट के नाम पर रुपये निकासी की 18 शिकायतें दर्ज करायी गयी हैं.

केवाइसी आपडेट करने [illegible] बढ़ी है. हर दिन कोई न कोई ठगी की शिकायत लेकर पहुंच रहा है. साइबर अपराधियों को ठगी करने वाले व्यक्ति के बैंक खाता का पूरा प्रोफाइल होता है. इस तरह वह आसानी से बैंक खाते से रुपये की निकासी कर लेता है. ऐसे मामले में पुलिस को तत्काल सूचित करने की जरूरत है.

उपेंद्र मंडल, साइबर थाना प्रभारी, बिष्टुपुर

बैंक खाते में वापस आये 80 हजार रुपये

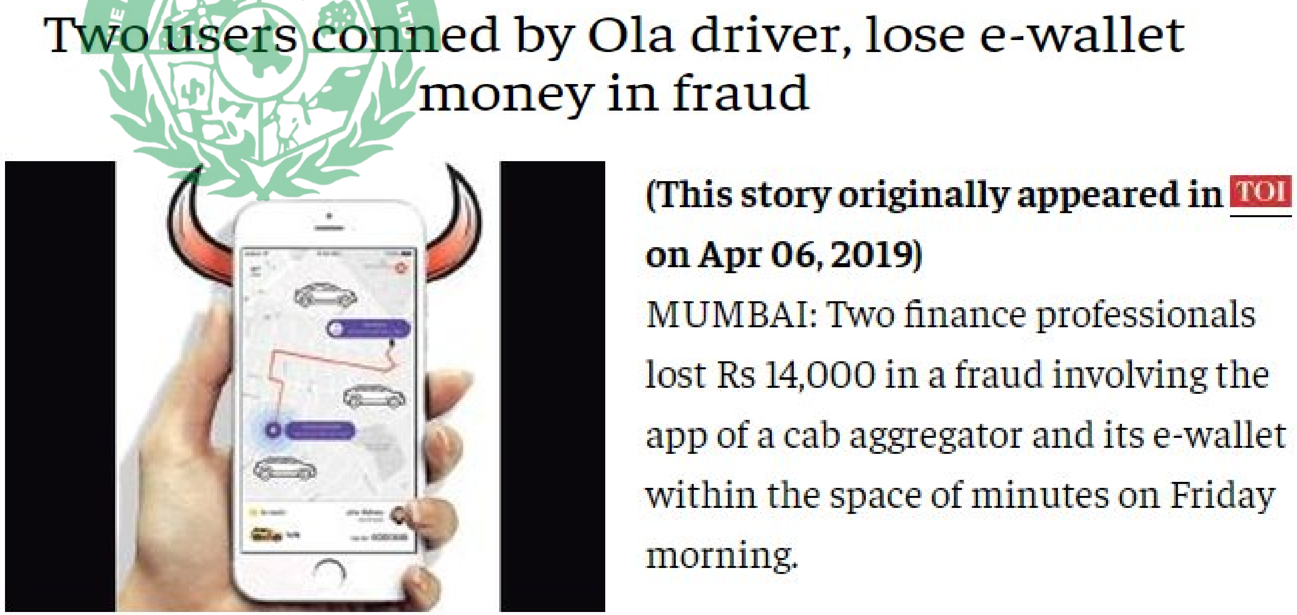
ऐसी ही एक घटना में मीरा देवी और किशोर वर्मा के बैंक खाते से 80 हजार की निकासी कर ली गयी थी, लेकिन सही समय पर जानकारी मिलने पर साइबर पुलिस ने संदिग्ध एकाउंट को फ्रिज कर बैंक खाता में रुपये वापस कराने में सफलता पायी . अधिकांश मामलों में बीएसएनएल के सिम को बंद होने की बात कहकर ठगी की जाती है . साइबर ठगों के निशाने पर बुजुर्ग ही हैं जो अकेले रहते है और उन्हें तत्काल कोई सहायता उपलब्ध नहीं हो पाती .

ऐसे होती है ठगी

एसएमएस से केवाइसी अपडेट नहीं होने के कारण मोबाइल नंबर बंद होने की सूचना दी जाती है . लोग कॉल कर अपडेट करने की जानकारी मांगते हैं . साइबर अपराधी ऑनलाइन अपडेट के नाम पर फोन पर एक एप डाउनलोड करने को कहता है . एप डाउनलोड करते ही उपभोक्ता के फोन स्क्रीन को साइबर ठग हैक कर लेते हैं . इसके बाद 10 या 12 रुपये ऑनलाइन पेमेंट करने को कहते हैं . मोबाइल से ऑनलाइन पेमेंट होते ही पूरा विवरण उसके पास चला जाता है .

24 घंटे के भीतर दें पुलिस को जानकारी

साइबर ठगी के अधिकांश मामलों में लोग रुपये वापस आने का इंतजार करते है . इसके बाद सूचना बैंक व पुलिस को देते हैं . इस बीच दूसरे एकाउंट में भेजी गयी राशि को ठग निकाल लेते हैं . साइबर थाना प्रभारी के अनुसार अगर 24 घंटे के भीतर पुलिस को सूचना दी जाये तो रुपये मिलने की उम्मीद होती है . साइबर अपराधी बड़ी ठगी के लिए उस दिन का चयन करते है जिसके अगले दिन बैंक में अवकाश हो ताकि उनके ट्रांजेक्टशन को रोका नहीं जा सके .

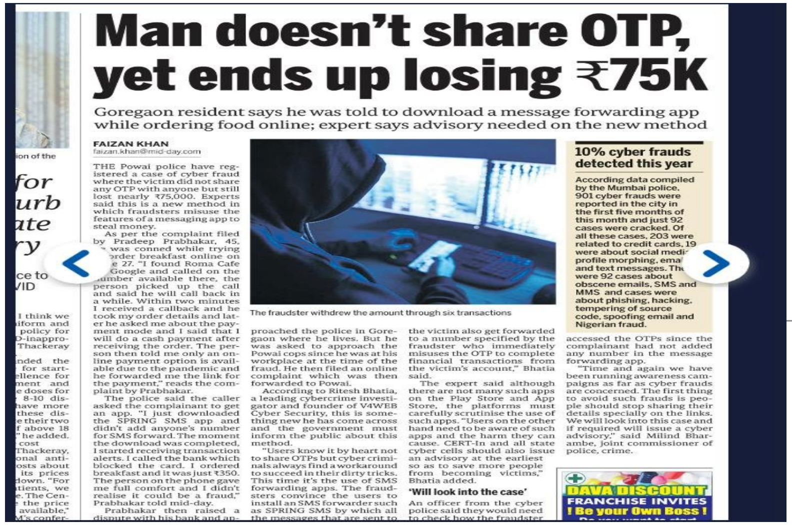


Two users conned by Ola driver, lose e-wallet money in fraud

(This story originally appeared in TOI on Apr 06, 2019)

MUMBAI: Two finance professionals lost Rs 14,000 in a fraud involving the app of a cab aggregator and its e-wallet within the space of minutes on Friday morning.

Remote APP Frauds



ion of the

for
urb
ate
ry

ce to
VID

I think we
iform and
policy for
D-inappro-
Thackeray

nded the
for start-
ellence for
ment and
e doses for
8-10 dis-
have more
these dis-
e their two
f above 18
" he added.
cost
Thackeray,
onal anti-
osts about
its prices
down. "For
tients, we
e. The Cen-
the price
available,"
M's confer-

Man doesn't share OTP, yet ends up losing ₹75K

Goregaon resident says he was told to download a message forwarding app while ordering food online; expert says advisory needed on the new method

FAIZAN KHAN
faizan.khan@mid-day.com

THE Powai police have registered a case of cyber fraud where the victim did not share any OTP with anyone but still lost nearly ₹75,000. Experts said this is a new method in which fraudsters misuse the features of a messaging app to steal money.

As per the complaint filed by Pradeep Prabhakar, 45, he was conned while trying to order breakfast online on June 27. "I found Roma Cafe on Google and called on the number available there, the person picked up the call and said he will call back in a while. Within two minutes I received a callback and he took my order details and later he asked me about the payment mode and I said that I will do a cash payment after receiving the order. The person then told me only an online payment option is available due to the pandemic and he forwarded me the link for the payment," reads the complaint by Prabhakar.

The police said the caller asked the complainant to get an app. "I just downloaded the SPRING SMS app and didn't add anyone's number for SMS forward. The moment the download was completed, I started receiving transaction alerts. I called the bank which blocked the card. I ordered breakfast and it was just ₹350. The person on the phone gave me full comfort and I didn't realise it could be a fraud," Prabhakar told mid-day.

Prabhakar then raised a dispute with his bank and approached the police in Goregaon where he lives. But he was asked to approach the Powai cops since he was at his workplace at the time of the fraud. He then filed an online complaint which was then forwarded to Powai.

According to Ritesh Bhatia, a leading cybercrime investigator and founder of V4WEB Cyber Security, this is something new he has come across and the government must inform the public about this method.

"Users know it by heart not to share OTPs but cyber criminals always find a workaround to succeed in their dirty tricks. This time it's the use of SMS forwarding apps. The fraudsters convince the users to install an SMS forwarder such as SPRING SMS by which all the messages that are sent to the victim also get forwarded to a number specified by the fraudster who immediately misuses the OTP to complete financial transactions from the victim's account," Bhatia said.

The expert said although there are not many such apps on the Play Store and App Store, the platforms must carefully scrutinise the use of such apps. "Users on the other hand need to be aware of such apps and the harm they can cause. CERT-In and all state cyber cells should also issue an advisory at the earliest so as to save more people from becoming victims," Bhatia added.

'Will look into the case'

An officer from the cyber police said they would need to check how the fraudster accessed the OTPs since the complainant had not added any number in the message forwarding app.

"Time and again we have been running awareness campaigns as far as cyber frauds are concerned. The first thing to avoid such frauds is people should stop sharing their details specially on the links. We will look into this case and if required will issue a cyber advisory," said Milind Bharambe, joint commissioner of police, crime.

The fraudster withdrew the amount through six transactions

10% cyber frauds detected this year

According data compiled by the Mumbai police, 901 cyber frauds were reported in the city in the first five months of this month and just 92 cases were cracked. Of all these cases, 203 were related to credit cards, 19 were about social medi profile morphing, ema and text messages. Th were 92 cases about obscene emails, SMS and MMS and cases were about phishing, hacking, tempering of source code, spoofing email and Nigerian fraud.

A

Social Engineering Frauds

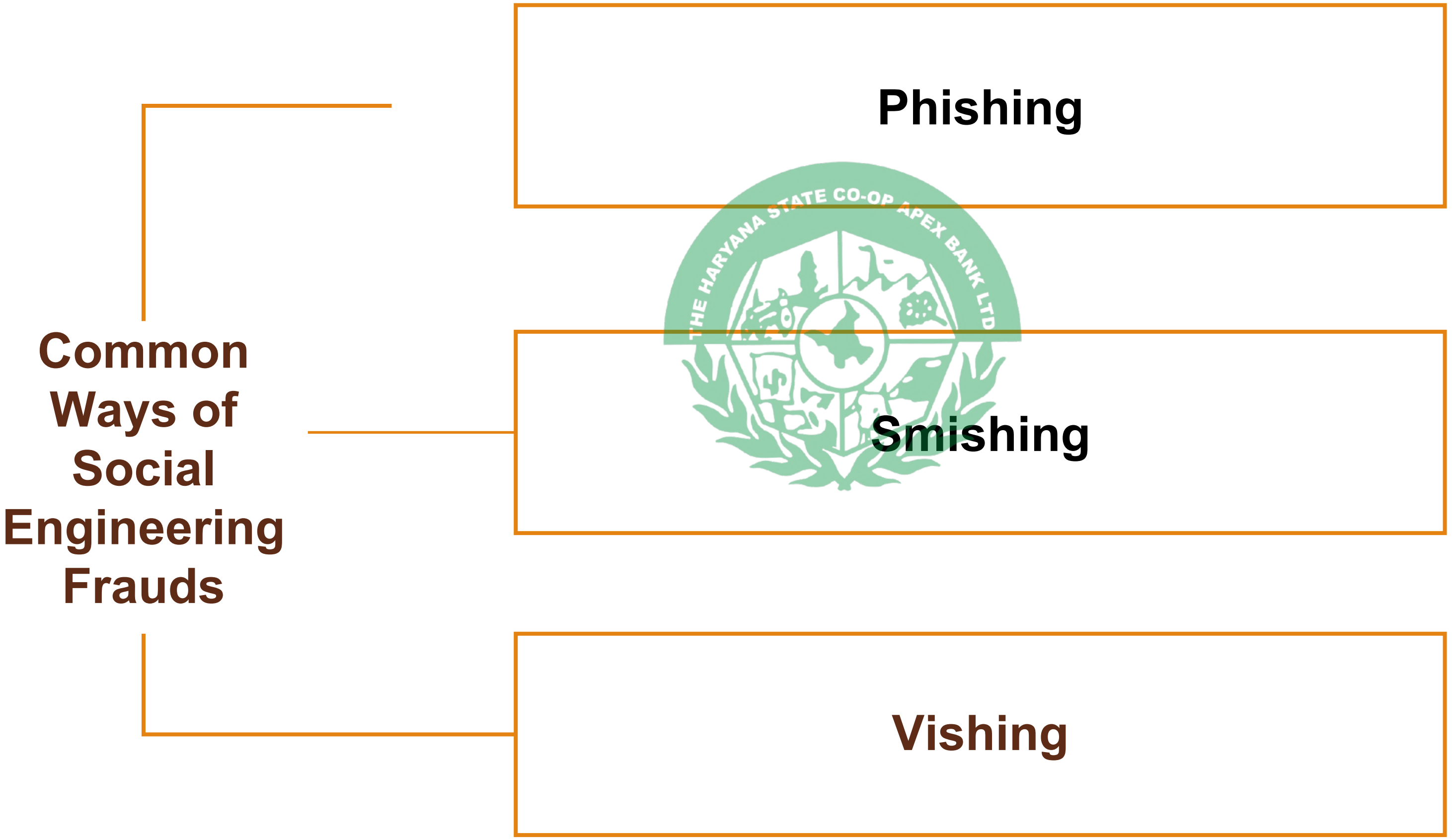
Social Engineering

What details should be shared with someone you meet online?

- Personal Information.
- Share Your Colleagues Phone Number.
- Bank Account Details.
- Username / Password etc.
- Property Details.
- Health Related Information.

What do you mean by Social Engineering?

Social engineering is a process to gain sensitive and confidential information through a friendly chat, over a drink, with kindness, etc.



Common Ways of Social Engineering Frauds

Phishing

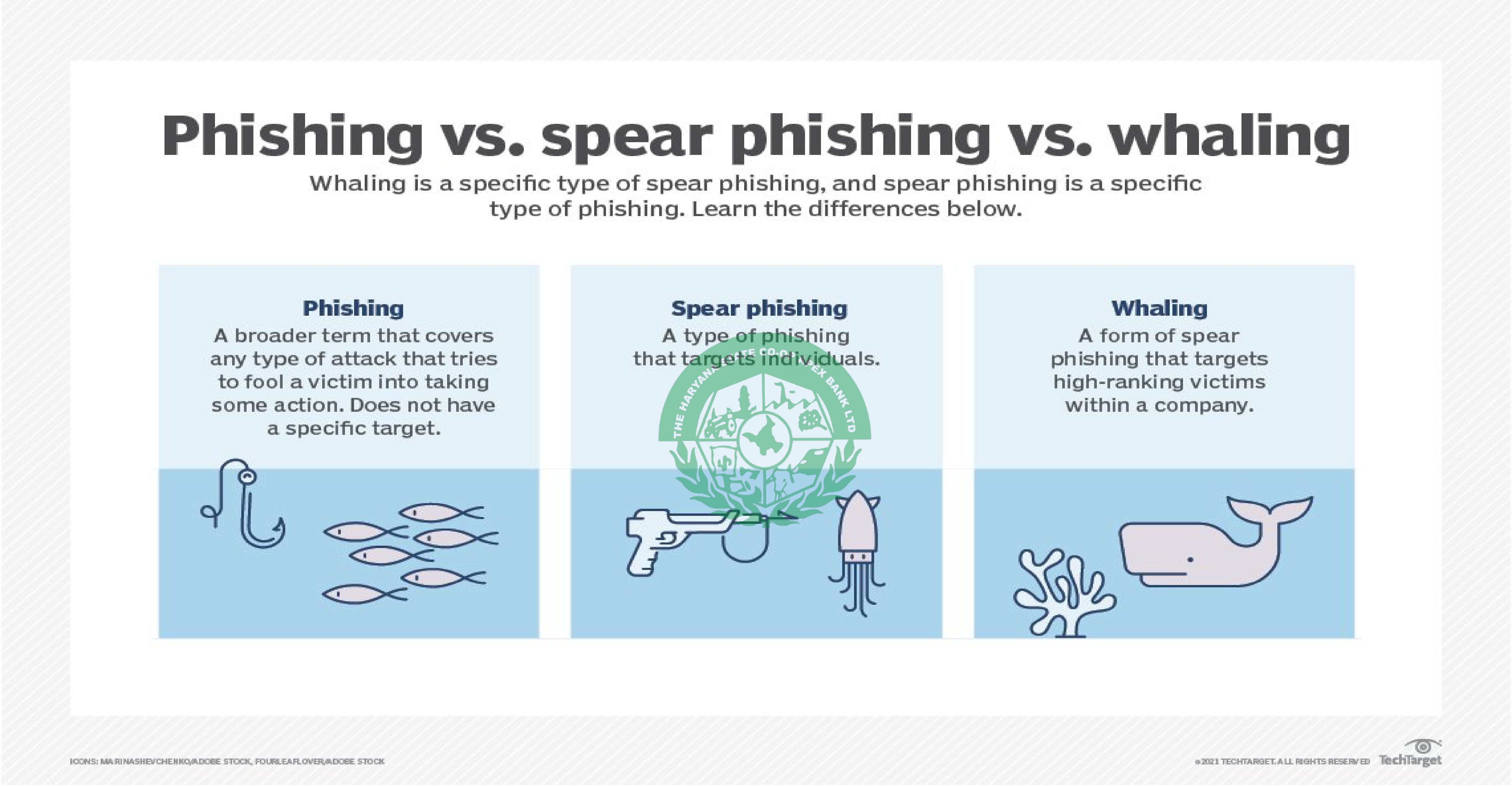
Smishing

Vishing

There are no free lunches in this world

Tactics used to get you to bite are curiosity, urgency, fear and greed.

Find out more about **phishing.**



Phishing vs. spear phishing vs. whaling

Whaling is a specific type of spear phishing, and spear phishing is a specific type of phishing. Learn the differences below.

Phishing

A broader term that covers any type of attack that tries to fool a victim into taking some action. Does not have a specific target.

Spear phishing

A type of phishing that targets individuals.

Whaling

A form of spear phishing that targets high-ranking victims within a company.

ICONS: MARINASHEVCHENKO/ADOBE STOCK, FOURLEAFLOVER/ADOBE STOCK

Angler phishing is a type of phishing attack where a scammer poses as a customer service agent on social media. Often, angler phishers target victims by scanning social media posts to find dissatisfied customers

SMISHING ATTACK PHASES

1
2
3
FRAUD ALERT

The attacker sends a message containing a malicious link

The user opens the text, clicks on the link, and gives away private data

The data is used by the attacker to commit fraud or for profit making.

JUICE JACKING

KRATIKAL
SECURE FOR SURE
Your personal files are encrypted
Copy
Decrypt
RANSOMWARE
ATTACKS
www.kratikal.com

How to Defend against Social Engineering Attacks?

- Confirm the identity of the person, whom you are talking to.
- Do **NOT** discuss confidential information at public places.
- Do **NOT** discuss confidential information with strangers, people whom you have met briefly.
- Do **NOT** share passwords and account numbers over the phone or email.
- Do **NOT** be intimidated especially by name droppers.

Keep Yourself Aware

1. More than half of business surveys believe, a lack of knowledge, carelessness is the main reason leading to cyber frauds.

2. Your Cyber Security is only as strong as your awareness, and a data breach is more likely to come from human negligence rather than a criminal hack.

Password Security

Your house keys and locks are important security measures for your house.

How do you choose locks or keep keys from being stolen and broken by a thief?

- Protect the house by putting a strong lock.
- Do NOT share the house key with a stranger.
- Do NOT leave the key unattended.
- Do NOT tell where you have kept the house key to a stranger.
- Don NOT keep the key in open, near a window or anywhere it is accessible to others.
- Choose a key which is difficult to copy.

Password Security

- Create longer password.
- Use Special Character and digit.
- Change password regularly.
- Keep unique and strong password for different account.
- Keep your password safe with you.
- Don’t use consecutive letters, dictionary word or personal information

A **passphrase** is a sentence-like string of words used for authentication that is longer than a traditional **password**, easy to remember and difficult to crack.

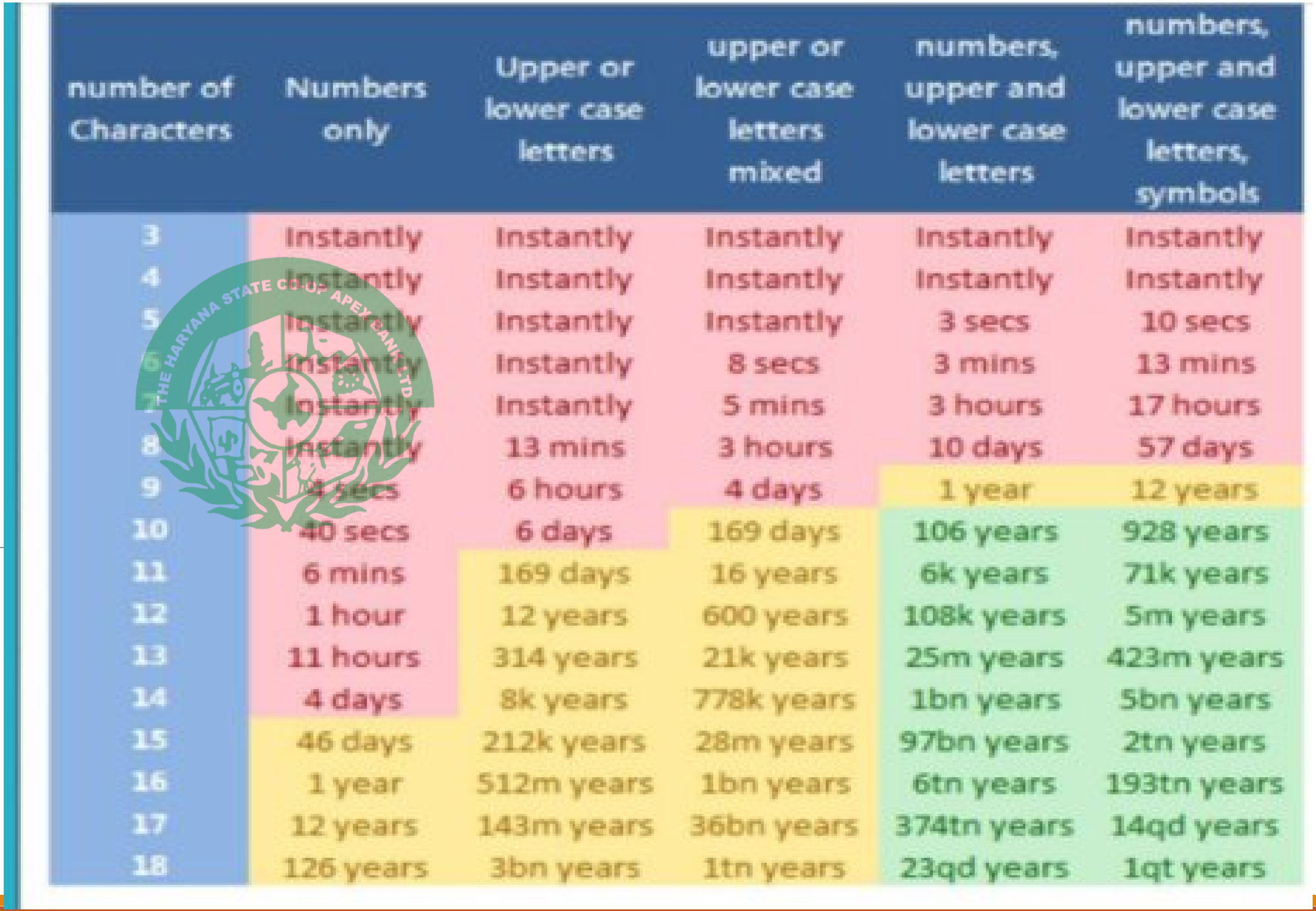
Passphrase Security

Phrase	Password
I got my first job at 22.	Igmfj@22.
My son was born on 14th	Mswbo14#
My favourite Bollywood star is Amitabh Bachhan.	Mfb*1$ab.

Brute Force Attack

A brute-force attack is an attempt to discover a password by trying every possible combination of letters, numbers, and symbols until the correct password is discovered.

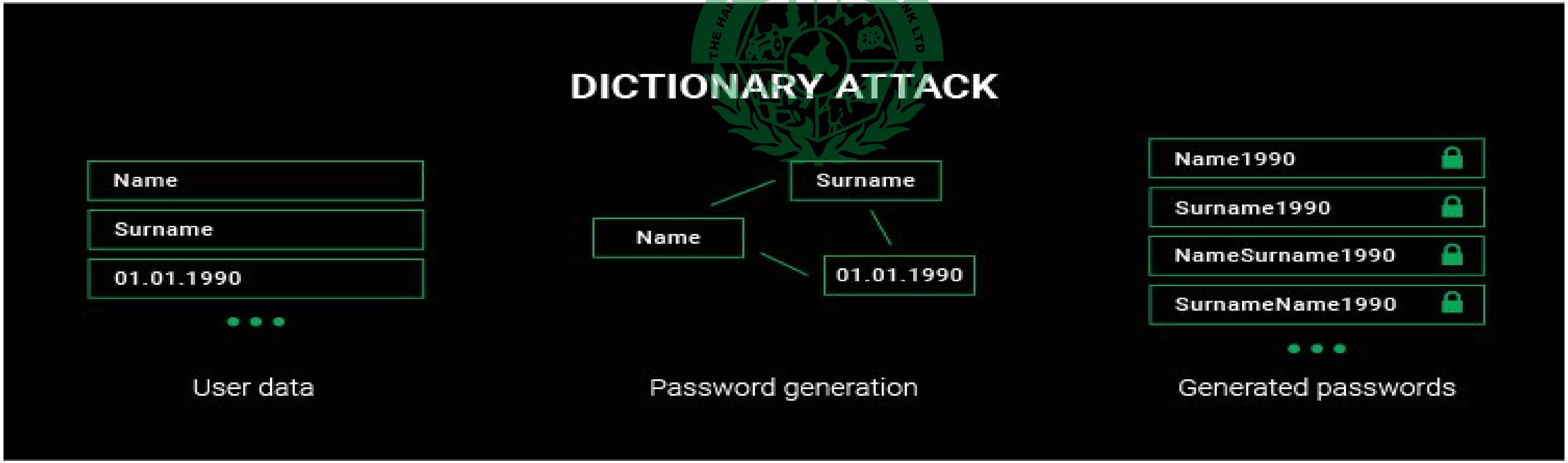
(e.g. a,aa,aaa to zzzzzzzzz, azbyex etc.)



number of Characters	Numbers only	Upper or lower case letters	upper or lower case letters mixed	numbers, upper and lower case letters	numbers, upper and lower case letters, symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 secs	10 secs
6	Instantly	Instantly	8 secs	3 mins	13 mins
7	Instantly	Instantly	5 mins	3 hours	17 hours
8	Instantly	13 mins	3 hours	10 days	57 days
9	4 secs	6 hours	4 days	1 year	12 years
10	40 secs	6 days	169 days	106 years	928 years
11	6 mins	169 days	16 years	6k years	71k years
12	1 hour	12 years	600 years	108k years	5m years
13	11 hours	314 years	21k years	25m years	423m years
14	4 days	8k years	778k years	1bn years	5bn years
15	46 days	212k years	28m years	97bn years	2tn years
16	1 year	512m years	1bn years	6tn years	193tn years
17	12 years	143m years	36bn years	374tn years	14qd years
18	126 years	3bn years	1tn years	23qd years	1qt years

DICTIONARY Attack

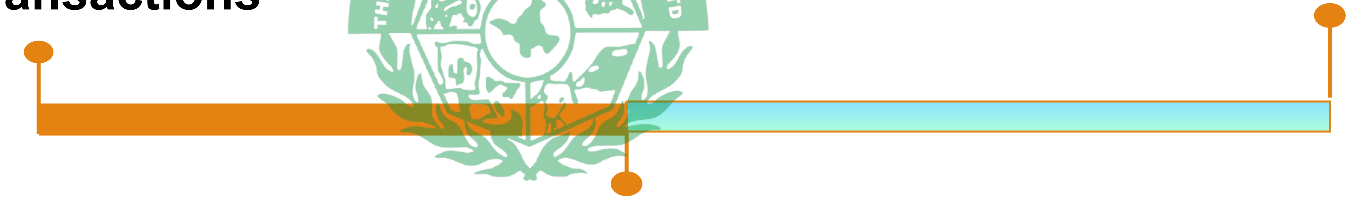
A dictionary attack is based on trying all the strings in a pre-arranged listing. Such attacks originally used words found in a dictionary (hence the phrase *dictionary attack*); however, now there are much larger lists available on the open Internet containing hundreds of millions of passwords recovered from past data breaches. There is also cracking software that can use such lists and produce common variations, such as substituting numbers for similar-looking letters.



Wireless Security

Do NOT connect to public network for performing banking transactions

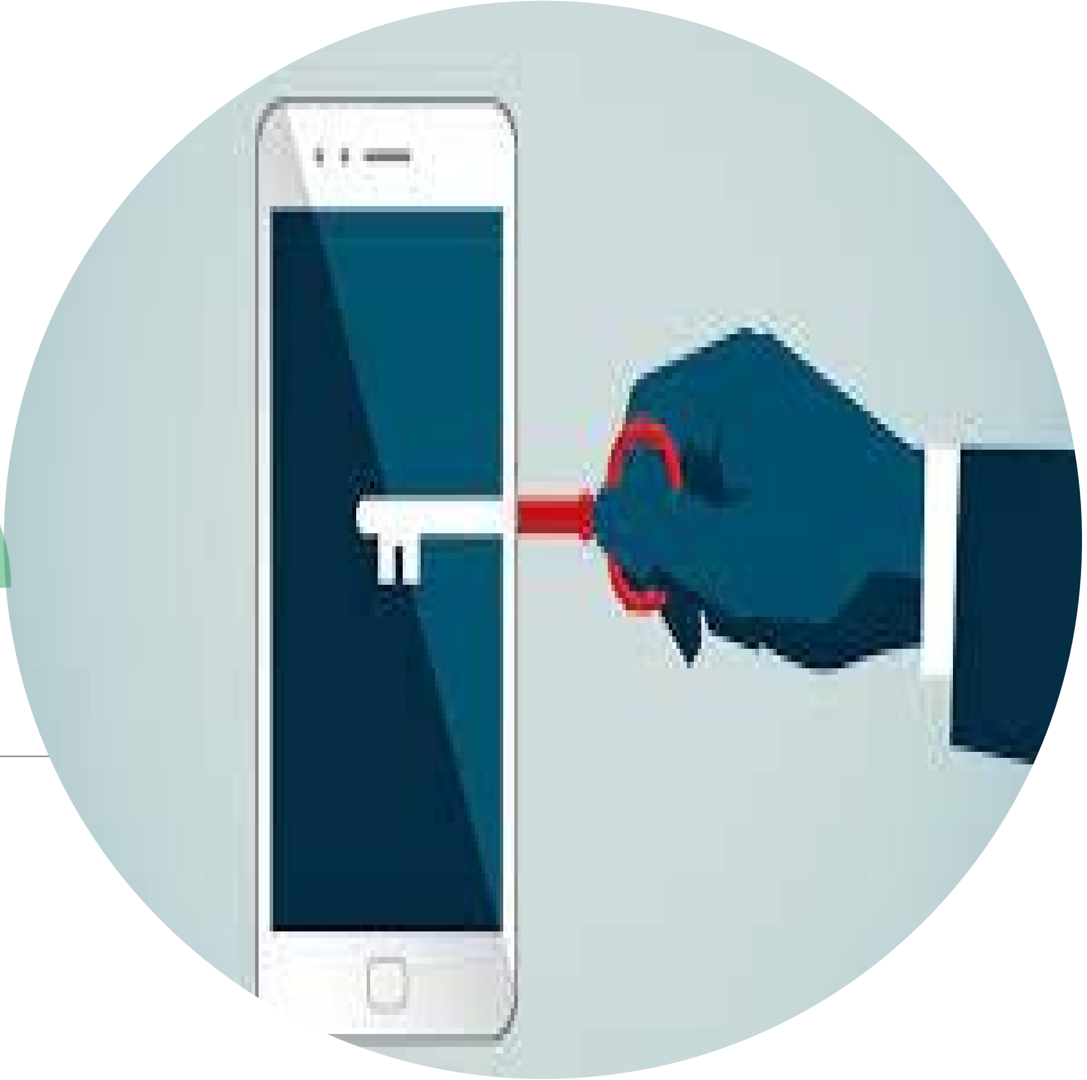
Do NOT disable your firewall or Anti-Virus software on your laptop.



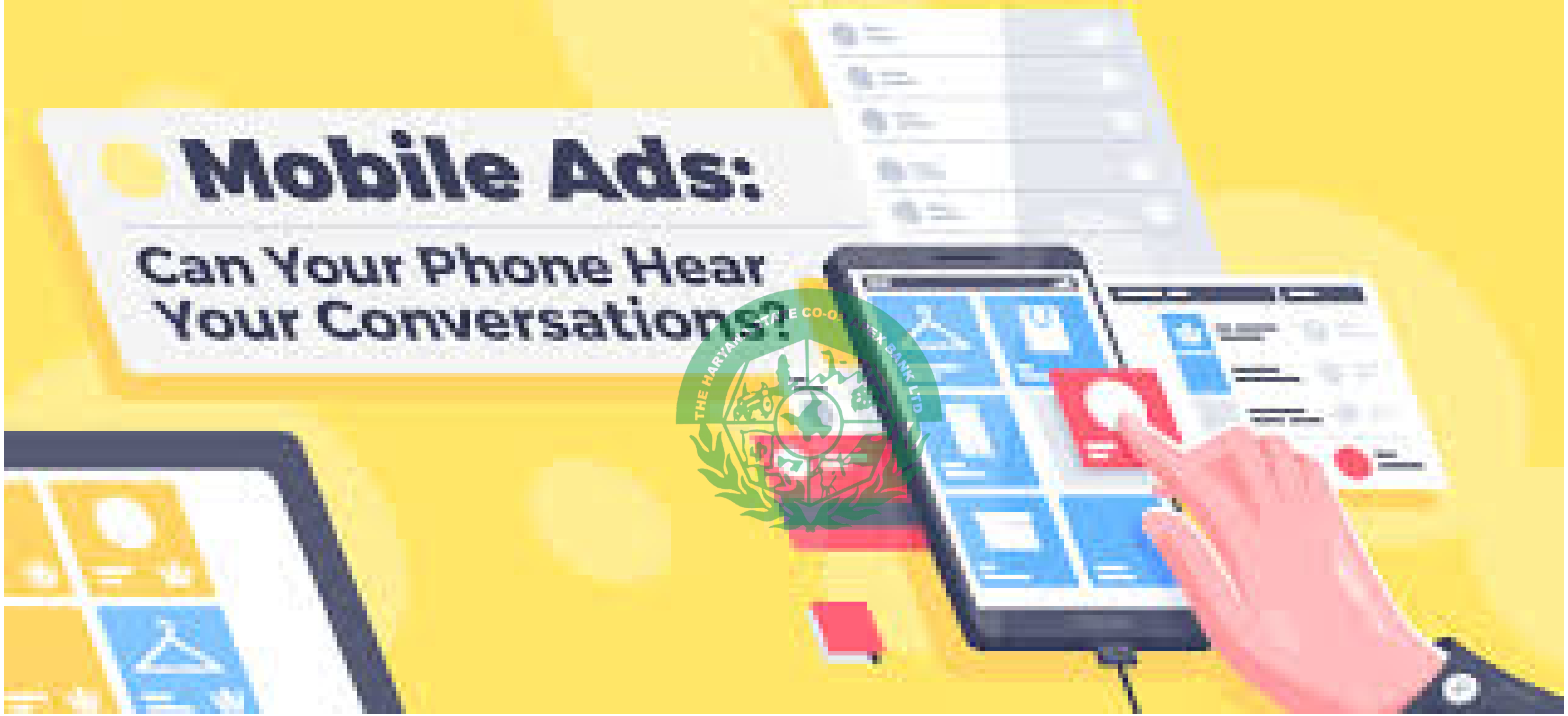
Take particular care when using your laptop and mobile phone in any public environment.

YOU DON'T NEED SOMEONE
TO BREAK INTO A HOUSE,

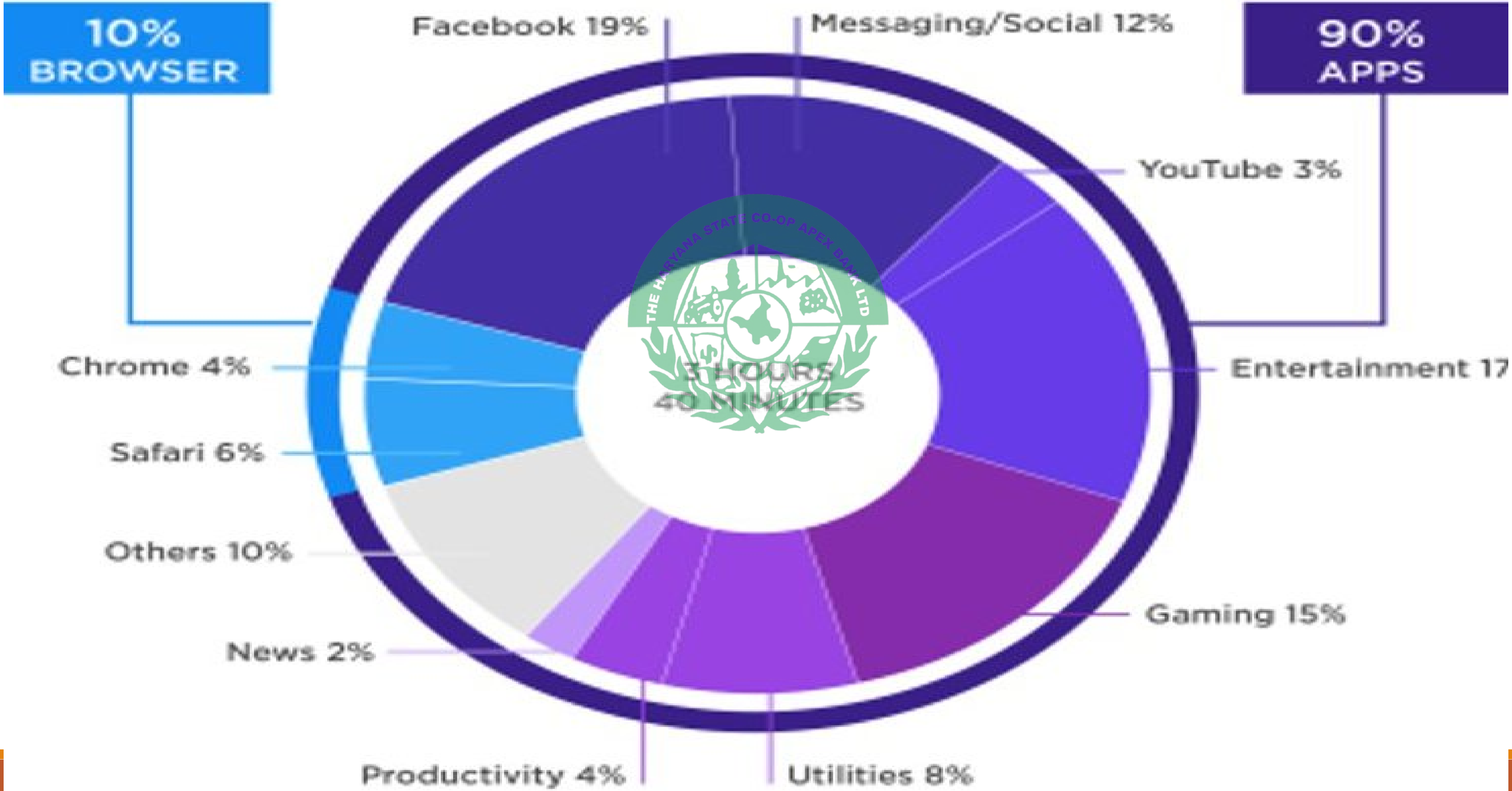
YOU JUST NEED SOMEONE
TO LET YOU IN.



Mobile Security

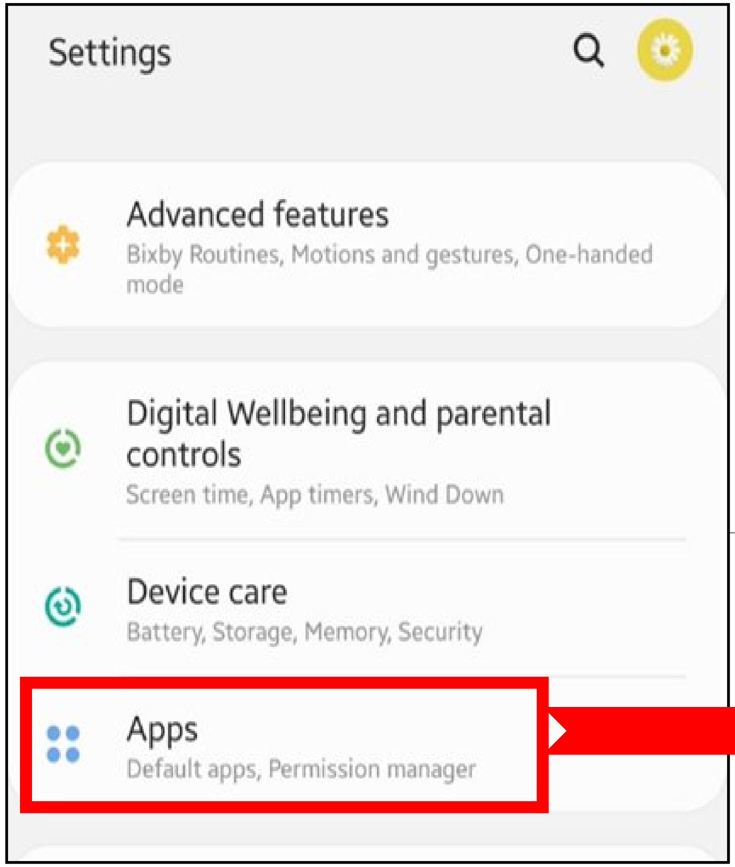

Mobile Ads:
Can Your Phone Hear Your Conversations?

90% of Time on Mobile is Spent in Apps



Monitor Permissions

Settings - Apps



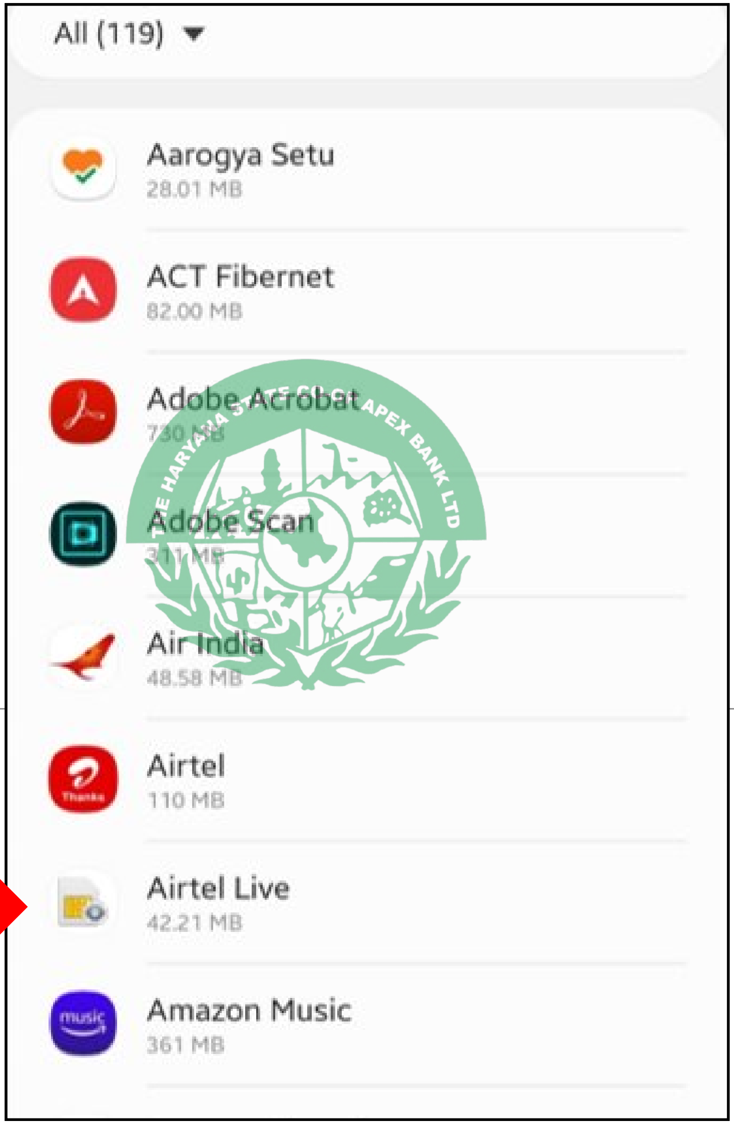
Settings

Advanced features
Bixby Routines, Motions and gestures, One-handed mode

Digital Wellbeing and parental controls
Screen time, App timers, Wind Down

Device care
Battery, Storage, Memory, Security

Apps
Default apps, Permission manager



All (119)

Aarogya Setu
28.01 MB

ACT Fibernet
82.00 MB

Adobe Acrobat
730 MB

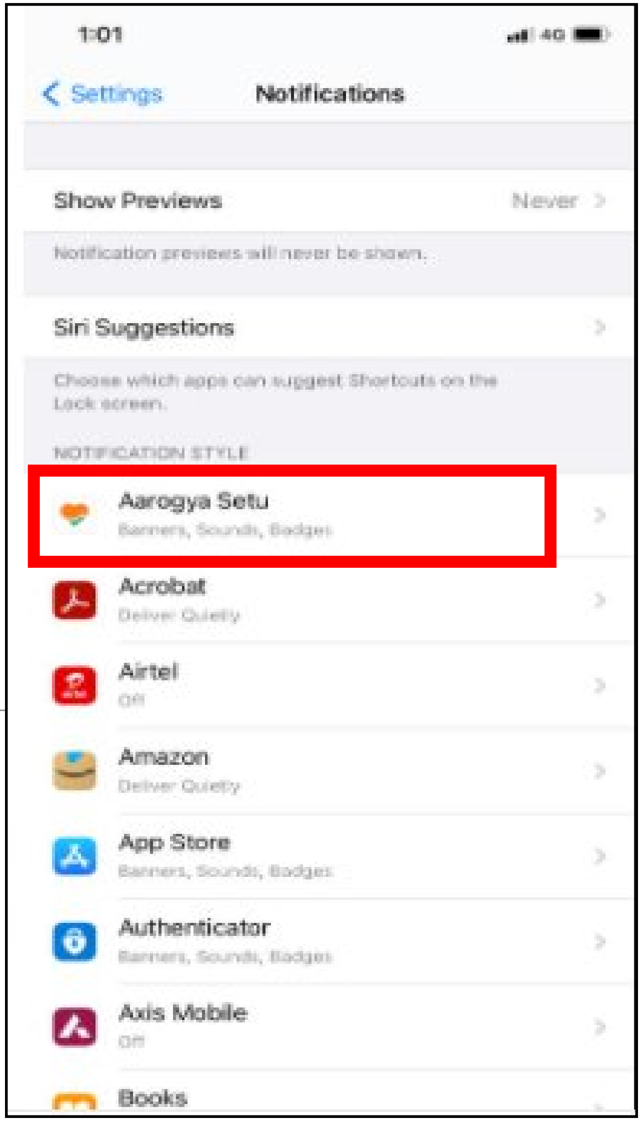
Adobe Scan
311 MB

Air India
48.58 MB

Airtel
110 MB

Airtel Live
42.21 MB

Amazon Music
361 MB



1:01 4G

< Settings Notifications

Show Previews Never >

Notification previews will never be shown.

Siri Suggestions >

Choose which apps can suggest Shortcuts on the Lock screen.

NOTIFICATION STYLE

Aarogya Setu
Banners, Sounds, Badges

Acrobat
Deliver Quietly

Airtel
Off

Amazon
Deliver Quietly

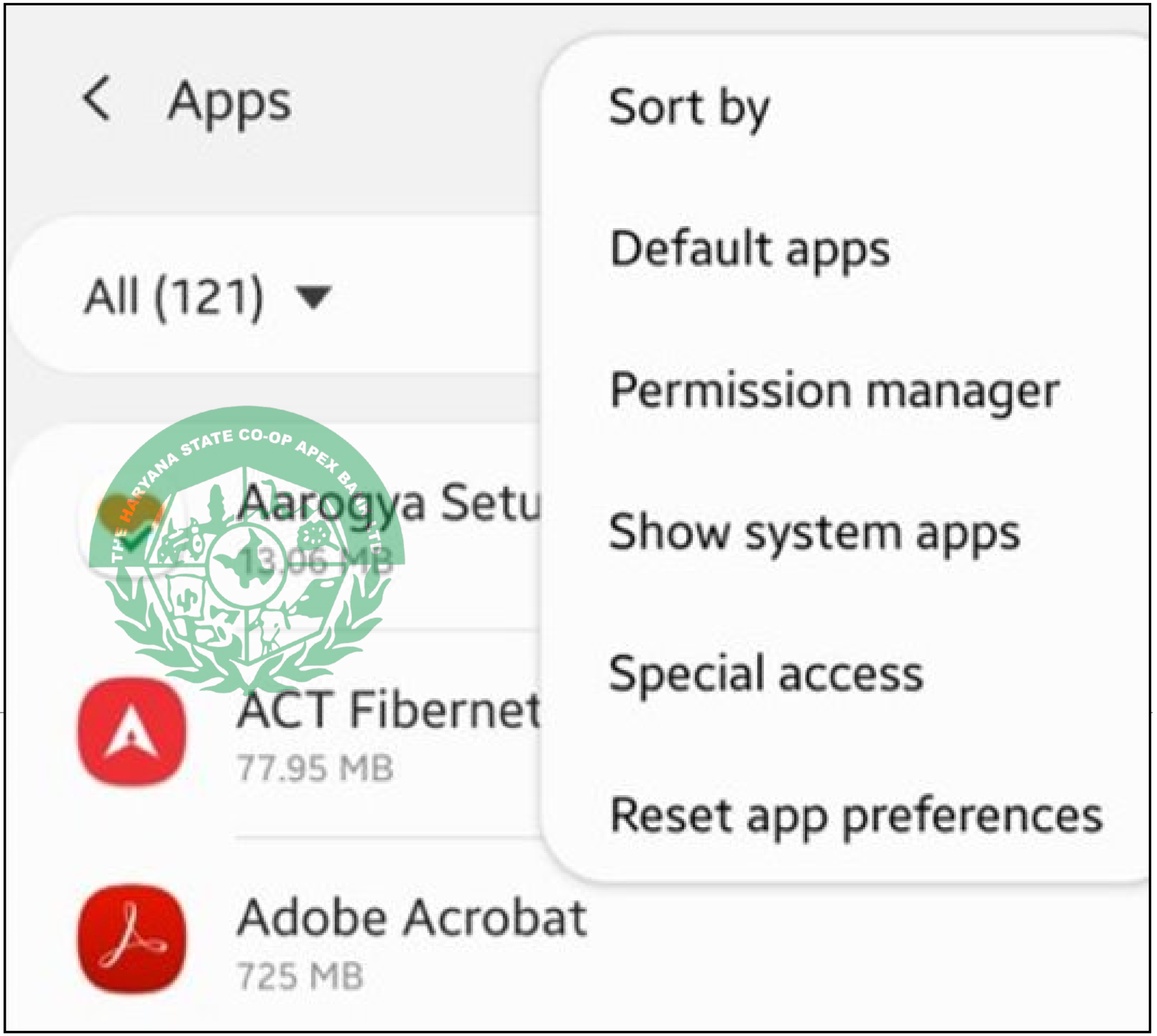
App Store
Banners, Sounds, Badges

Authenticator
Banners, Sounds, Badges

Axis Mobile
Off

Books

- Access Permission Manager in your Mobile
- Settings – Apps – Permission Manager (OR)
- Settings - Privacy



SURFACE WEB, DARK WEB, DEEP WEB

SURFACE WEB

Facebook

Google

YouTube

Instagram

DEEP WEB

Medical Records

Legal Documents

Private Forums

Research Papers

Non Indexed Content

DARK WEB

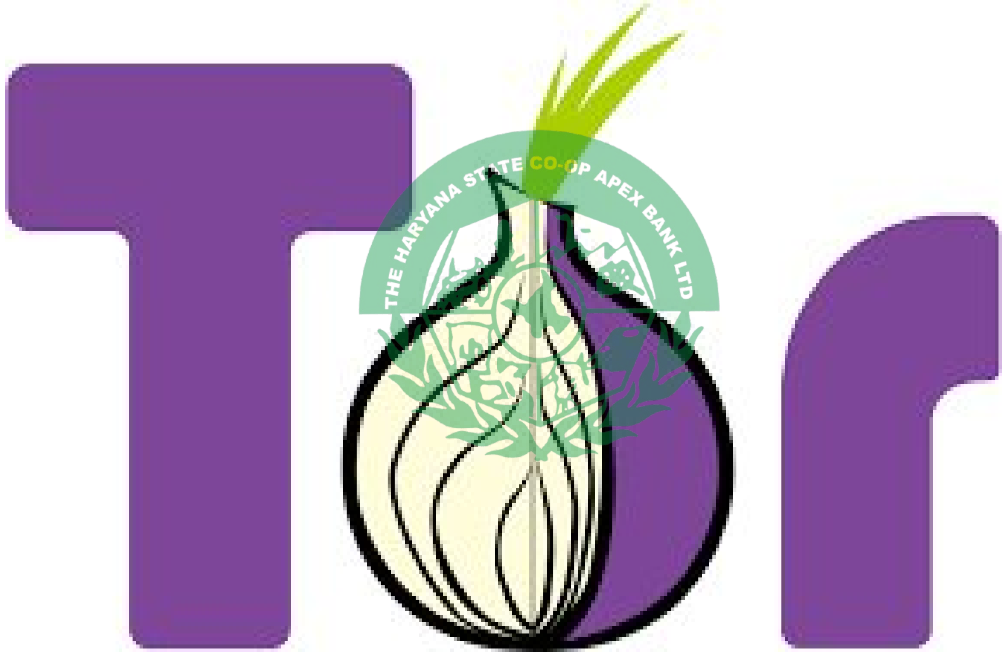
Private Communication Forums

TOR

Illegal Trade

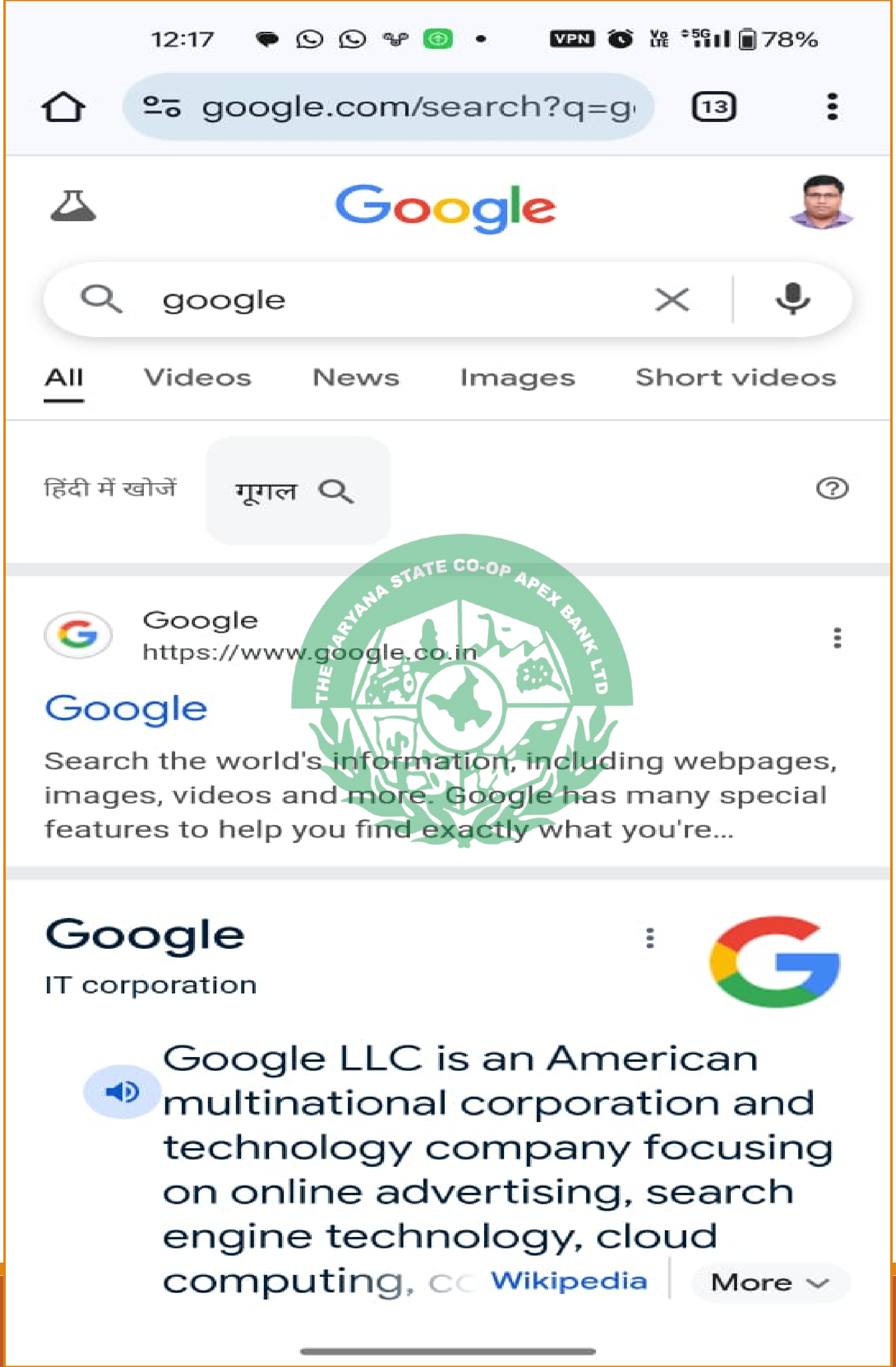
Illegal Activities

The Onion Router



Can I check which Apps on my mobile phone have divulged my information on Dark Web?

Yes



Google
https://www.google.co.in

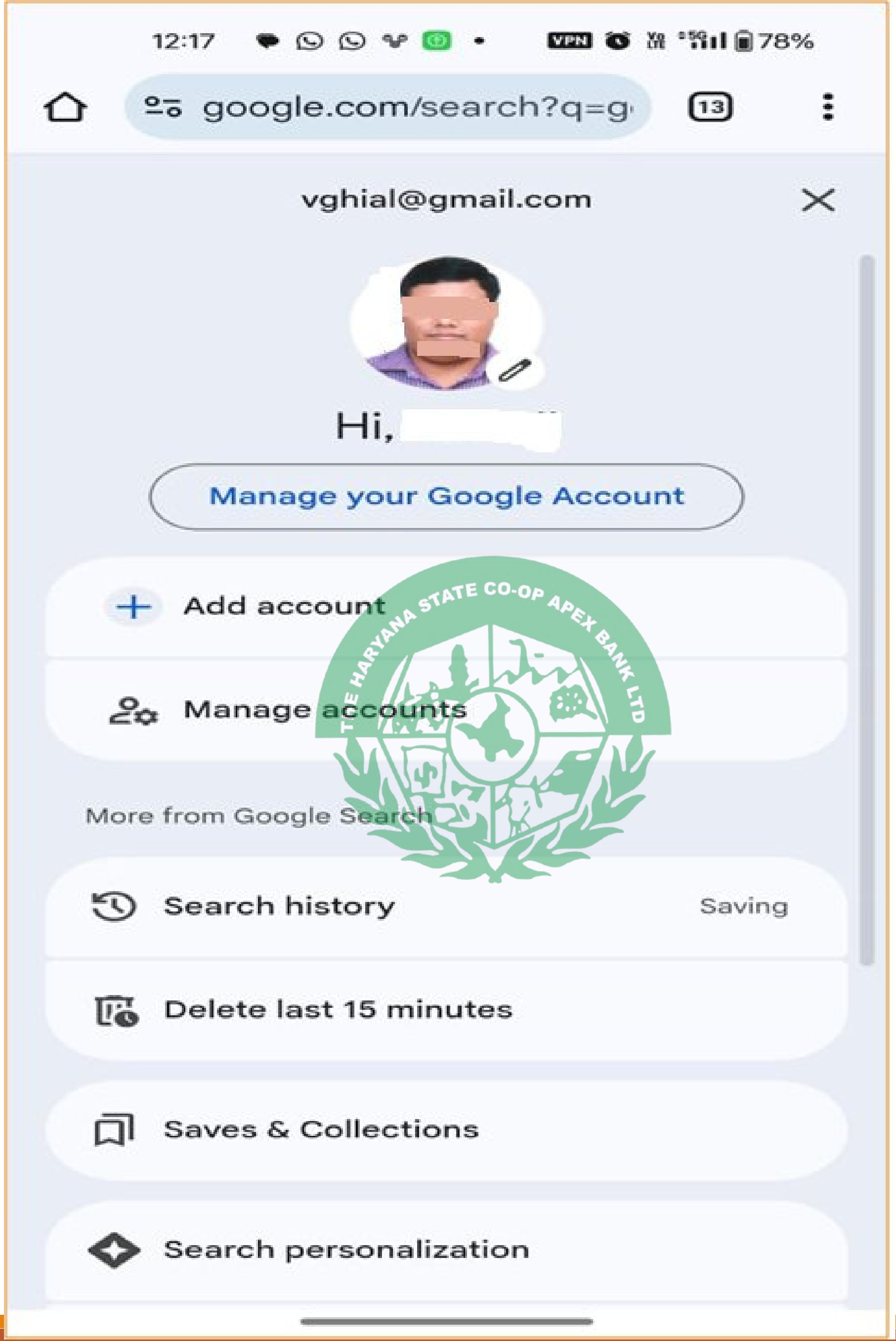
Google

Search the world's information, including webpages, images, videos and more. Google has many special features to help you find exactly what you're...

Google

IT corporation

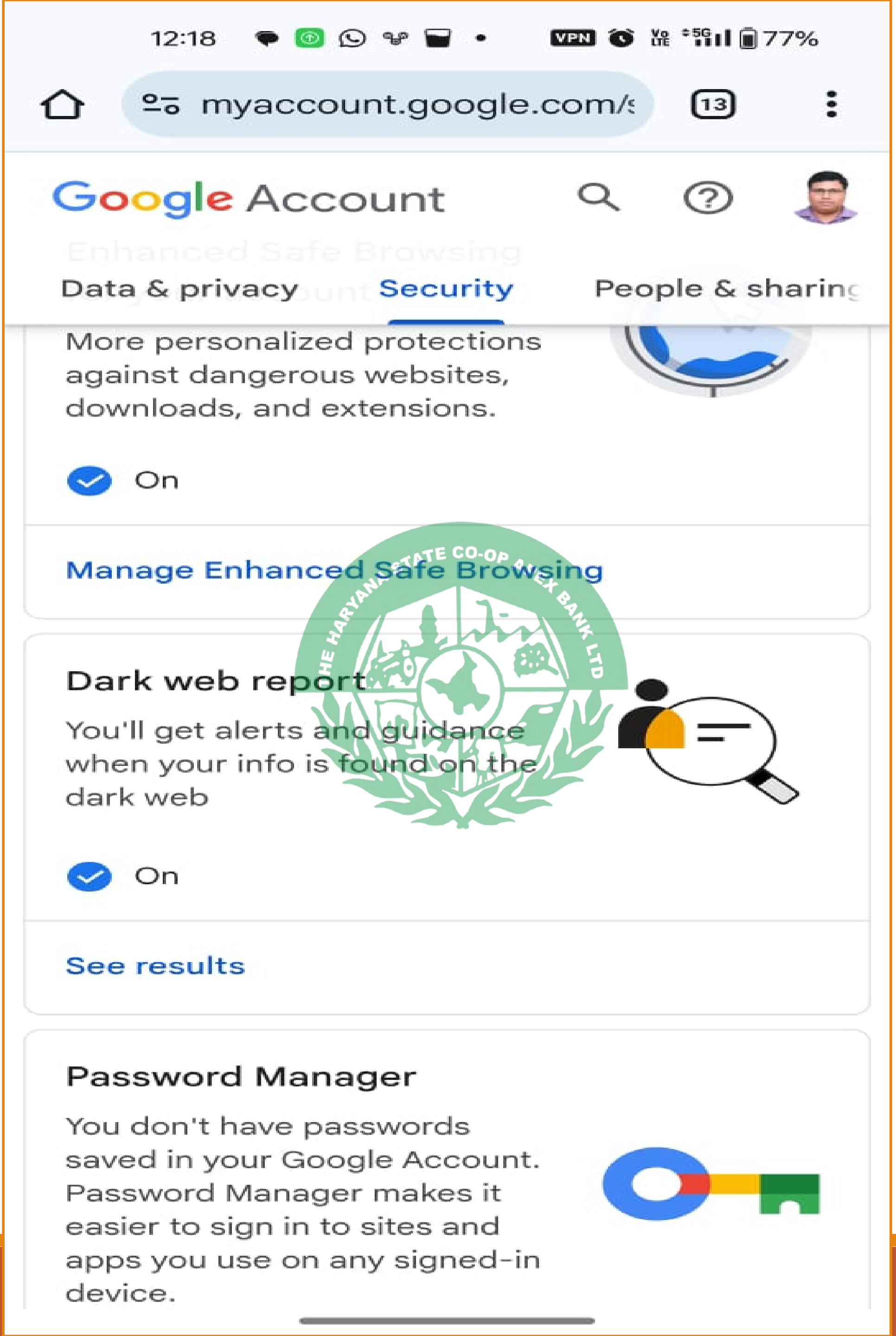
Google LLC is an American multinational corporation and technology company focusing on online advertising, search engine technology, cloud computing, cc Wikipedia



vghial@gmail.com

Hi, [redacted]

Search history Saving



Google Account

Data & privacy | Security | People & sharing

More personalized protections against dangerous websites, downloads, and extensions.

✓ On

Manage Enhanced Safe Browsing

Dark web report

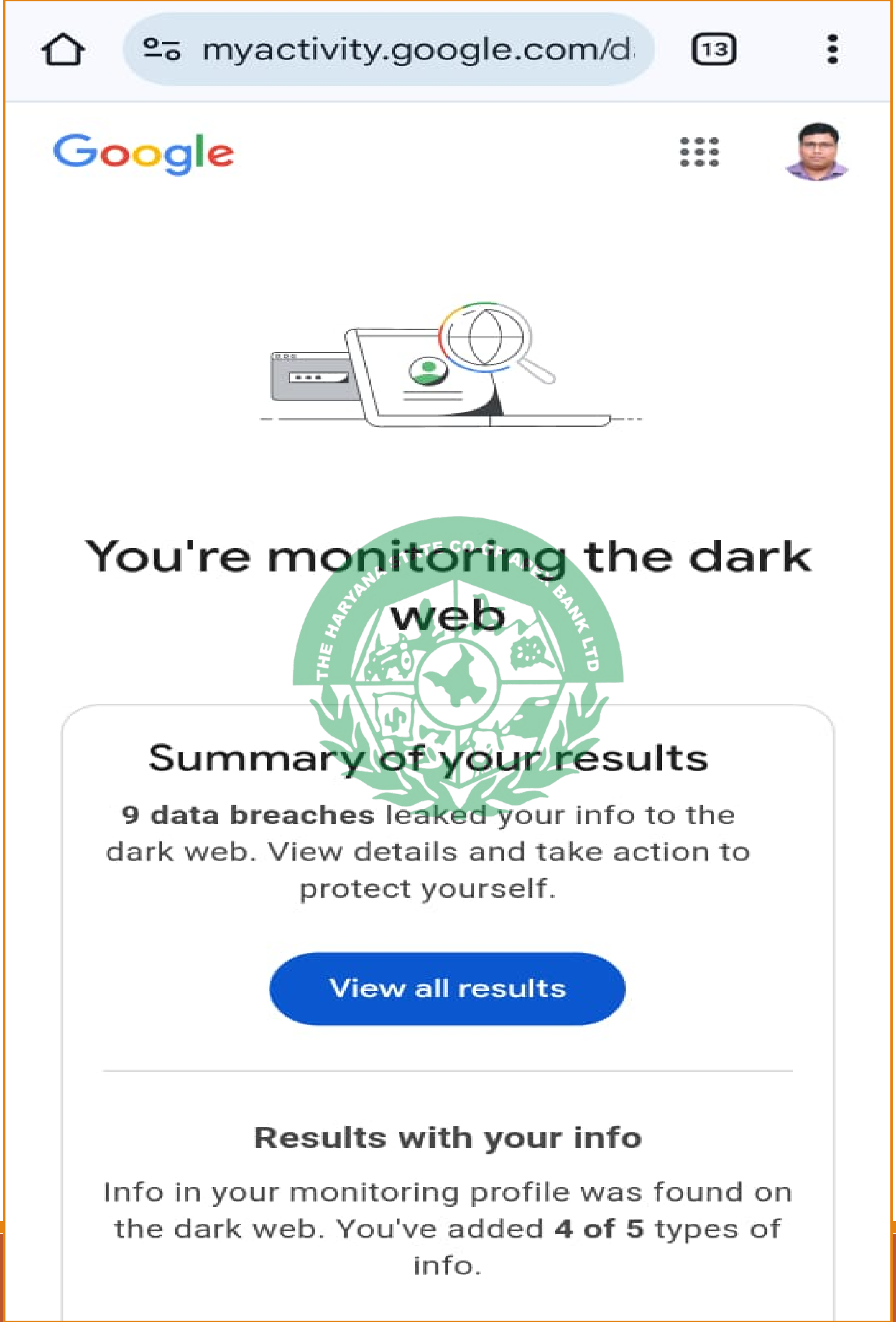
You'll get alerts and guidance when your info is found on the dark web

✓ On

See results

Password Manager

You don't have passwords saved in your Google Account. Password Manager makes it easier to sign in to sites and apps you use on any signed-in device.



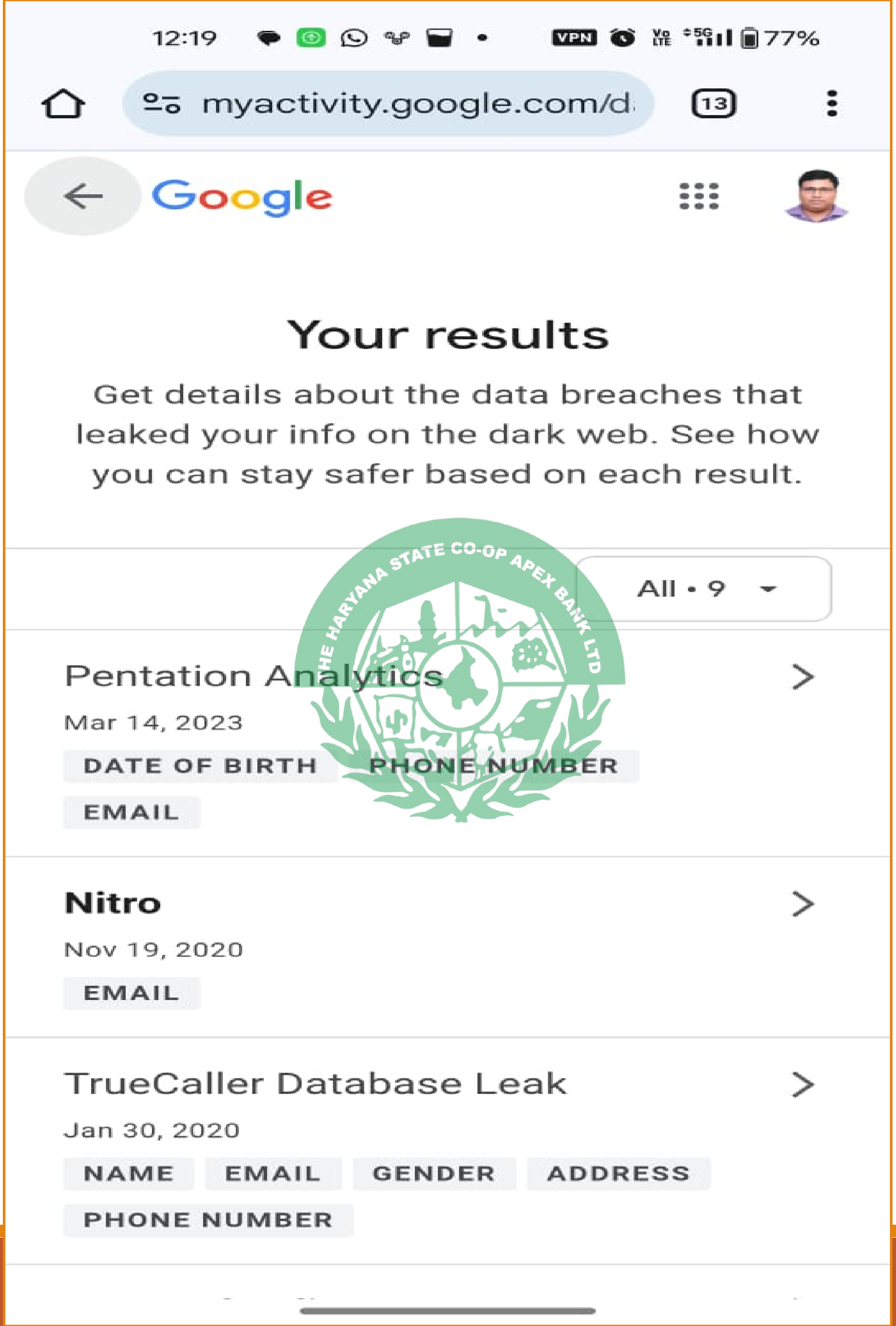
You're monitoring the dark web

Summary of your results

9 data breaches leaked your info to the dark web. View details and take action to protect yourself.

Results with your info

Info in your monitoring profile was found on the dark web. You've added **4 of 5** types of info.



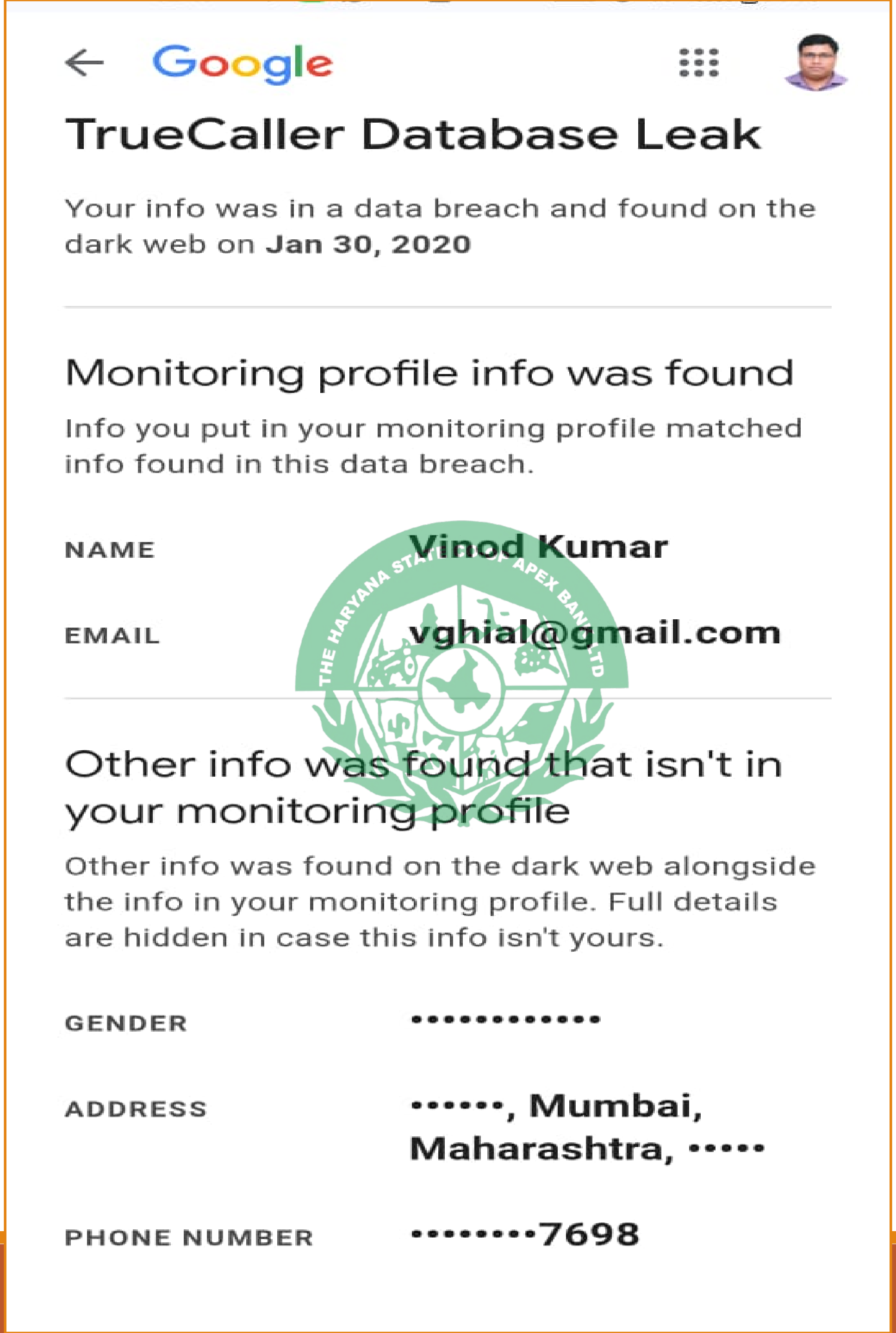
Your results

Get details about the data breaches that leaked your info on the dark web. See how you can stay safer based on each result.

Pentation Analytics
Mar 14, 2023
DATE OF BIRTH PHONE NUMBER
EMAIL

Nitro
Nov 19, 2020
EMAIL

TrueCaller Database Leak
Jan 30, 2020
NAME EMAIL GENDER ADDRESS
PHONE NUMBER



TrueCaller Database Leak

Your info was in a data breach and found on the dark web on **Jan 30, 2020**

Monitoring profile info was found

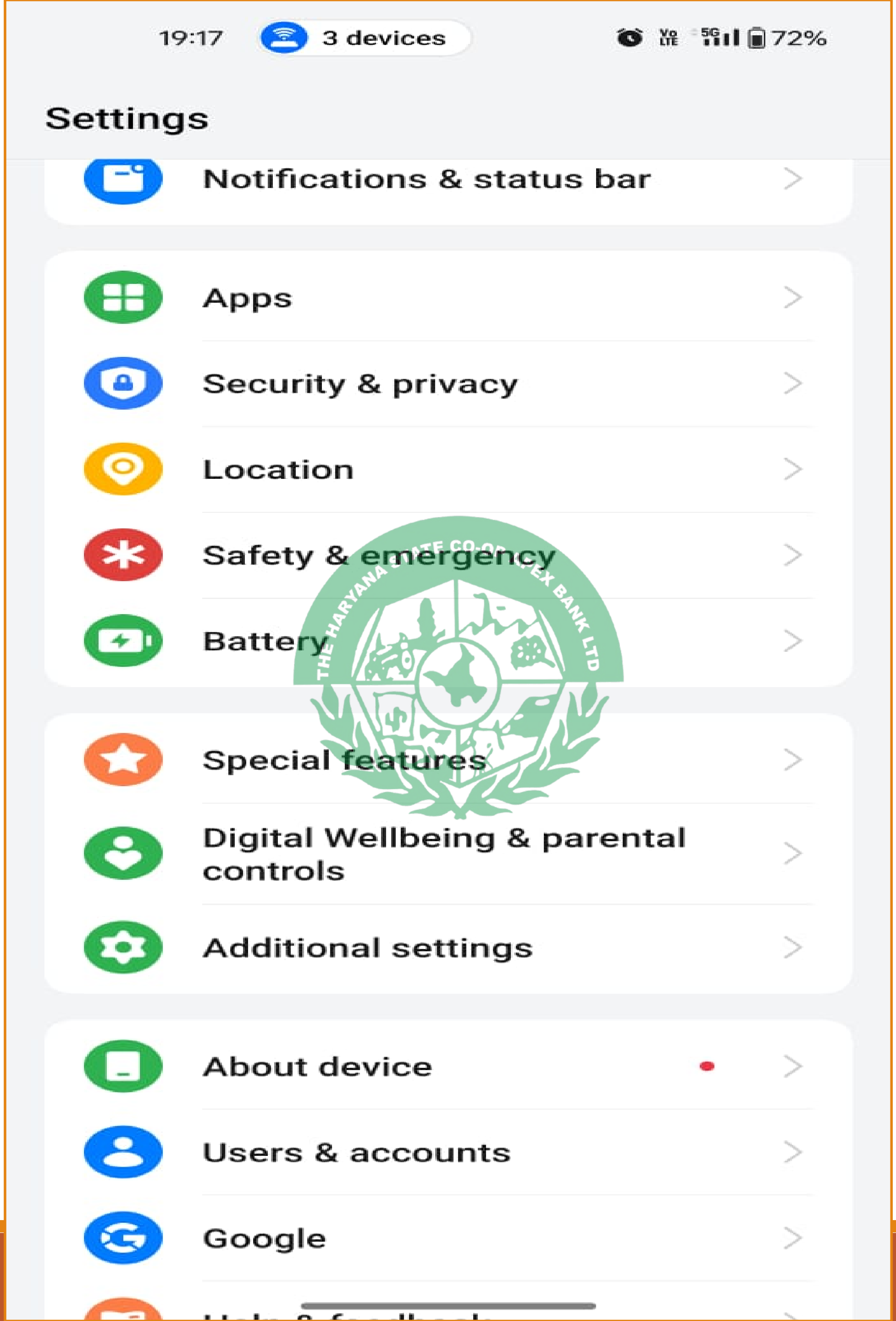
Info you put in your monitoring profile matched info found in this data breach.

NAME	**Vinod Kumar**
EMAIL	**vghial@gmail.com**

Other info was found that isn't in your monitoring profile

Other info was found on the dark web alongside the info in your monitoring profile. Full details are hidden in case this info isn't yours.

GENDER	•••••••••••••
ADDRESS	**••••••, Mumbai, Maharashtra, •••••**
PHONE NUMBER	**••••••••7698**



19:17 3 devices 72%

Settings

Notifications & status bar

Apps

Security & privacy

Location

Safety & emergency

Battery

Special features

Digital Wellbeing & parental controls

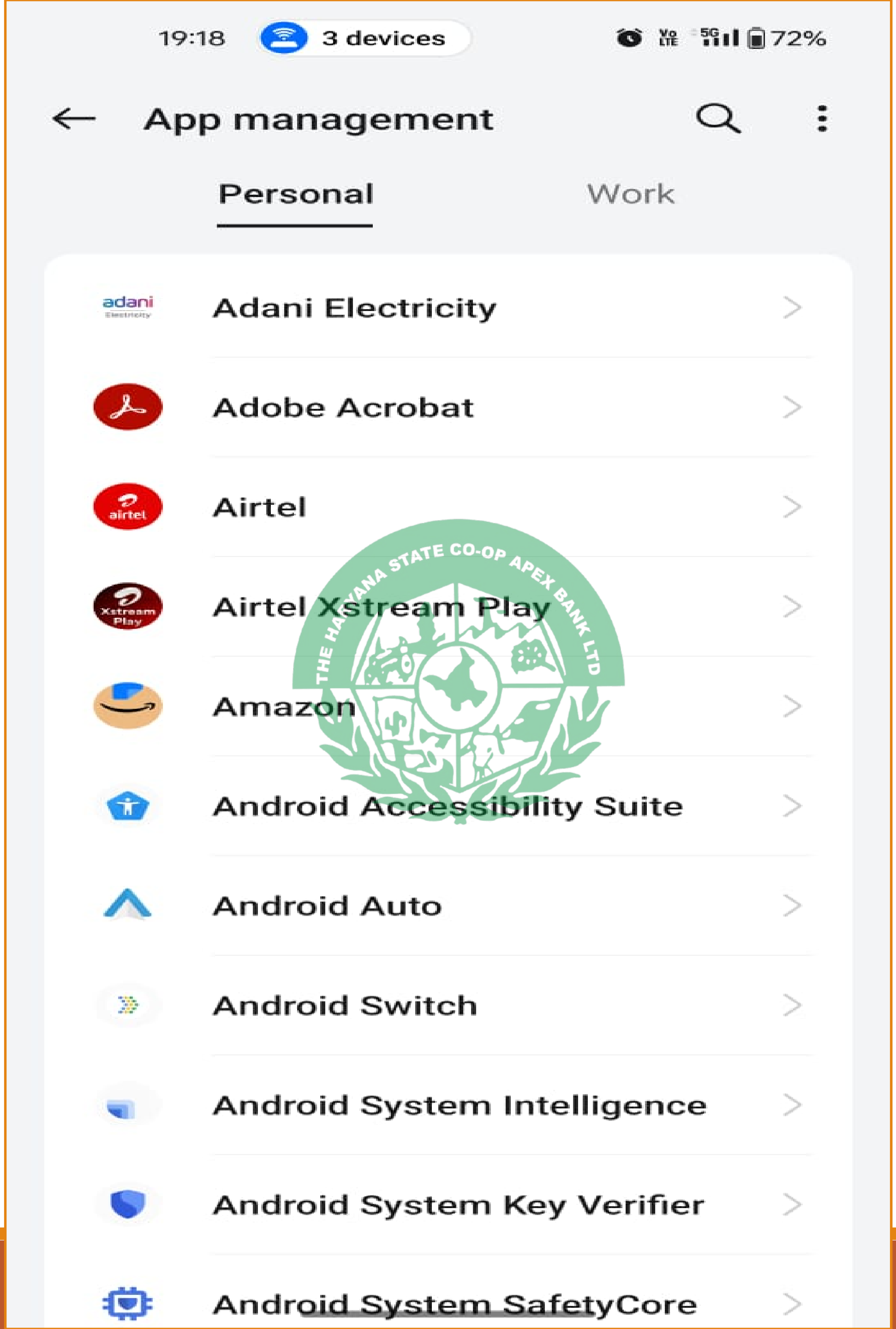
Additional settings

About device

Users & accounts

Google

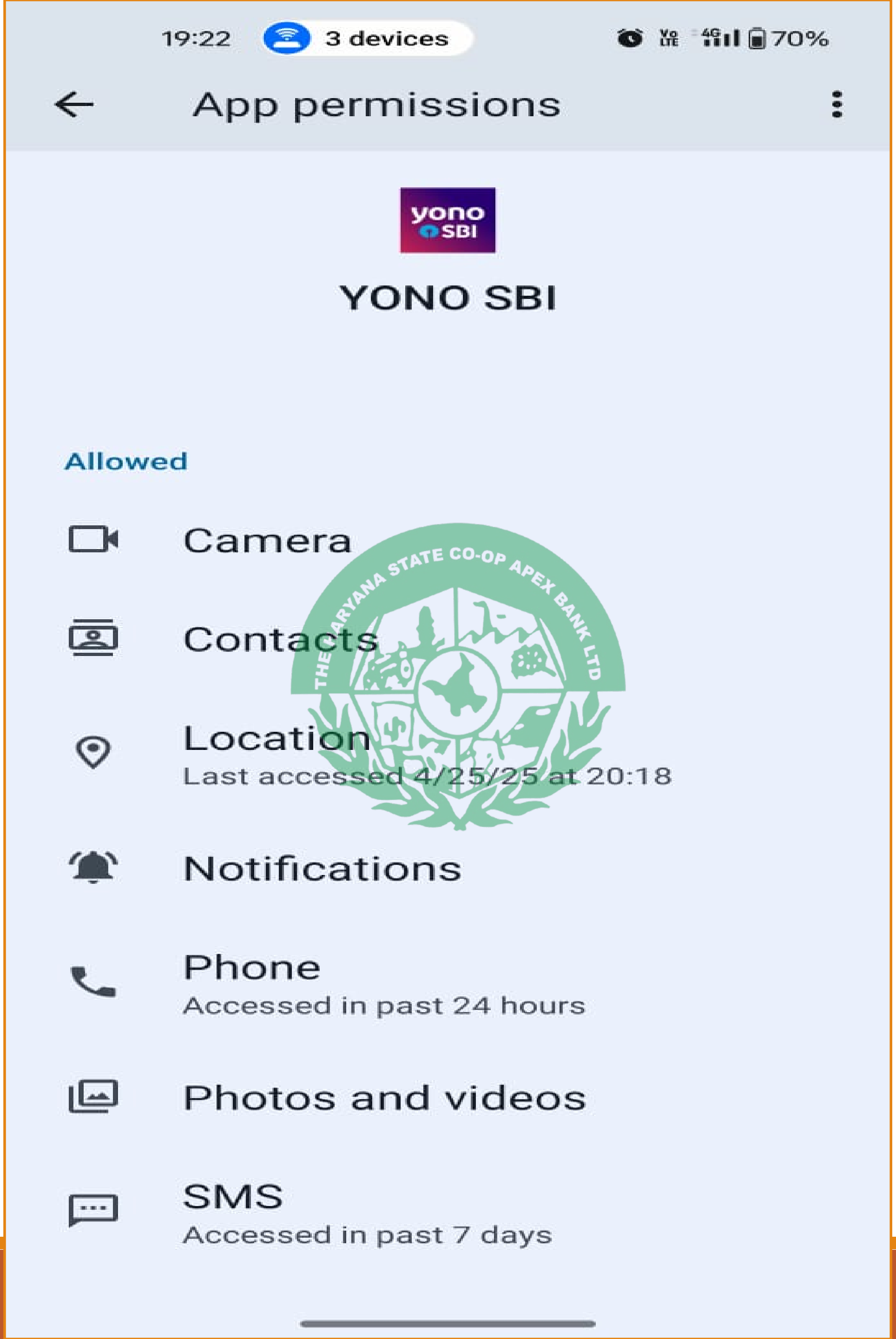
Help & feedback



App management

Personal | Work

- Adani Electricity
- Adobe Acrobat
- Airtel
- Airtel Xstream Play
- Amazon
- Android Accessibility Suite
- Android Auto
- Android Switch
- Android System Intelligence
- Android System Key Verifier
- Android System SafetyCore



App permissions

YONO SBI

Allowed

Camera

Contacts

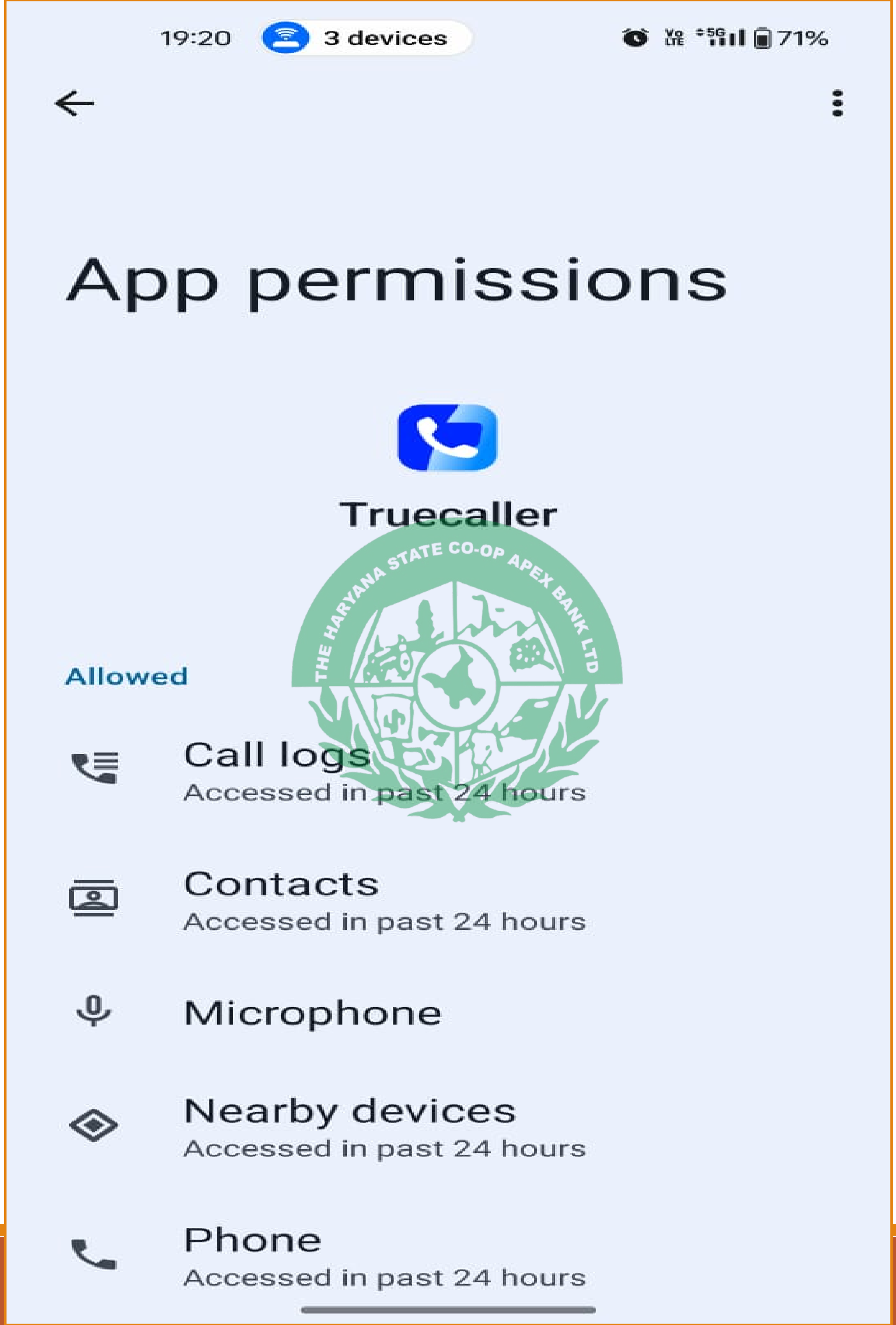
Location
Last accessed 4/25/25 at 20:18

Notifications

Phone
Accessed in past 24 hours

Photos and videos

SMS
Accessed in past 7 days

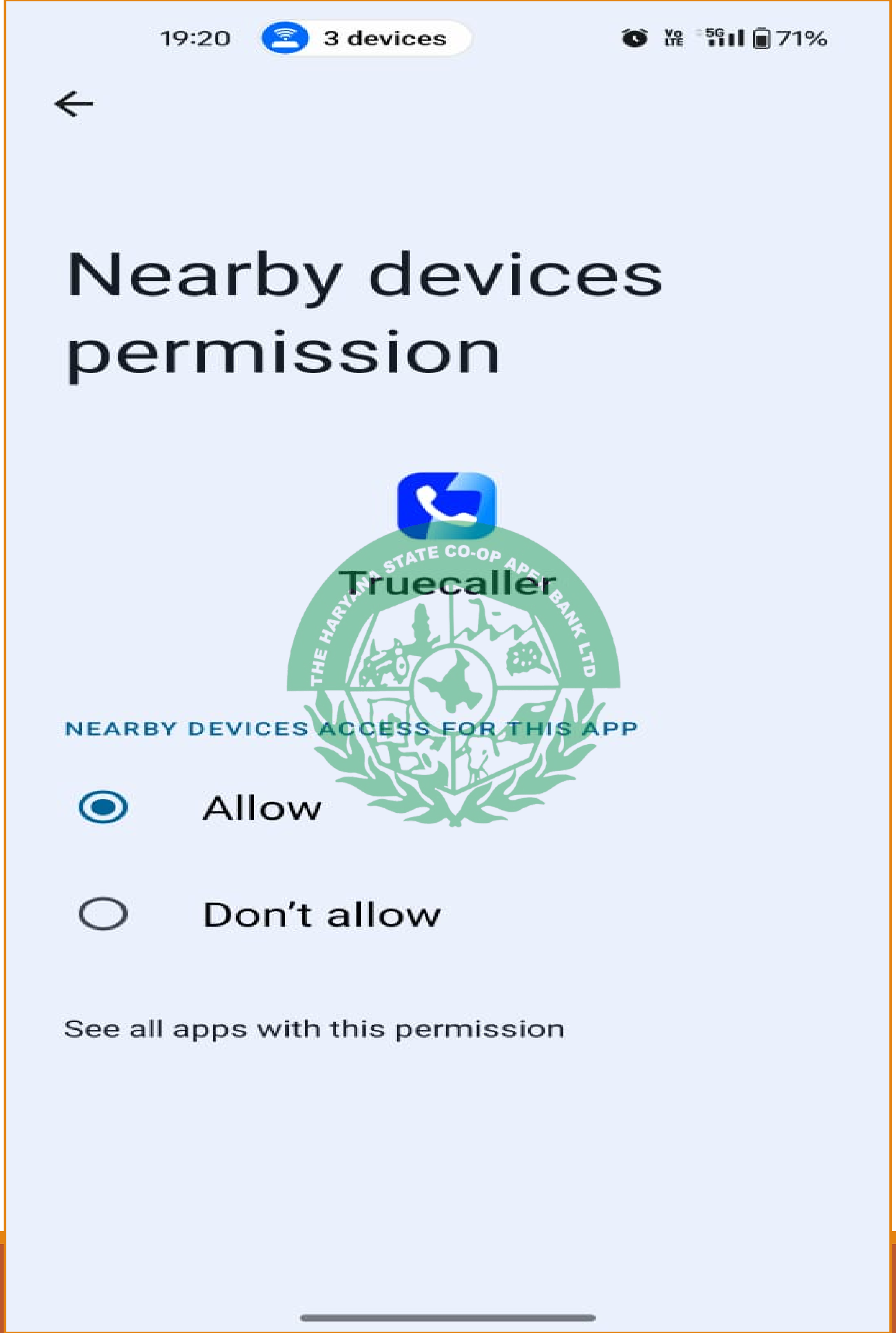


App permissions

Truecaller

Allowed

- Call logs
  Accessed in past 24 hours
- Contacts
  Accessed in past 24 hours
- Microphone
- Nearby devices
  Accessed in past 24 hours
- Phone
  Accessed in past 24 hours



19:20 3 devices 71%

Nearby devices permission

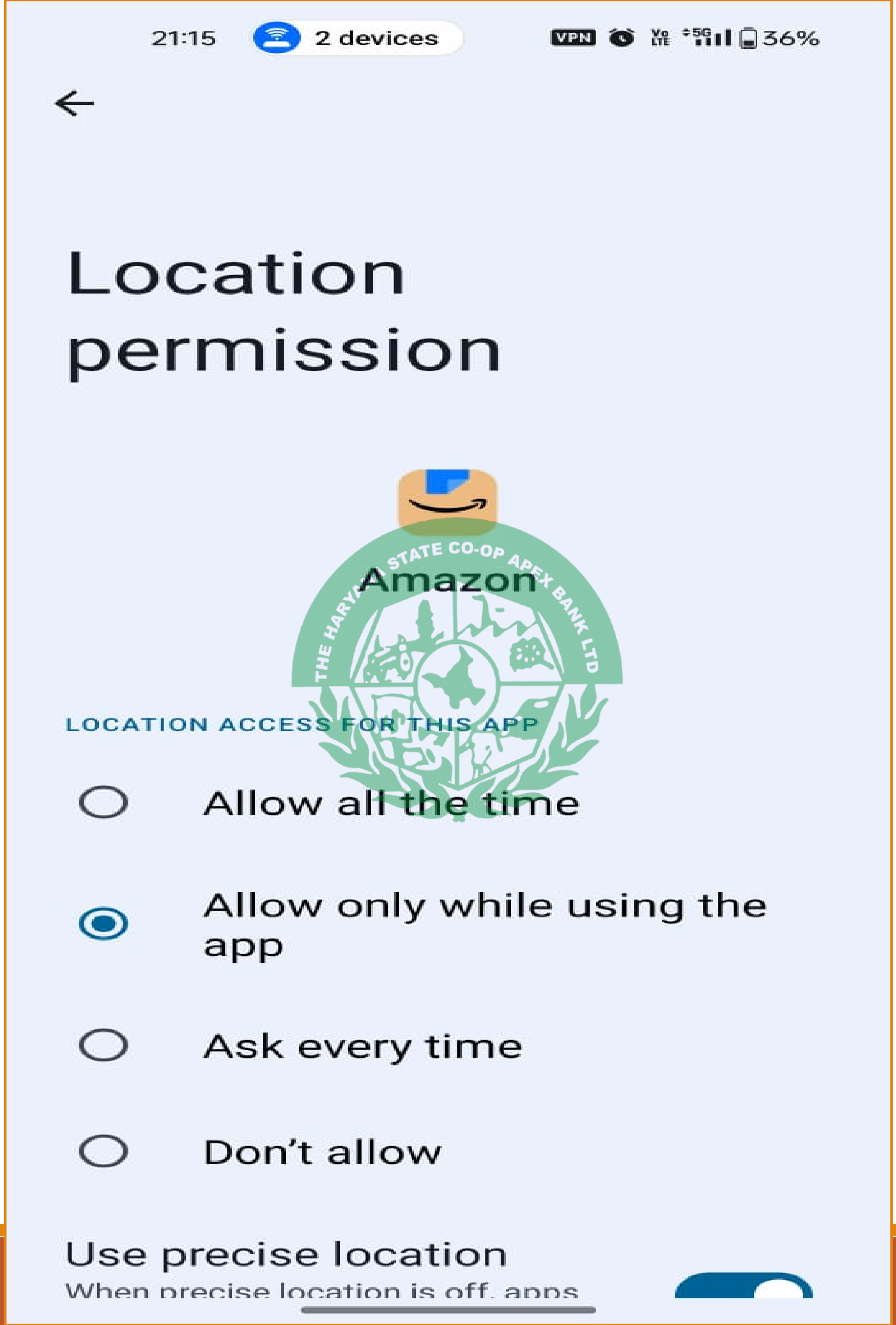
Truecaller

NEARBY DEVICES ACCESS FOR THIS APP

● Allow

○ Don't allow

See all apps with this permission



21:15 2 devices VPN 36%

Location permission

Amazon

LOCATION ACCESS FOR THIS APP

○ Allow all the time

● Allow only while using the app

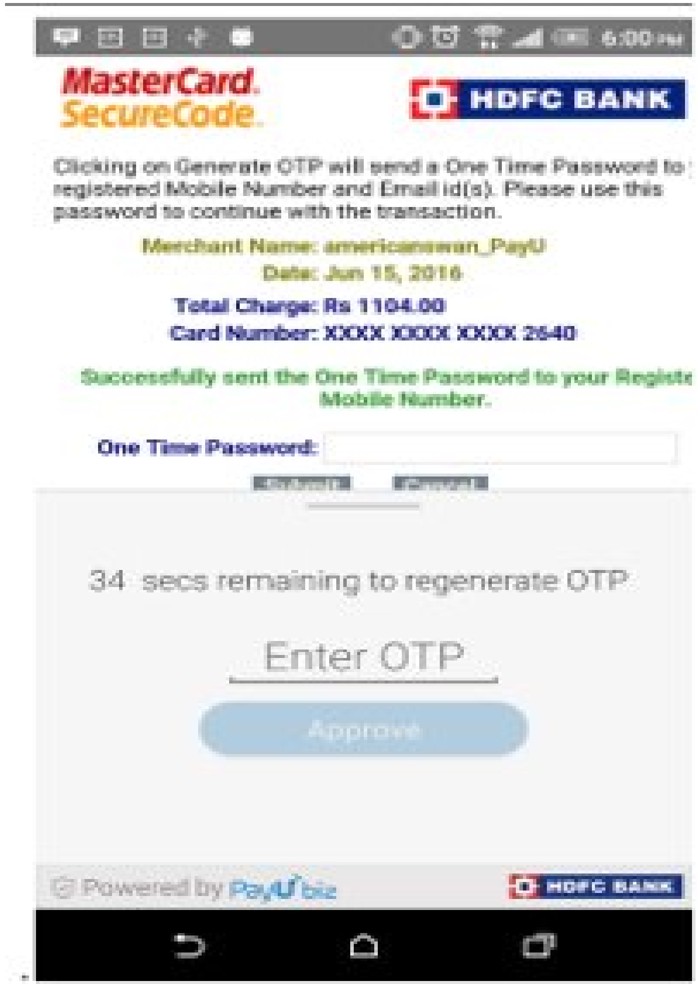
○ Ask every time

○ Don't allow

Use precise location

When precise location is off, apps

Warning States - OTP


6:00 PM

MasterCard SecureCode

HDFC BANK

Clicking on Generate OTP will send a One Time Password to registered Mobile Number and Email id(s). Please use this password to continue with the transaction.

Merchant Name: americanswan_PayU

Date: Jun 15, 2016

Total Charge: Rs 1104.00

Card Number: XXXX XXXX XXXX 2640

Successfully sent the One Time Password to your Registe Mobile Number.

One Time Password:

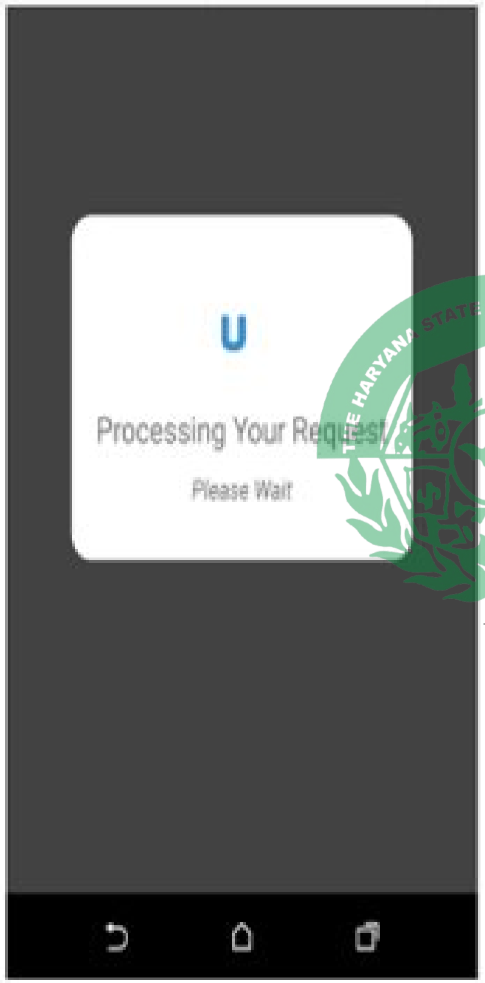
34 secs remaining to regenerate OTP

Enter OTP

Approve

Powered by PayU biz

HDFC BANK


U

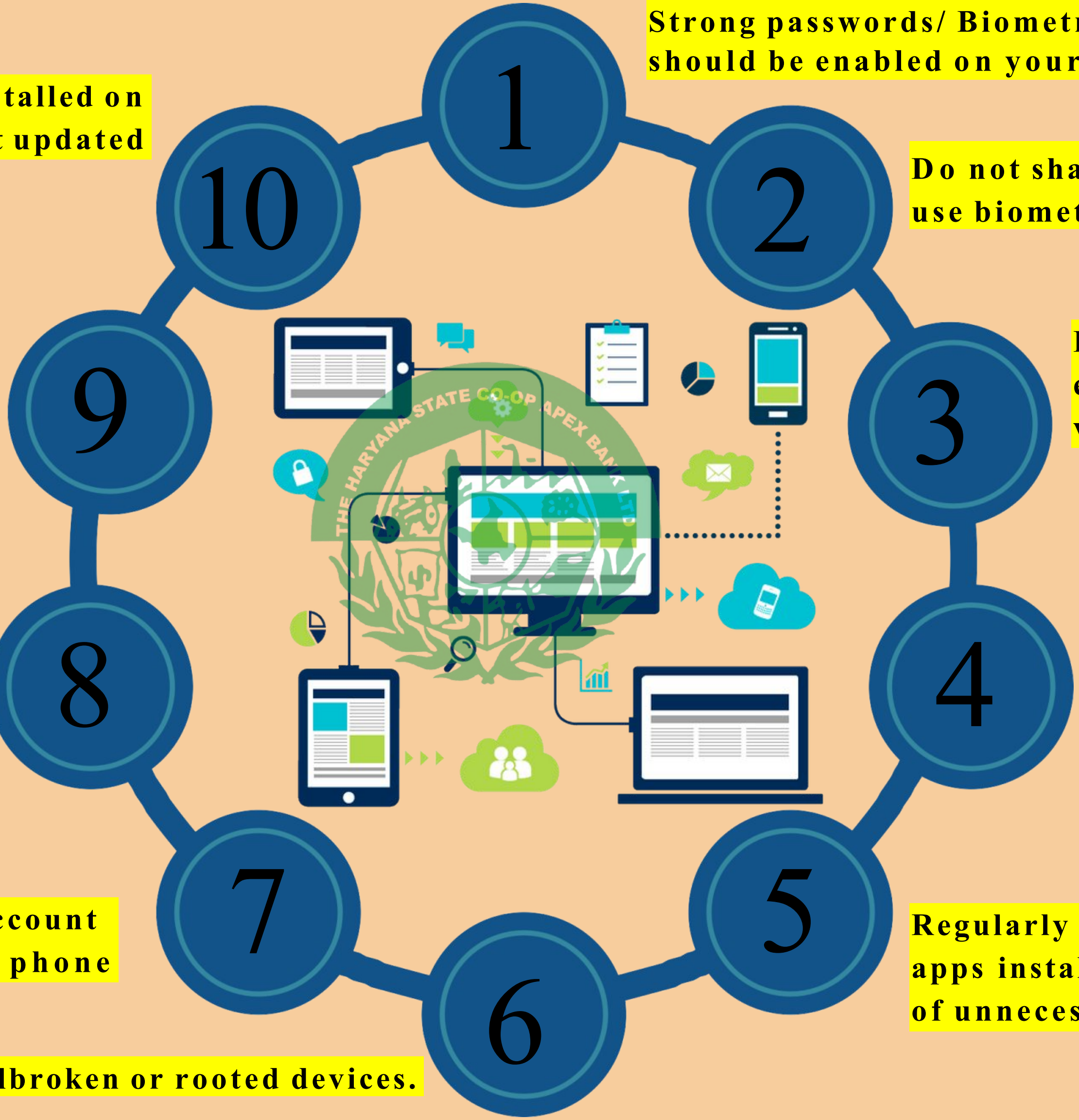
Processing Your Request

Please Wait

- If OTP is filled automatically by your application while performing any transaction or filling any page, it means that the app is having permissions to read your SMS automatically.

- We can disable the **SMS** permission in Permission Manager of the app/browser to disable OTP autofilling.

Mobile Device Best Practices



1. Strong passwords/ Biometric permission should be enabled on your phone, tablets.

2. Do not share your Mobile PIN with anyone, use biometric authentication wherever feasible.

3. Ensure that Auto Updates are enabled for your mobile OS, anti-virus, and applications

4. Avoid installing apps on the devices of unknown persons or through links received in emails, messages or through social media, etc. Applications should be downloaded only through official stores

5. Regularly monitor the permissions of critical apps installed in your mobile and keep a track of unnecessary and unused apps.

6. Never use Banking apps on jailbroken or rooted devices.

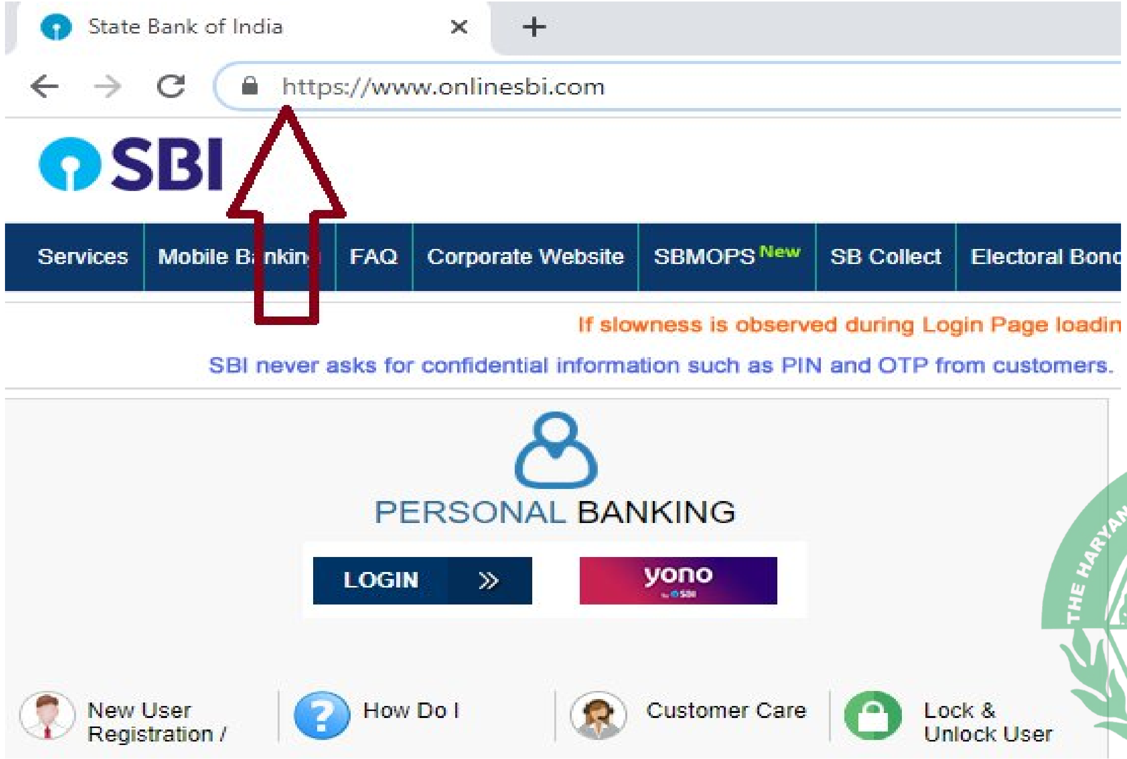
7. Do not store your Bank account number or PIN on mobile phone

8. Report the loss of mobile phone to the Bank to disable Mobile Banking services.

9. Avoid connecting phones to public wireless networks.

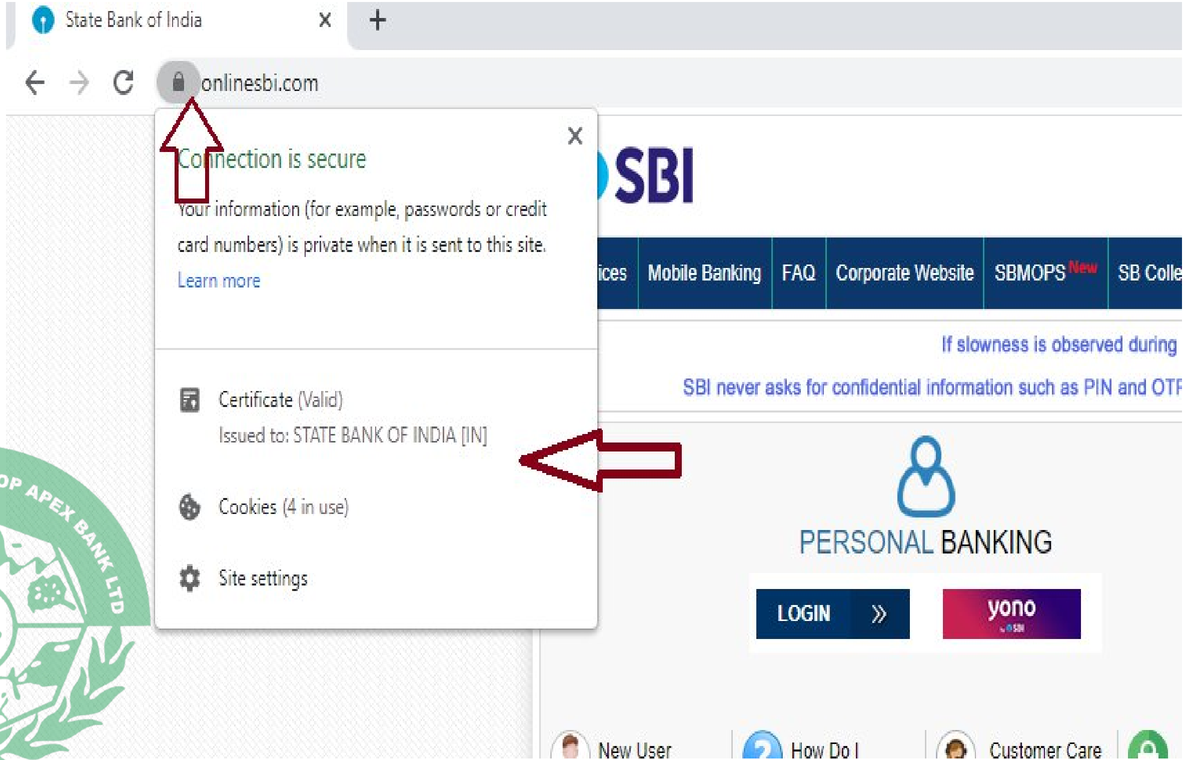
10. Get an anti-virus software installed on your mobile and keep it updated

Access Digital Banking securely.



If slowness is observed during Login Page loadin

SBI never asks for confidential information such as PIN and OTP from customers.



Connection is secure

Your information (for example, passwords or credit card numbers) is private when it is sent to this site.

Certificate (Valid)

Issued to: STATE BANK OF INDIA [IN]

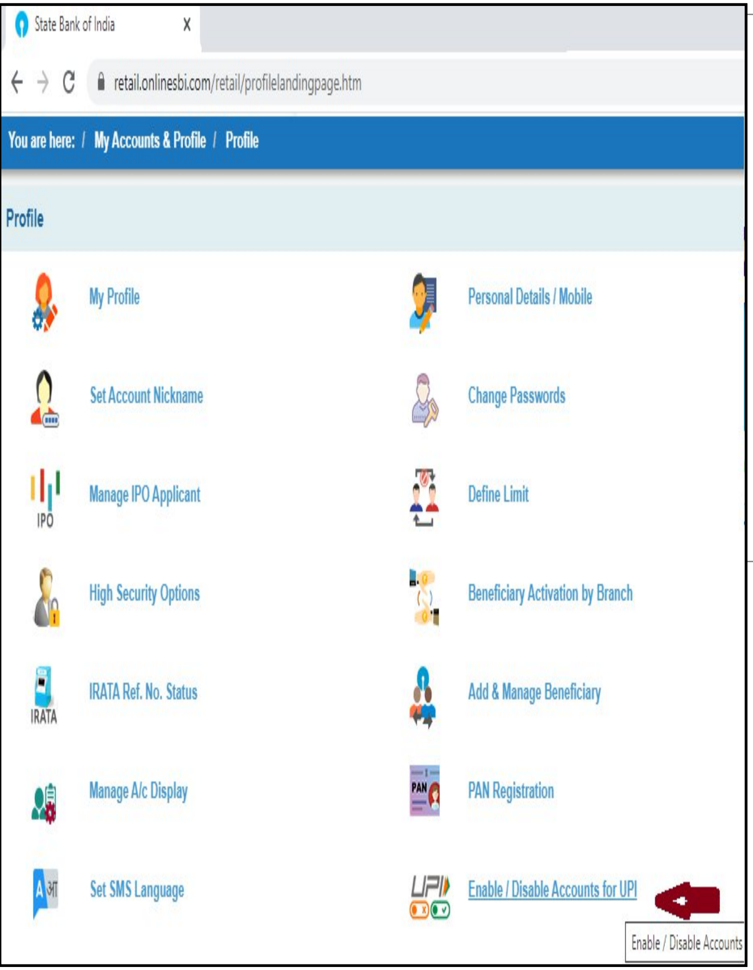
If slowness is observed during

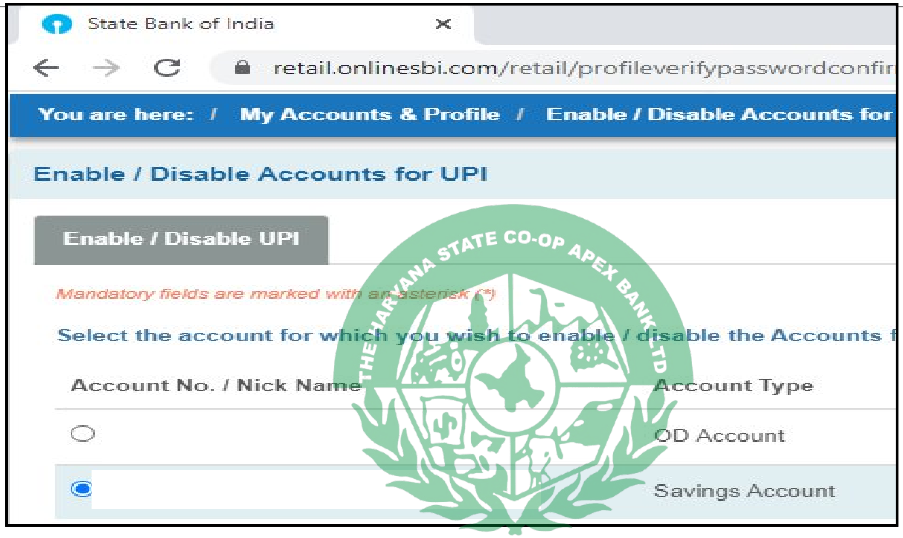
SBI never asks for confidential information such as PIN and OTP

1. Remember URL of the Bank
2. Check for "HTTPS" in the URL
3. Click on the pad lock and verify the certificate.
4. Make sure the certificate is issued to " STATE BANK OF INDIA [IN].
5. Please check the spelling and character of "SBI".

UPI Security

Enable and Disable UPI-

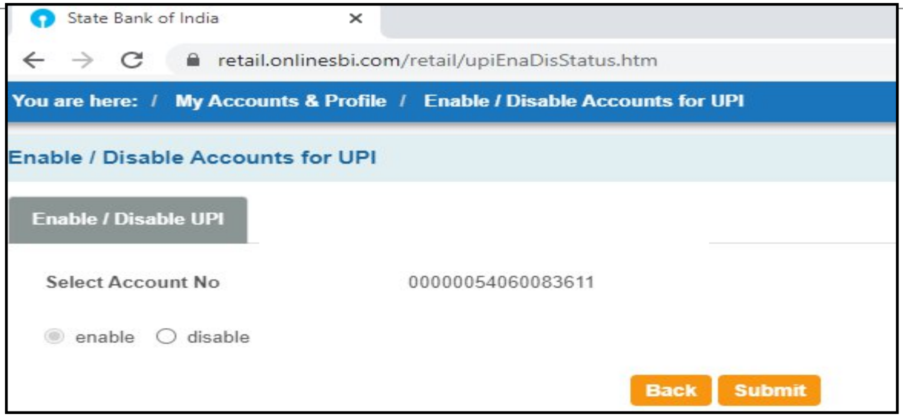



State Bank of India
retail.onlinesbi.com/retail/profileverifypasswordconfir
You are here: / My Accounts & Profile / Enable / Disable Accounts for
Enable / Disable Accounts for UPI
Enable / Disable UPI

Mandatory fields are marked with an asterisk (*)

Select the account for which you wish to enable / disable the Accounts f

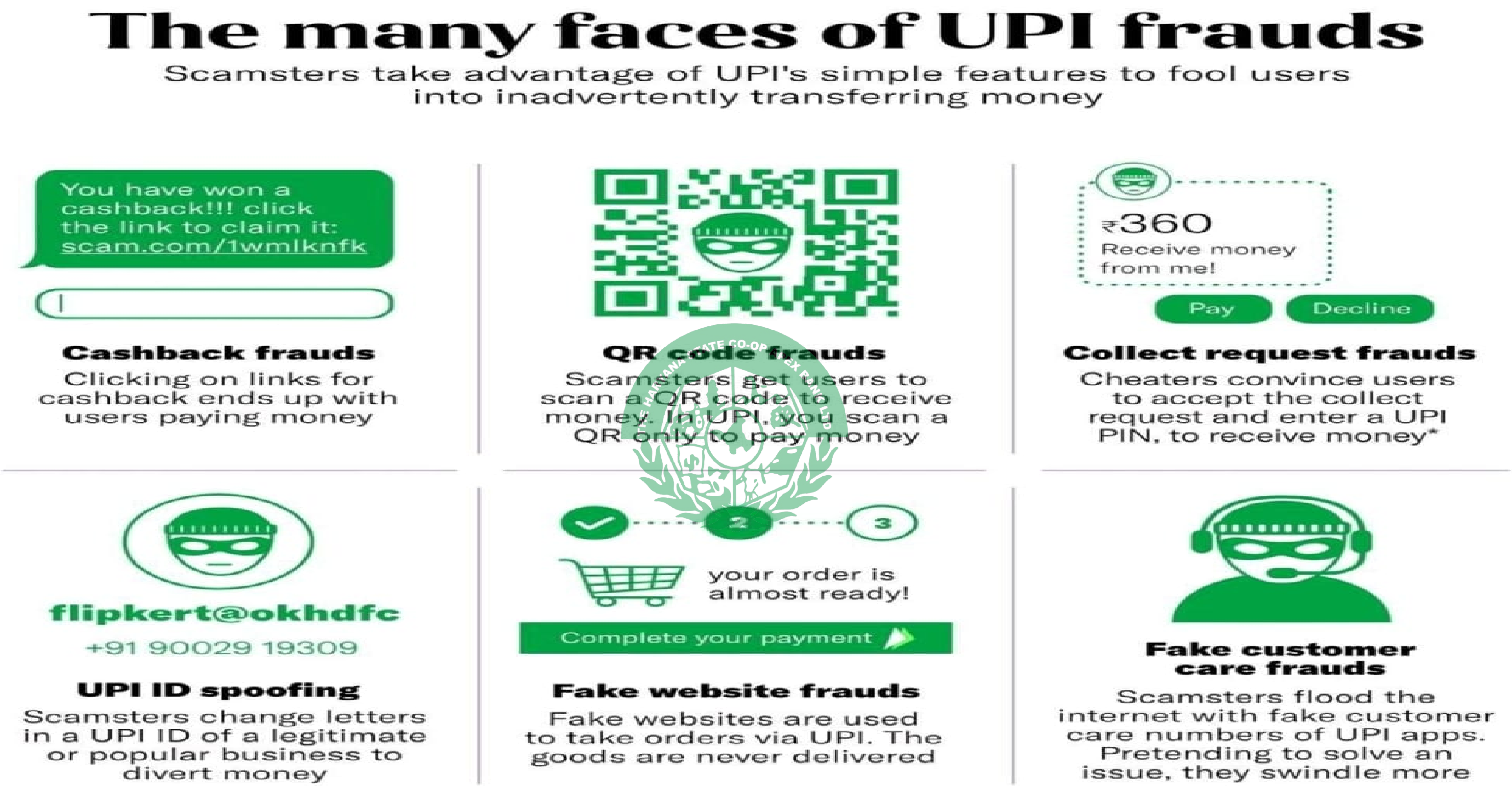
Account No. / Nick Name	Account Type
○	OD Account
●	Savings Account


State Bank of India
retail.onlinesbi.com/retail/upiEnaDisStatus.htm
You are here: / My Accounts & Profile / Enable / Disable Accounts for UPI
Enable / Disable Accounts for UPI
Enable / Disable UPI
Back
Submit

Select Account No 00000054060083611

● enable ○ disable

Disable your UPI if you notice any fraud which has happened through UPI platform or your PIN is compromised.



The many faces of UPI frauds

Scamsters take advantage of UPI's simple features to fool users into inadvertently transferring money

You have won a cashback!!! click the link to claim it: scam.com/1wmlknfk

Cashback frauds

Clicking on links for cashback ends up with users paying money

QR code frauds

Scamsters get users to scan a QR code to receive money. In UPI, you scan a QR only to pay money

₹360

Receive money from me!

Collect request frauds

Cheaters convince users to accept the collect request and enter a UPI PIN, to receive money*

flipkert@okhdfc

+91 90029 19309

UPI ID spoofing

Scamsters change letters in a UPI ID of a legitimate or popular business to divert money

your order is almost ready!

Fake website frauds

Fake websites are used to take orders via UPI. The goods are never delivered

Fake customer care frauds

Scamsters flood the internet with fake customer care numbers of UPI apps. Pretending to solve an issue, they swindle more

Reporting of Cyber Crime

SBI
The banker to every Indian
JOIN THE FIGHT AGAINST
CYBER CRIME.
DON'T LET IT GO UNREPORTED.
गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Report complaints related to Cyber Frauds at National Cyber Crime Reporting Portal of Ministry of Home Affairs:

https://cybercrime.gov.in

Or dial the helpline number: **155260**

Please educate our Customers and General Public

Report complaints related to Cyber Frauds @ gov website

https://cybercrime.gov.in

Or dial the helpline number

155260

[redacted]

Internet Safety Tips

- Keep and eye on unknown apps from your phone. Uninstall if not required.
- DO NOT WRITE down your passwords and security questions.
- Do NOT CLICK on bumper festive offers links in Whatsapp messages/ SMSs or emails.
- Always lookup Customer care numbers from official websites. Or save them on your phone for future use.

ATM Safety Tips

- Don’t get distracted

- Never withdraw in hurry.

- Keep your Hands Empty

- Cover Keypad with other hand while input PIN.

Savdhaan Rahe! Satark Rahe!

Always check for a secure payment gateway.

Never open emails from unknown sources containing suspicious attachment or phishing links.

Change passwords at regular intervals.

Change passwords periodically.

Keep your PIN, password, and credit or debit card number, CVV private.

Do not leave your device unlocked.

Always use virtual keyboard on public devices since the keystrokes can also be captured through compromised devices, keyboard, etc.

Avoid saving details on websites /devices/ public laptop / desktops.

Do not share private information to unknown persons on social media.

Do not use same passwords for email and internet banking

Turn on two-factor authentication where facility is available.

Always scan unknown USB drives / devices before usage.

Install antivirus on the device and install updates whenever available.

How to Make an Online Complaint?

Complaint to RBI

➢ Please visit the link at https://cms.rbi.org.in/

Complaint to SEBI

➢ Please visit the link at https://scores.gov.in/

Complaint to IRDAI

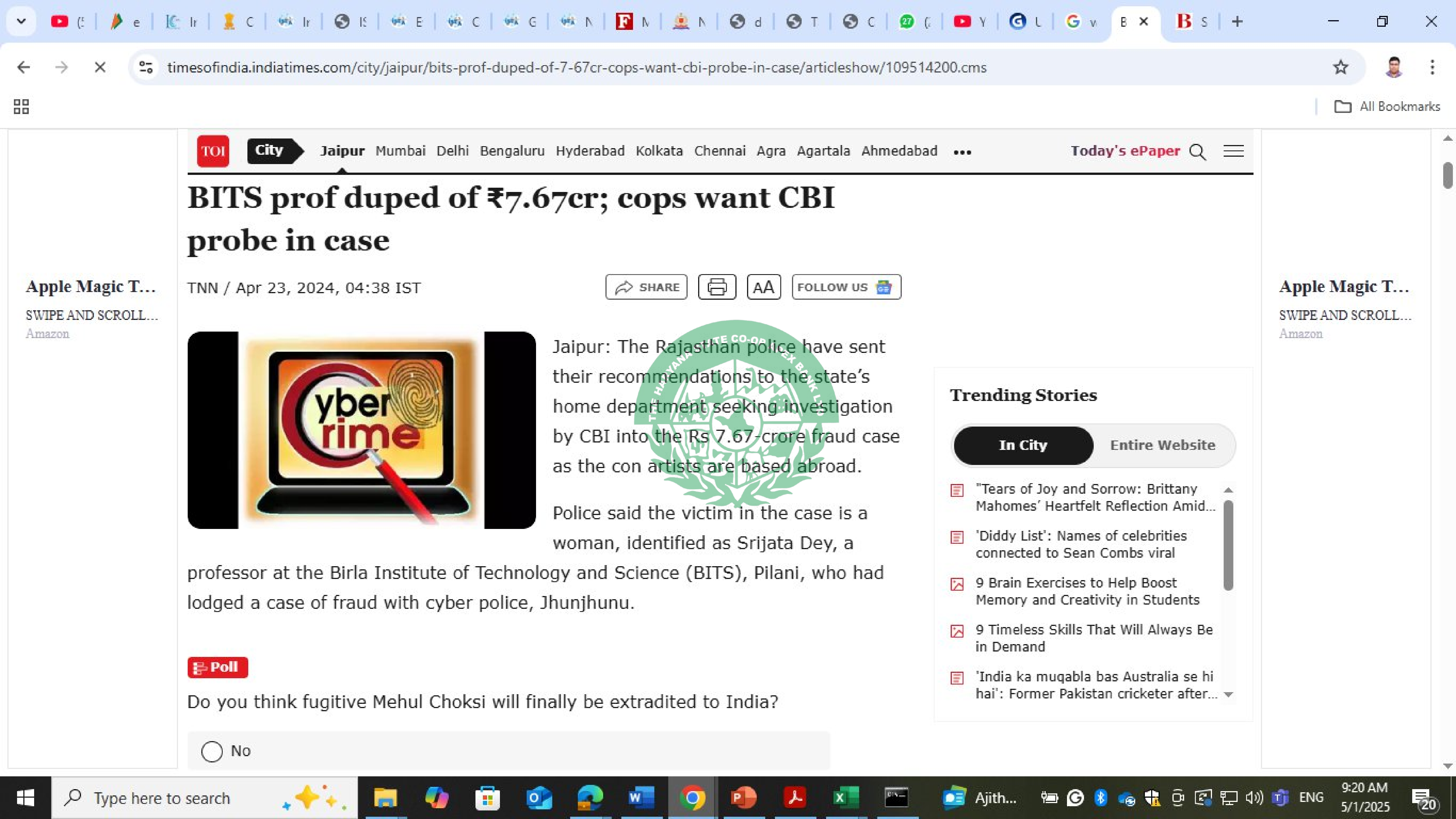
➢ Please visit the link at https://igms.irda.gov.in/

Complaint to National Housing Bank (NHB)

➢ Please visit the link at https://grids.nhbonline.org.in/

Complaint to Cyber Police Station

➢ Please visit https://cybercrime.gov.in/



BITS prof duped of ₹7.67cr; cops want CBI probe in case

TNN / Apr 23, 2024, 04:38 IST

Jaipur: The Rajasthan police have sent their recommendations to the state's home department seeking investigation by CBI into the Rs 7.67-crore fraud case as the con artists are based abroad.

Police said the victim in the case is a woman, identified as Srijata Dey, a professor at the Birla Institute of Technology and Science (BITS), Pilani, who had lodged a case of fraud with cyber police, Jhunjhunu.

Poll

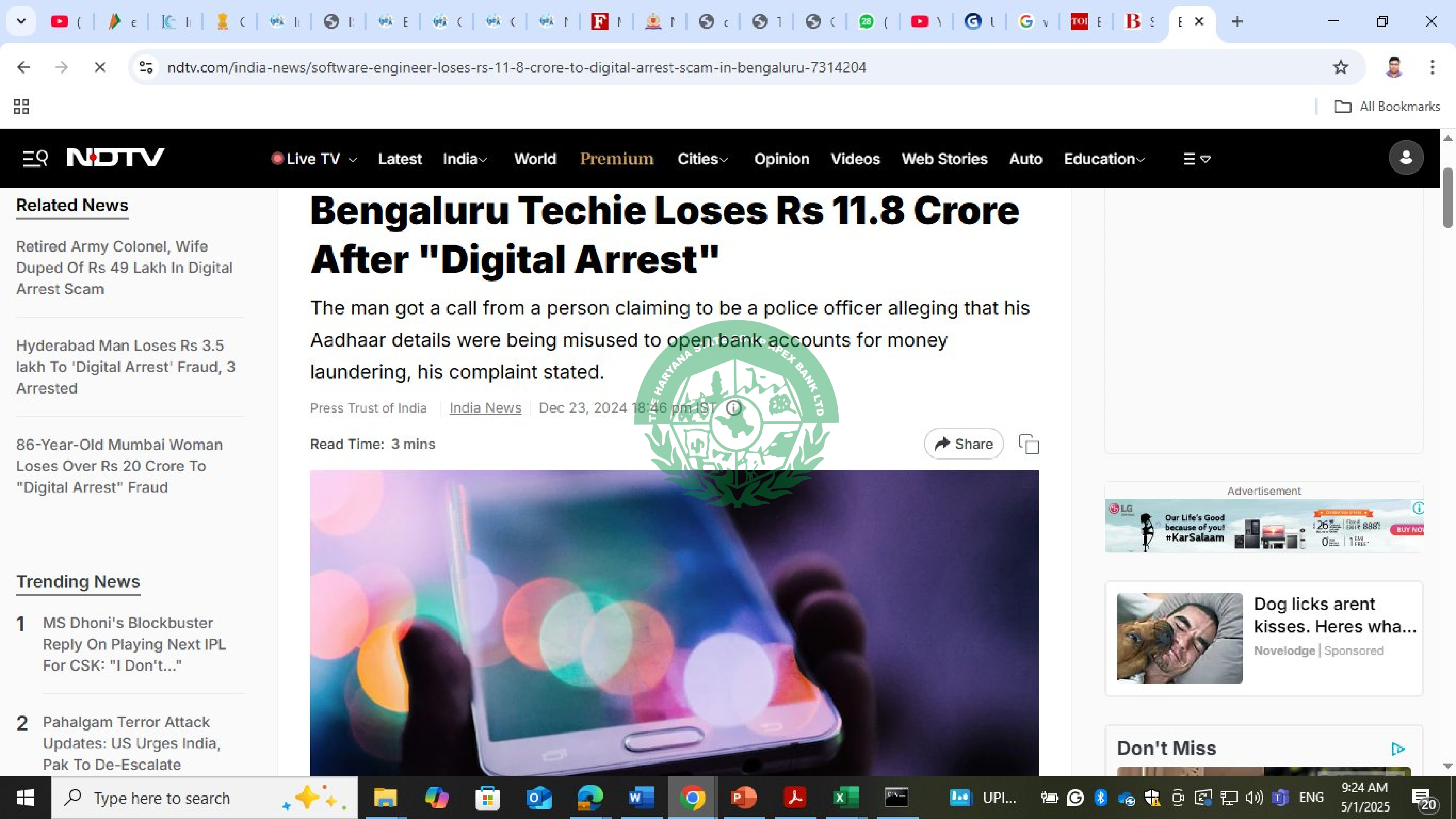
Do you think fugitive Mehul Choksi will finally be extradited to India?

○ No

Trending Stories

In City | Entire Website

- "Tears of Joy and Sorrow: Brittany Mahomes' Heartfelt Reflection Amid...
- 'Diddy List': Names of celebrities connected to Sean Combs viral
- 9 Brain Exercises to Help Boost Memory and Creativity in Students
- 9 Timeless Skills That Will Always Be in Demand
- 'India ka muqabla bas Australia se hi hai': Former Pakistan cricketer after...



Related News

Retired Army Colonel, Wife Duped Of Rs 49 Lakh In Digital Arrest Scam

Hyderabad Man Loses Rs 3.5 lakh To 'Digital Arrest' Fraud, 3 Arrested

86-Year-Old Mumbai Woman Loses Over Rs 20 Crore To "Digital Arrest" Fraud

Trending News

1 MS Dhoni's Blockbuster Reply On Playing Next IPL For CSK: "I Don't..."

2 Pahalgam Terror Attack Updates: US Urges India, Pak To De-Escalate

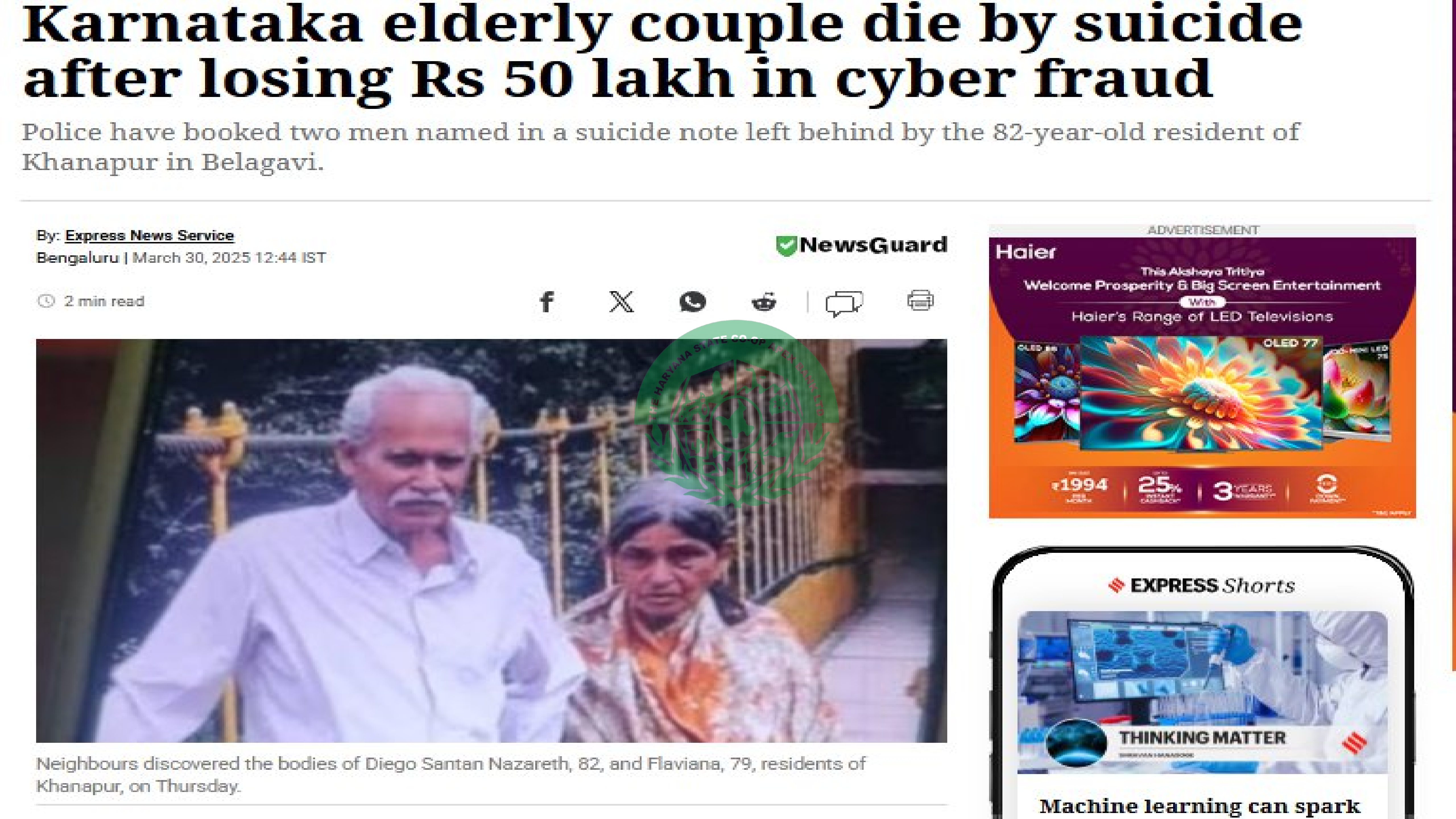
Bengaluru Techie Loses Rs 11.8 Crore After "Digital Arrest"

The man got a call from a person claiming to be a police officer alleging that his Aadhaar details were being misused to open bank accounts for money laundering, his complaint stated.

Press Trust of India | India News | Dec 23, 2024 18:46 pm IST

Read Time: 3 mins

Don't Miss



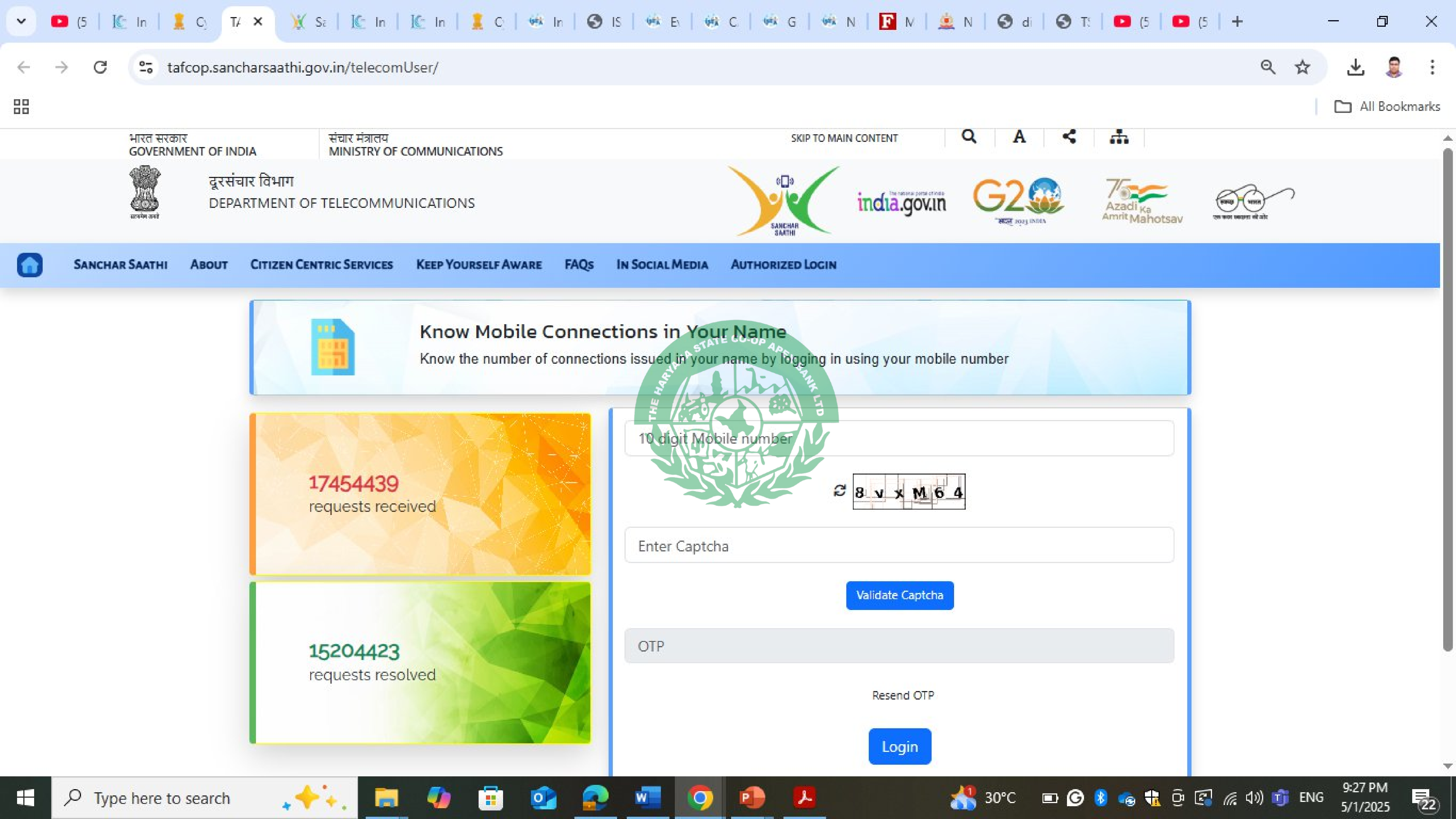
Karnataka elderly couple die by suicide after losing Rs 50 lakh in cyber fraud

Police have booked two men named in a suicide note left behind by the 82-year-old resident of Khanapur in Belagavi.

By: Express News Service
Bengaluru | March 30, 2025 12:44 IST

Neighbours discovered the bodies of Diego Santan Nazareth, 82, and Flaviana, 79, residents of Khanapur, on Thursday.

Machine learning can spark



भारत सरकार
GOVERNMENT OF INDIA

संचार मंत्रालय
MINISTRY OF COMMUNICATIONS

दूरसंचार विभाग
DEPARTMENT OF TELECOMMUNICATIONS

Know Mobile Connections in Your Name

Know the number of connections issued in your name by logging in using your mobile number

17454439
requests received

15204423
requests resolved

10 digit Mobile number

8 v x M 6 4

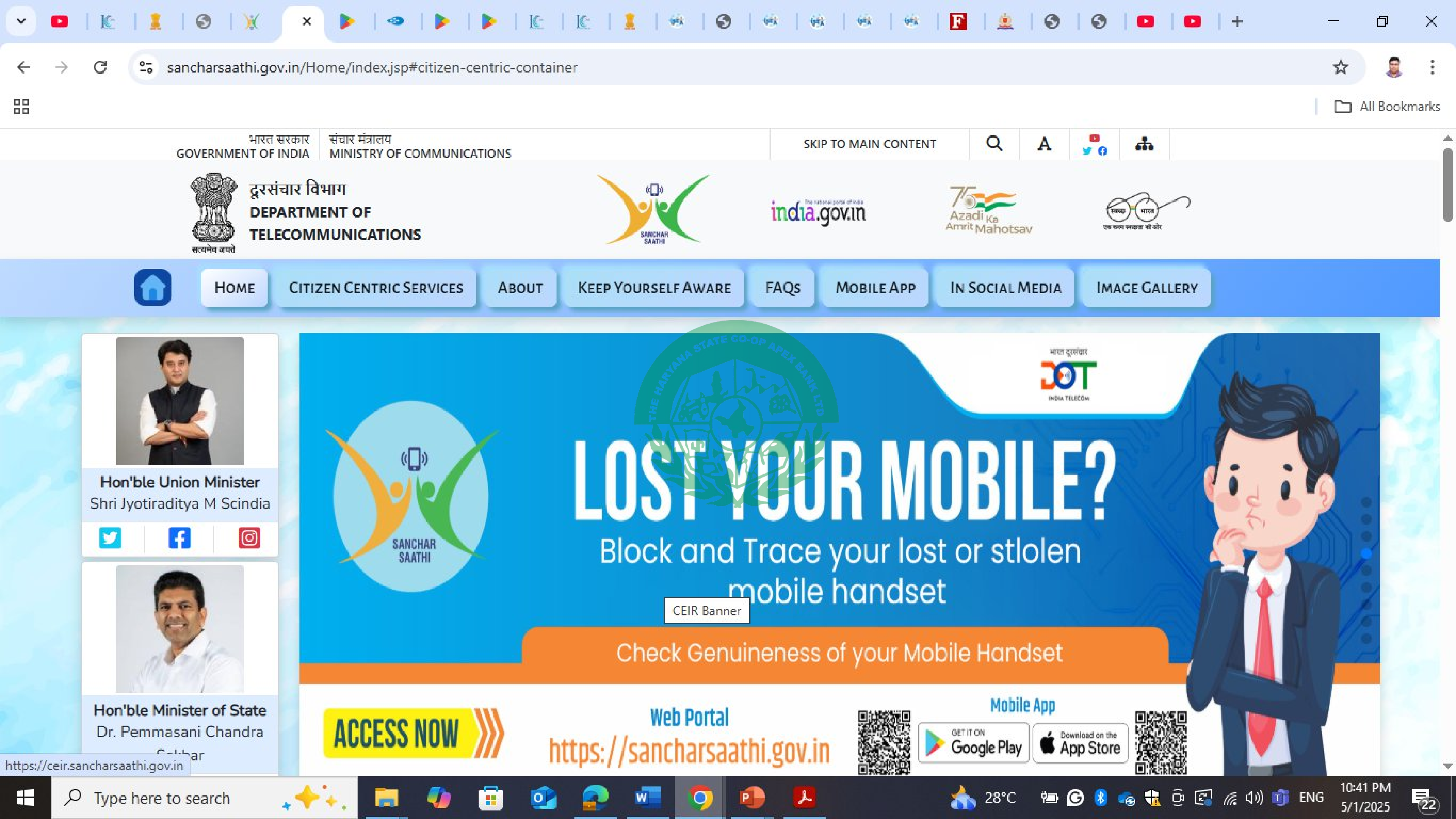
Enter Captcha

Validate Captcha

OTP

Resend OTP

Login



Hon'ble Union Minister
Shri Jyotiraditya M Scindia

Hon'ble Minister of State
Dr. Pemmasani Chandra Sekhar

LOST YOUR MOBILE?

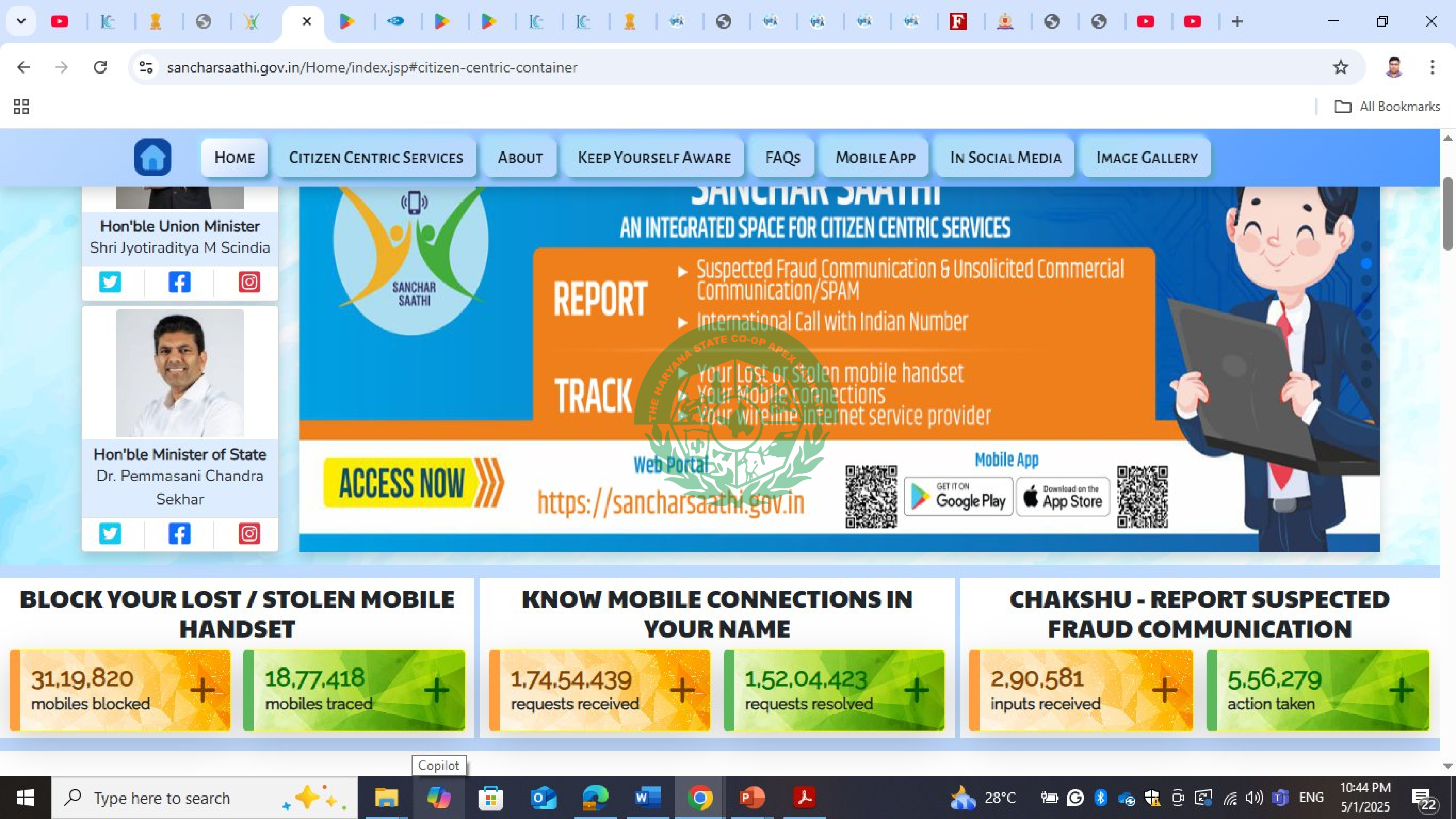
Block and Trace your lost or stlolen mobile handset

Check Genuineness of your Mobile Handset

ACCESS NOW

Web Portal
https://sancharsaathi.gov.in

Mobile App



sancharsaathi.gov.in/Home/index.jsp#citizen-centric-container

Hon'ble Union Minister
Shri Jyotiraditya M Scindia

Hon'ble Minister of State
Dr. Pemmasani Chandra Sekhar

SANCHAR SAATHI

AN INTEGRATED SPACE FOR CITIZEN CENTRIC SERVICES

REPORT
- Suspected Fraud Communication & Unsolicited Commercial Communication/SPAM
- International Call with Indian Number

TRACK
- Your Lost or Stolen mobile handset
- Your Mobile connections
- Your wireline internet service provider

BLOCK YOUR LOST / STOLEN MOBILE HANDSET

31,19,820 mobiles blocked

18,77,418 mobiles traced

KNOW MOBILE CONNECTIONS IN YOUR NAME

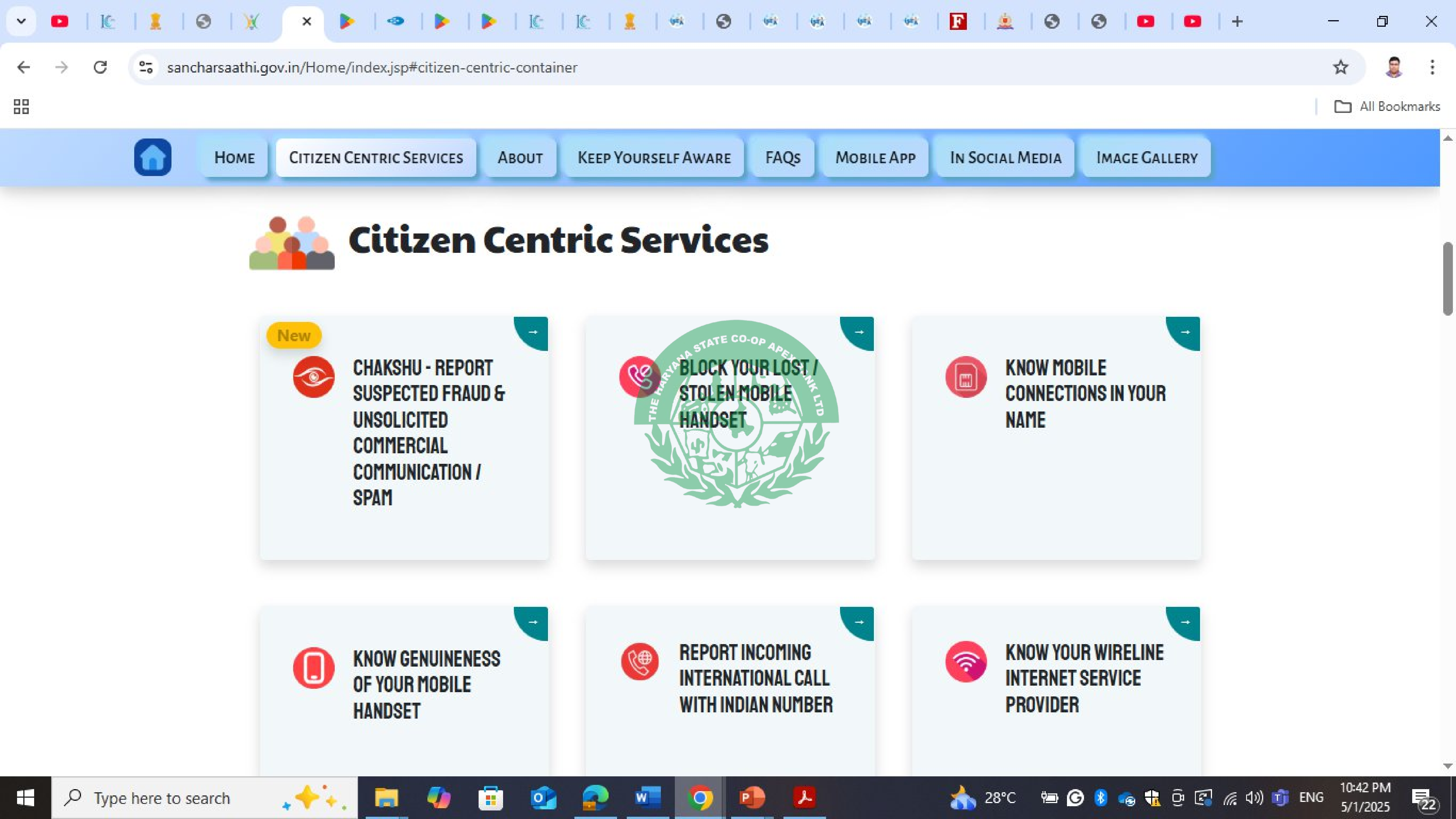
1,74,54,439 requests received

1,52,04,423 requests resolved

CHAKSHU - REPORT SUSPECTED FRAUD COMMUNICATION

2,90,581 inputs received

5,56,279 action taken



Citizen Centric Services

New

CHAKSHU - REPORT SUSPECTED FRAUD & UNSOLICITED COMMERCIAL COMMUNICATION / SPAM

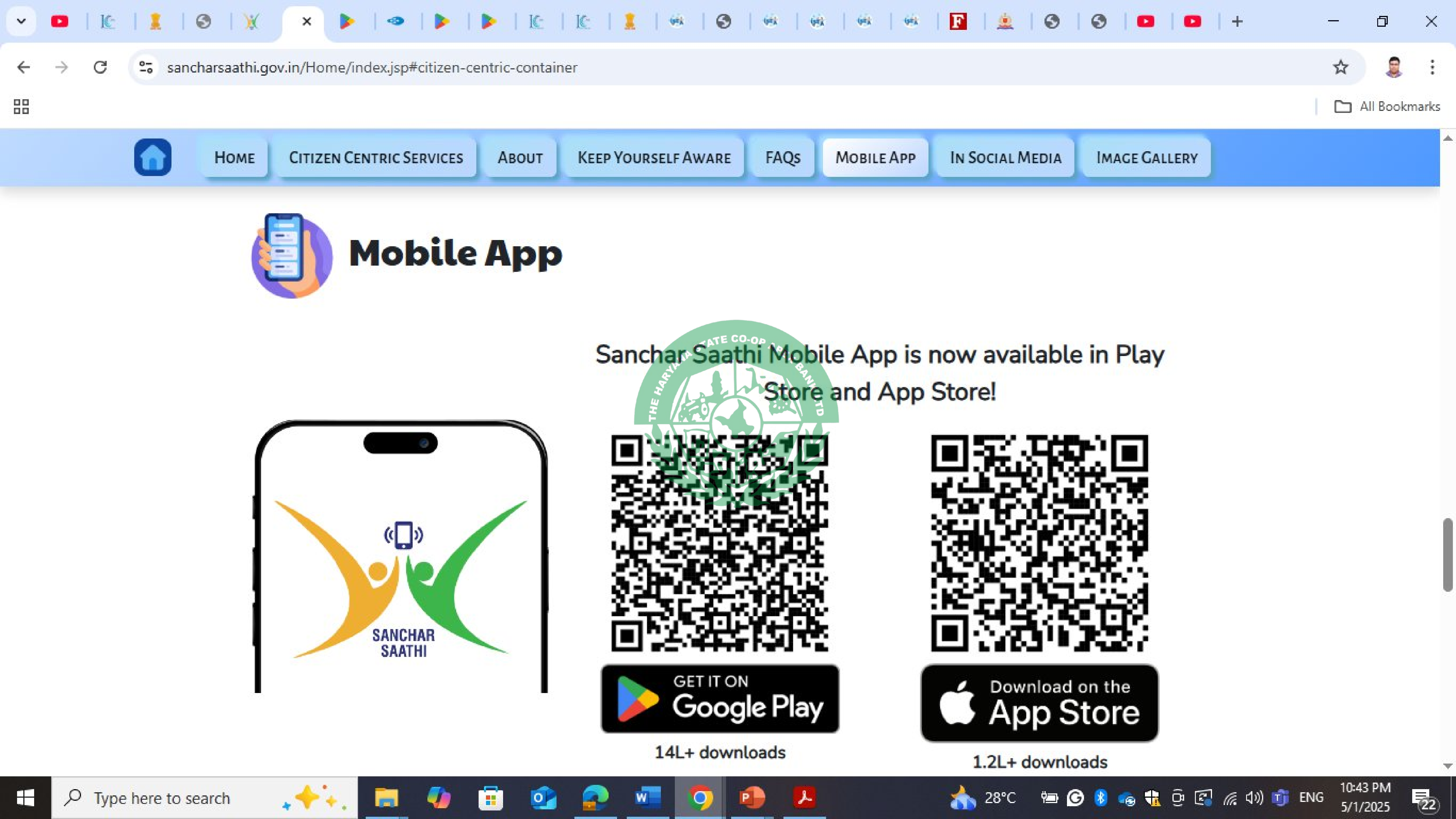
BLOCK YOUR LOST / STOLEN MOBILE HANDSET

KNOW MOBILE CONNECTIONS IN YOUR NAME

KNOW GENUINENESS OF YOUR MOBILE HANDSET

REPORT INCOMING INTERNATIONAL CALL WITH INDIAN NUMBER

KNOW YOUR WIRELINE INTERNET SERVICE PROVIDER

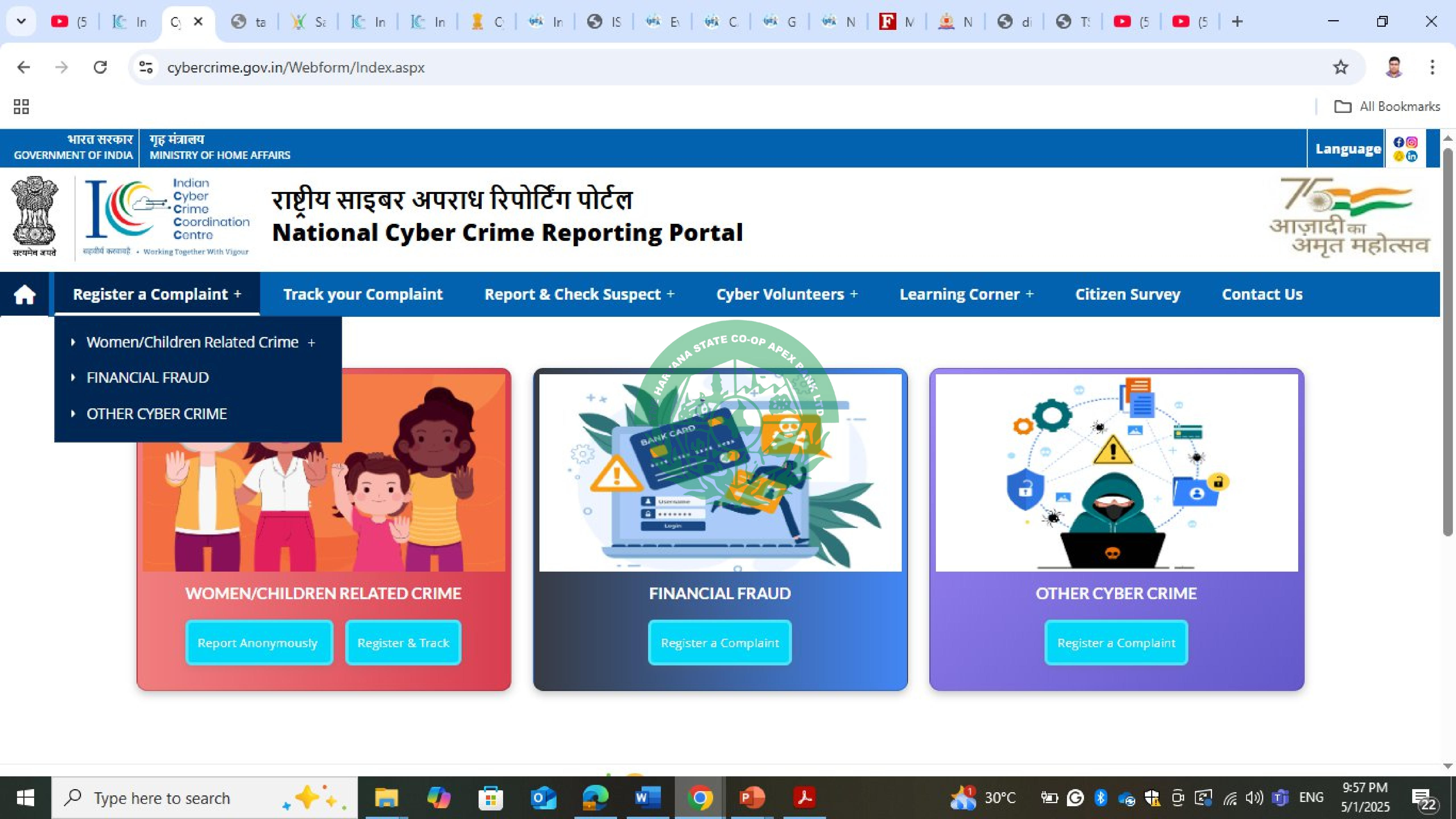


Mobile App

Sanchar Saathi Mobile App is now available in Play Store and App Store!

14L+ downloads

1.2L+ downloads



cybercrime.gov.in/Webform/Index.aspx

All Bookmarks

भारत सरकार
GOVERNMENT OF INDIA

गृह मंत्रालय
MINISTRY OF HOME AFFAIRS

Language

सत्यमेव जयते

Indian Cyber Crime Coordination Centre
राष्ट्रीय करवाएं • Working Together With Vigour

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

आज़ादी का अमृत महोत्सव

Register a Complaint + | Track your Complaint | Report & Check Suspect + | Cyber Volunteers + | Learning Corner + | Citizen Survey | Contact Us

- Women/Children Related Crime +
- FINANCIAL FRAUD
- OTHER CYBER CRIME

WOMEN/CHILDREN RELATED CRIME

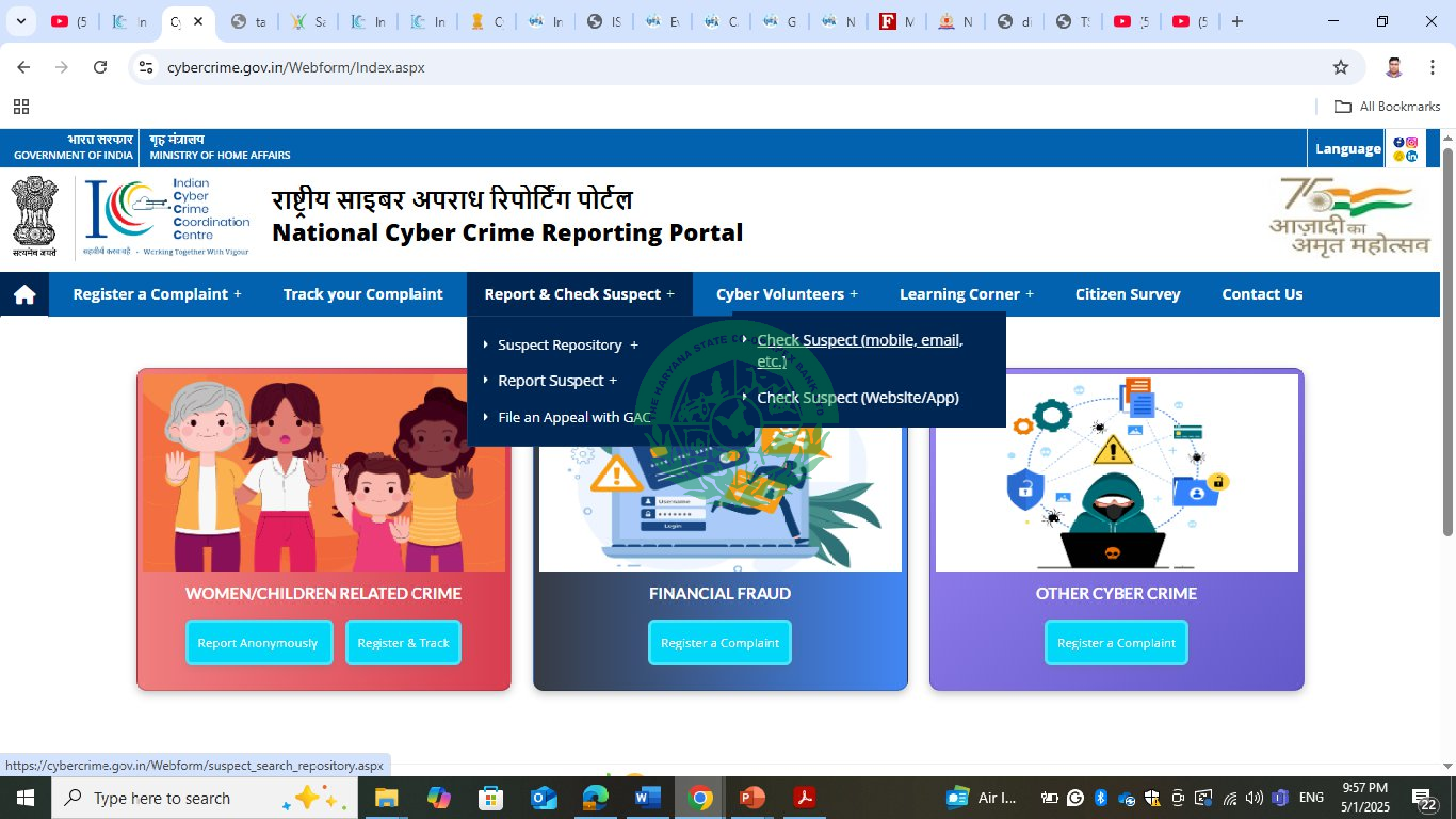
Report Anonymously | Register & Track

FINANCIAL FRAUD

Register a Complaint

OTHER CYBER CRIME

Register a Complaint


cybercrime.gov.in/Webform/Index.aspx
All Bookmarks

भारत सरकार GOVERNMENT OF INDIA | गृह मंत्रालय MINISTRY OF HOME AFFAIRS

Language

Indian Cyber Crime Coordination Centre
सहयोग करवाइये • Working Together With Vigour

सत्यमेव जयते

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal

75 आज़ादी का अमृत महोत्सव

Register a Complaint + | Track your Complaint | Report & Check Suspect + | Cyber Volunteers + | Learning Corner + | Citizen Survey | Contact Us

- Suspect Repository +
- Report Suspect +
- File an Appeal with GAC

- Check Suspect (mobile, email, etc.)
- Check Suspect (Website/App)

WOMEN/CHILDREN RELATED CRIME

Report Anonymously | Register & Track

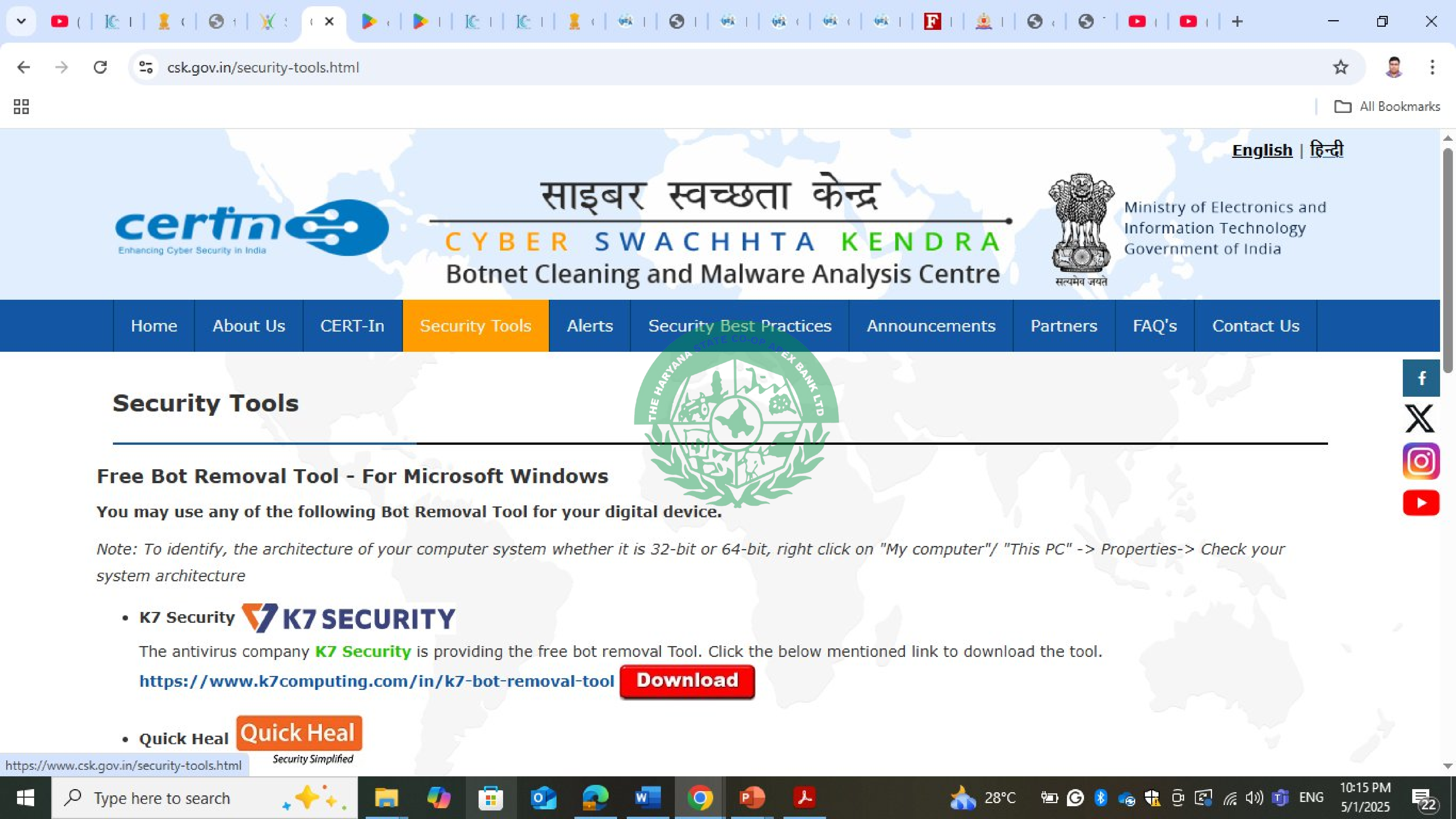
FINANCIAL FRAUD

Register a Complaint

OTHER CYBER CRIME

Register a Complaint

https://cybercrime.gov.in/Webform/suspect_search_repository.aspx



Security Tools

Free Bot Removal Tool - For Microsoft Windows

You may use any of the following Bot Removal Tool for your digital device.

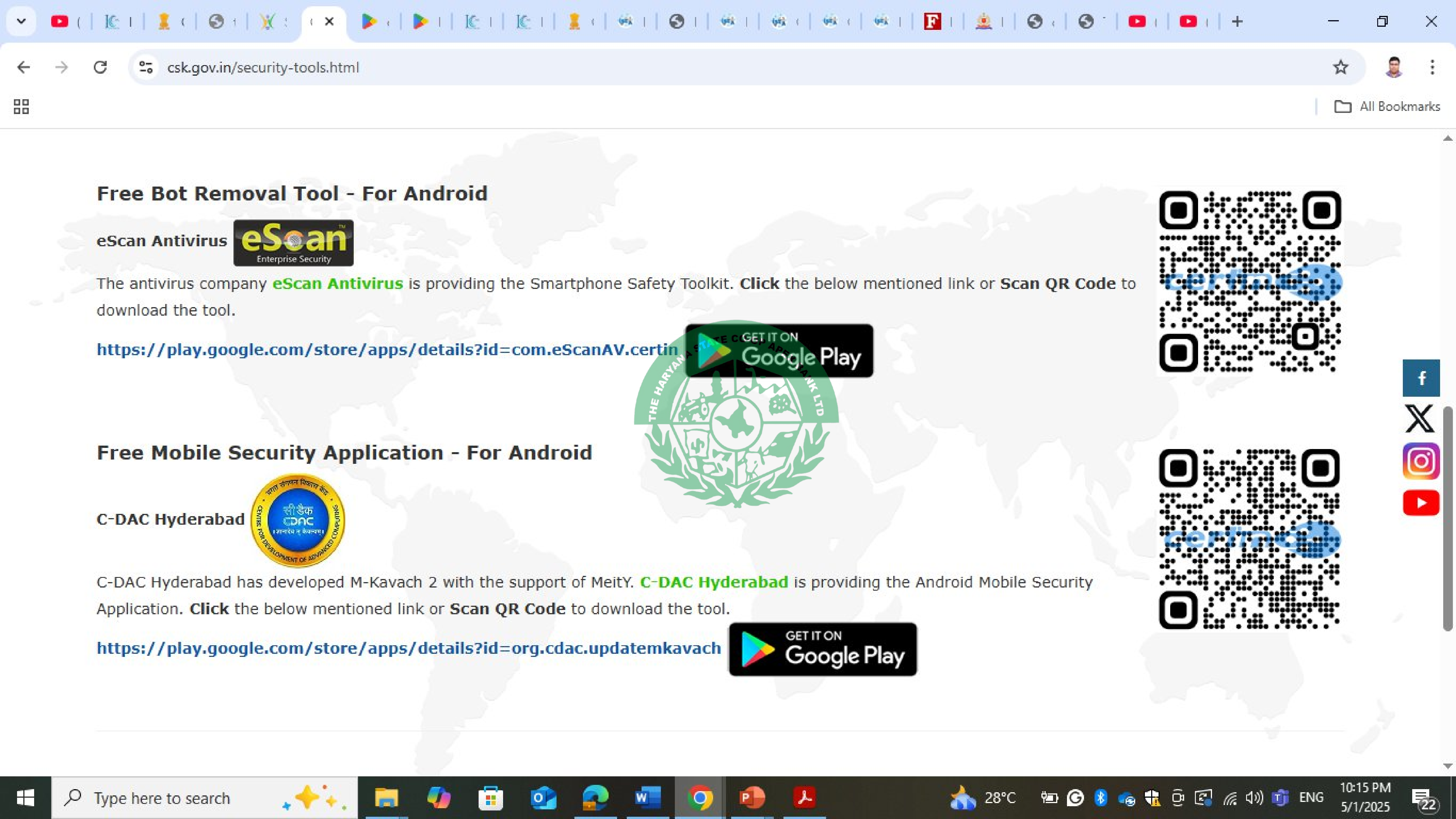
Note: To identify, the architecture of your computer system whether it is 32-bit or 64-bit, right click on "My computer"/ "This PC" -> Properties-> Check your system architecture

- **K7 Security** K7 SECURITY

  The antivirus company **K7 Security** is providing the free bot removal Tool. Click the below mentioned link to download the tool.

  https://www.k7computing.com/in/k7-bot-removal-tool Download

- **Quick Heal** Quick Heal Security Simplified



Free Bot Removal Tool - For Android

eScan Antivirus

The antivirus company **eScan Antivirus** is providing the Smartphone Safety Toolkit. **Click** the below mentioned link or **Scan QR Code** to download the tool.

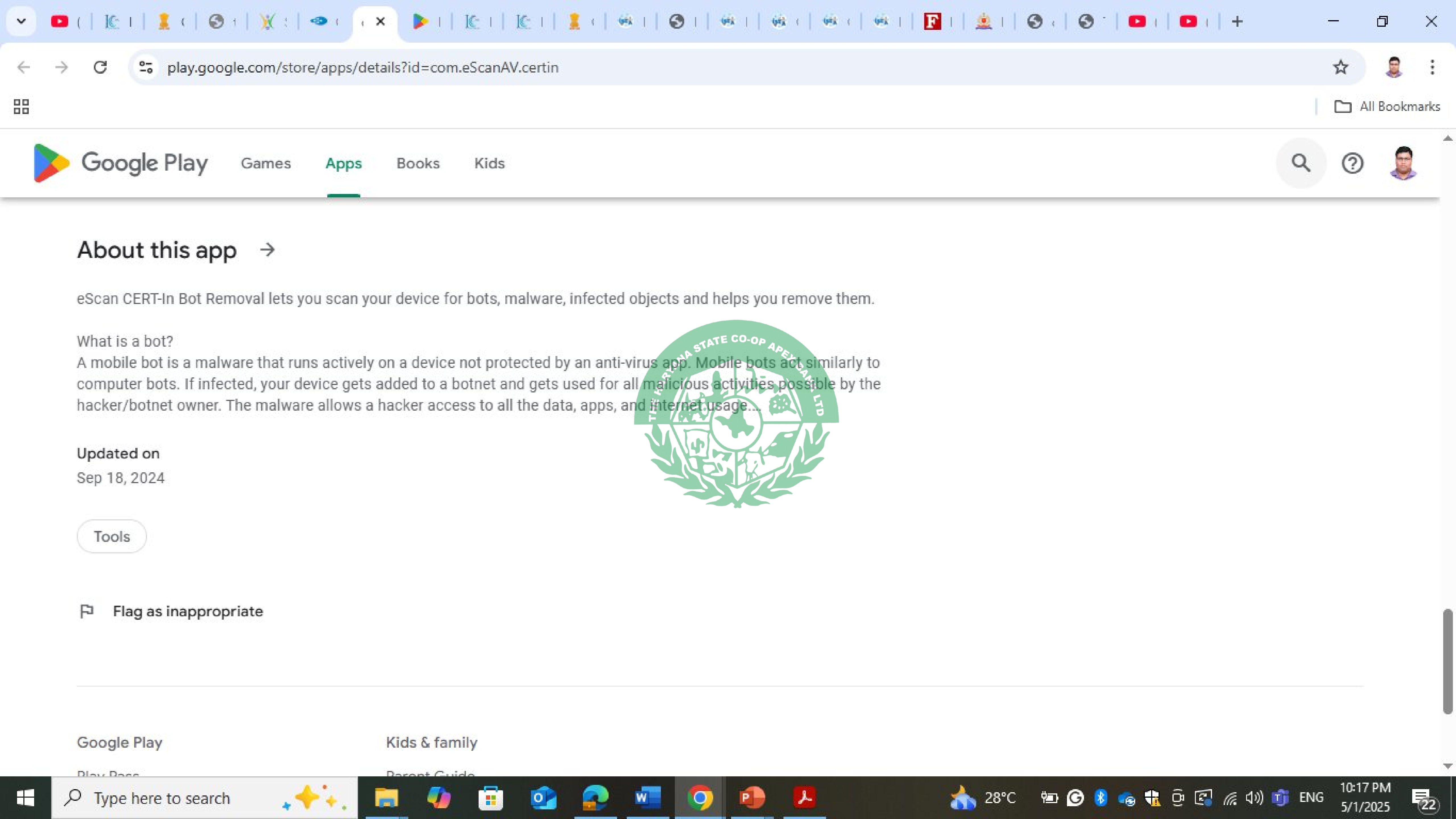
https://play.google.com/store/apps/details?id=com.eScanAV.certin

Free Mobile Security Application - For Android

C-DAC Hyderabad

C-DAC Hyderabad has developed M-Kavach 2 with the support of MeitY. **C-DAC Hyderabad** is providing the Android Mobile Security Application. **Click** the below mentioned link or **Scan QR Code** to download the tool.

https://play.google.com/store/apps/details?id=org.cdac.updatemkavach

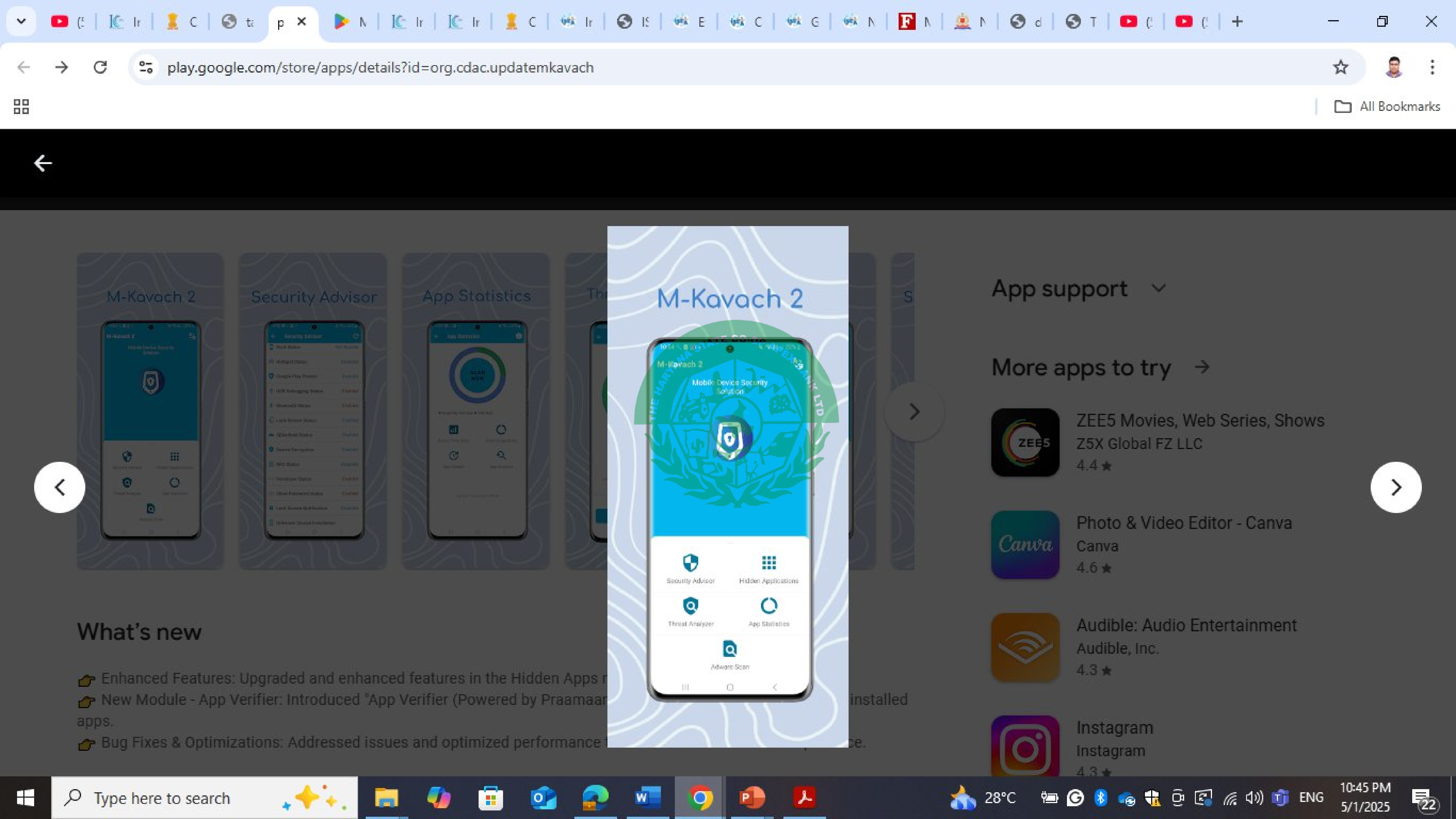


About this app →

eScan CERT-In Bot Removal lets you scan your device for bots, malware, infected objects and helps you remove them.

What is a bot?
A mobile bot is a malware that runs actively on a device not protected by an anti-virus app. Mobile bots act similarly to computer bots. If infected, your device gets added to a botnet and gets used for all malicious activities possible by the hacker/botnet owner. The malware allows a hacker access to all the data, apps, and internet usage....

Updated on
Sep 18, 2024



play.google.com/store/apps/details?id=org.cdac.updatemkavach

App support

More apps to try

ZEE5 Movies, Web Series, Shows
Z5X Global FZ LLC
4.4 ★

Photo & Video Editor - Canva
Canva
4.6 ★

Audible: Audio Entertainment
Audible, Inc.
4.3 ★

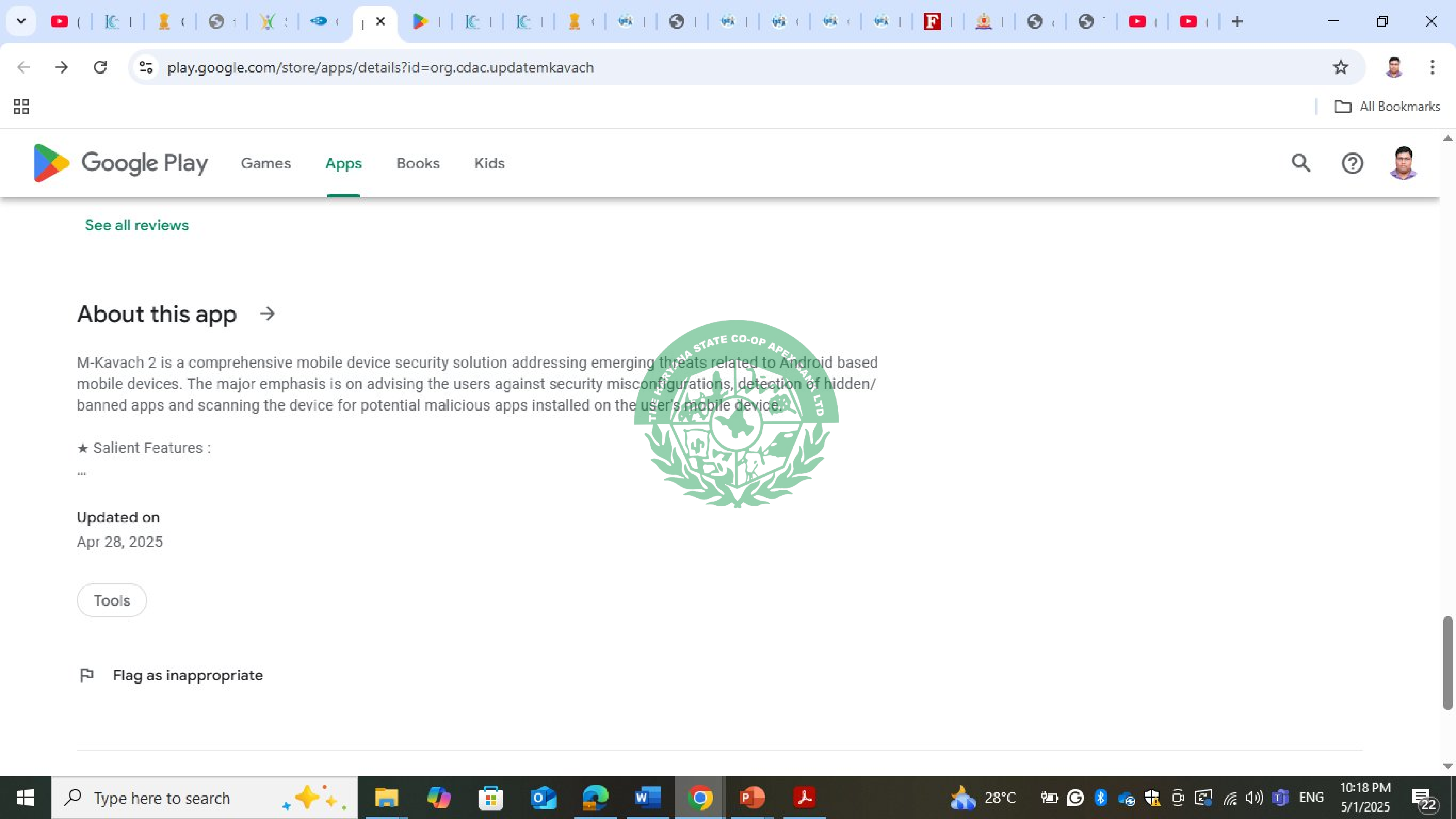
Instagram
Instagram
4.3 ★

What's new

👉 Enhanced Features: Upgraded and enhanced features in the Hidden Apps r

👉 New Module - App Verifier: Introduced "App Verifier (Powered by Praamaan installed apps.

👉 Bug Fixes & Optimizations: Addressed issues and optimized performance t ce.



About this app →

M-Kavach 2 is a comprehensive mobile device security solution addressing emerging threats related to Android based mobile devices. The major emphasis is on advising the users against security misconfigurations, detection of hidden/ banned apps and scanning the device for potential malicious apps installed on the user's mobile device.

★ Salient Features :

...

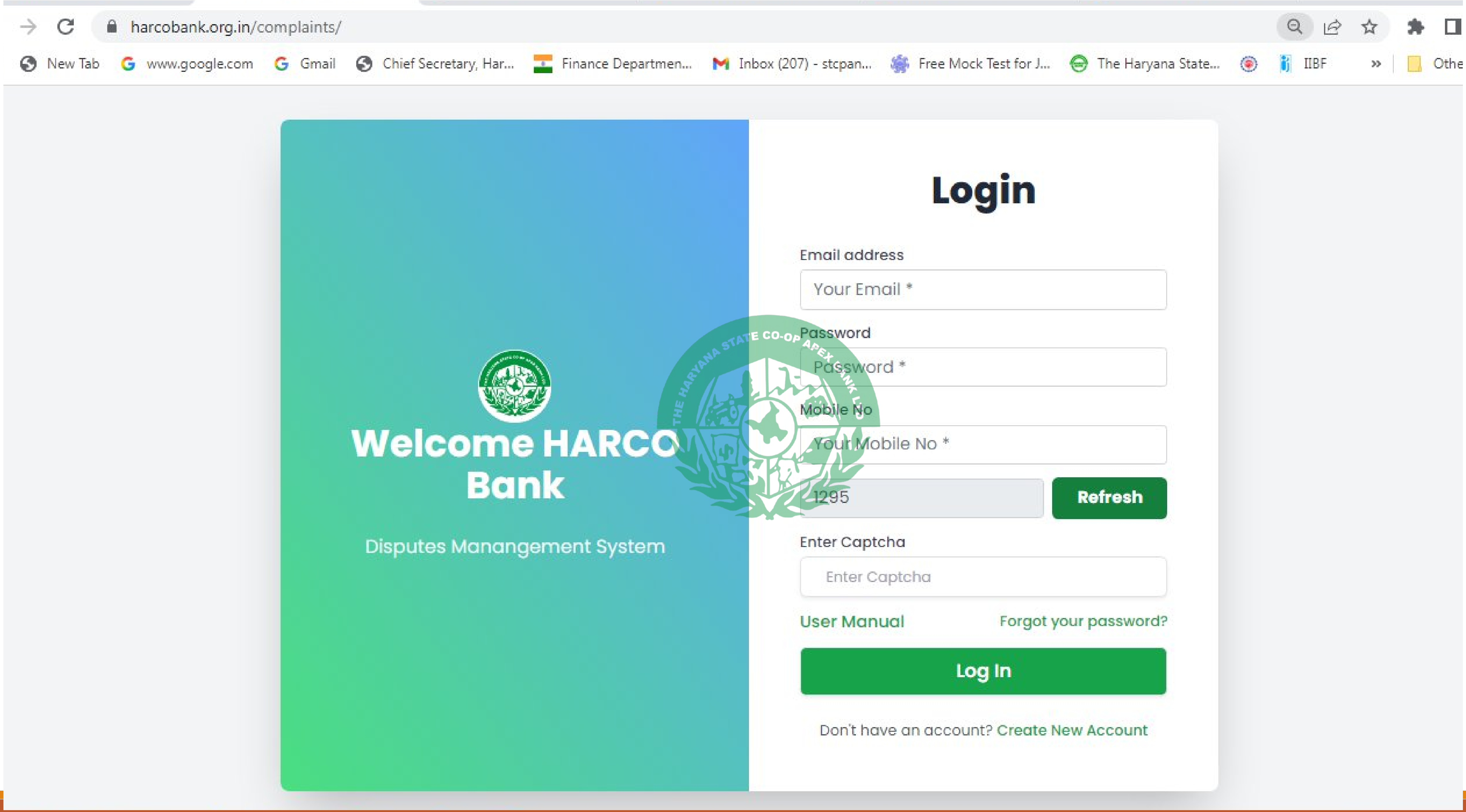
Updated on

Apr 28, 2025

Tools

Flag as inappropriate

How I can Complaint in HARCO Bank?



Welcome HARCO Bank

Disputes Manangement System

Login

Email address

Your Email *

Password

Password *

Mobile No

Your Mobile No *

1295 Refresh

Enter Captcha

Enter Captcha

User Manual

Forgot your password?

Log In

Don't have an account? Create New Account

CUSTOMER CARE NUMBER FOR DIGITAL SERVICES

0172-2713293

THANK YOU