राष्ट्रीय इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी संस्थान, रोपड़

National Institute of Electronics and Information Technology (NIELIT), Ropar

SOCIAL NETWORKING THREAT IN DIGITAL ERA

SHRI AKASH SHARAN

SCIENTIST 'B', NIELIT

Content of the Presentation

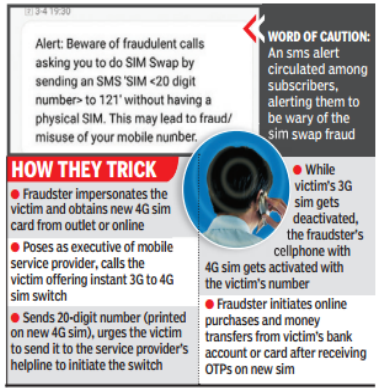
- Social Networking Threats
- Cyber Crime
- Type Of Cyber Crimes
- Threats through Social Media
- Social Media Attacks
  - Password Threats
- Psychological Tricks.
  - Phishing
  - Fake profile
  - Sympathy Fraud
  - Romance Fraud
  - Cyber Stalking
  - Cyber Bullying
  - Online Predators
  - Suicide Games
- Incident Reporting

Many B'lureans lose cash to sim card swap fraud

Bank Insiders Part Of Ploy: Investigators

Petlee.Peter@timesgroup.com

Bengaluru: If you are using a cellphone number with a 3G sim card and your online banking account is linked to it, you could be the next victim of a thriving 'sim card swap fraud'. At least 30 Bengalureans have reportedly fallen prey to scamsters, losing huge sums of money since mid-2016.



BEWARE THE TRAP

For insurance executive Aroop Ghosh (39) from Domlur, the ordeal began when he attended a phone call at his lunch table in mid-February. "The male caller claimed he was calling from a mobile service provider and confirmed with me if I was still using a 3G sim. He told me that there is an offer for easy swapping to 4G for better internet speed and sent me a 20-digit number by SMS after disconnecting the call," he said.

An ignorant Ghosh took the bait by texting the 20-digit number to the mobile service provider's helpline and selected option 1 to confirm the 4G swap as advised by the conman. "Within a few seconds my sim card got deactivated and it remained so," rued Ghosh. The following day, electronics good worth over Rs 2 lakh were purchased online using his HDFC bank account.

According to an investigating officer with the CID's cybercrime unit, the modus operandi is thus: The culprits obtain a new 4G sim for the victim's cellphone number by either impersonating him at an outlet of the service provider or online, using the 4G sim swap page on the service provider's website. The new sim is then delivered to the given address within a day.

"The culprits then call the victim claiming to be executives from the service provider and send the 20-digit number printed on the new 4G sim card via SMS and convince him or her to activate it. Once the 3G sim on the victim's cellphone becomes inactive, the 4G one on the fraudsters' cellphone becomes active. The fraudsters then use it to receive OTPs," the officer added.

Investigators suspect the scamsters must be obtaining victims' confidential bank account or card details, including cellphone details, from bank insiders. "They try every number pertaining to the accounts and some 3G sim card users fall for it," the officer added.

Over 30 victims of the sim swap fraud have approached cybercrime police stations of state CID and Bengaluru city police (BCP) since mid-2016.

Some like Manish Raj, a city-based BPO employee, who are tech aware have also fallen prey to the fraud. "I didn't receive a call but only an internet-generated SMS with the 20-digit number from the fraudster, which I carelessly activated and lost Rs 30,000 from my ICICI account," recalled Raj.

(Names of victims have been changed on request).

वीडियो कॉल रिकॉर्ड कर रंगदारी वसूल रहा गिरोह

माई सिटी रिपोर्टर

अनावश्यक एप इंस्टाल न करें, आपत्तिजनक बातें न करें

गाजियाबाद। आपत्तिजनक फोटो व वीडियो के बाद अब वीडियो कॉल रिकार्ड करके ब्लेकमैल करने वाला गिरोह सक्रिय हो गया है। यह गिरोह दोस्त बनवाने का झांसा देकर युवक-युवतियों को अपने जाल में फंसा रहा है। शुरूआत में नॉर्मल बातचीत और फिर अश्लील वीडियो कॉल की जाती है। इसके बाद अश्लील कॉल में किसी तरह की आपत्तिजनक बातें न करें।

मेरठ जोन पुलिस के साइबर एक्सपर्ट कमेंवीर सिंह का कहना है कि गूगल प्ले स्टोर पर तमाम डमी एप उपलब्ध हैं, जिनसे ठगी ब्लैकमेलिंग की घटनाओं को अंजाम दिया जा सकता है। वीडियो चैट रिकॉर्ड करने के लिए स्क्रीन रिकॉर्ड एप की भरमार है। ऐसे में किसी भी एप को डाउनलोड करने से पहले उसे वेरिफाई कर लें। किसी भी तरह के लोभ या लालच में न आएं। मोबाइल पर वॉयस या वीडियो

Online markets are the new fraud hubs

Cons Pose As Armymen To Lure Buyers

TIMES NEWS NETWORK

Hyderabad: Online marketplaces have become the new playground for fraudsters. According to Cybercrime police, though one-time password (OTP) frauds have declined, cases of cons at marketplaces like Olx have seen a rise.

There is a peculiar modus operandi. Fraudsters pretend to be army personnel on these sites to build a rapport with prospective buyers. They then post an ad on OLX or Quickr for the sale of mobile phones or other electronic items. If any buyer is interested, the fraudster sends a photo of a fake army identity card to lure them. Insisting on urgency of the sale, the fraudsters ask buyers to send money in advance. They then send a fake courier receipt to convince the buyer that they are sending the goods. Once the money is transferred over PayTm, the fraudsters stop picking buyers' calls.

At least 15 such complaints are received every month, say Cybercrime cops.

POLICE VIGIL ON PORTALS

- Cybercrime cops advised Olx to add a pop-up on **their website warning users of such frauds**
- They also asked the online marketplace portal to **delete duplicate ads and get an ID proof of every seller**
- Police advise users **not to transfer money to PayTm or bank accounts** before receiving the product
- **Victims lose ₹10 lakh on an average in such frauds**

"There are at least15 such cases where the victim was cheated by a seller who claimed to be an Army personnel. As people believe armymen to be honest, the fraudsters could con victims easily," said Additional Deputy Commissioner of Police (Cyber Crime) KCS Raghu Vir.

With rise of such fraud cases in the city the Cybercrime team along with detective department head and additional commissioner of police (crime) held a meeting with the Olx team.

"We had a meeting with the Olx director and his team on before Diwali. We raised concern about several such cases being recorded. In the past few months we have already registered almost 10 FIRs of such Olx frauds," said the Additional DCP.

A source in cybercrime police claimed that very few people file FIR and most of the cases are verbal petitions as the amount is less. There is a dedicated team to sniff out such suspicious ads on the online marketplace portals. If any suspicious activity is observed, the team informs the portal to block the user

"But once the offender is blocked on a particular platform, they move to another forum to lure innocent buyers," said the source.

टिकटॉक प्रो समेत अन्य ऑफर वाले लिंक और मैसेज से रहें दूर

लॉकडाउन के दौरान साइबर क्राइम में 60% तक इजाफा

Manish.Jha@timesgroup.com

Rising 'sextortion' cases put cyber users on the edge

Video Calls, Chats Used To Blackmail Net Users

Kanishma.Kotwal@timesgroup.com

Indore: Small chat on messenger followed by a video call with exchange of compromising messages two months ago, changed the life of a 25-year-old IT professional Shikhar Singh (name changed) who became a victim when scammers from the other end started blackmailing him.

Shikhar had been in a relationship with a woman for past six years but the recorded video call and subsequent harassment that followed broke his ties with her.

He is one of the thousands of people in India caught by a growing internet scam the investigators call 'sextortion'. Here the scamsters usually monitor activities of their targets online for days and weeks. After sifting through all the profile details, relationship links, profile pictures, activities and victim's habits based on the updates, a friend request is sent and conversation is initiated.

The woman on the other end sends objectionable pictures to the victim and asks him to do the same. In most of the cases, the video that victim sees is either a pre-recorded video or a completely fake one. While the technical help we can but once a video or a picture is uploaded, it is very difficult to take it back. So it's important that the victim is counselled in a proper way to deal with the situation.

How does cyber bullying affect the victims?

The impact of cyber bullying and sextortion on the victims is so severe that they feel extremely guilty. We have to put them on medications as the trauma is deep and painful. In one of the cases, the victim was so paranoid after the incident that he stopped using social media and used to think that people are staring at him.

What should people do to avoid being dragged into such crimes?

One should always stick to basic instinct and common sense to avoid such things. If you feel that someone seems suspicious, do not talk to that person. Even if you fall prey to sextortion or cyber bullying, remember that it's not the end of the world and you can be saved by right kind of technical and psychological help.

TAKE PRECAUTIONS WHILE SHARING INFO ONLINE

- Use least amount of information necessary to register for and using the site. Opt for nickname or handle
- Use highest level privacy setting that a site allows & don't accept default settings
- Make sure you cover web cameras of laptops, mobile phone when not in use
- Verify emails, links in emails you get from social networking sites. They are often designed to gain access to your personal information
- Be certain of both the source and content of each file you download. When in doubt, don't open or download any content shared with you
- Never post publicly your address, phone number, driver's licence number, Aadhaar number, PAN card or student ID number
- Only connect with people you know and trust
- Read privacy and security policies closely - know what you are getting into. Some major social networking sites actually say they will use or sell information about you in order to display advertising or other information they believe might be useful to you

Cyber bullying makes the victims feel extremely guilty

Q&A

Nirali Bhatia
psychologist

How many cases of cyber bullying and sextortion do you come across every month and how you deal with the victims?

I deal with a number of cases on a day to day basis through social media, over mails or calls. Most of the victims, who approach me, come with extreme suicidal thoughts. I first make sure that they are safe and then speak about the issue. We provide whatever

Two held for cheating people using fake Patanjali website

Shafaque.Alam@timesgroup.com

Noida: The cyber cell on Friday arrested two persons for operating a fake website offering dealership of Baba Ramdev's Patanjali products. Anoop Verma (26) from Shekhpura in Bihar and Sameer Sharma (35) of Gomti in Tripura were accused of cheating one Rajendra Kumar Verma.

Zahir Khan, inspector at Noida's Centre for Cyber Crime Investigation (CCCI), said in November 2017, Verma came across the website www.patanjalidistributors.org while searching for Patanjali dealerships. Verma contacted a number he got from the website and the receiver identified himself as Rishikesh Acharya, personal assistant to Acharya Balkrishna of Patanjali.

Anoop Verma (top); Sameer Sharma

Verma was told deposit Rs 50,000 as registration fee and Rs 4.5 lakh security deposit within 24 hours to get the dealership for Noida region.

Verma deposited Rs 10 lakh on two bank accounts as discussed, and sought an appointment to discuss the deal. However, the accused told him to deposit another Rs 6 lakh. Suspecting foul play, Verma informed police on November 10, 2017 and a case was registered.

The accused were then put on surveillance, said Khan. A police team conducted a raid in Noida and Delhi but the accused escaped. They were arrested from near Khoda crossing on Friday.

Anoop, a graduate, told police he was planning to develop a website and a Google search landed him at – www.website99.net, run by Sameer, in Delhi. Anoop asked Sameer to develop a fake website for Patanjali product distribution and paid Rs 38,000 in March 2017.

Anoop also roped in three others – Roshan, Vikas, and Viru – for the business. Sameer helped them with online marketing and the website started getting hits. Anoop said in April 2017, he cheated a Kerala resident of Rs 8 lakh. In May, Rs 12 lakh was taken from a native of Tamil Nadu. Again, he trapped a Chennai resident and cheated him of Rs 14 lakh. In October, it was Verma.

The two accused were produced in court and sent to judicial custody.

Social Networking Threats

When scammers and hackers gain unauthorized access to a user's personal information is called as Social Networking Threats. Fraudsters typically target consumers who are unaware of the risks associated with cyberattacks and accounts with low security.

Cyber Crime

A cybercrime is a crime involving computers and networks.

- This includes a wide range of activities, from illegally downloading music files to stealing money from online bank accounts.
- Cyber criminals are not always financially motivated. Cybercrimes include non-monetary offenses such as Cyber stalking.
- It can include frauds such as job related frauds, matrimonial frauds; stealing and misusing sensitive personal information (Aadhaar details, credit/debit card details, bank account credentials, etc.), defamation of an individual on social media; distribution of computer viruses etc.
- Cybercrimes can also lead to physical or sexual abuse.

Types of Cyber Crimes

Computer as a Weapon	Computer as a Target
• Using a computer to commit real world crimes. • Cyber Frauds. • Cyber terrorism. • Child Pornography etc.	• Using a computer to attack other computers. • Hacking • Virus/Worm attacks • DOS attack etc.

Social Media Threats

Against All

- Password Threat
- Threats via websites/Apps
- Frauds
- Privacy

Against Children

- Cyber Bullying
- Suicide Games
- Online Predators

Against Women

- Cyber Stalking
- Morphing
- Hate/Revenge Crime

Social Media Related Attacks

- Social Media has become an integral part of our lives. We share our day to day lives on social media in the form of self and family photographs e.t.c.
- One can understand the entire history of an individual through their social media profile and can even predict future events based on patterns in the past.
- This poses a threat to an individual as unwanted access to social media profile can cause loss of information, defamation or even worse consequences such as physical/sexual assault, Fraud etc.

Password Threats

- Password is used for authentication, to prove our identity or to gain access to our own resources. It should be kept as a secret to prevent access by unauthorized users.
- In social networking sites like Facebook, and LinkedIn each of which is studded with answers to commonly used security questions such as favorite place, school, college, etc.
- A password helps individuals in protecting personal information being viewed by unauthorized users. Hence it is important to secure passwords

Password Threats

- Simple passwords, including ones containing a name, birthdate, or mobile number, are easily guessed and misused by anyone.
- What if you use the same password for all of your accounts, hackers have 90% easier access to all of your account passwords.
- **Shoulder Surfing** is a direct observation technique, such as looking over someone's shoulder to get passwords, PINs, other sensitive personal information.
- Writing your passwords on papers or storing it on hard disk, Strangers search for papers or the disk for passwords where they could be written.

Password Attack Types

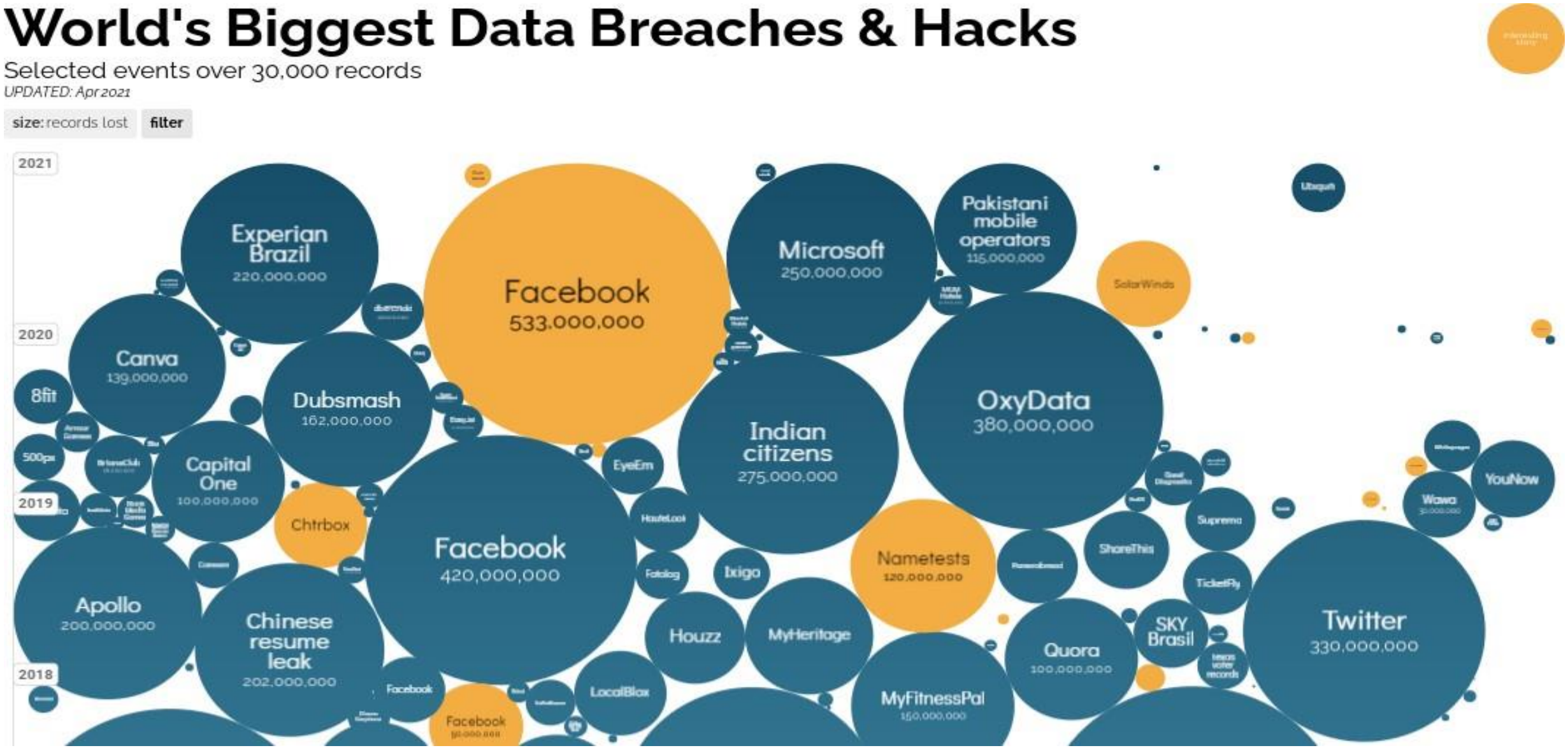
Brute Force Attacks

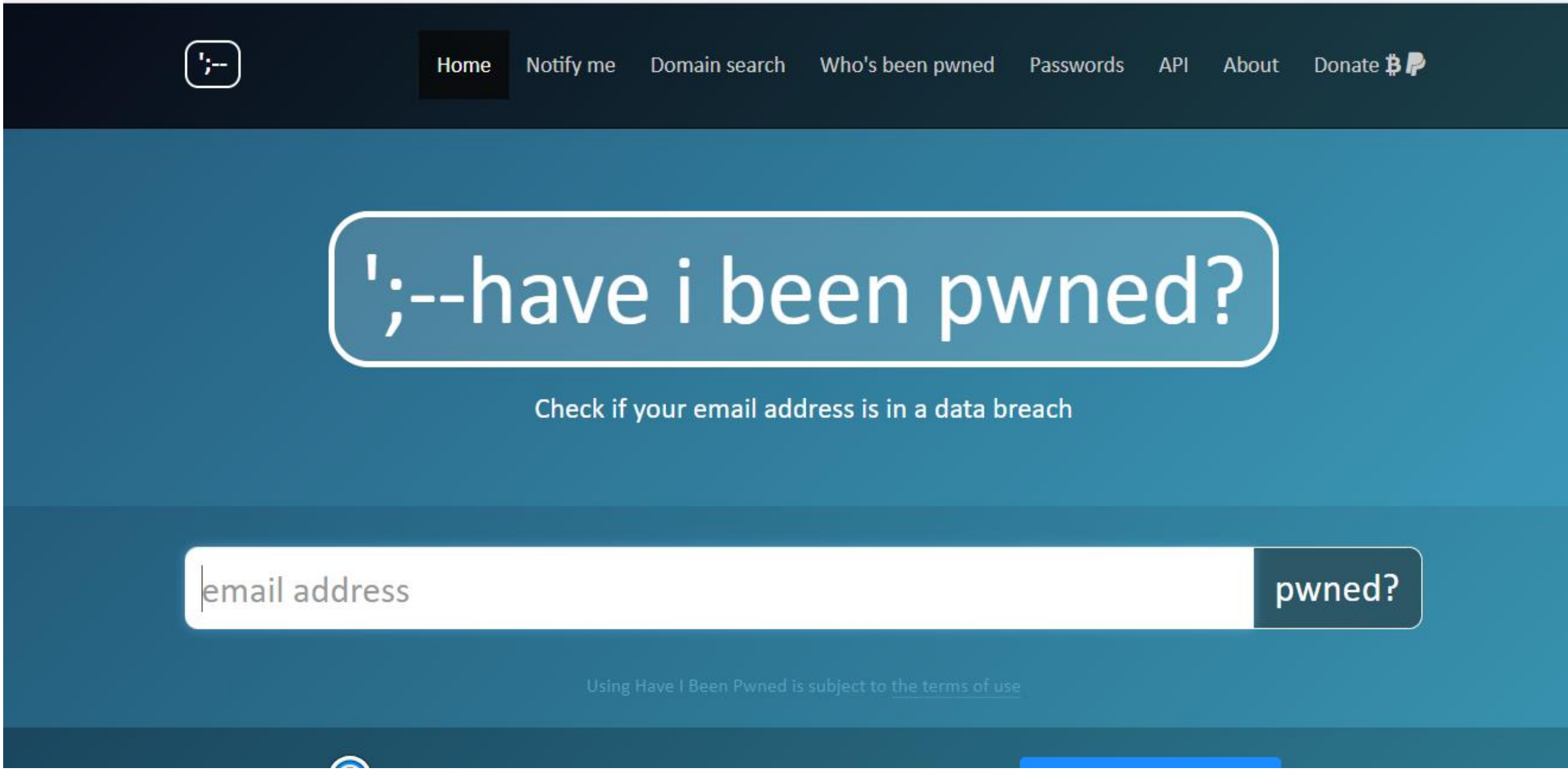
Dictionary Attacks

Keylogger Attacks

The Big Picture !

http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/




';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if your email address is in a data breach
email address
pwned?
Using Have I Been Pwned is subject to the terms of use

PSYCHOLOGICAL TRICKS

- Psychological tricks are where attackers play with the minds of the user to trap them with lucrative offers.
- Once trapped, the attackers can exploit the victim by either stealing money or stealing sensitive personal information (name, Aadhaar details, bank account details etc.) or harm the victim in any other way.
- The entire basis of this kind of attack is to make the victim fall into their trap by sending fake messages , e-mails, calls or SMSs.
  - **Lottery Fraud**
  - **Credit/Debit Card Fraud**
  - **Job Related Fraud**

Safeguard

- Do not share your PIN, password, card number, CVV number, OTP etc. with any stranger, even if he/she claims to be bank employee. Bank will never ask for any vital information.
- Always search and apply for jobs posted on authentic job portals, newspapers etc.
- If an e-mail has spelling, grammatical and punctuation errors, it could be a scam
- Beware of the fake calls/e-mails impersonating themselves as recruiters and requesting for personal information or money

Phishing

- Phishing : Cybercriminals send fraudulent emails or whatsapp texts that may look legitimate. The links in these emails or texts may be used to download malicious software.
- Vishing : Instead of e-mail, in this type of crime, the fraudster uses telephone to obtain sensitive personal and financial information.
- Smishing : It uses SMS to send fraudulent text messages. The SMS asks the recipient to visit a website/weblink or call a phone number. The victim is then tricked into providing sensitive personal information, debit/credit card details or passwords etc.

Safeguard

- Do not respond to messages from unknown source requesting personal or financial details even if it assures credit of money into your bank account.
- Do not respond to suspicious e-mails or click on suspicious links.
- Do not transfer money to any un-trusted unknown account.
- Remember you can never win a lottery if you have not participated in it.
- Always verify the correctness of the domain of the e-mail ID, for example, all government websites have “.gov.in” or “.nic.in” as part of their web address.
- Have proper spam filters enabled in your e-mail account.

Fake Profiles

- Attackers choose a fake identity as per his requirement. Either a fictional one or false identity of others
- They create a profile accordingly with the chosen false identity And contact the victim/s and send friend requests.
- The victim suffers in various ways through the fake social media account it can be
  - Monetary loss
  - Loss of reputation and public image e.t.c

Safeguard

- Profile Lock or privacy Features.
- Limited sharing of personal Information
- Never Accept Friend Request with proper verification.
- Be aware of security and privacy features and enable them on the social media accounts

Sympathy Fraud

The attacker becomes friends with the victim on social media. The attacker gains trust by frequent interactions. The attacker later extracts money/harms the victim.

Safeguard

- Be cautious while responding to unknown friend requests on social media platforms. Do not respond to unknown friend requests.
- Never share intimate pictures with anyone on online platform as they can be misused later.
- Do not share personal details or get into financial dealings with an unknown person whom you have met on social media platform.

Romance Fraud/ Sextortion

- The attacker becomes friends with the victim on social media. Over a period, the attacker gains victim's affection. The attacker later exploits the victim physically, financially and/or emotionally.
- Cyber Flashing : Sending unwanted sexual images to someone without their permission is known as "cyber flashing." It is a sexual offense and a type of online harassment.

Safeguard

- Be cautious while responding to unknown friend requests on social media platforms. Do not respond to unknown friend requests.
- Never share intimate pictures with anyone on online platform as they can be misused later.
- Do not share personal details or get into financial dealings with an unknown person whom you have met on social media platform.

26-yr-old held for stalking woman

TIMES NEWS NETWORK

New Delhi: A 26-year-old man was arrested for stalking a woman and sending her obscene messages.

"A team was formed to track down the man and he was traced to Gurgaon. He was arrested and the messages were found in his cellphone," said DCP west Vijay Kumar. The woman in her complaint said that the man also called her and threatened to put her number on porn sites.

Police said the man, Ajay Pathak was a school dropout and unemployed at present. He stayed with his parents in Gurgaon. During interrogation, Pathak said he had found a cellphone on the road in December. He threw the phone but kept the SIM and created a WhatsApp profile. He then started sending vulgar messages to many girls. He found the woman's phone number through her Facebook profile. A case under sections of the IT Act has been registered against him.

Cyber Stalking

- Cyber stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail, instant messaging (IM), messages posted on a website or a discussion group.
- A cyber stalker relies upon the fact that his/her true identity is not known in the digital world.
- A cyber stalker targets the victim with threatening/abusive messages and follows them/their activities in the real world.

Tips

- Restrict access to your profile. Social media sites offer privacy settings for you to manage who can view your posts, photos, send you friend request etc.
- Ensure your personal information, photos and videos are accessible only to your trusted ones.
- Be careful while uploading your photos on social media which show your location or places you frequently visit as cyber stalkers may keep tabs on your daily life.

Cyber Bullying

- Cyber bullying is bullying that takes place over digital devices. Cyber bullying can occur through SMS, social media, forums or gaming apps where people can view, participate or share content.
- Cyber bullying includes sending, posting or sharing negative, harmful, false content about someone else. The intention is to cause embarrassment or humiliation.

Safeguard

- Make your children aware that cyber bullying is a punishable crime so that neither do they indulge themselves in cyber bullying nor do they let anyone tease them.
- Monitor your kid's activity on internet/social media. Enable parental controls on computer/mobile devices.
- Even if the children or students know about any friend who is a victim of cyber bullying, they should help the victim. Report the matter to parents or teachers immediately.
- Do not delete offensive messages as it will help the police in investigation.

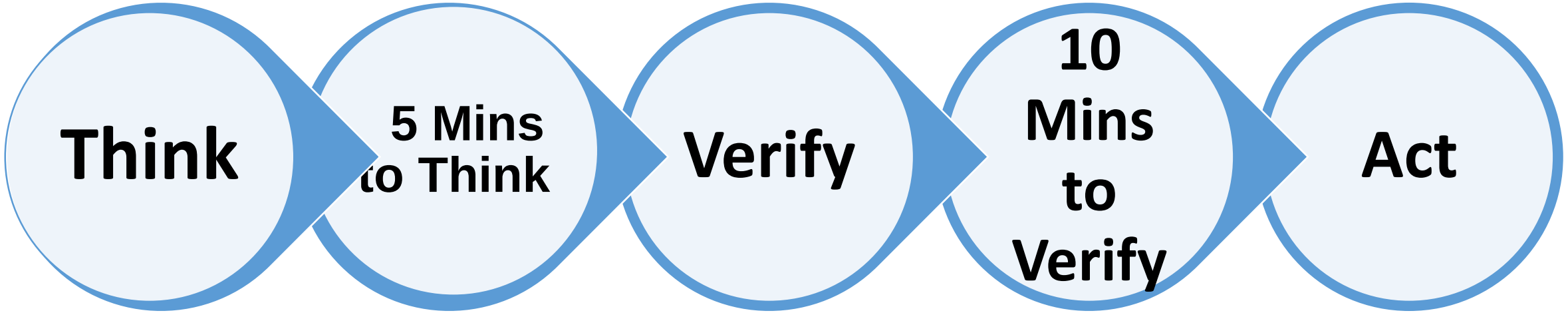
ONLINE PREDATORS

- Internet users that take advantage of kids and teenagers for violent and/or sexual intentions are known as online predators.
- Child grooming, engaging in sexual activity, uninvited exposing of materials and images, online abuse, and threats to incite fear or humiliation are a few examples of this
- Online predators employ chat rooms, instant messaging, social networking, email, and grooming processes for in-person meetings in addition to other communication methods.

Safeguard

- Be calm, stop chatting and get out of the chat room or log off.
- If you are not willing to do things asked by predator don't be scared to say no.
- If someone threatens you, immediately inform your parents.
- If someone uses bad language or threatens, take a screen shot of your conversation and tell them that you would report to police

Anti Cyber Fraud Tactic



- Trusted Source
- Expected
- Urgency

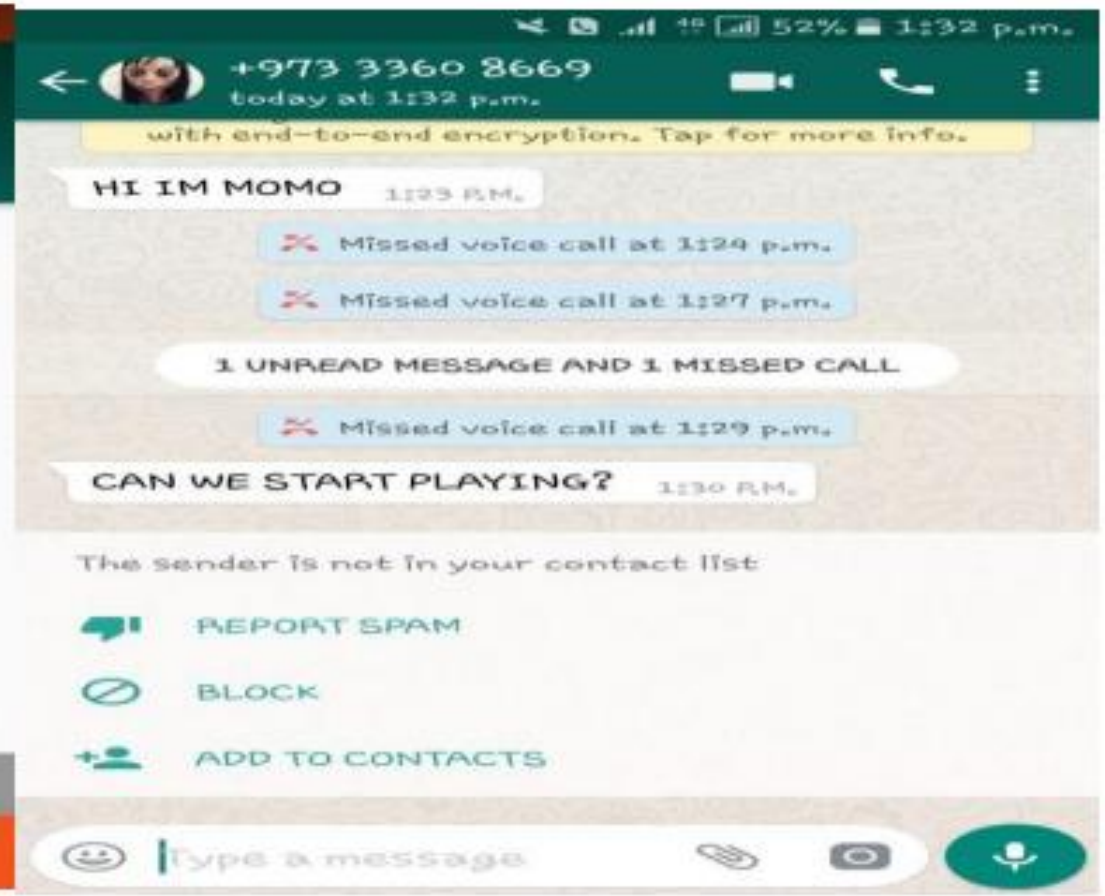
- Verify or Confirm

- Block , Report or Accept

Suicide Games

- On social media a game which involve real world Challenge is being circulated by some mischievous and criminal minded people. This game can instigates people, especially children to commit suicide as final task.
- Some innocent people around the world have fallen prey to this malicious game.
- There is need for parents and teachers to be aware of this threat and save the children from it.

For Example : MOMO Challenge



Sd/-
Addl. DG of Police, CID,CB
Odisha, Cuttack..

Sign of Victim of these games

- Becoming withdrawn from friends and family
- Persistent low mood and unhappiness
- Looking worried
- Not carrying out day to day tasks
- Sudden outbursts of anger directed at themselves or others
- Loss of interest in activities that they used to enjoy Visible marks like deep cuts or wounds on any part of the body of the child

Advice to Parents

- Check with your child, ask how things are going. Ask if there have been things stressing them or anything that has them worried.
- Monitor your child's online and social media activity to ensure they are not engaging with this game.
- Take reports from teachers in the school at regular intervals.
- If you fear your child may be at risk, get professional help right away.
- Remind your child that you are there and will support them as they face life challenges.
- Keep a constant watch if your child or child’s friends are involved in some violent act.

Case Study: Incident Report

This Article is From Feb 19, 2023

Farmer Loses Lakhs To Fraudsters. This Is How He Recovered Money

The money swindled was a loan that his father had taken under Kisan Credit Card Scheme for farming oses.

ews | Press Trust of India | Updated: February 19, 2023 1:55 pm IST

Case Study : Incident Reporting

- 55-year-old Pawan Kumar Soni, a farmer based in Sri Ganganagar City in Rajasthan, became a victim of a cyber fraud when his 26-year-old son Harsh Vardhan opened a link from a phishing message that flashed on his mobile phone. Within minutes, more than ₹ 8 lakh was withdrawn from his account in four different transactions.
- Harsh Vardhan, who lives in Dwarka in Delhi, had his phone number registered with his father's account at the State Bank of India branch of Sri Ganganagar City.
- The message, which was delivered on his mobile at around 3.45 PM on Saturday, January 7, said, "Your account is blocked, please update your KYC." Harsh already had a YONO application but the moment he clicked on the link, another duplicate app downloaded on his phone.
- "I thought that I should update my KYC on this new app so I entered my user ID and password. Suddenly, I started receiving messages for the withdrawal of money from my father's account and in seven minutes we lost ₹ 8,03,899," Mr Vardhan said.

Case Study : Incident Reporting

- Later on, he realized that with the help of the duplicate app, his phone was hacked and the user ID and password that he had entered, were accessed by a cyber fraud sitting somewhere else
- Mr Vardhan called his father in Ganganagar City, who rushed to the bank to inform the manager. Vardhan went to the District Cyber Cell in Dwarka where he was asked to lodge an online complaint and visit the office on any working day.
- The bank manager, at the request of his father, acted swiftly and called the local cyber cell. The manager also sent an email to financial institutions to get those accounts blocked in which the money was transferred.
- Mr Soni said, "The manager informed me that money went from my account to three accounts - ₹ 5 lakh and 1.24 lakh went into PayU, 1,54,899 was transferred into CCAvenue, and the rest ₹ 25,000 went into Axis Bank." Both PayU and CCAvenue are digital payment companies that act as a bridge between customers and business ventures. They collect payments from buyers when they make online purchases and deliver these to the merchants' bank accounts.

Case Study : Incident Reporting e Study

- "The bank manager informed me that PayU reverted to his email and said that it withheld the money. It also said that if it wouldn't receive any email from the cybercrime dept within two days for the reversal of the amount, it would release the money into the merchant's account," Mr Soni alleged.
- CCAvenue said that it also responded to the cyber officials and provided all information on January 7, when the company came to know about the said fraud.
- On the other hand, his son Vardhan made an online complaint and, two days later, on Monday, went to lodge an FIR which was denied.
- In the End, he got all his money Back by proactively reporting incident to authorities and stakeholders.

Incident Reporting

- Visit the nearest police station/Cyber Cell immediately and contact your near branch of your bank account.
- To report cybercrime complaints online, visit the **National Cyber Crime Reporting Portal**. This portal can be accessed at **https://cybercrime.gov.in/.** In this portal, there are two sections. One section is to report crimes related to Women and Children (where reports can be filed anonymously as well). Another section is to report other types of cybercrimes. You can also file a complaint offline by dialing the helpline number **1930.**
- Nodal Cyber cell Officer can also be found in National Cyber Crime Reporting Portal in contact us tab of portal.
- In case you receive or come across a fraud sms, e-mail, link, phone call asking for your sensitive personal information or bank details, please report it on **Maharashtra Cyber's web portal** by visiting **www.reportphishing.in**.

NCCRP


GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS
Language
Indian Cyber Crime Coordination Centre
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal
आज़ादी का अमृत महोत्सव
G20 भारत 2023 INDIA
Filing a Complaint on National Cyber Crime Reporting Portal
This portal is an initiative of Government of India to facilitate victims/complainants to report cyber crime complaints online. This portal caters to complaints pertaining to cyber crimes only with special focus on cyber crimes against women and children. Complaints reported on this portal are dealt by law enforcement agencies/ police based on the information available in the complaints. It is imperative to provide correct and accurate details while filing complaint for prompt action.
Please contact local police in case of an emergency or for reporting crimes other than cyber crimes. National police helpline number is 112. National women helpline number is 181 and Cyber Crime Helpline is 1930.
Learn about cyber crime
File a complaint
Media Gallery
Cyber Awareness
Internet Safety Tips for Kids
Tweets from @Cyberdost
Follow

NCCRP

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

Indian Cyber Crime Coordination Centre

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

National Cyber Crime Reporting Portal

Report Cyber Crime Related to Women/Child

Report Anonymously »

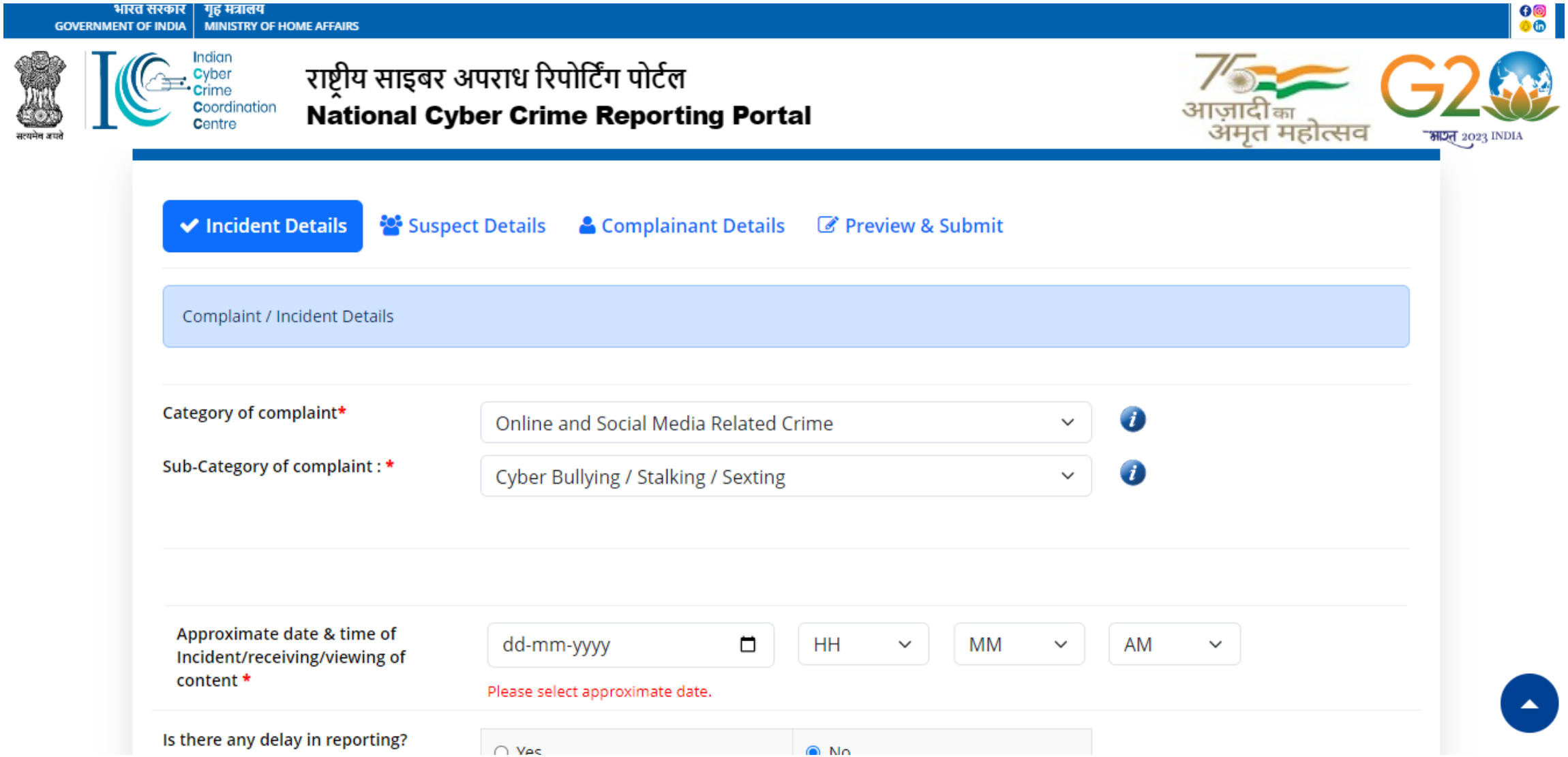
Report And Track »

REPORT CYBER CRIME

REPORT CYBER CRIME »

Frequently Asked Questions

NCCRP


भारत सरकार
GOVERNMENT OF INDIA
गृह मंत्रालय
MINISTRY OF HOME AFFAIRS
Indian Cyber Crime Coordination Centre
राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
National Cyber Crime Reporting Portal
आज़ादी का अमृत महोत्सव
G20 भारत 2023 INDIA
Incident Details
Suspect Details
Complainant Details
Preview & Submit
Complaint / Incident Details
Category of complaint*
Online and Social Media Related Crime
Sub-Category of complaint : *
Cyber Bullying / Stalking / Sexting
Approximate date & time of Incident/receiving/viewing of content *
dd-mm-yyyy
HH
MM
AM
Please select approximate date.
Is there any delay in reporting?
Yes
No

Incident Reporting Cont…

Social Media Account

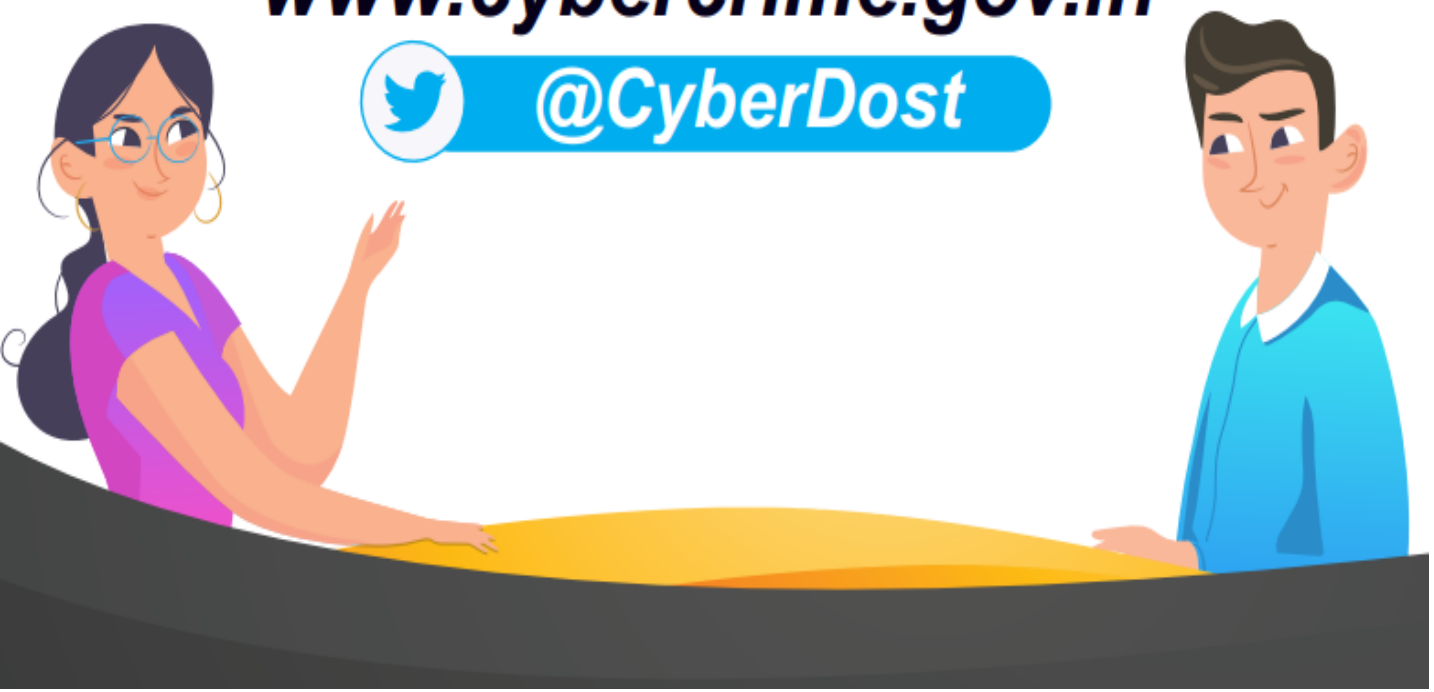
Twitter - https://twitter.com/Cyberdost
Facebook - https://www.facebook.com/CyberDost/4C
Instagram - https://www.instagram.com/cyberdosti4c
Telegram - https://t.me/cyberdosti4c

If you want to report something other than Cybercrime cases or in case of an emergency please contact your local police by dialing 100.

National Cyber Crime Reporting Portal

www.cybercrime.gov.in

@CyberDost



आज का साइबर (Cyber) सुविचार

सुरक्षित फाइनैनशियल ट्रानसेकशन (Financial Transaction) नहीं रहेगा अब सपना, जब 2- फेक्टर औथेंटीकेशन (2-Factor Authentication) साथ देगी अपना

Thankyou