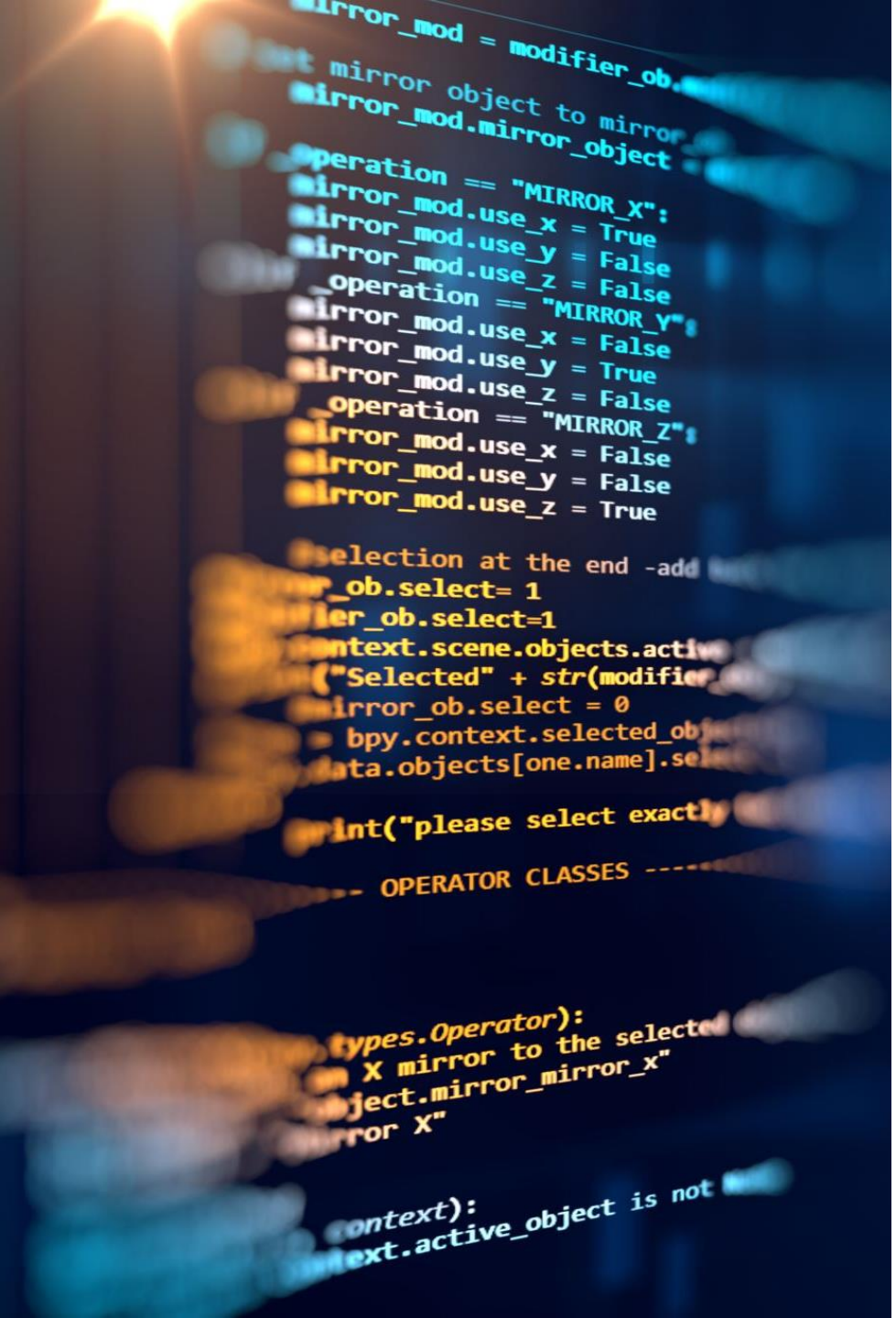


Cyber RISKS!

Dr. Ananth Prabhu G

BE, MBA, MTech, DCL, PhD, Post Doctoral Fellow

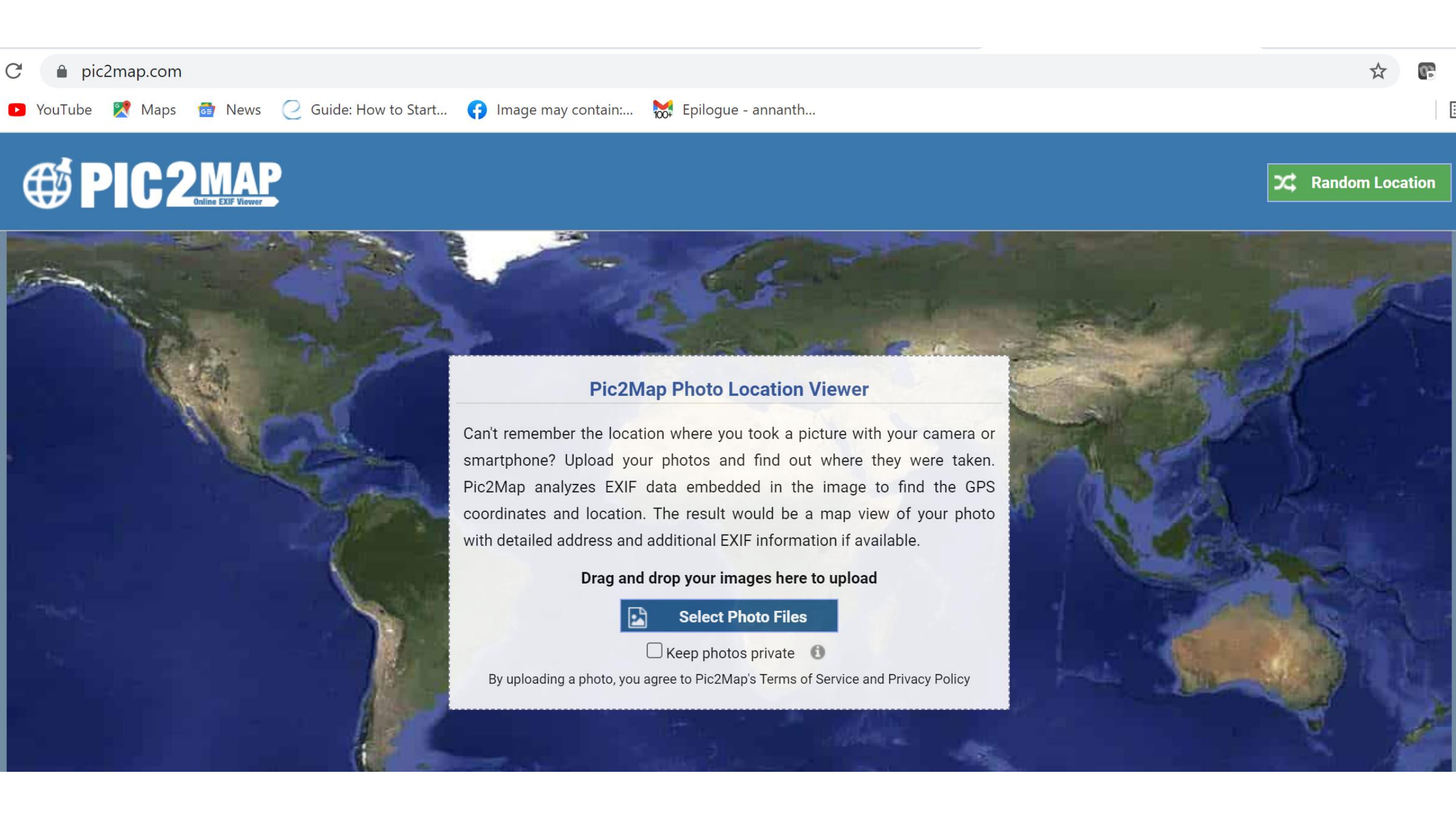
Professor & Principal Investigator- Cyber Sec and Digital Forensics CoE, Sahyadri

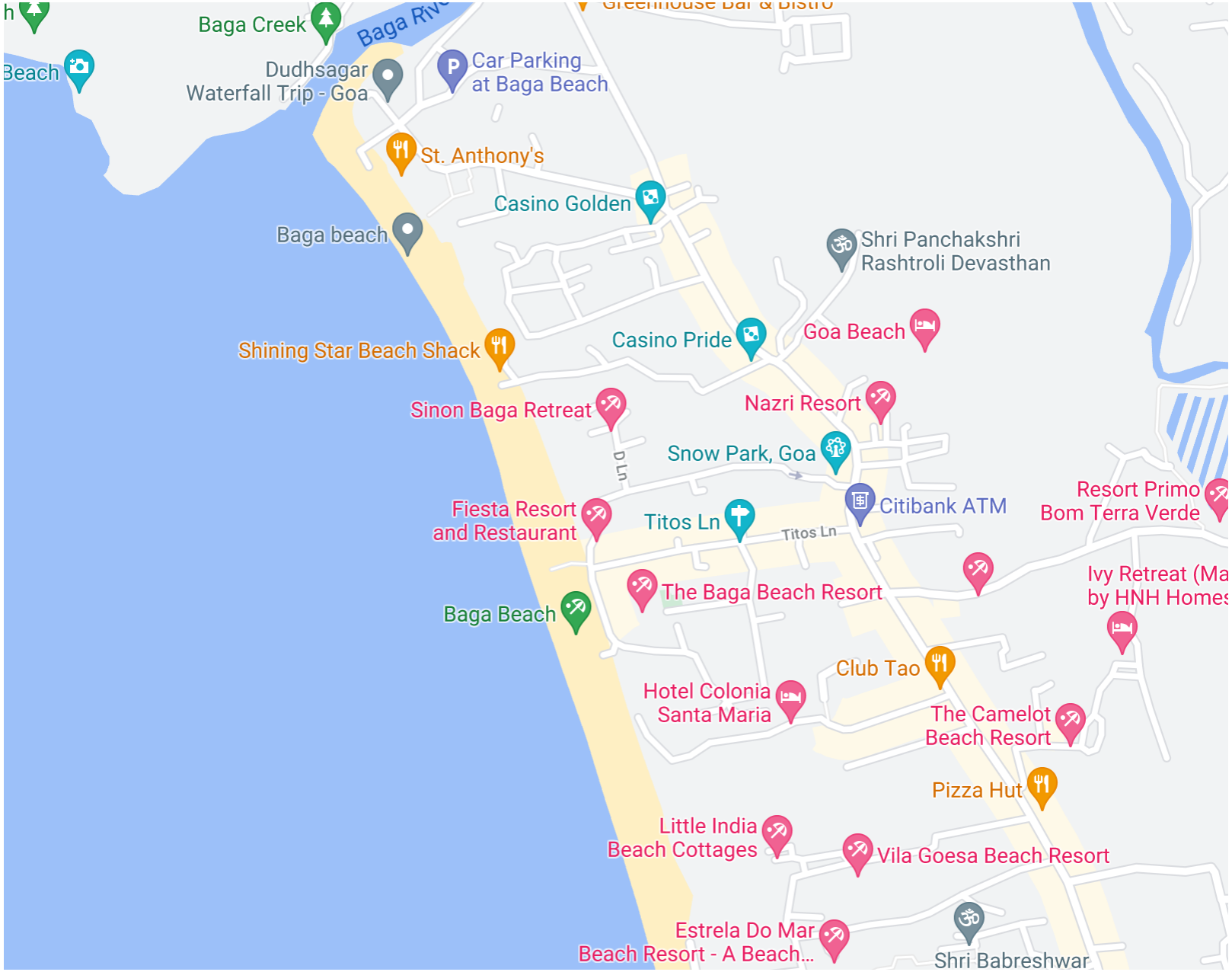
Cyber Law Trainer- Karnataka Judicial Academy

Cyber Security Trainer- Karnataka Police Academy

Director- SUREPASS Academy

Pray for KARNATAKA


pic2map.com
YouTube
Maps
News
Guide: How to Start...
Image may contain:...
Epilogue - annanth...
PIC2MAP
Online EXIF Viewer
Random Location
Pic2Map Photo Location Viewer
Can't remember the location where you took a picture with your camera or smartphone? Upload your photos and find out where they were taken. Pic2Map analyzes EXIF data embedded in the image to find the GPS coordinates and location. The result would be a map view of your photo with detailed address and additional EXIF information if available.
Drag and drop your images here to upload
Select Photo Files
Keep photos private
By uploading a photo, you agree to Pic2Map's Terms of Service and Privacy Policy


Baga Creek
Baga River
Beach
Dudhsagar
Waterfall Trip - Goa
Car Parking
at Baga Beach
St. Anthony's
Casino Golden
Baga beach
Shri Panchakshri
Rashtroli Devasthan
Shining Star Beach Shack
Casino Pride
Goa Beach
Sinon Baga Retreat
Nazri Resort
Snow Park, Goa
D Ln
Fiesta Resort
and Restaurant
Titos Ln
Titos Ln
Citibank ATM
Resort Primo
Bom Terra Verde
The Baga Beach Resort
Ivy Retreat (Ma
by HNH Homes
Baga Beach
Club Tao
Hotel Colonia
Santa Maria
The Camelot
Beach Resort
Pizza Hut
Little India
Beach Cottages
Vila Goesa Beach Resort
Estrela Do Mar
Beach Resort - A Beach...
Shri Babreshwar

UK14FC808

nehakakkar

Follow

2,083 posts **57.1m** followers **428** following

Neha Kakkar (Mrs. Singh)
Blessed! ♥🙏 Living My Dream 😇
Matlabi Yariyan Unplugged 🥰👇🏻
youtu.be/kCKMfYr_bYE

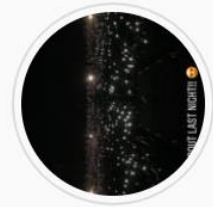
NehuPreet...

MxTakatak...

Fashion 🔥💄

DeepuSun...

SweetHom...

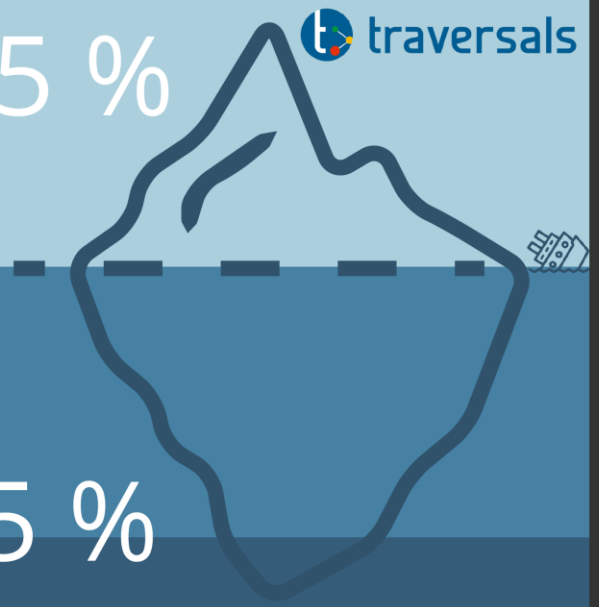

NehaKakka...

Travel😍

Surface Web is only the Tip of the Iceberg

SURFACE WEB
Google, Yahoo, Naver, Yandex, Wikipedia, Reddit, ...

5 %



DEEP WEB
Cloud Storage, Patent Data, Research Articles, LegaL Documents, Financial Records, ...

95 %

DARK WEB
Onion Sites, Hidden Marketplaces, Anonymous Journalism, ...

OSINT
MEDIA
TERRORIST'S DELIVERABLE
ARTICLES
INTERNET
REPORTS
Interviews, CT
News ops CT
Academic research
Journalists
NGO
Governments
Courts and law enforcement
International agencies
Social media
Websites, forums
Videos, audio recordings
Leaflets, booklets, books

Which is the third largest economy

1. USA
2. CHINA
3. ??????

?

Global Cybercrime Damage Costs:

- $6 Trillion USD a Year. *
- $500 Billion a Month.
- $115.4 Billion a Week.
- $16.4 Billion a Day.
- $684.9 Million an Hour.
- $11.4 Million a Minute.
- $190,000 a Second.

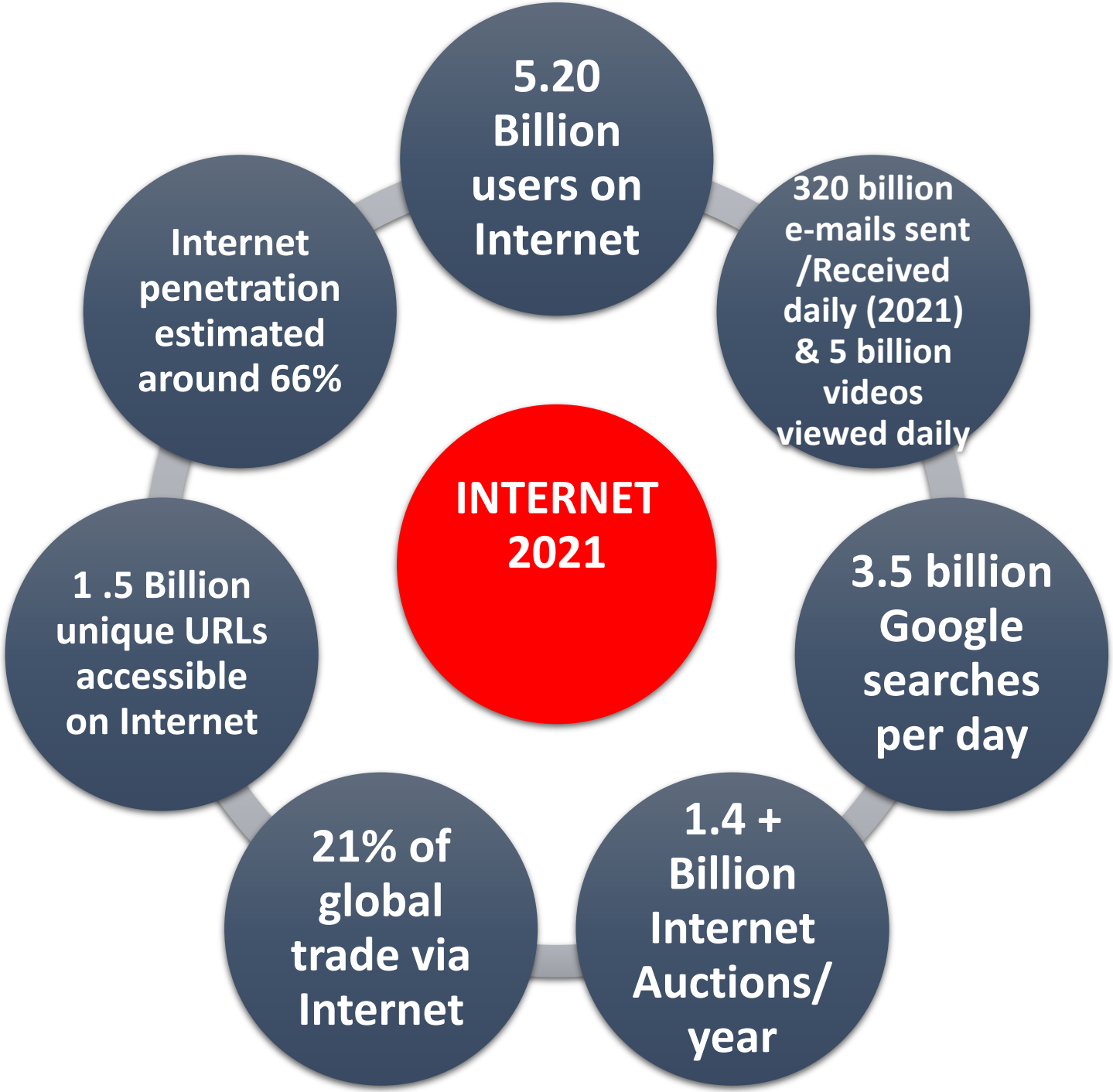
ALL FIGURES ARE PREDICTED BY 2021

* SOURCE: CYBERSECURITY VENTURES

CYBERSECURITY VENTURES

We have already spoken for 9 minutes and the damages globally for now is ONLY

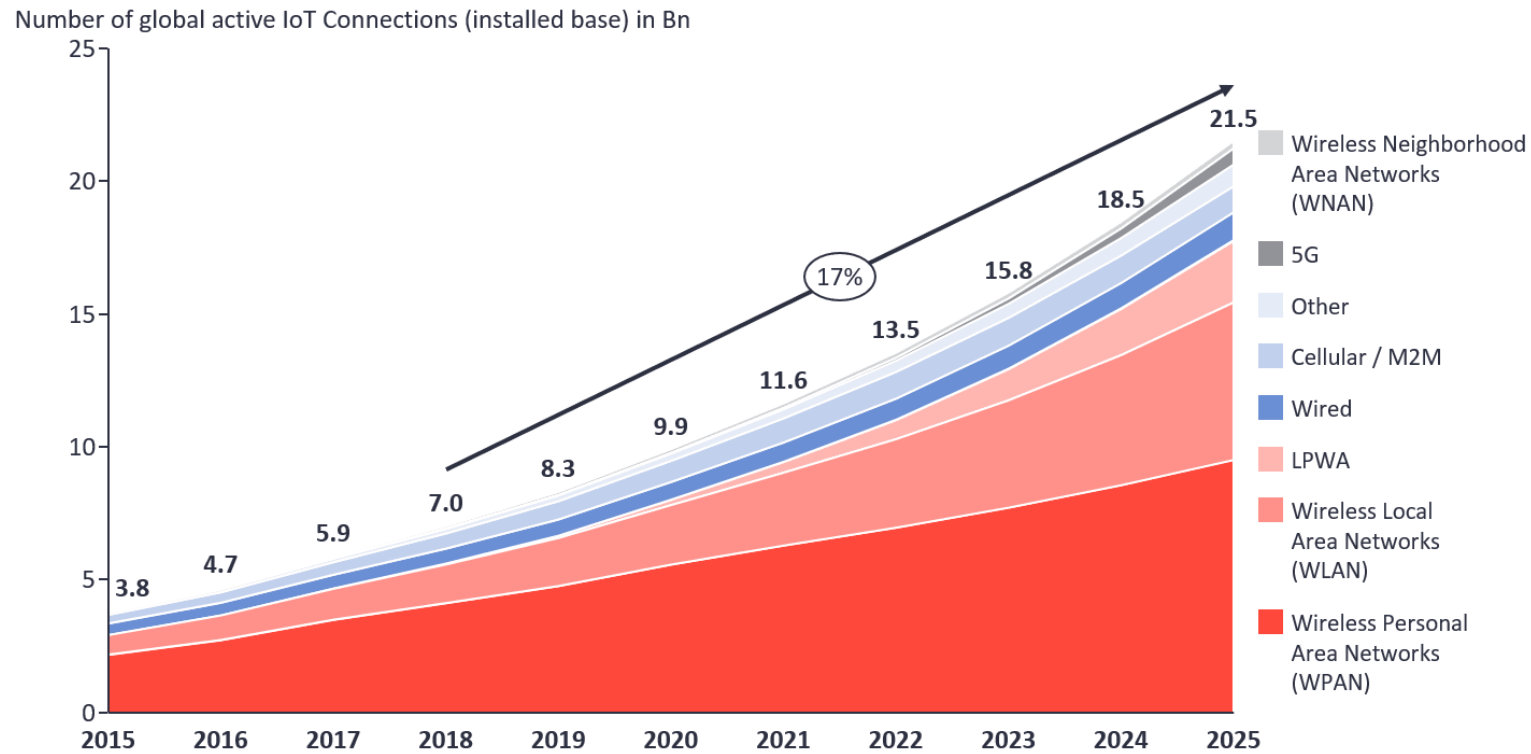
100 Million Dollars


INTERNET 2021
5.20 Billion users on Internet
320 billion e-mails sent /Received daily (2021) & 5 billion videos viewed daily
3.5 billion Google searches per day
1.4 + Billion Internet Auctions/ year
21% of global trade via Internet
1 .5 Billion unique URLs accessible on Internet
Internet penetration estimated around 66%

IOT ANALYTICS

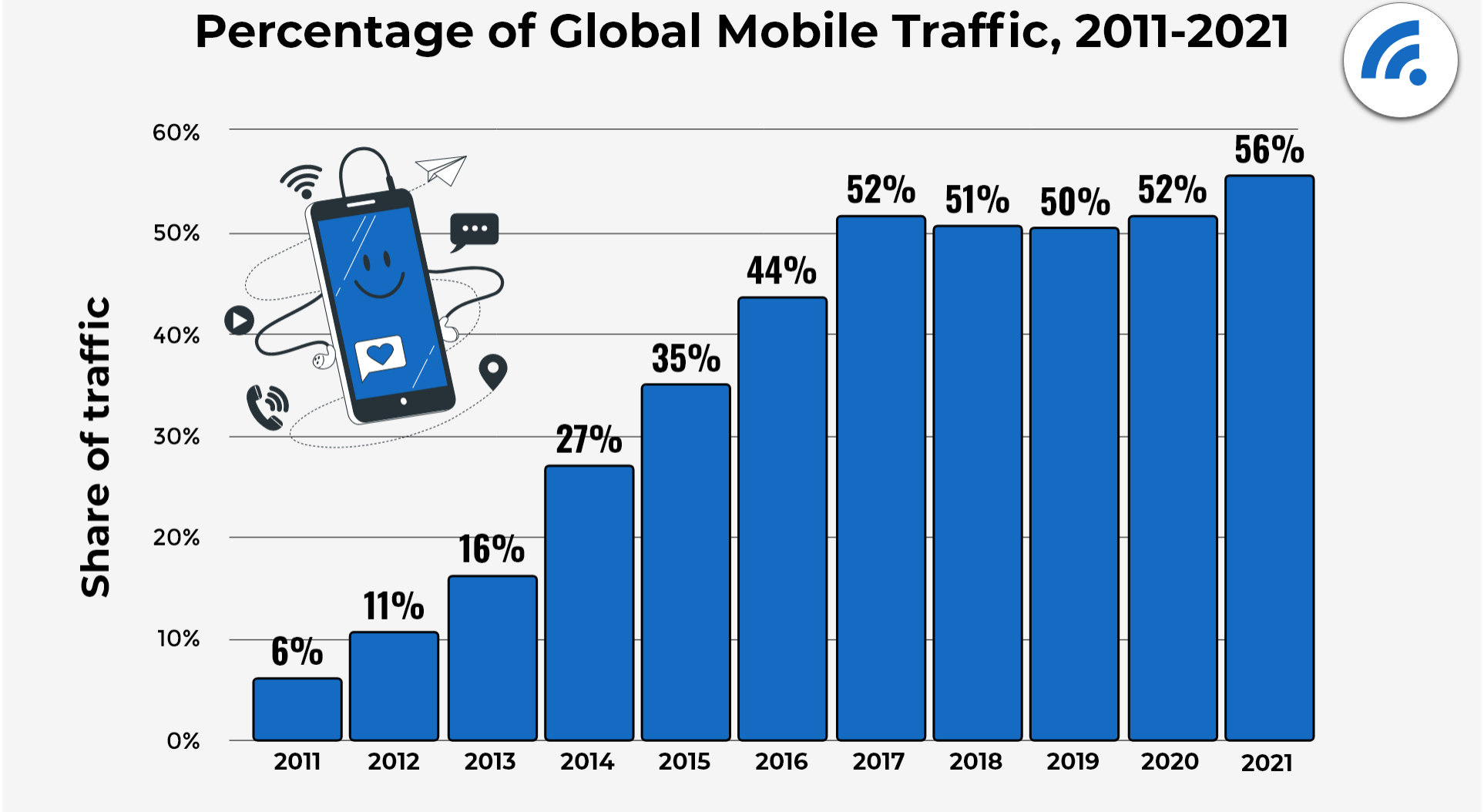
Insights that empower you to understand IoT markets

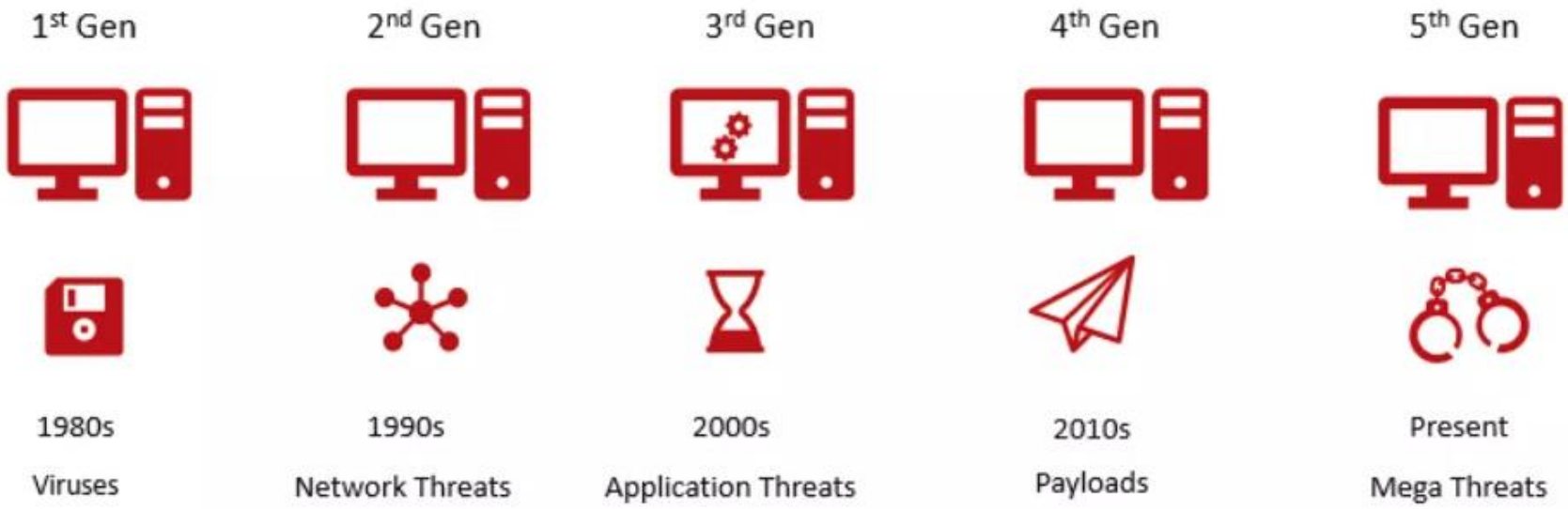
Global Number of Connected IoT Devices



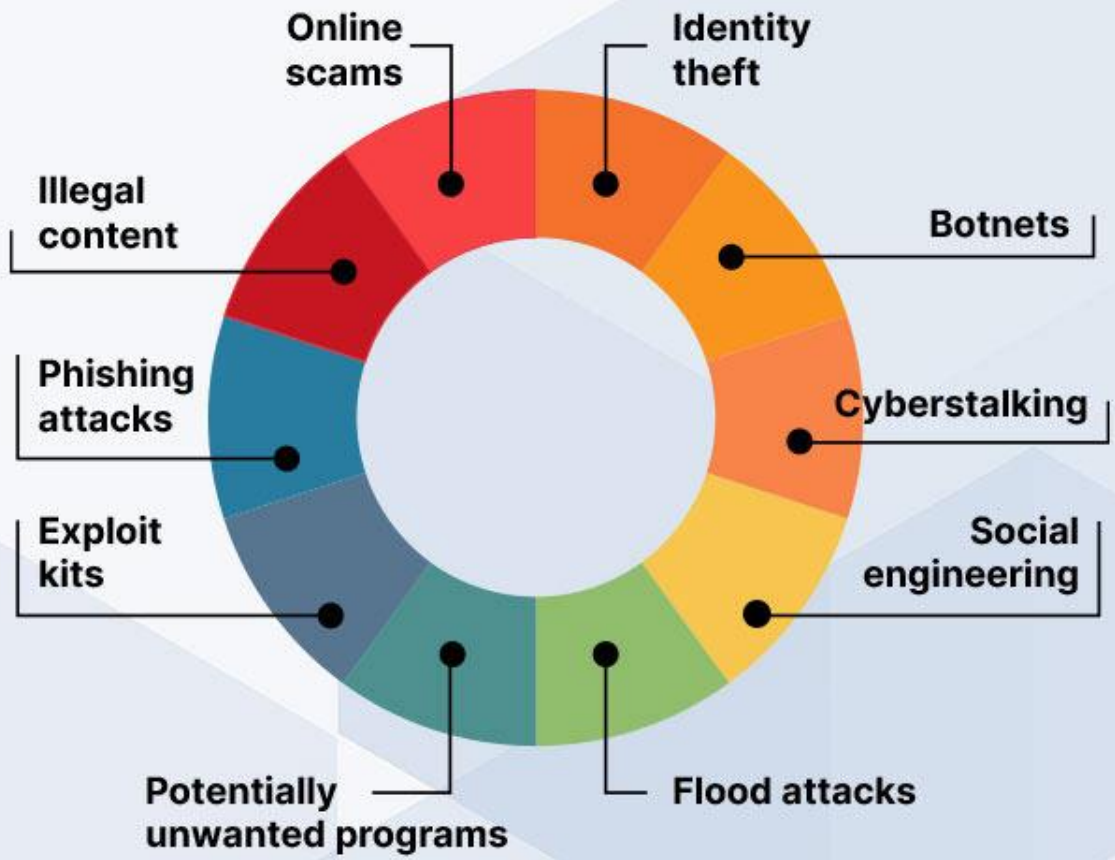
Note: IoT Connections do not include any computers, laptops, fixed phones, cellphones or tablets. Counted are active nodes/devices or gateways that concentrate the end-sensors, not every sensor/actuator. Simple one-directional communications technology not considered (e.g., RFID, NFC). Wired includes Ethernet and Fieldbuses (e.g., connected industrial PLCs or I/O modules); Cellular includes 2G, 3G, 4G; LPWAN includes unlicensed and licensed low-power networks; WPAN includes Bluetooth, Zigbee, Z-Wave or similar; WLAN includes Wi-fi and related protocols; WNAN includes non-short range mesh; Other includes satellite and unclassified proprietary networks with any range.
Source: IoT Analytics Research 2018

Percentage of Global Mobile Traffic, 2011-2021




1st Gen
2nd Gen
3rd Gen
4th Gen
5th Gen
1980s
Viruses
1990s
Network Threats
2000s
Application Threats
2010s
Payloads
Present
Mega Threats

Types of Cybercrime



SecurityTrails

5 Types of Cyber Criminals

The Social Engineer

The Spear Phisher

The Hacker

The Rogue Employee

The Ransom Artist

COVID19 Tip

Respect the real heroes who are helping you during COVID-19 pandemic situation.

Security Tip

Respect the privacy of others just as you expect the same from them.

COVID19 Tip

Refer government authorised sources for COVID-19 updates and news.

Security Tip

Refer authorised sources for downloading genuine app.

COVID19 Tip

Clean and disinfect your belongings after you reach home to secure your family from COVID-19.

Security Tip

Clear cookies and delete browsing history at end of session and stay safe.

COVID19 Tip

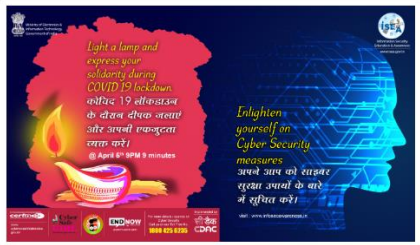
Include superfoods in your diet to boost your immunity and fight against COVID-19.

Security Tip

Pay extra attention when using public Wi-Fi, and avoid making payments while you are on unprotected Wi-Fi.

COVID19 Tip

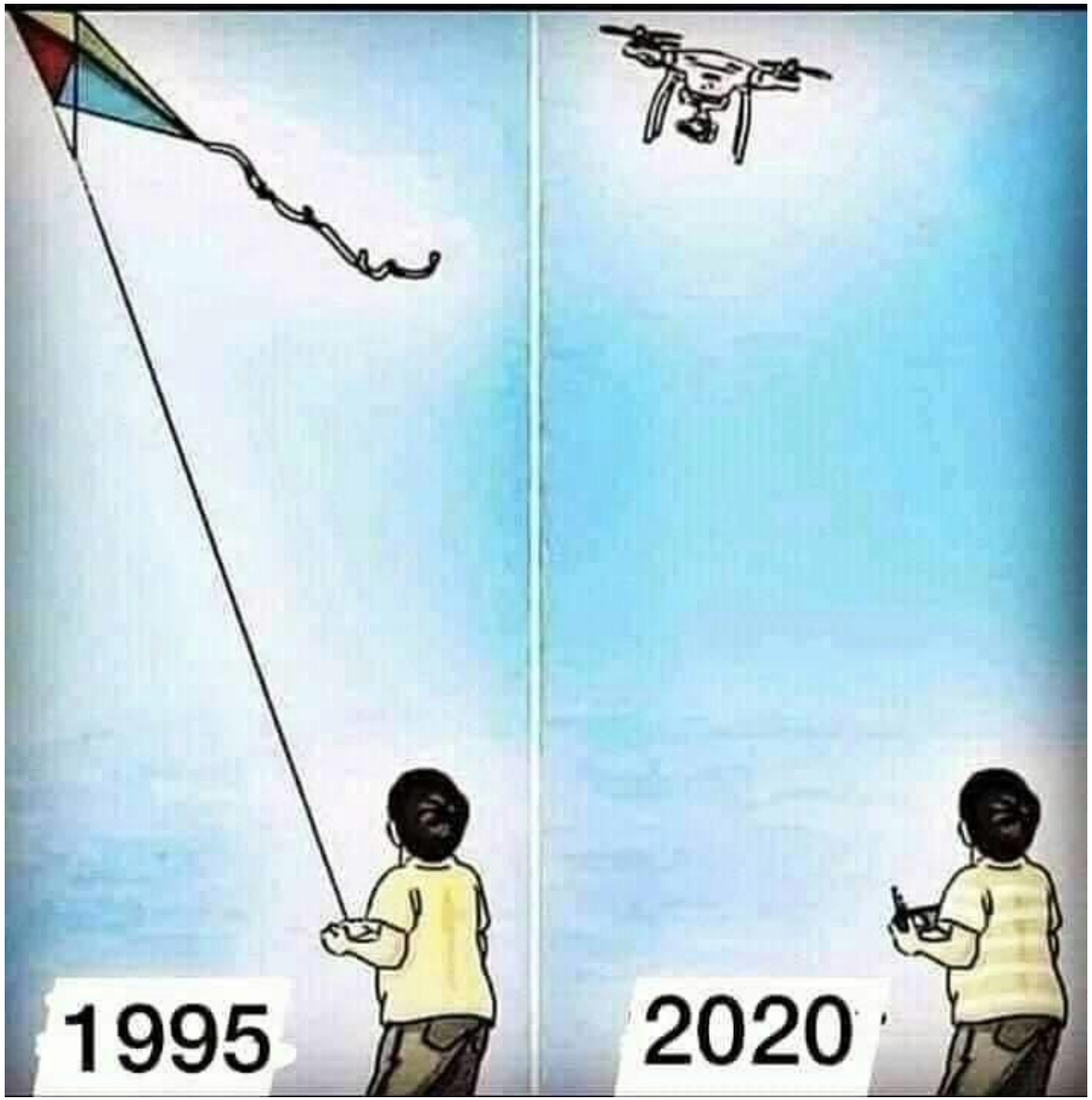
COVID19 Tip



COVID19 Tip

COVID19 Tip

Ministry of Electronics & Information Technology, Government of India
Dose 1
Dose 2
Ensure taking both the vaccine shots to sufficiently prepare your immune system to effectively fight against COVID- 19 virus as per Government guidelines
कोविड-19 वायरस से प्रभावी रूप से लड़ने के लिए अपनी प्रतिरक्षा प्रणाली को पर्याप्त रूप से तैयार करने के लिए दोनों वैक्सीन शॉट्स लेना सुनिश्चित करें।
certin
http://cert-in.org.in/
www.
cyberswachhtakendra.
gov.in
Cyber Safe GIRL
For more details / queries on Cyber Security Call us on our Toll free No.
1800 425 6235
Implemented by
ISEA
Information Security Education & Awareness
www.isea.gov.in
updating
Ensure updating your software with required patches and install regular updates to avoid dangers of software vulnerabilities and security issues
आवश्यक पैच के साथ अपने सॉफ़्टवेयर को अपडेट करना सुनिश्चित करें और सॉफ़्टवेयर भेद्यता और सुरक्षा समस्याओं के खतरों से बचने के लिए नियमित अपडेट स्थापित करें।
For more details visit :
www.
InfoSec
awareness.in


1995
2020

Coronavirus lockdown: Drone delivers pan masala in Gujarat. Video goes viral

A video of pan masala getting delivered using a drone in Morbi, a town in Gujarat has gone viral on the internet.

ADVERTISEMENT

India Today Web Desk
New Delhi
April 12, 2020 UPDATED: April 12, 2020 20:08 IST

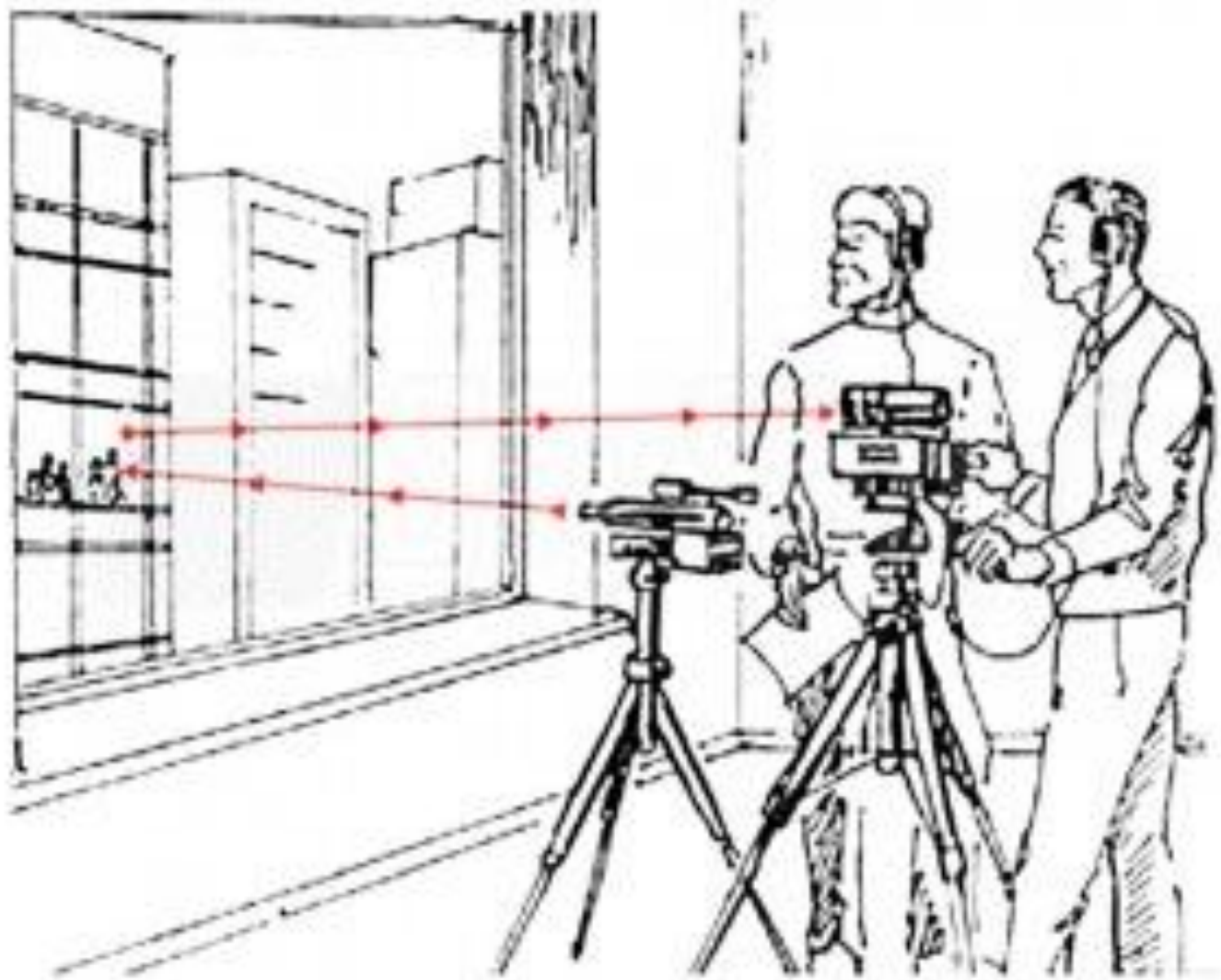
Drone delivers pan masala in Gujarat Photo: Instagram

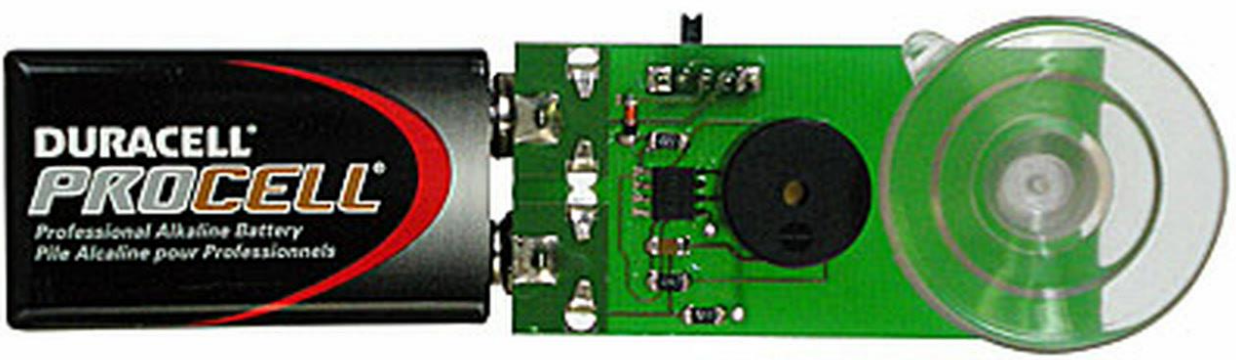
'Peeping drone' spies on girls in bathroom

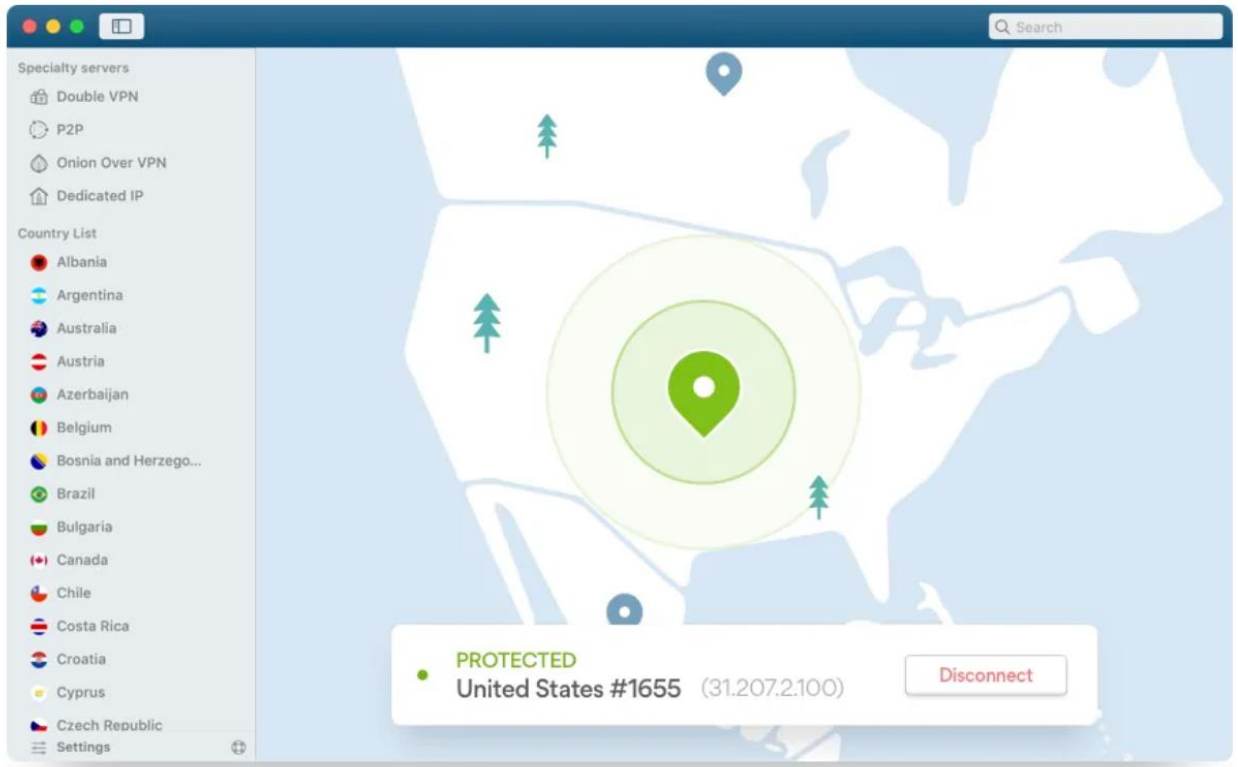
New Generation Spy Devices

Courtesy of ATN

BUY: SUPERIOR TACTICAL PVS-7 GOGGLES $2,095.00 BUY IT




DURACELL
PROCELL
Professional Alkaline Battery
Pile Alcaline pour Professionnels



Courtesy of NordVPN

BUY: NORDVPN SUBSCRIPTION $11.95/MONTH BUY IT

Courtesy of Amazon

ProElite

Courtesy of Amazon

BUY: SPY FINDER PRO $148.00 BUY IT

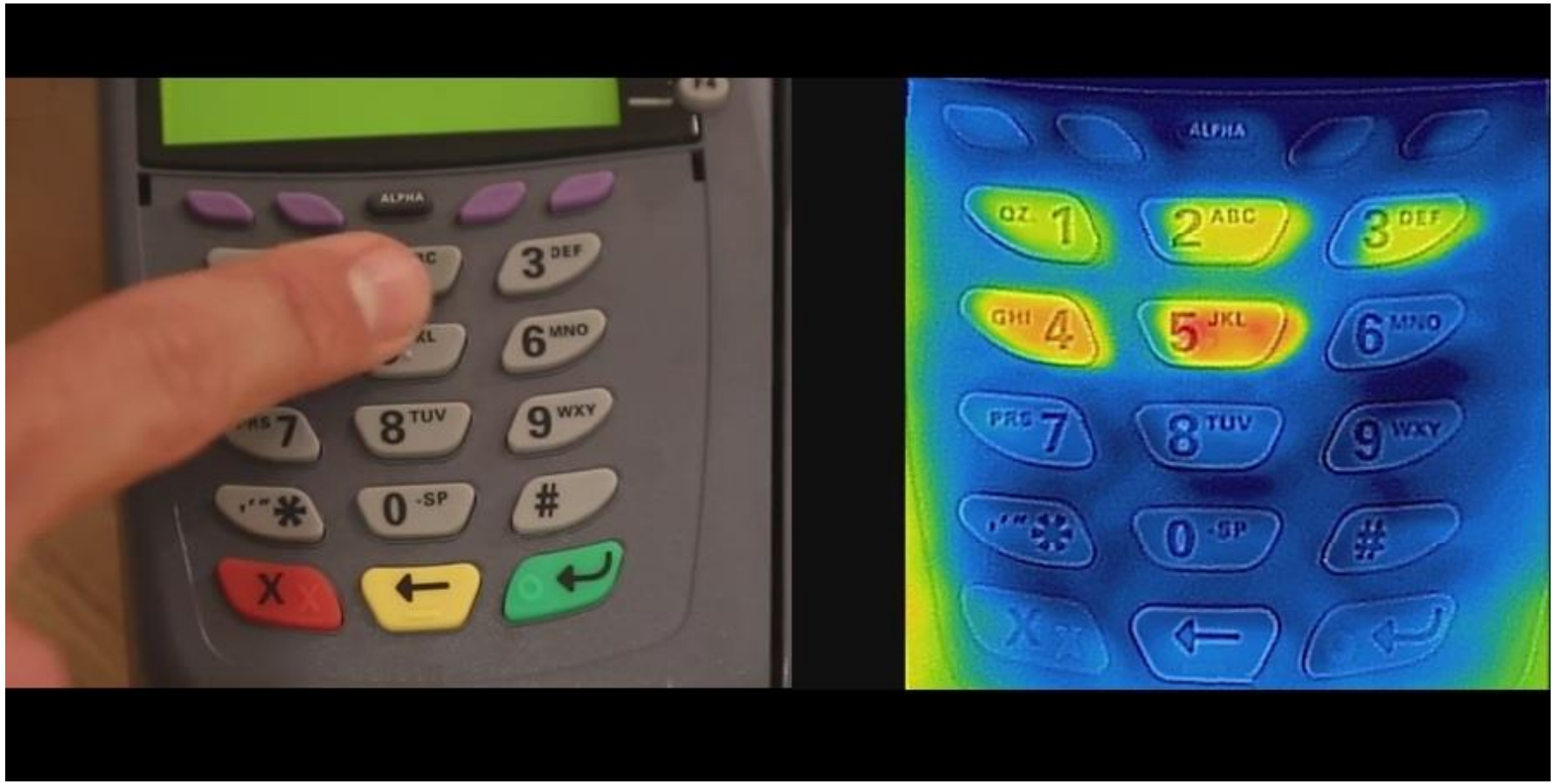
Courtesy of Amazon

BUY: JMDHKK M8000 AI RF DETECTOR $189.00 BUY IT

Courtesy of Amazon

BUY: FLIR ONE PRO LT (IOS) $249.00 BUY IT

BUY: FLIR ONE PRO LT (ANDROID) $299.99 BUY IT


ALPHA
3 DEF
6 MNO
8 TUV
9 WXY
0 SP
ALPHA
QZ 1
2 ABC
3 DEF
GHI 4
5 JKL
6 MNO
PRS 7
8 TUV
9 WXY
0 SP

Courtesy of Amazon

BUY: KINGSTON IRONKEY S1000 $129.54 BUY IT

9:41

HausBell®
LOW
HIGH
FREE
Headphone

FILTER CIGARETTES
Marlboro
HÚT THUỐC
GÂY UNG THƯ PHỔI

lintratek

CDMA
GSM
3G
4G LTE
Wi Fi
GPS
LOJACK
POWER
CHARGE

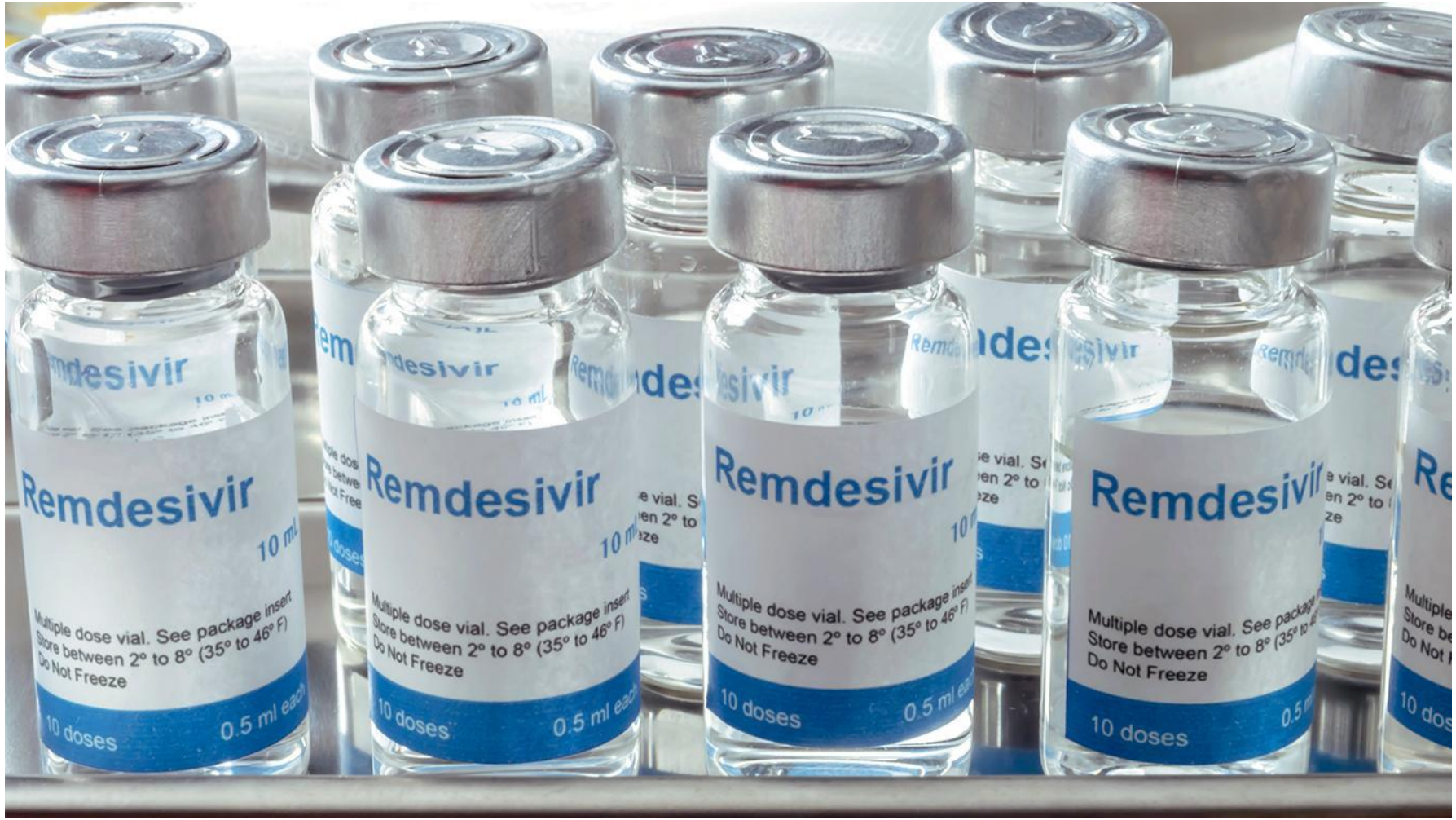
POWER
BATTERY PACK
MADE IN KOREA

Clear
5′ 9″
Measure
Level

COVID-19 IMPACT

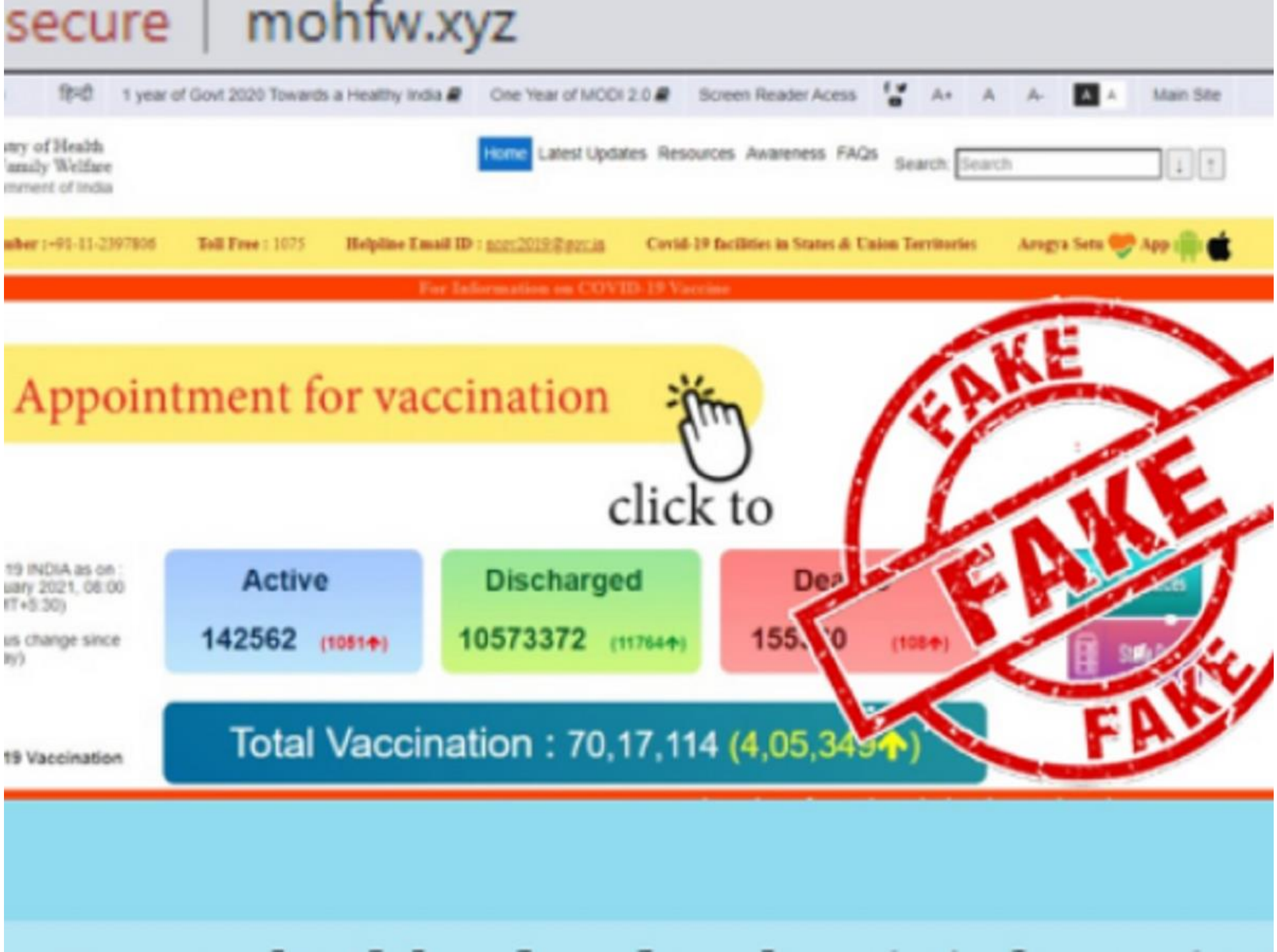
ON CYBERCRIME

FAKE
FAKE
FAKE
PULSE OXIMETER
97
84
%SpO2
PRbPm
BREAKING NEWS
Fake Oximeter App to Steal Mobile Data
ISH NEWS


Remdesivir
10 ml
Multiple dose vial. See package insert
Store between 2° to 8° (35° to 46° F)
Do Not Freeze
10 doses
0.5 ml each

OTP Fraud Call !!!
Can i have your OTP?
NO WAY!
https
Your OTP is:
****
COVID-19
VACCINE
NAGPURTODAY.IN

HAWAIAN
Memorial Hospital
Intentional Self
Suicide Preve
We hear


secure | mohfw.xyz
1 year of Govt 2020 Towards a Healthy India
One Year of MODI 2.0
Screen Reader Acess
Main Site
Home
Latest Updates
Resources
Awareness
FAQs
Search
Search
Toll Free : 1075
Helpline Email ID : ncov2019@gov.in
Covid-19 facilities in States & Union Territories
Aarogya Setu App
Appointment for vaccination
click to
Active
142562 (1051↑)
Discharged
10573372 (11764↑)
Total Vaccination : 70,17,114 (4,05,349↑)
FAKE
FAKE
FAKE
FAKE

Top stories

INDIA TV

Sonu Sood notifies followers about fake COVID-19 donation campaign in his name

1 day ago

The Tribune

Sonu Sood notifies followers about fake Covid-19 donation campaign in his name

1 day ago

FIRSTPOST.

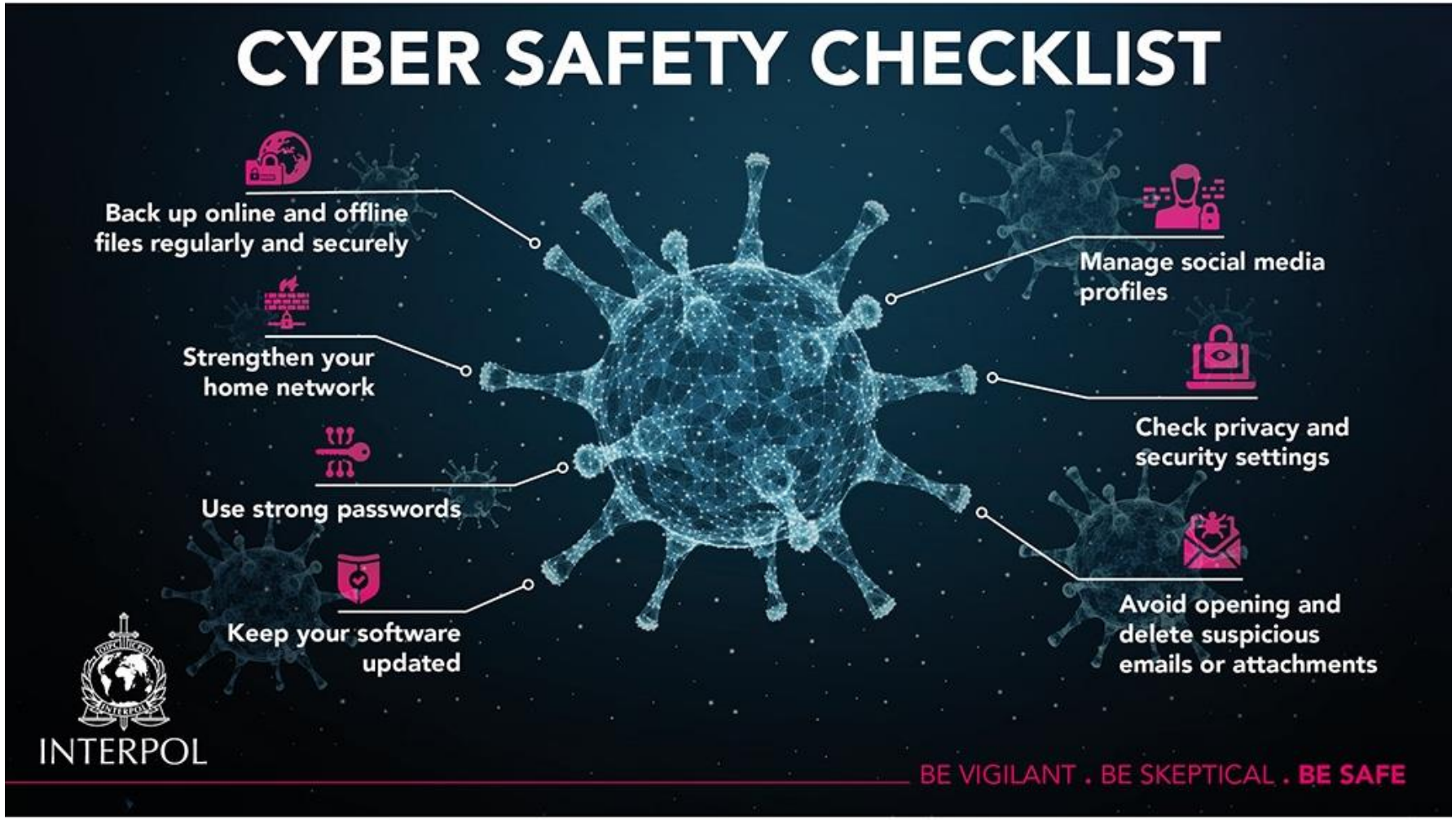
Sonu Sood warns people about fake COVID-19 donation campaign under his…

22 hours ago

View all

Alert ! OTP Fraud
LOAN EMI Moratorium

सावधान ! कही आपका LOAN EMI टालना आपका खाता खाली तो नहीं कर देगा।


CYBER SAFETY CHECKLIST
Back up online and offline files regularly and securely
Strengthen your home network
Use strong passwords
Keep your software updated
Manage social media profiles
Check privacy and security settings
Avoid opening and delete suspicious emails or attachments
INTERPOL
BE VIGILANT . BE SKEPTICAL . BE SAFE

GOOD CYBER HYGIENE
#WashYourCyberHands
of ransomware
INTERPOL

NOTHING BAD IS GOING
TO HAPPEN TO ME

Hacking is the new Normal

Sanjay Sahay

DON’T TRY THIS UNLESS YOU LOVE **INDIAN JAILS**

Cyber Crime

- **Cyber crime is defined as a crime in which a Digital communication Device is the object of the crime, or used as a tool / target or used incidental or as a witness to commit an offence.**
- **Cybercriminals may use Information technology to access personal information, business trade secrets or use the internet for exploitive or malicious purposes.**

Cybercrime

- **Global in Character** - The whole world could be the crime scene in a cybercrime.
- **Intangible evidence** - The evidence may have been erased, damaged or secreted/Encrypted. Correct facts may not come to light.
- **Silent in Nature** - There are no signs of physical violence or struggle at the scene of crime
- **Substantial Losses** – Cyber Crime losses are huge. Bank frauds value-wise and volume-wise have increased substantially. Its impact is severe and it may be a long term.

In just 10 years camera man & pilot both lost their jobs. UPGRADE YOURSELF

How to attend Online Class :

Step 1 : 🎙

Step 2 : 🔇

Step 3 :

Online classes

behind the camera. 😂

One last pic before **I go to sleep!**

ANI
filmymonkey
OPINION POLL
EXIT POLL
ANI
RESULT

Chat Applications

Safest

- SilentCircle
- Redphone
- OSTel
- ChatSecure
- SignalChat

Safe

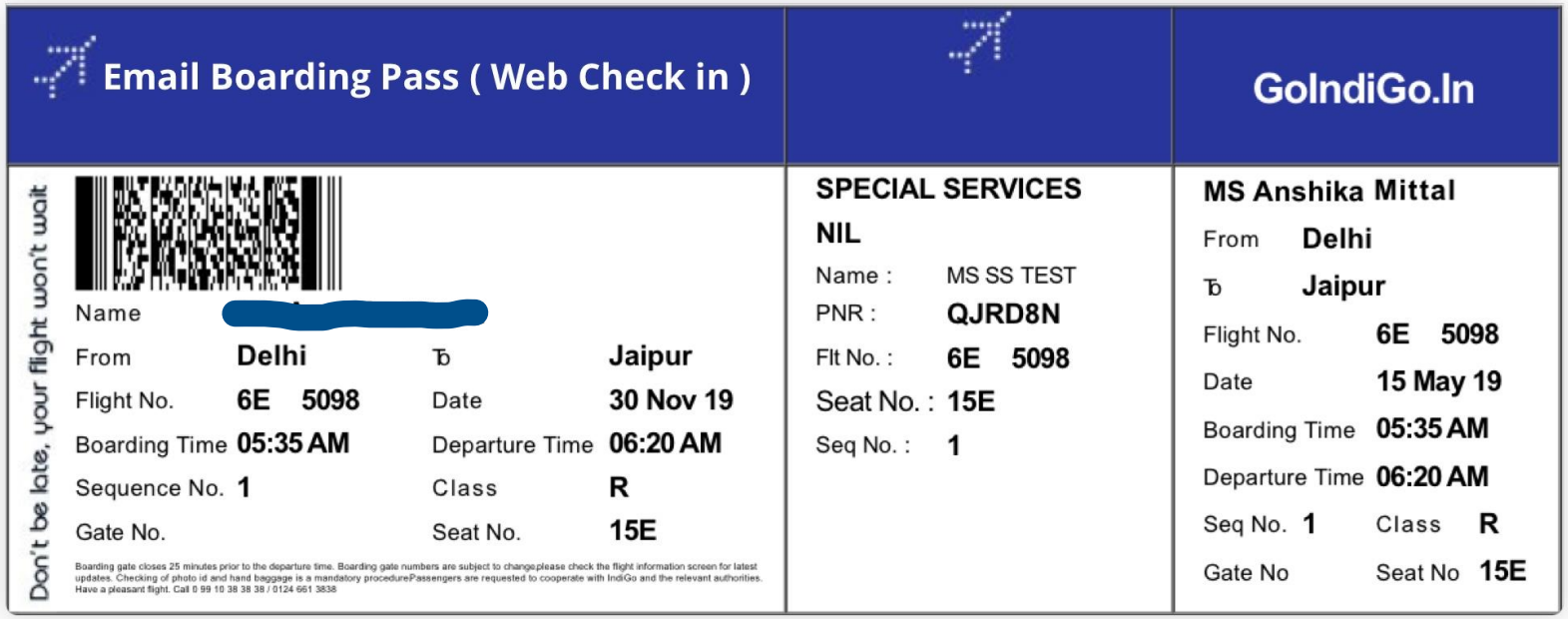
- Telegram
- Wickr
- Threema
- Surespot

Moderate Safe

- CoverMe
- BBM
- iMessage
- FaceTime
- Hangouts
- Facebook Messenger

Unsafe

- Viber
- WhatsApp
- LINE
- Tango
- ooVoo
- Kakao Talk
- WeChat
- IM+Pro
- Nimbuzz
- Hike
- Chat ON
- Kik
- Voxer
- imo
- GroupMe



Email Boarding Pass (Web Check in)

GoIndiGo.In

Don't be late, your flight won't wait

Name [redacted]

From	Delhi	To	Jaipur
Flight No.	6E 5098	Date	30 Nov 19
Boarding Time	05:35 AM	Departure Time	06:20 AM
Sequence No.	1	Class	R
Gate No.		Seat No.	15E

Boarding gate closes 25 minutes prior to the departure time. Boarding gate numbers are subject to change,please check the flight information screen for latest updates. Checking of photo id and hand baggage is a mandatory procedure.Passengers are requested to cooperate with IndiGo and the relevant authorities. Have a pleasant flight. Call 0 99 10 38 38 38 / 0124 661 3838

SPECIAL SERVICES

NIL

Name : MS SS TEST

PNR : **QJRD8N**

Flt No. : **6E 5098**

Seat No. : **15E**

Seq No. : **1**

MS Anshika Mittal

From	**Delhi**
To	**Jaipur**
Flight No.	**6E 5098**
Date	**15 May 19**
Boarding Time	**05:35 AM**
Departure Time	**06:20 AM**
Seq No. **1**	Class **R**
Gate No	Seat No **15E**

ReadMyBoP - Read My Boarding Pass

www.bighugesystems.com Travel & Local

★★★½☆ 33

3+

This app is compatible with all of your devices.

Add to Wishlist

Install

A. Gender
B. Which passenger number in the ticket
C. Passenger Last name
D. Passenger First name
E. Ticket Type (Online/Physical)
F. PNR
G. Source
H. Destination
I. Flight Carrier
J. Flight Number
K. Passenger Seat Class
L. Seat Number
M. Flight Sequence Number
N. Passenger Clearance Status
O. Passenger Checked IN/Not
P. What document type this is
Q. Where this document was printed ar airport or somewhere else
R. Printed
S. Flight Date
T. Document issuing Flight company
U. Document is authorised or not

AMS
eezeetags

Beware
before you scan QR
code
iam
cheated

FILL UP & GO
FILL UP & GO
HERE
WITH OUR SPEEDY PAYMENT SERVICE
Powered by PayPal
0557#02
SCAN OR ENTER CODE FROM YOUR CAR TO PAY
0557#02
NOT SET UP? PICK UP A LEAFLET IN STORE
HERE'S TO KEEPING BRITAIN MOVING

DIGITAL FOOTPRINTS

What do yours say?

BE CAREFUL ABOUT:

- What you share.
- Where you share.
- With whom you share.

BE SMART ABOUT:

- Sites you visit.
- Emails you open.
- Links you click.

BE YOURSELF

but be your best self.

Room No 632

K.R.Ramamoorthi

26-11-2008

Google

- **Google knows you better than you know about yourself!**
- **Google does not forget**
- **Google does not delete**
- **Over 271 Google Products & Services You Probably Don't Know**

Google My Activity

- https://myactivity.google.com/myactivity
- **1.Activity controls**
- **2.Web & App Activity**
- **3.Location History**
- **4.Device Information**
- **5.Voice & Audio Activity**
- **6.YouTube Search History**
- **7.YouTube Watch History**

Privacy…

- **You are not the Customer**
  You are the Product.
- **Smart Phone etc**
- **Cookies**
- **GPS**
- **Maps**
- **E mail issues**
- **You are exposed!**

MY DAD TOLD ME YOU'RE SPYING ON US
HE'S NOT YOUR DAD

CYBER
LAW
?

Chapter	Section	Description
Chapter 1	Section 1 to 2	Preliminary
Chapter 2	Section 3 to 3A	Digital Signature and Electronic Signature
Chapter 3	Section 4 to 10A	E-Governance
Chapter 4	Section 11 to 13	Attribution Acknowledgement & Distribution of Electronic Records
Chapter 5	Section 14 to 16	Secure Electronic Records & Secure Electronic Signatures
Chapter 6	Section 17 to 34	Regulation of Certifying Authorities
Chapter 7	Section 35 to 39	Electronic Signature Certificates
Chapter 8	Section 40 to 42	Duties of Subscribers
Chapter 9	Section 43 to 47	Penalties, Compensation and Adjudication
Chapter 10	Section 48 to 64	The Cyber Regulations Appellate Tribunal
Chapter 11	Section 65 to 78	Offences
Chapter 12	Section 79	Intermediaries not to be liable in certain cases
Chapter 12A	Section 79A	Examiner of Electronic Evidence
Chapter 13	Section 80 to 90	Miscellaneous

Section	Offence	Description	Penalty
66	Hacking with computer system	If a person with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hack.	Imprisonment up to three years, or/and with fine up to ₹500,000
66B	Receiving stolen computer or communication device	A person receives or retains a computer resource or communication device which is known to be stolen or the person has reason to believe is stolen.	Imprisonment up to three years, or/and with fine up to ₹100,000
66C	Using password of another person	A person fradulently uses the password, digital signature or other unique identification of another person.	Imprisonment up to three years, or/and with fine up to ₹100,000

Section	Offence	Description	Penalty
67	Publishing information which is obscene in electronic form.	If a person publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it.	Imprisonment up to five years, or/and with fine up to ₹1,000,000
67A	Publishing images containing sexual acts	If a person publishes or transmits images containing a sexual explicit act or conduct.	Imprisonment up to seven years, or/and with fine up to ₹1,000,000
67B	Publishing child porn or predating children online	If a person captures, publishes or transmits images of a child in a sexually explicit act or conduct. If a person induces a child into a sexual act. A child is defined as anyone under 18.	Imprisonment up to five years, or/and with fine up to ₹1,000,000 on first conviction. Imprisonment up to seven years, or/and with fine up to ₹1,000,000 on second conviction.
67C	Failure to maintain records	Persons deemed as intermediatary (such as an ISP) must maintain required records for stipulated time. Failure is an offence.	Imprisonment up to three years, or/and with fine.

CYBER LAW IN INDIA

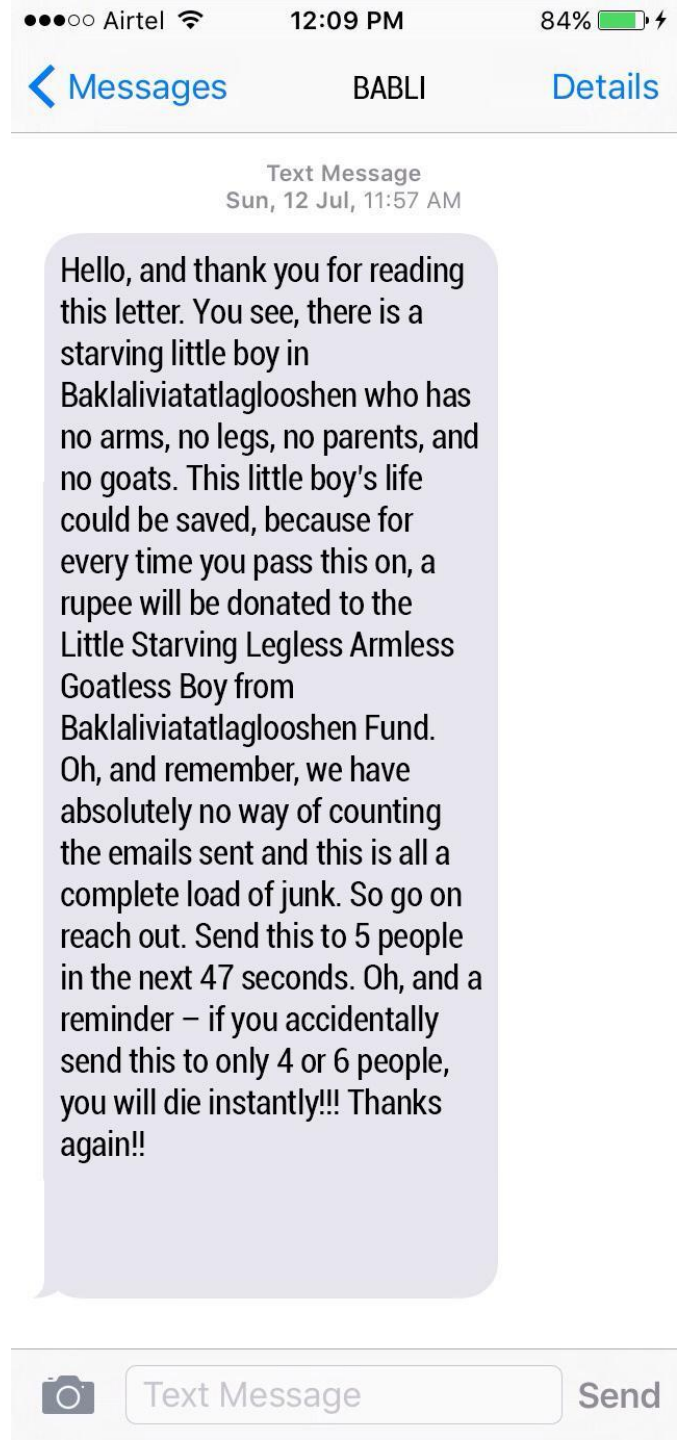
Sl. No	Offences	Section Under IT Act
1	Tampering with computer source Documents	Sec.65
2	Hacking with computer systems, Data Alteration	Sec.66
3	Dishonestly receiving stolen computer resource or communication device	Sec.66B
4	Identity theft	Sec.66C
5	Cheating by personation by using computer resource	Sec.66D
6	Violation of privacy	Sec.66E
7	Cyber terrorism	Sec.66F
8	Publishing or transmitting obscene material in electronic form	Sec .67
9	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form	Sec.67A
10	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form	Sec.67B
11	Preservation and Retention of information by intermediaries	Sec.67C
12.	Powers to issue directions for interception or monitoring or decryption of any information through any computer resource	Sec.69

13.	Power to issue directions for blocking for public access of any information through any computer resource	Sec.69A
14.	Power to authorize to monitor and collect traffic data or information through any computer resource for Cyber Security	Sec.69B
15.	Un-authorized access to protected system	Sec.70
16.	Penalty for misrepresentation	Sec.71
17.	Breach of confidentiality and privacy	Sec.72
18.	Publishing False digital signature certificates	Sec.73
19.	Publication for fraudulent purpose	Sec.74
29.	Act to apply for offence or contraventions committed outside India	Sec.75
21.	Compensation, penalties or confiscation not to interfere with other punishment	Sec.77
22.	Compounding of Offences	Sec.77A

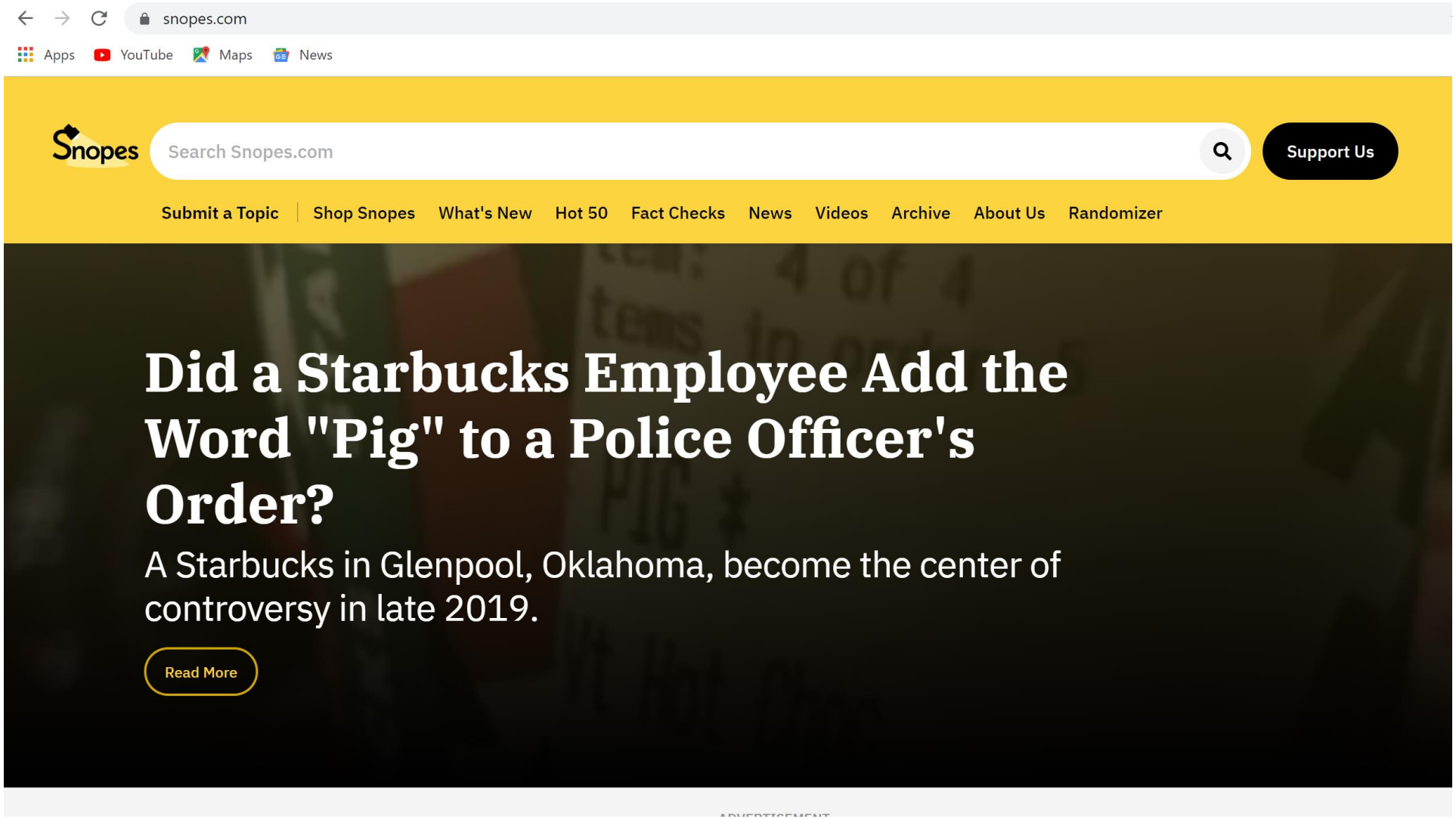
23.	Offences with three years imprisonment to be cognizable	Sec.77B
24.	Exemption from liability of intermediary in certain cases	Sec.79
25.	Punishment for abetment of offences	Sec.84B
26.	Punishment for attempt to commit offences	Sec.84C
27.	Offences by Companies	Sec.85
	Note : Sec.78 of I.T. Act empowers Police Inspector to investigate cases falling under this Act	
28.	Sending threatening messages by e-mail	Sec .503 IPC
29.	Word, gesture or act intended to insult the modesty of a woman	Sec.509 IPC
30.	Sending defamatory messages by e-mail	Sec .499 IPC
31.	Bogus websites, Cyber Frauds	Sec .420 IPC
32.	E-mail Spoofing	Sec .463 IPC
33.	Making a false document	Sec.464 IPC
34.	Forgery for purpose of cheating	Sec.468 IPC
35.	Forgery for purpose of harming reputation	Sec.469 IPC
36.	Web-Jacking	Sec .383 IPC
37.	E-mail Abuse	Sec .500 IPC
38.	Punishment for criminal intimidation	Sec.506 IPC
39.	Criminal intimidation by an anonymous communication	Sec.507 IPC

40.	When copyright infringed: Copyright in a work shall be deemed to be infringed	Sec.51
41.	Offence of infringement of copyright or other rights conferred by this Act. Any person who knowingly infringes or abets the infringement of	Sec.63
42.	Enhanced penalty on second and subsequent covictions	Sec.63A
43.	Knowing use of infringing copy of computer programme to be an offence	Sec.63B
44.	Obscenity	Sec. 292 IPC
45.	Printing etc. of grossly indecent or scurrilous matter or matter intended for blackmail	Sec.292A IPC
46.	Sale, etc., of obscene objects to young person	Sec .293 IPC
47.	Obscene acts and songs	Sec.294 IPC
48.	Theft of Computer Hardware	Sec. 378
49.	Punishment for theft	Sec.379
50.	Online Sale of Drugs	NDPS Act
51.	Online Sale of Arms	Arms Act

HOW YOUR PHONE CAN BE HACKED


●●●○○ Airtel
12:09 PM
84%
Messages
BABLI
Details
Text Message
Sun, 12 Jul, 11:57 AM
Hello, and thank you for reading this letter. You see, there is a starving little boy in Baklaliviatatlaglooshen who has no arms, no legs, no parents, and no goats. This little boy's life could be saved, because for every time you pass this on, a rupee will be donated to the Little Starving Legless Armless Goatless Boy from Baklaliviatatlaglooshen Fund. Oh, and remember, we have absolutely no way of counting the emails sent and this is all a complete load of junk. So go on reach out. Send this to 5 people in the next 47 seconds. Oh, and a reminder – if you accidentally send this to only 4 or 6 people, you will die instantly!!! Thanks again!!
Text Message
Send

DIED
From not forwarding
that text message to
10 people


snopes.com
Apps
YouTube
Maps
News
Snopes
Search Snopes.com
Support Us
Submit a Topic
Shop Snopes
What's New
Hot 50
Fact Checks
News
Videos
Archive
About Us
Randomizer
Did a Starbucks Employee Add the Word "Pig" to a Police Officer's Order?
A Starbucks in Glenpool, Oklahoma, become the center of controversy in late 2019.
Read More

Are you safe with your e mail Accounts?

Gmail,yahoo,etc not safe

No social media platform is safe

.ios/ icloud also not safe!

Use privacy settings pl

Use your own office/institutions

e mail accounts…

Which is the safe e mail?

1.CounterMail

2. Protonmail

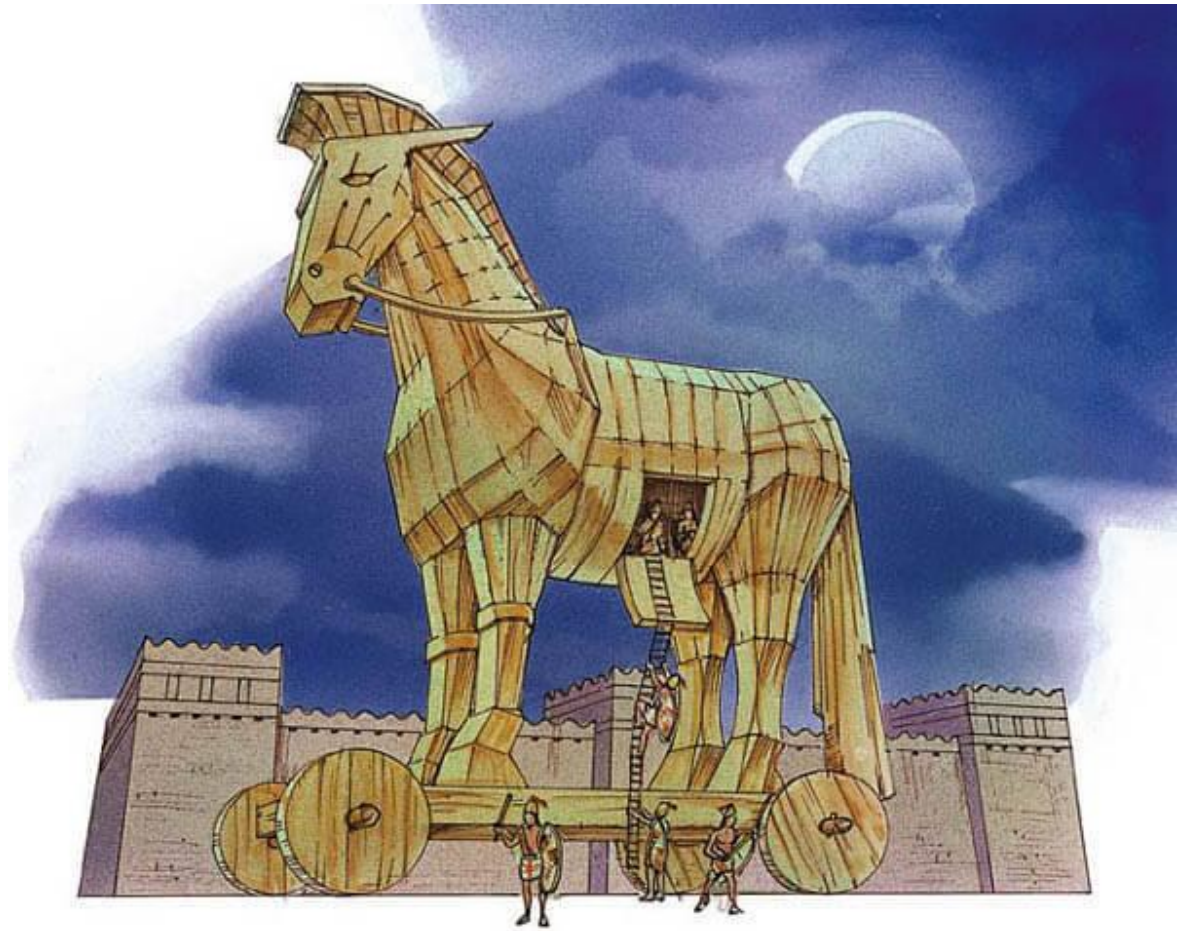
3. Hushmail

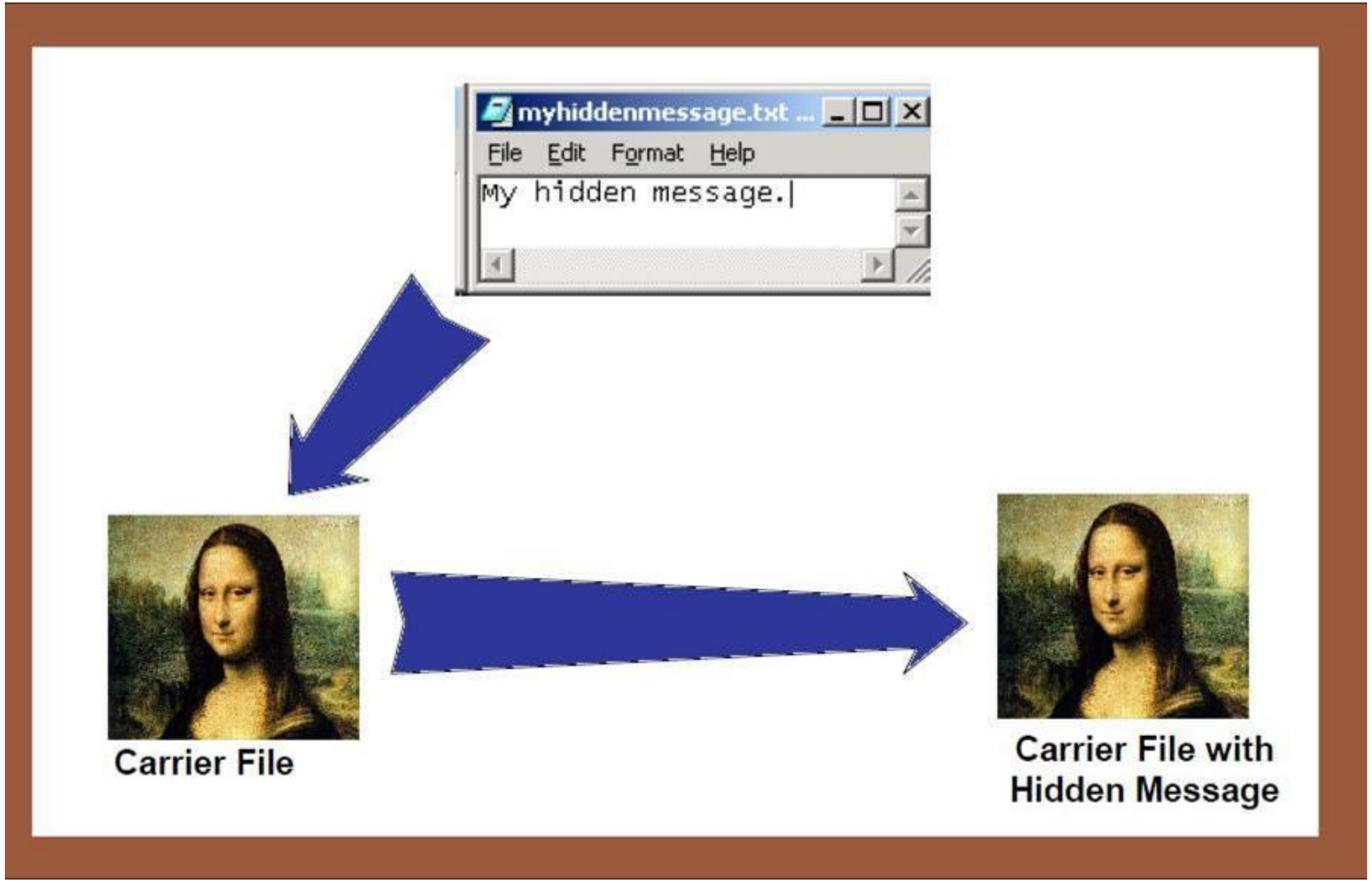
4. Mailfence

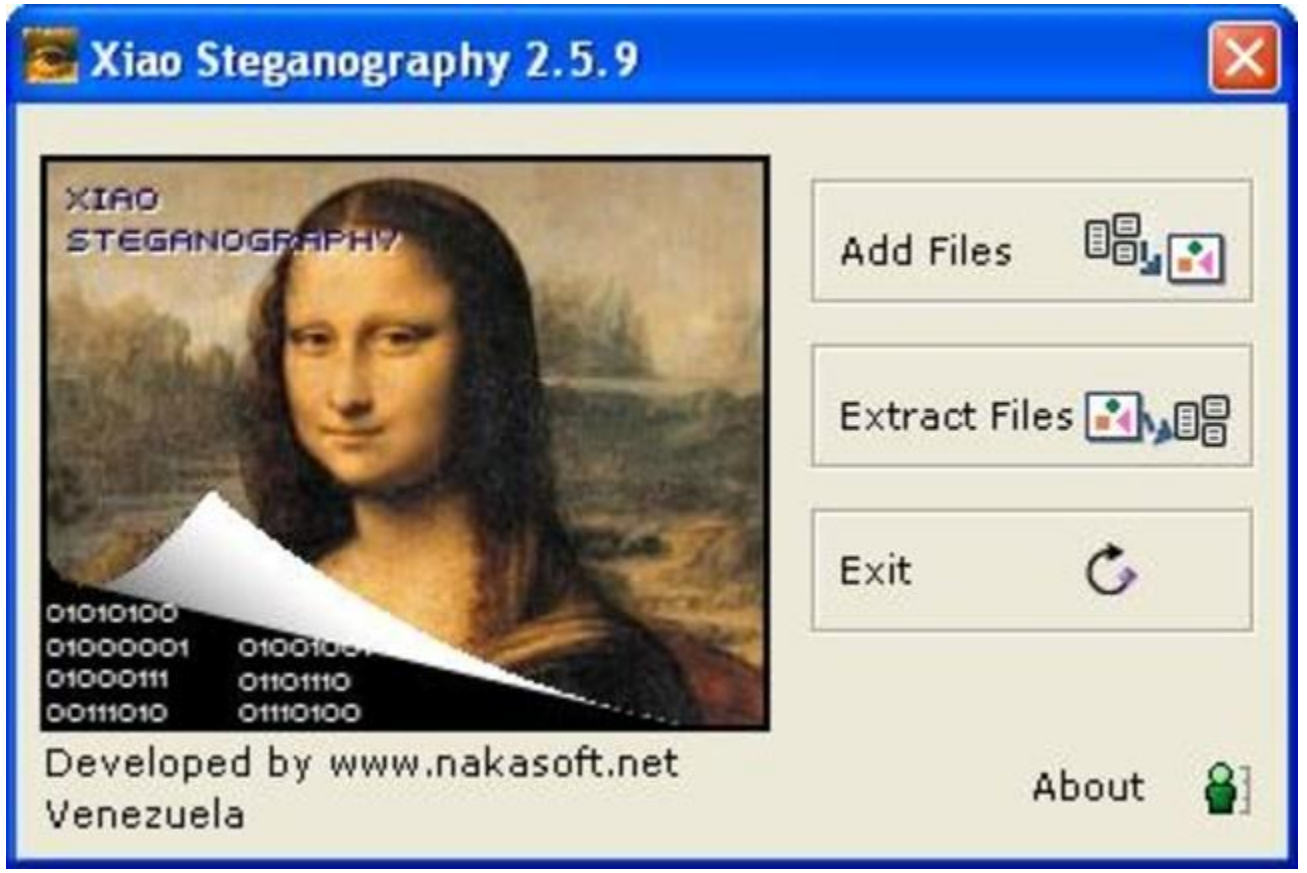
5. Tutanota

Email encryption

Institutions e mails




myhiddenmessage.txt ...
File Edit Format Help
My hidden message.
Carrier File
Carrier File with
Hidden Message


Xiao Steganography 2.5.9
XIAO
STEGANOGRAPHY
01010100
01000001
01000111
00111010
01101110
01110100
Add Files
Extract Files
Exit
Developed by www.nakasoft.net
Venezuela
About

Nobody is safe, no matter the post

Some of the Indians whose phone numbers figured on the leaked list of potential surveillance targets, according to The Wire, *The Guardian* and 14 other media outlets that formed a collective for the Pegasus Project

Rahul Gandhi's number and that of his advisers and friends was on the list before 2019 elections

Ashok Lavasa became election commissioner in January 2019 and resigned in August 2020

Supreme Court employee who accused then CJI Ranjan Gogoi of sexual harassment

Rona Wilson, later named an accused in the Elgaar Parishad case, was on the list in 2017

Gagandeep Kang, virologist who was in 2018 helping with the Nipah response

Prashant Kishor, political strategist whose latest assignment was the Bengal election

Abhishek Banerjee, nephew of Mamata Banerjee and Trinamool general secretary

Sachin Rao, close associate of Rahul Gandhi, was on the list in 2019

Alankar Sawai, another close associate of Rahul Gandhi, on the list in 2019

Jagdeep Chhokar, a member of the Association for Democratic Reforms

Ashwini Vaishnaw, appointed IT minister in the latest shuffle, was on the list in 2017

Prahlad Singh Patel, a Union minister, his family and staff were on the list in 2019

M. Hari Menon, director of the Bill and Melinda Gates Foundation's Indian operations

Sushant Singh, journalist who investigated the controversial Rafale deal

Siddharth Varadarajan, founding editor of The Wire

M.K. Venu, founding editor of The Wire

Rohini Singh, journalist who investigated into the finances of Amit Shah's son Jay Shah

Swati Chaturvedi, journalist and author of *I am a troll*, a book on the BJP's digital army

Use of data not spying: Minister

J.P. YADAV

New Delhi: New information technology minister Ashwini Vaishnaw on Monday told the Lok Sabha that use of data did not amount to surveillance, reacting to allegations that the Centre had snooped on opponents and critics using the Israeli spyware Pegasus.

His predecessor Ravi Shankar Prasad wondered at a media briefing why India alone was being put in the dock when 45 nations were using Pegasus, thus appearing to acknowledge that the government had used the armament had used the spyware.

Vaishnaw told the House: "It is also beyond doubt that the data has nothing to do with surveillance or NSO (the Israeli company that developed Pegasus), so there can be no factual basis to suggest that use of the data somehow equates to surveillance."

He added: "Any form of illegal surveillance is not possible with the checks and balances in our laws and our robust institutions."

The minister was making a statement on the controversy over a global investigation report that said the Indian government had used its snoop-ware on more than 300 mobile phones in India.

A fresh list released on Monday by the international exposé suggests that even Vaishnaw had been selected as a potential surveillance target in 2017.

The Centre has so far evaded any direct reply to the specific question whether it had purchased the Pegasus spyware from NSO.

Relying heavily on NSO's statement, Vaishnaw termed the investigative report a conspiracy to malign India's democracy while denying any unauthorised snooping by the government.

Prasad seemed to indirectly admit government use of Pegasus but sought to deny it when asked directly.

"Sabhiyo, yeh asaval phir relevant hota hai, ki jab 45 se adhik desh Pegasus ka agyog kar rahe hain, jaise ki NSO se hamara koi, tech nir/ Bharat ko hi target kyon kiya jaa raha hai? Therefore, the question again becomes relevant that if 45 countries in the world are using Pegasus, as NSO has said, why in India alone being targeted?" Prasad said.

Recently sacked as law, IT and communications minister, Prasad had been fielded to attack those using the Pegasus controversy to corner the government.

Asked directly whether his party's government at the Centre used the Pegasus spyware, Prasad first sought to avoid a direct reply.

On being pressed, he said: "We have never said that we have purchased it."

He added that there was a foolproof legal framework for phone tapping and that the government never breaks it.

Put on the defensive by the international exposé, the government tried to play victim, alleging a design to defame it.

"In this same kind of revenge for the way India handled Covid, the way 73 per cent of the people are getting free vaccines and the way India's global clout has increased under Prime Minister Modi?" Prasad asked.

Shah goes back to 'chronology'

OUR SPECIAL CORRESPONDENT

New Delhi: Union home minister Amit Shah, under attack from the Opposition on Monday over an explosive report on the alleged phone-tapping of opposition leaders in the country using Israeli spyware Pegasus, called it "a report by the dispirited for the obstructors".

He questioned the timing of the leak and said it was done to create disruptions on the first day of the monsoon session of Parliament. Shah also used his much controversial phrase *"Aage chronology samajhiye"* to counter criticism of the government over the Pegasus reports.

"People have often associated this phrase with me in the lighter vein, but today I want to seriously say — the timing of the sensitive leaks, the disruptions... Aage chronology samajhiye! This is a report by the disrupters for the obstructors," he said in a statement.

"Disrupters are global organisations that have no role in India's progress. Obstructors are political players in India who do not want India to progress. People of India are very good at understanding this chronology and connection," he added.

An international media consortium had on Sunday reported that more than 300 verified mobile phone numbers, including that of two serving ministers, over 40 journalists, three Opposition leaders and one sitting judge besides scores of businessmen and activists in India, could have been targeted for hacking through an Israeli spyware sold only to governments/agencies.

The Wire, a digital news platform, on Monday reported that senior Congress leader Rahul Gandhi, election strategist Prashant Kishor, former election commissioner Ashok Lavasa, ministers Ashwini Vaishnaw and Prahlad Patel, TMC leader Abhishek Banerjee and the entire family of a Supreme Court staffer who had accused the then Chief Justice of India Ranjan Gogoi of sexual harassment in 2019 were among those whose phone numbers were either breached or were listed as potential targets by Israeli company NSO Group's Pegasus spyware.

Without naming Pegasus, the home minister said: "The facts and sequence of events are for the entire nation to see. Today the monsoon session of Parliament has started. In what seemed like a perfect cue, late last evening we saw a report, which has been amplified by a few sections with only one aim — to do whatever is possible and humiliate India at the world stage, peddle the same old narratives about our nation and derail India's development trajectory."

Shah also slammed the Congress for the uproar in Parliament on Monday and accused the party of "trying to run away from discussions that matter most to us in Parliament".

"Just a few days ago the council of ministers was expanded with great emphasis given to women, SC, ST and OBC members. But there are forces unable to digest this. They also want to derail national progress. This merits the question — to whose tune are these people dancing, who want to keep showing India in poor light? What pleasure do they get to show India in bad light time and again?" Shah said.

Amit Shah

Congress seeks probe on PM

FROM PAGE 1

Surjewala said: "Who in the Government of India purchased and deployed the illegal spyware Pegasus? Who authorised the purchase? How many hundred or thousand crores were spent?"

The Congress underlined that the government had admitted snooping via Pegasus in Parliament on November 29, 2019, contrary to Monday's denial of spying by new information technology minister Ashwini Vaishnaw.

"Why could the minister Amit Shah not be summoned in this? Is this not a case for a full investigation of the Prime Minister?" Surjewala said.

Both Kharge and Adhir said Shah should be sacked if the government had any pretensions to morality.

Two numbers used by Rahul were allegedly among the potential targets. Rahul gave up those numbers after WhatsApp alerted him about possible hacking. Several members of Rahul's social circles and office staff too were allegedly put under surveillance.

The Wire reported that the phone number of IT minister Vaishnaw was among the potential targets between 2017 and 2019. Minister Prahlad Singh Patel's name also figures in the list.

Former finance minister and Congress veteran P. Chidambaram contested Vaishnaw's claim, made in the Lok Sabha on Monday, that illegal snooping was impossible in India.

"NSO Group, the owner of Pegasus, has said that NSO sells its technologies only to law enforcement and intelligence agencies of vetted governments. It is a matter of utmost concern that I have been named in this list. Is this not a case for a full investigation of the Prime Minister?" Surjewala said.

"In his statement, the minister has omitted to quote the crucial part of Pegasus's statement. The services that are 'openly available to anyone, anywhere, and anytime' refer to HLR Lookup services, not to Pegasus. The minister should answer a simple question: Did the government acquire the Pegasus software/ spyware?"

The Congress and other Opposition parties plan to jointly raise the matter during the ongoing session of Parliament.

On Monday, the Congress released a report by Cert-In, a department under the IT ministry, that had on May 17, 2019, said: "A vulnerability has been reported in WhatsApp which could be exploited by a remote attacker to execute arbitrary code on the affected systems."

The party also recalled that then IT minister Ravi Shankar Prasad had said in the Rajya Sabha on November 29, 2019, that the hacking of 121 telephones had been reported and a notice issued to the NSO.

"The NSO Group had written to Citizen Lab of the Munk School of Global Affairs, University of Toronto stating clearly that 'Our product is licensed to government and law enforcement agencies for the sole purpose of investigating and preventing crime and terror', Surjewala said.

"It is thus clear that the Government of India and its agencies bought the spyware. It could neither be bought nor deployed by any private operator. The Citizen Lab submitted a report on September 18, 2018, saying the Pegasus software was used to target politicians in India."

Surjewala said Indian citizens should realise that the government was spying on their daughters, sons and wives by murdering privacy.

Rahul taunted the Prime Minister for "reading everything on your phone".

Virologist Kang was a potential target in 2018 while tackling the Nipah infection.

On the woman who accused Justice Gogoi of sexual harassment, The Wire said her family and she received her allegations in a secure manner on April 20, 2019, and was marked as a "potential threat just days after the CJI's ordeal".

The leaked records show that eight other phone numbers belonging to her husband and two of his brothers were flagged as possible candidates for surveillance in the same week, when her allegations against the CJI were first reported, the portal said.

"All told, a total of 11 numbers associated with the complainant and her family were selected, making them among the largest cluster of associated phone numbers in the India leg of the Pegasus Project," The Wire added.

Bengal polls were not spared either

FROM PAGE 1

According to The Wire, Amnesty's forensic analysis found traces of infection on Kishor's phone on April 29, just a day before the last of the eight phases of polling in Bengal.

It added that traces of Pegasus on Kishor's phone were also detected on 14 days in June 2021 and 12 days in July 2021, including July 12, the day he met Congress leaders Rahul Gandhi and Priyanka Gandhi Vadra in Delhi.

On Monday evening, Abhishek, Trinamul general secretary, MP and Mamata's nephew, tweeted: "Two Minutes of SILENCE for the SORE LOSERS!"

He added: "Despite ALLIES like ED, CBI, NIA, IT, ECI, @BJP4India's money + might and @PegasusSpying, Mr @AmitShah couldn't save his face in #BengalElections2021. Please COME Prepared with Better RESOURCES in 2026"

Several senior Trinamul leaders said they expected Mamata to focus on the issue on Wednesday. July 21, when the party commemorates Martyrs' Day.

"Expect fireworks from her on Wednesday," said a party vice-president. Mamata is scheduled to address the huge annual event on the Trinamul calendar virtually — because of the pandemic — from Spec. This time, the party has made arrangements for the event to be shown live at various locations across India, including Gujarat and Delhi.

"She realises the firepower of this issue, and she will utilise it optimally," he said, adding that a reminder about Mamata's repeated allegations in the past couple of years that her phone had been hacked by the BJP and the agencies at its disposal.

"If the use of such methods during the Bengal elections is taken as a test case, then it is quite clear that such things hardly have any impact on the electoral outcome," Kishor told The Wire.

Kishor, who helped Trinamul script a remarkable turnaround within two years of the party being routed in the 2019 Lok Sabha polls, said on there is no denying that those who did so were looking to take undue advantage of their position of power with the help of illegal snooping."

Kishor's I-Pac has been retained by Trinamul for not only the general election of 2024 but also the Assembly polls of 2026 in Bengal.

Don't treat computer content as proof: Hany's wife

FROM PAGE 1

Among the surveillance targets named by the exposé are academics Hany Babu MT, Vernon Gonsalves, Anand Teltumbde and Sheetal Sathe, activists Gautam Navlakha and Rona Wilson, and lawyers Arun Ferreira and Sudha Bharadwaj.

The members of several relatives and suspected associates of Elgaar detainees too were on the list.

They include: "Varavara Rao's daughter Pavana; lawyer Surendra Gadling's wife Miral Gadling, his associate lawyers Nihalsingh Rathod and Jagadish Meshram, one of his former clients Maruti Kurwatkar, who was charged in multiple cases under the Unlawful Activities (Prevention) Act (UAPA), incarcerated for over four years and later released on bail; Bharadwaj's lawyer Shalini Gera; Teltumbde's friend Jaison Cooper, a Kerala-based rights activist; scholar of the Naxalite movement and Dalit-based writer Anand Teltumbde and his wife Rama Sathe, one of the oldest members of the Kabir Kala Manch cultural group Rupali Jadhav, said to chair rights activist Mahesh Raut's defence committee; Sudha Bharadwaj's daughter Jabala Nagoti," a report in The Wire news website, which participated in the exposé, said.

Gonsalves's wife Susan Abraham — who is also a lawyer for Sen, Teltumbde and two fellow detainees, author Sudhir Dhawale and the Kabir Kala Manch's Jyoti Jagtap — told **The Telegraph**: "It is absolutely shocking that this should have happened and must still be happening. Of course, this has led to Vernon's arrest and continued incarceration for almost three years now without a trial. This is completely unlawful and unjust. This kind of surveillance web that we all are trapped in needs to be exposed."

Earlier this year, Arsenal Berlin found that "evidence" had been planted on the computers of the accused activists Wilson and Nagpur-based lawyer Gadling, both of whom are in a Navi Mumbai jail awaiting trial in the case.

However, both the National Investigating Agency (NIA) and the Maharashtra police have opposed Wilson's plea to Bombay High Court to quash the case.

The NIA told the court that "documents which are not part of the charsheet cannot be relied upon", while the state police argued in court earlier this month that the accused can challenge the evidence only when it comes to trial.

Babu's wife Jenny Rowena, who lives at Delhi University, told this newspaper: "It shows how unscrupulous the government is in tampering with them. Yet, the courts have taken the documents found in the laptops of the accused as prima facie evidence. The Arsenal report shows the computers have been tampered with, and in the light of these disclosures we must take it for granted that the government can tamper with our devices.

"The courts must refuse to take the documents on the computers of the accused in the case as prima facie evidence and give them bail as soon as possible without us having to prove the purported tampering in fake after years of incarceration, as it happens in UAPA cases."

Last year, rights group Amnesty International and the University of Toronto's watchdog Citizen Lab had revealed that in 2019, a co-ordinated spyware operation was used to target at least nine human rights defenders, eight of whom are campaigning for the release of the Elgaar case accused.

Also in 2019, Pegasus was discovered to have been used to spy on human rights defenders by penetrating their mobile phones via WhatsApp.

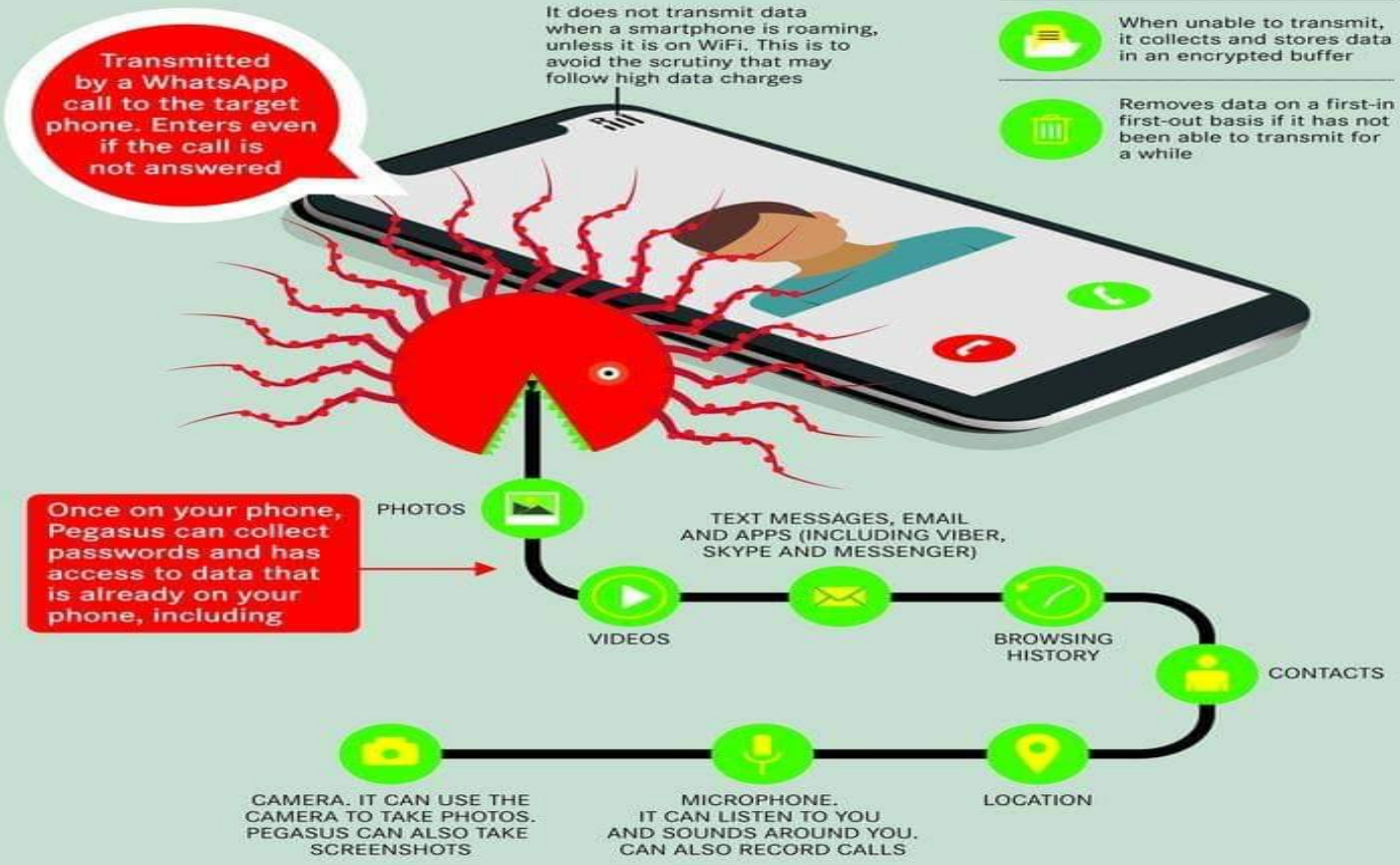
Teltumbde's wife Rama Ambedkar-Teltumbde — who happens to be B.R. Ambedkar's granddaughter — told this newspaper: "We already knew of his devices being compromised with Pegasus through Citizen Lab way back in 2019. The new since certainly expose a great threat in today's India against the entire democratic fabric of our Constitution at large. It is strange that on one hand the Arsenal report is being dismissed for being foreign, but we (are using) foreign technology to snoop on our own countrymen."

Navlakha was also grilled in the money-laundering case against investigative portal Newsclick. His partner Sabha Hussain said: "First he was arrested (in the Elgaar case), now this ED case is also being brought ... When so much has come to the glaring of *proof* and surveillance, why does the government not investigate if they are not involved with Pegasus but even the Maharashtra government send an 'no' to the Arsenal evidence in the high court. They should have ordered a special investigation team immediately."

The NIA reports to the central government, which is under the BJP. Maharashtra has a coalition government of the Shiv Sena, NCP and the Congress. The home department is helmed by an NCP minister, with a minister of state each from the Congress and the Sena.

SUPERSPY

The Pegasus spyware, developed by Israeli cyberarms firm NSO Group, can infiltrate Android devices and certain versions of Apple's iOS. Here is how it works



RESEARCH: **PRADIP R. SAGAR**
SOURCE: **PRASHANT MALI, CYBER LAW AND CYBER SECURITY EXPERT**

GRAPHICS: **SREEMANIKANDAN S.**

How Pegasus works?

- **end-to-end encryption became commonplace as messaging moved onto encrypted email and apps like WhatsApp and Signal.**
- **Governments unable to listen in — and desperate for a solution.**
- **To meet that need, Pegasus was born.**

What is Pegasus?

Pegasus is the hacking software – or spyware – that is developed, marketed and licensed to governments around the world by the Israeli company NSO Group. It has the capability to infect billions of phones running either iOS or Android operating systems.

First it was discovered in 2016; it infected the phones through a method called spear-phishing – text messages or emails that trick a target into clicking on a malicious link.

Now after the previous hacks what Pegasus has done the method is known to people and agencies;

A new method came up called "Zero-Click"

which do not require any interaction from the phone's owner in order to succeed.

• In 2019 WhatsApp revealed that NSO's software had been used to send malware to more than 1,400 phones by exploiting a zero-click vulnerability. Simply by placing a WhatsApp call to a target device, malicious Pegasus code could be installed on the phone, even if the target never answered the call.

• More recently NSO has begun exploiting vulnerabilities in Apple's iMessage software, giving it backdoor access to hundreds of millions of iPhones. Apple says it is continually updating its software to prevent such attacks.

• Where neither spear-phishing nor zero-click attacks succeed, Pegasus can also be installed over a wireless transceiver located near a target, or, according to an NSO brochure, simply manually installed if an agent can steal the target's phone.

• NSO main is also to make sure to find a bug in your phone; security researchers and hackers spend a lot of time and effort to uncover these bugs. One with the intention of reporting/fixing them, while the other with the intent of using them to "hack" your phones.

NSO

- **The NSO Group is a private company based in Israel that is a leading maker of spyware.**
- **Its signature product, Pegasus, is designed to break into iPhones and Android devices.**
- **Founded in 2010, the company says it has 60 government customers in 40 countries.**
- **The company, which also has offices in Bulgaria and Cyprus, reportedly has 750 employees and recorded revenue of more than $240 million last year,**

Pegasus…

- NSO Group claims that its Pegasus spyware is only used to “investigate terrorism and crime” and “leaves no traces whatsoever”.

- This Forensic Methodology Report shows that neither of these statements are true.

WHAT DO YOUR DEVICES KNOW ABOUT YOU?

Whether it's a computer on your desk or a phone in your pocket, your devices retain a lot of personal data. And all of that information may be vulnerable to cybercriminals.

WINDOWS PCs | MACS | ANDROID TABLETS | SMART PHONES

Passwords
- Web browser autofill
- Stored in the file System

Credit Card Numbers
- Web browser autofill
- Downloaded credit card statements

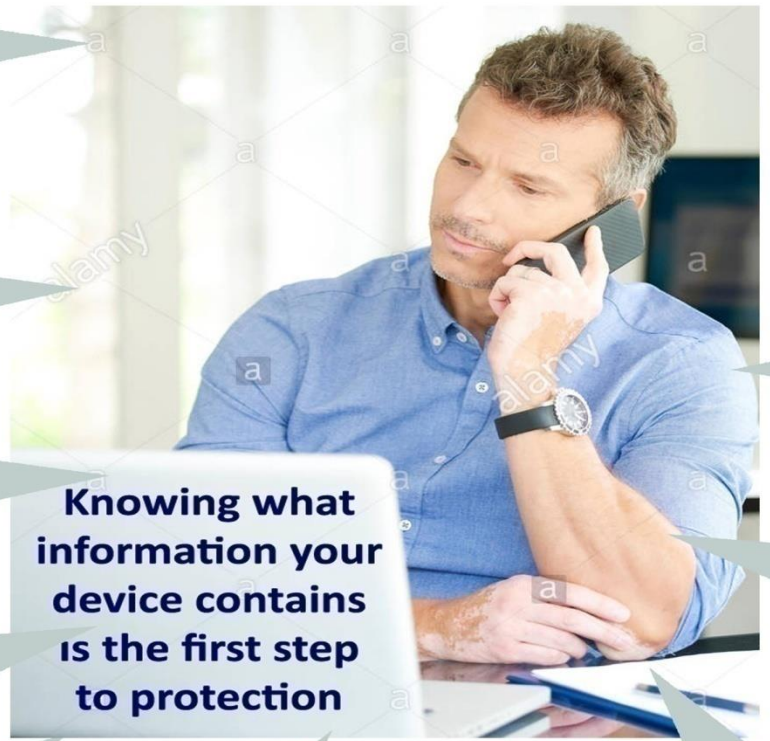
Social Security Number
- Aadhar Number
- Downloaded Tax documents

Deleted Files
- All deleted files, including ones no longer in recycle bin or trash, can be recovered until physical storage space overwritten.

Text Messages
- Text log stored on phone

Phone Calls
- Call log Stored on phone

Bank Account Info
- Downloaded bank statements



Recently Visited Sites, Viewed area, Used app, Searched for
- Browser's cache
- Browser's history
- Cookies

Recent Files
- Various applications keep their own recent file lists
- List kept by operating system

Name and Address
- Web browser autofill
- Windows Contacts
- Address Book
- Contact manager

Current Locations
- Readable off your GPS

Contacts
- Windows Contacts
- Address Book
- Contact manager

Recent Locations
- Photos
- Navigation apps

Biometric Info
- Unique identifiers include fingerprints, retina and iris patterns, voice waves.
- Spy CAM & Micro Phones

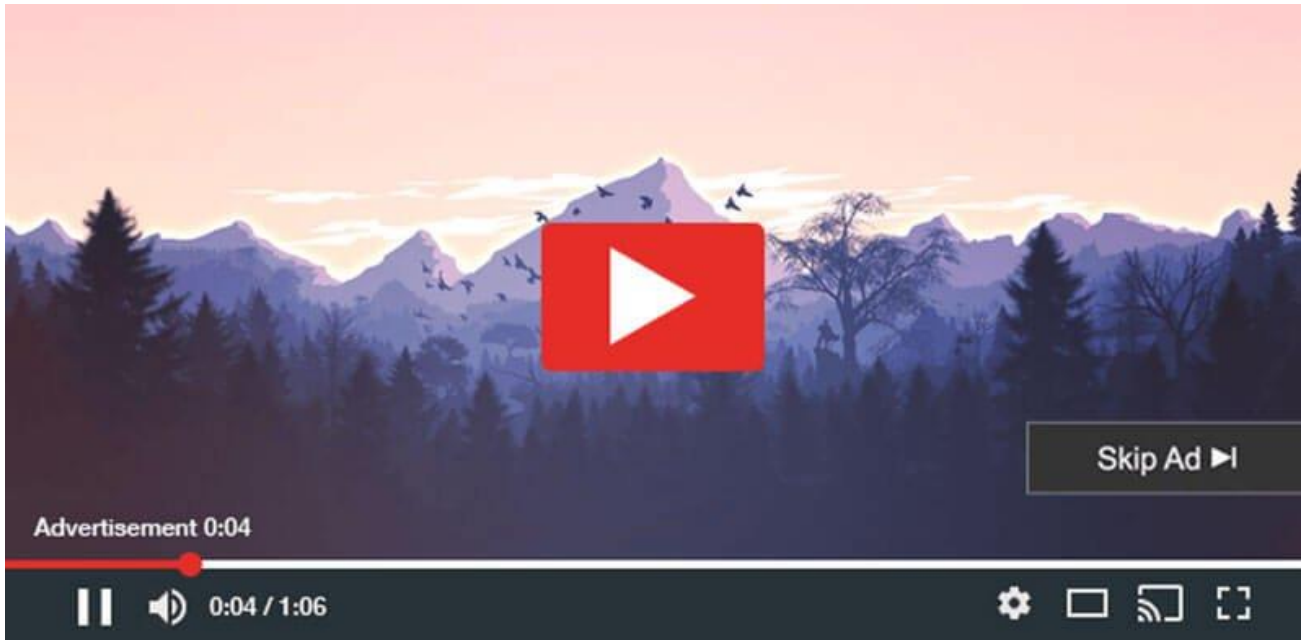
Solution!

AI CAMERA
SAMSUNG

TELEPHONE BOOTH

EARLIER

NOW


Skip Ad
Advertisement 0:04
0:04 / 1:06

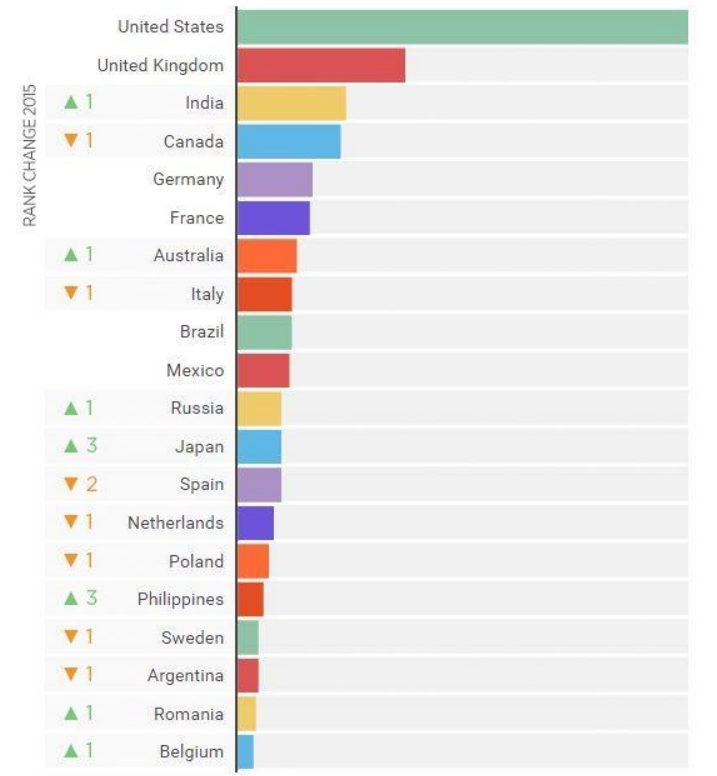
How This 7-Year-Old Made $22 Million Playing With Toys

Madeline Berg Forbes Staff
Media
Following the money

Pornhub's Top 20 Countries

Pornhub

Proportion of Worldwide Traffic

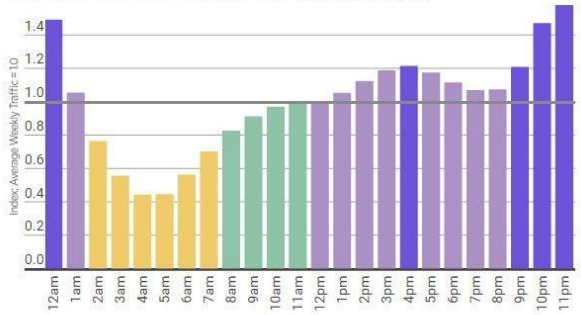


pornhub.com/insights

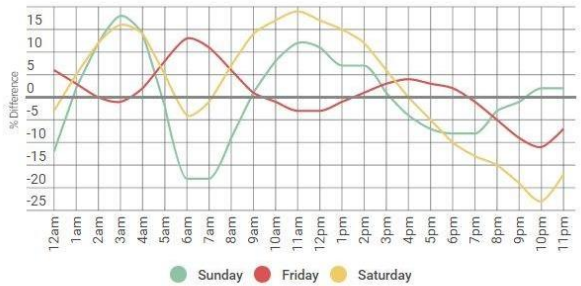
Hourly Traffic Worldwide

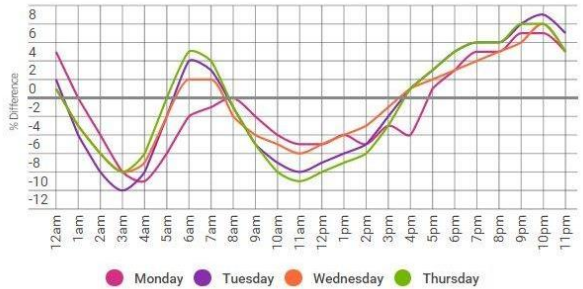
Pornhub

Favorite Times to Watch Porn (weekly average)



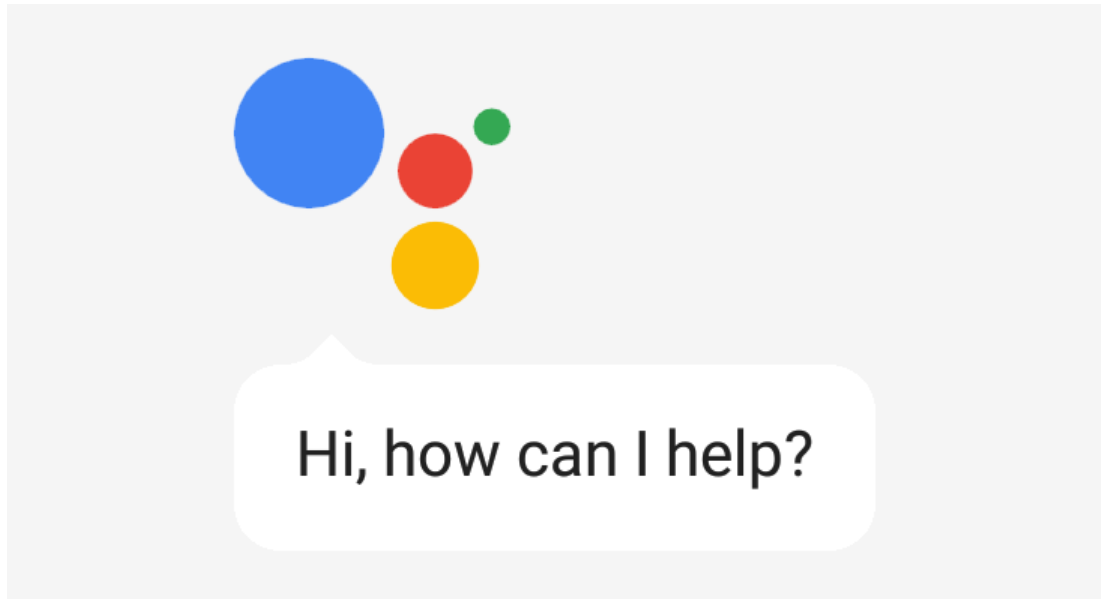
Percent Change in Traffic by Day (compared to weekly average)





HOW MANY WORDS IN ENGLISH LANGUAGE?

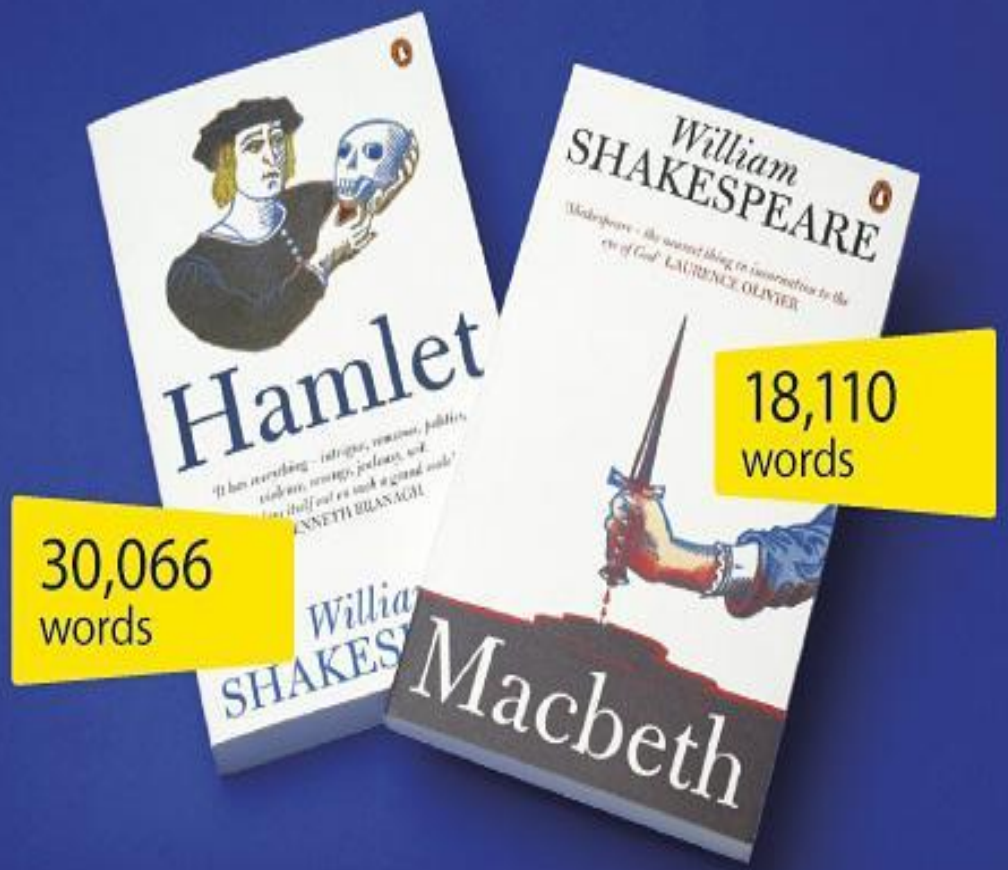
05
SEC


Hi, how can I help?

How many words in the English language?

- **171,476 words (approximately)**

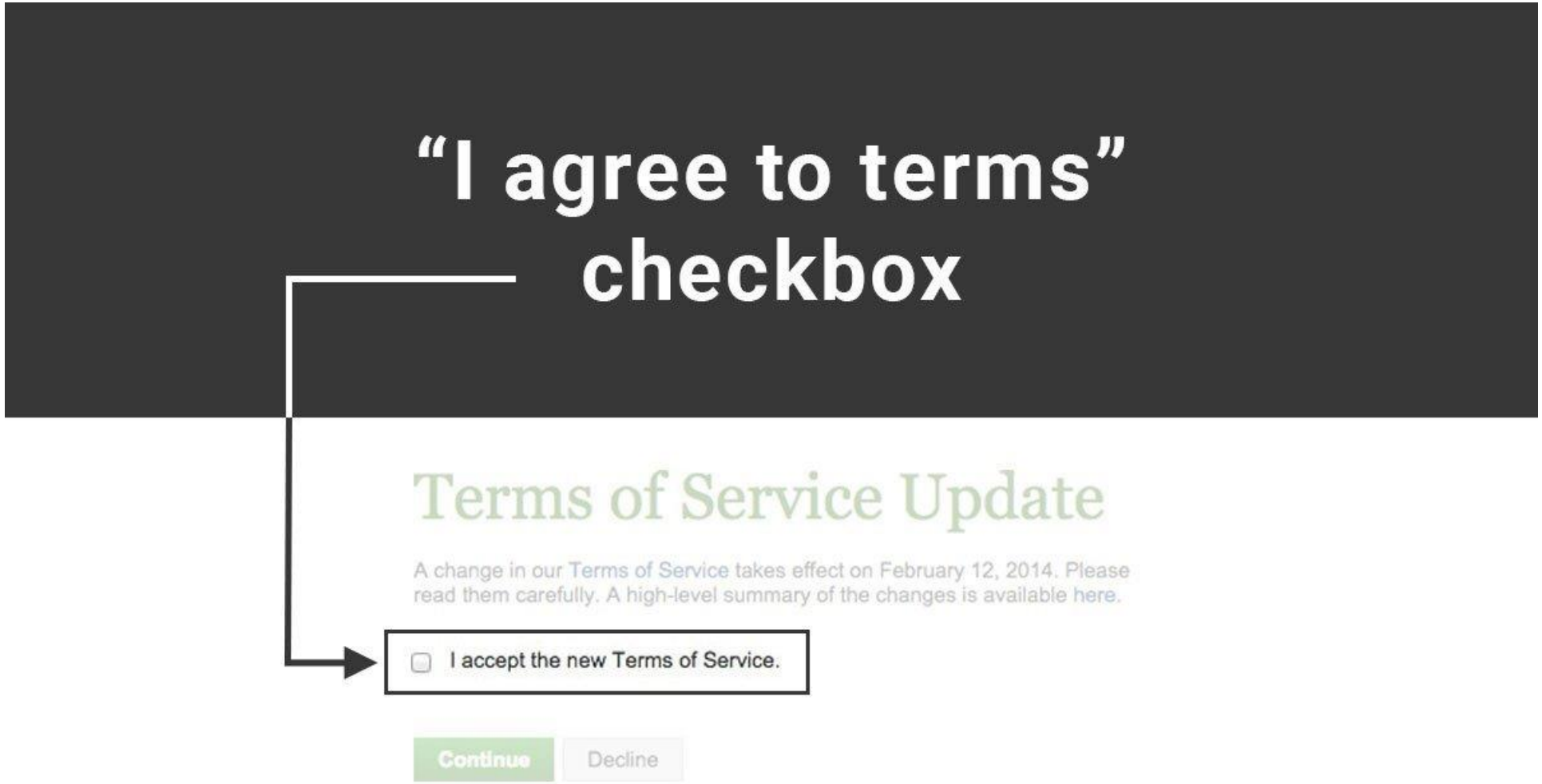
- **The Second Edition of the 20-volume Oxford English Dictionary contains full entries for 171,476 words in current use,**

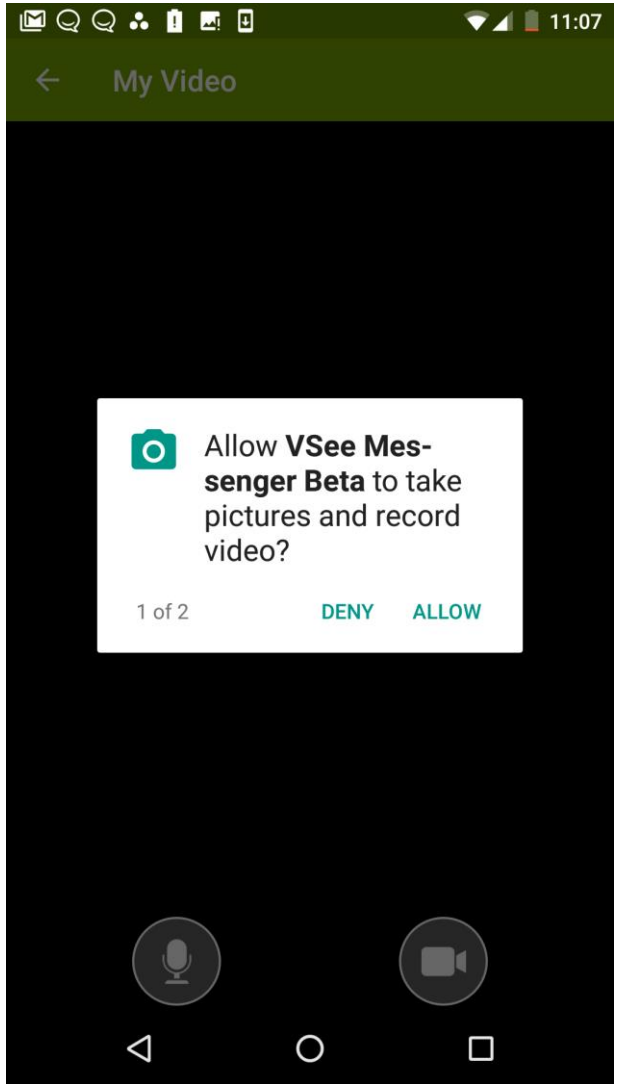


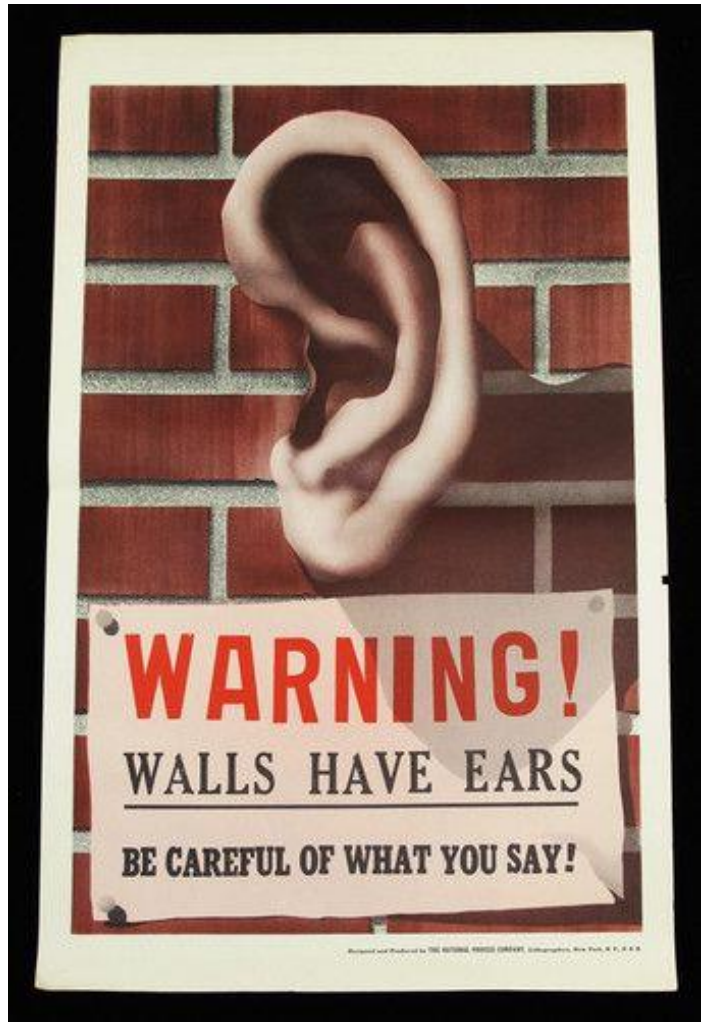
Which?

WEBSITE/SERVICE/BOOK	TOTAL WORDS*
PAYPAL	36,275
HAMLET	30,066
APPLE iTUNES	19,972
MACBETH	18,110
WINDOWS LIVE	14,714
APPLE iOS 5	13,366
FACEBOOK	11,195
GOOGLE ALL-INCLUSIVE	10,640
APPLE iCLOUD	10,724
AMAZON KINDLE	7,115
AMAZON.CO.UK	5,212
TWITTER	4,445
GOOGLE	4,099

“I agree to terms” checkbox



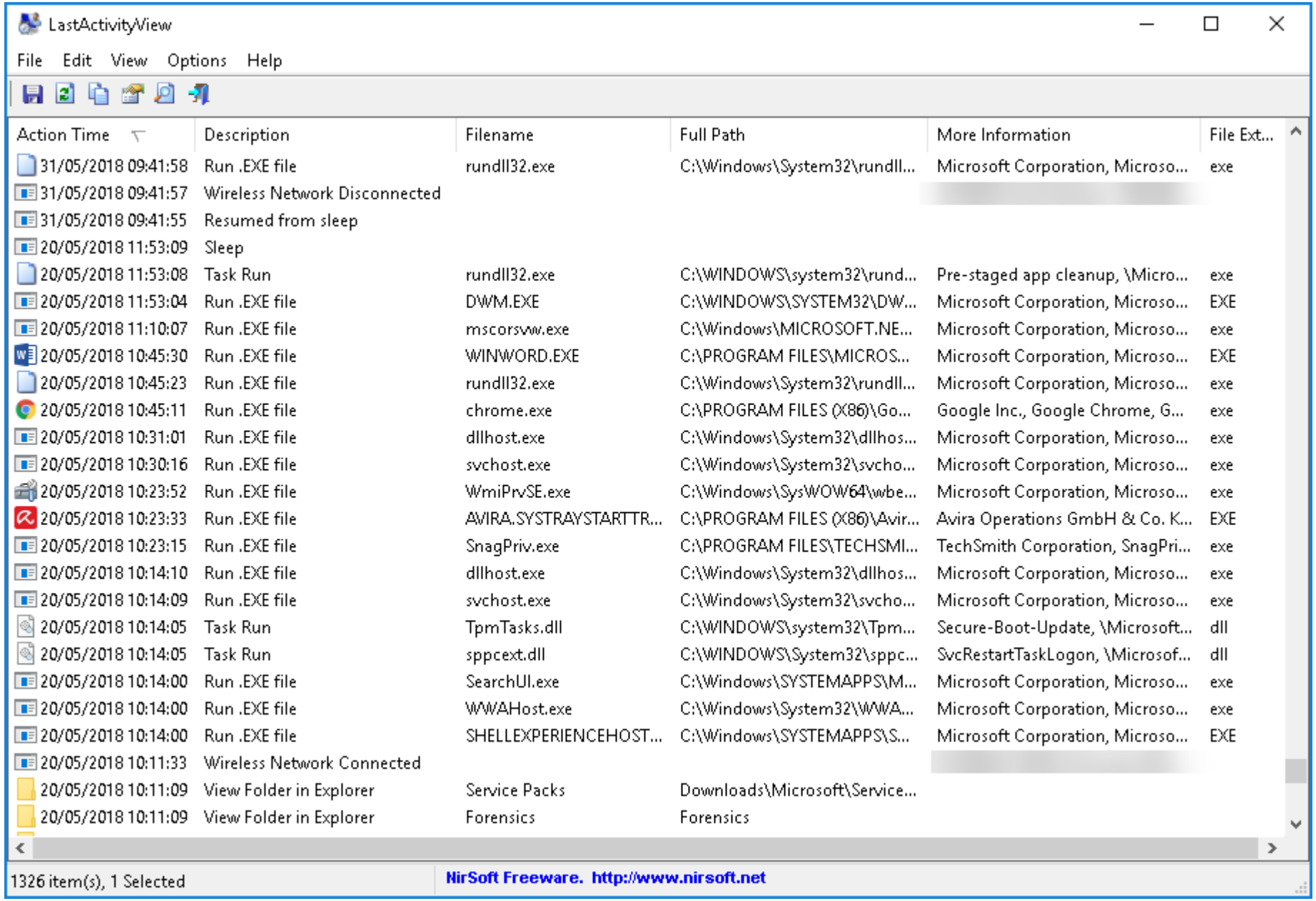

11:07
My Video
Allow VSee Messenger Beta to take pictures and record video?
1 of 2
DENY
ALLOW

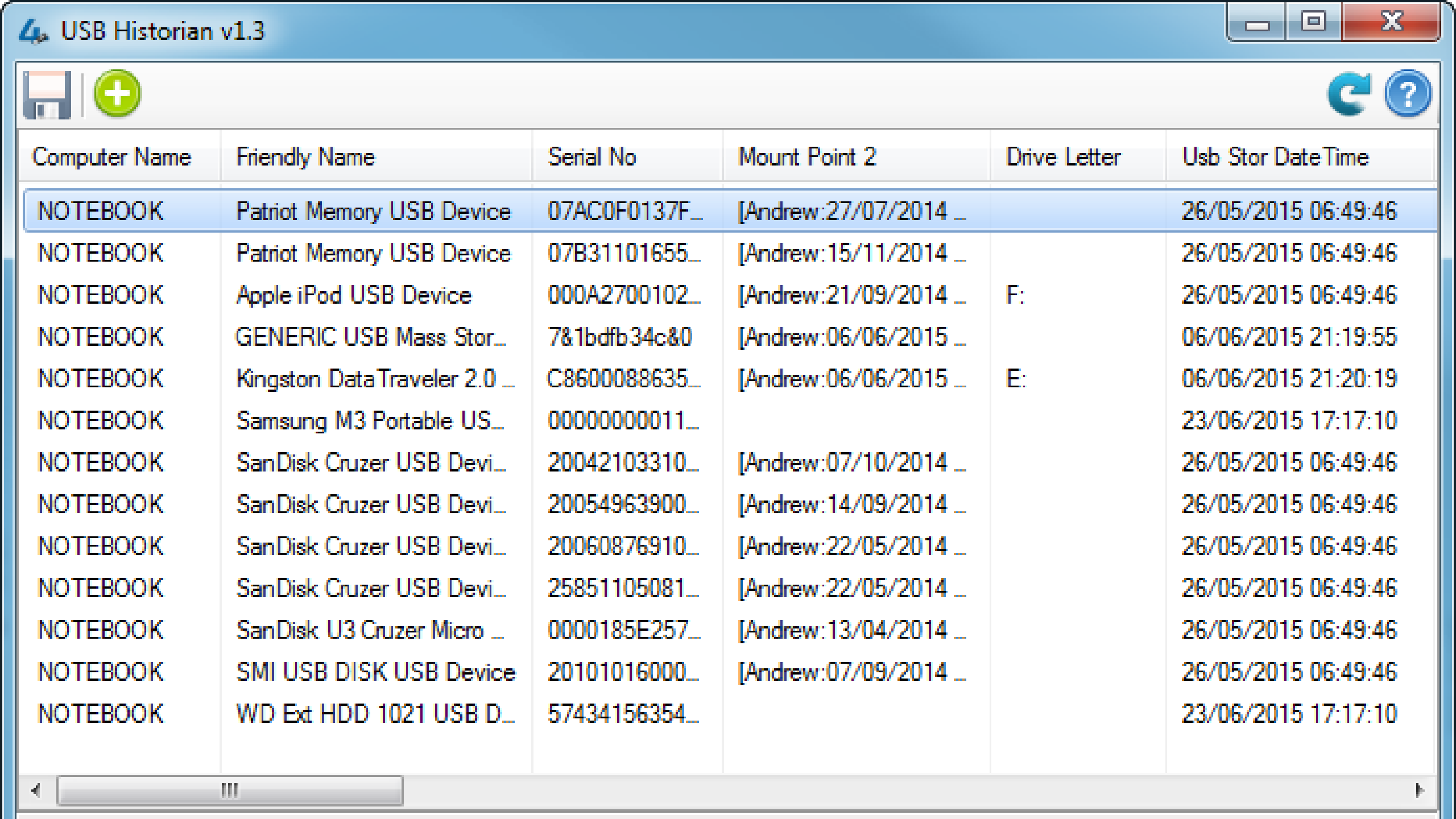

WARNING!
WALLS HAVE EARS
BE CAREFUL OF WHAT YOU SAY!

Edmond Locard's (Sherlock Holmes of France) Principle

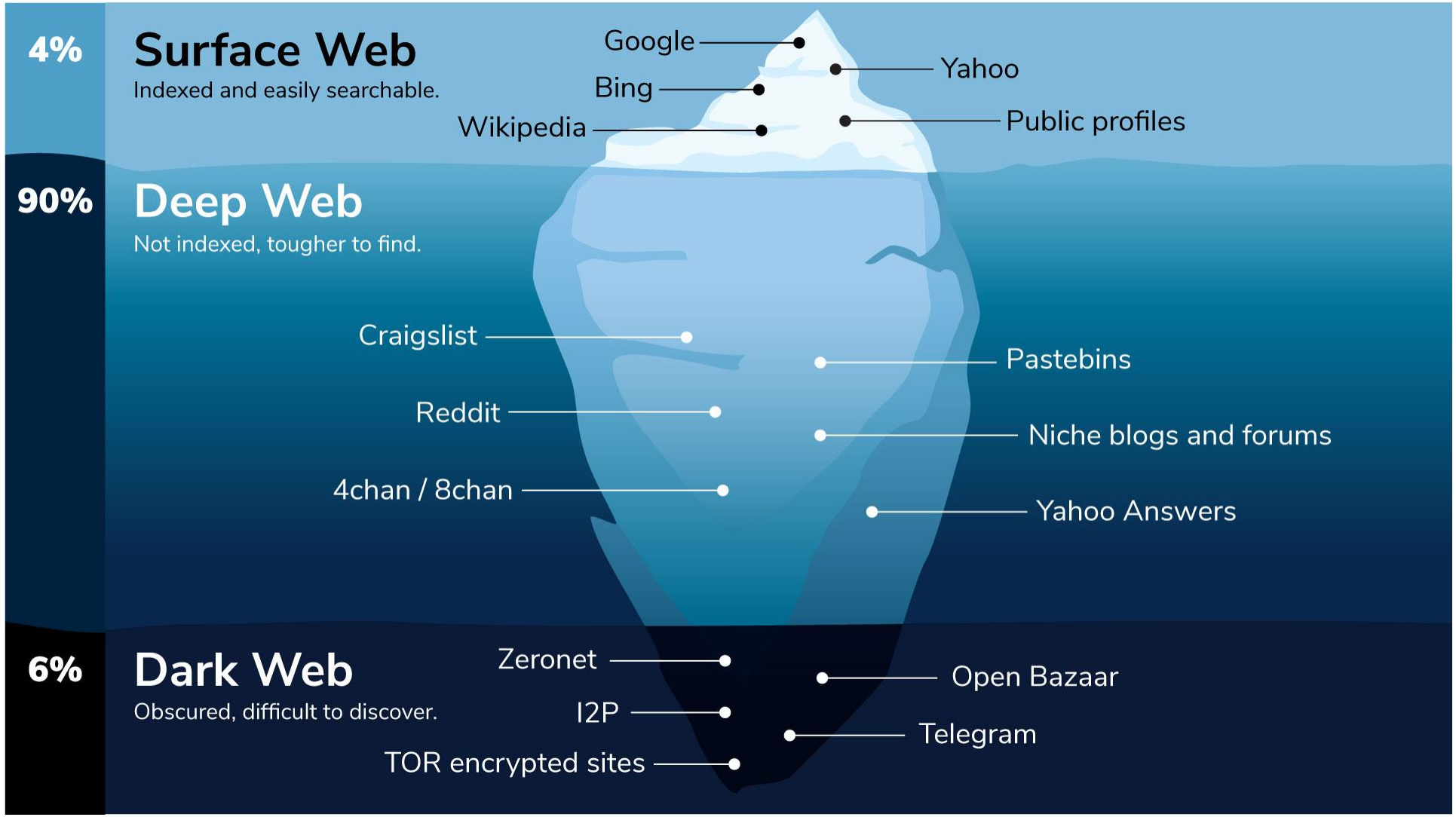
Every contact by a criminal leaves behind a trace.

Buzzle.com


LastActivityView
File Edit View Options Help
Action Time | Description | Filename | Full Path | More Information | File Ext...
31/05/2018 09:41:58 | Run .EXE file | rundll32.exe | C:\Windows\System32\rundll... | Microsoft Corporation, Microso... | exe
31/05/2018 09:41:57 | Wireless Network Disconnected
31/05/2018 09:41:55 | Resumed from sleep
20/05/2018 11:53:09 | Sleep
20/05/2018 11:53:08 | Task Run | rundll32.exe | C:\WINDOWS\system32\rund... | Pre-staged app cleanup, \Micro... | exe
20/05/2018 11:53:04 | Run .EXE file | DWM.EXE | C:\WINDOWS\SYSTEM32\DW... | Microsoft Corporation, Microso... | EXE
20/05/2018 11:10:07 | Run .EXE file | mscorsvw.exe | C:\Windows\MICROSOFT.NE... | Microsoft Corporation, Microso... | exe
20/05/2018 10:45:30 | Run .EXE file | WINWORD.EXE | C:\PROGRAM FILES\MICROS... | Microsoft Corporation, Microso... | EXE
20/05/2018 10:45:23 | Run .EXE file | rundll32.exe | C:\Windows\System32\rundll... | Microsoft Corporation, Microso... | exe
20/05/2018 10:45:11 | Run .EXE file | chrome.exe | C:\PROGRAM FILES (X86)\Go... | Google Inc., Google Chrome, G... | exe
20/05/2018 10:31:01 | Run .EXE file | dllhost.exe | C:\Windows\System32\dllhos... | Microsoft Corporation, Microso... | exe
20/05/2018 10:30:16 | Run .EXE file | svchost.exe | C:\Windows\System32\svcho... | Microsoft Corporation, Microso... | exe
20/05/2018 10:23:52 | Run .EXE file | WmiPrvSE.exe | C:\Windows\SysWOW64\wbe... | Microsoft Corporation, Microso... | exe
20/05/2018 10:23:33 | Run .EXE file | AVIRA.SYSTRAYSTARTTR... | C:\PROGRAM FILES (X86)\Avir... | Avira Operations GmbH & Co. K... | EXE
20/05/2018 10:23:15 | Run .EXE file | SnagPriv.exe | C:\PROGRAM FILES\TECHSMI... | TechSmith Corporation, SnagPri... | exe
20/05/2018 10:14:10 | Run .EXE file | dllhost.exe | C:\Windows\System32\dllhos... | Microsoft Corporation, Microso... | exe
20/05/2018 10:14:09 | Run .EXE file | svchost.exe | C:\Windows\System32\svcho... | Microsoft Corporation, Microso... | exe
20/05/2018 10:14:05 | Task Run | TpmTasks.dll | C:\WINDOWS\system32\Tpm... | Secure-Boot-Update, \Microsoft... | dll
20/05/2018 10:14:05 | Task Run | sppcext.dll | C:\WINDOWS\System32\sppc... | SvcRestartTaskLogon, \Microsof... | dll
20/05/2018 10:14:00 | Run .EXE file | SearchUI.exe | C:\Windows\SYSTEMAPPS\M... | Microsoft Corporation, Microso... | exe
20/05/2018 10:14:00 | Run .EXE file | WWAHost.exe | C:\Windows\System32\WWA... | Microsoft Corporation, Microso... | exe
20/05/2018 10:14:00 | Run .EXE file | SHELLEXPERIENCEHOST... | C:\Windows\SYSTEMAPPS\S... | Microsoft Corporation, Microso... | EXE
20/05/2018 10:11:33 | Wireless Network Connected
20/05/2018 10:11:09 | View Folder in Explorer | Service Packs | Downloads\Microsoft\Service...
20/05/2018 10:11:09 | View Folder in Explorer | Forensics | Forensics
1326 item(s), 1 Selected
NirSoft Freeware. http://www.nirsoft.net



Computer Name	Friendly Name	Serial No	Mount Point 2	Drive Letter	Usb Stor DateTime
NOTEBOOK	Patriot Memory USB Device	07AC0F0137F...	[Andrew:27/07/2014 ...		26/05/2015 06:49:46
NOTEBOOK	Patriot Memory USB Device	07B31101655...	[Andrew:15/11/2014 ...		26/05/2015 06:49:46
NOTEBOOK	Apple iPod USB Device	000A2700102...	[Andrew:21/09/2014 ...	F:	26/05/2015 06:49:46
NOTEBOOK	GENERIC USB Mass Stor...	7&1bdfb34c&0	[Andrew:06/06/2015 ...		06/06/2015 21:19:55
NOTEBOOK	Kingston DataTraveler 2.0 ...	C8600088635...	[Andrew:06/06/2015 ...	E:	06/06/2015 21:20:19
NOTEBOOK	Samsung M3 Portable US...	00000000011...			23/06/2015 17:17:10
NOTEBOOK	SanDisk Cruzer USB Devi...	20042103310...	[Andrew:07/10/2014 ...		26/05/2015 06:49:46
NOTEBOOK	SanDisk Cruzer USB Devi...	20054963900...	[Andrew:14/09/2014 ...		26/05/2015 06:49:46
NOTEBOOK	SanDisk Cruzer USB Devi...	20060876910...	[Andrew:22/05/2014 ...		26/05/2015 06:49:46
NOTEBOOK	SanDisk Cruzer USB Devi...	25851105081...	[Andrew:22/05/2014 ...		26/05/2015 06:49:46
NOTEBOOK	SanDisk U3 Cruzer Micro ...	0000185E257...	[Andrew:13/04/2014 ...		26/05/2015 06:49:46
NOTEBOOK	SMI USB DISK USB Device	20101016000...	[Andrew:07/09/2014 ...		26/05/2015 06:49:46
NOTEBOOK	WD Ext HDD 1021 USB D...	57434156354...			23/06/2015 17:17:10

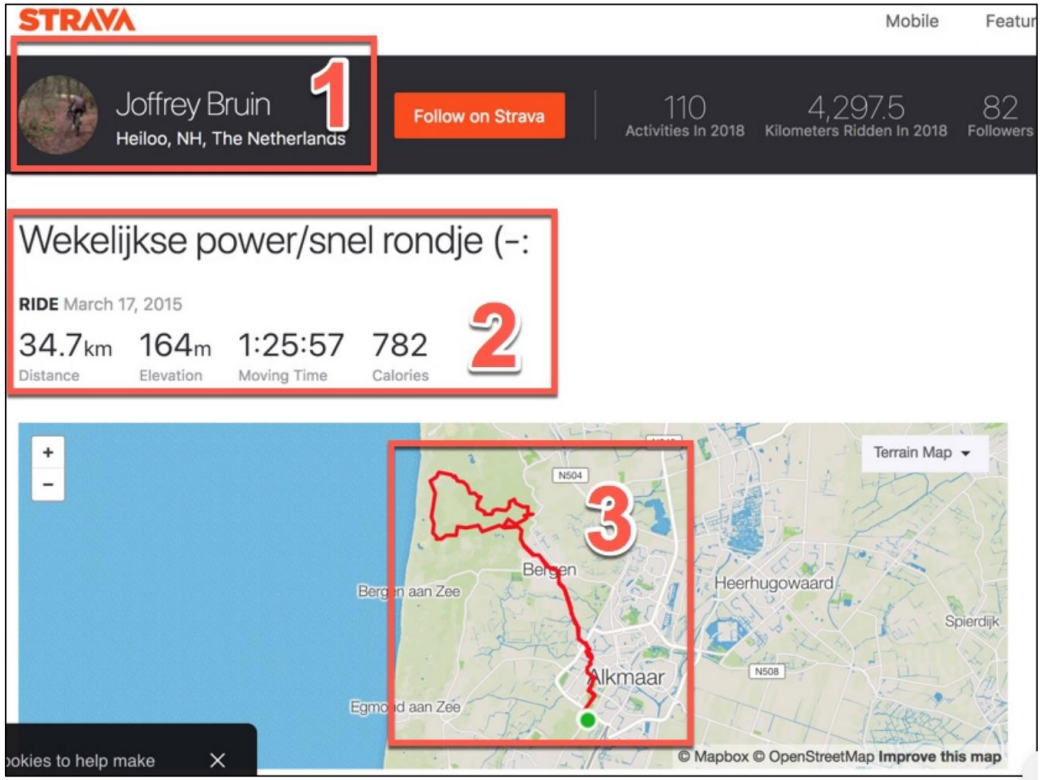

4%
Surface Web
Indexed and easily searchable.
Google
Bing
Wikipedia
Yahoo
Public profiles
90%
Deep Web
Not indexed, tougher to find.
Craigslist
Reddit
4chan / 8chan
Pastebins
Niche blogs and forums
Yahoo Answers
6%
Dark Web
Obscured, difficult to discover.
Zeronet
I2P
TOR encrypted sites
Open Bazaar
Telegram

Joffrey Bruin

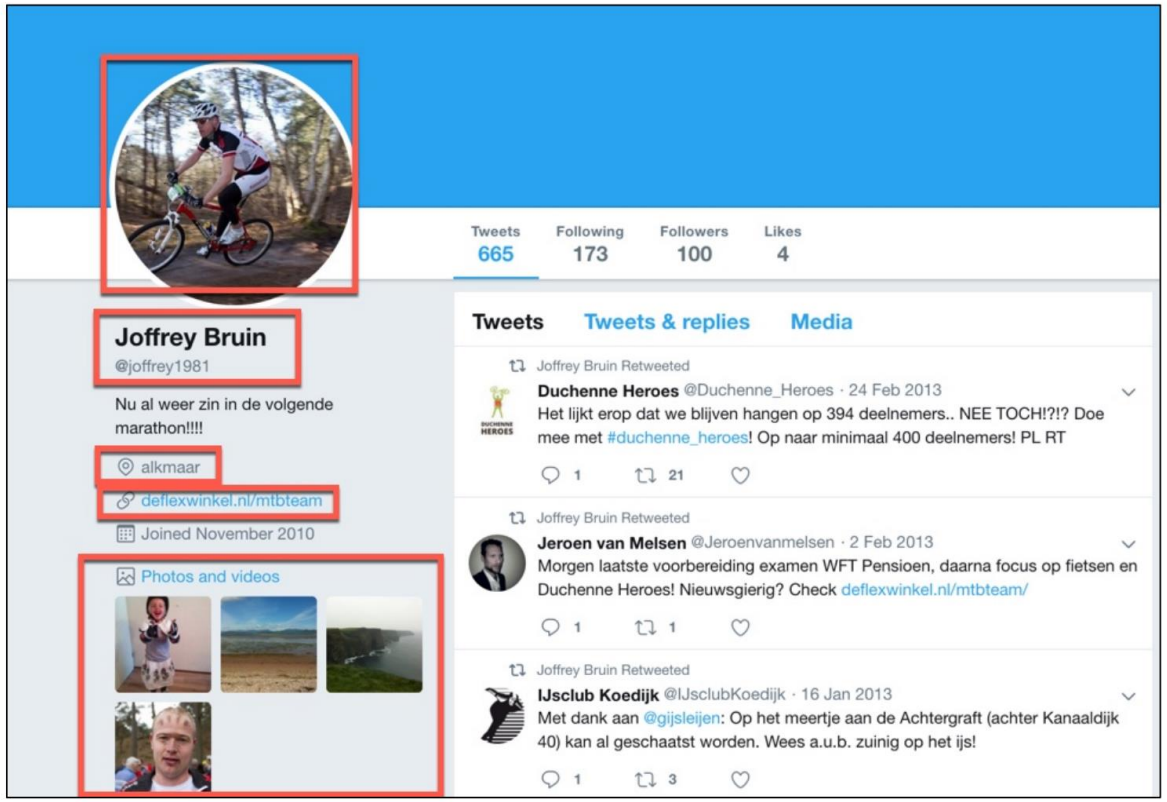
- He cycles
- He is from Netherlands

What a sports app tells us

1. Joffrey Bruin
1. Heiloo, Netherlands
2. Weekly Bicycle ride
2. 17 march 2015 = Tuesday
2. Duration ride 1:25:57
3. Map of the Route

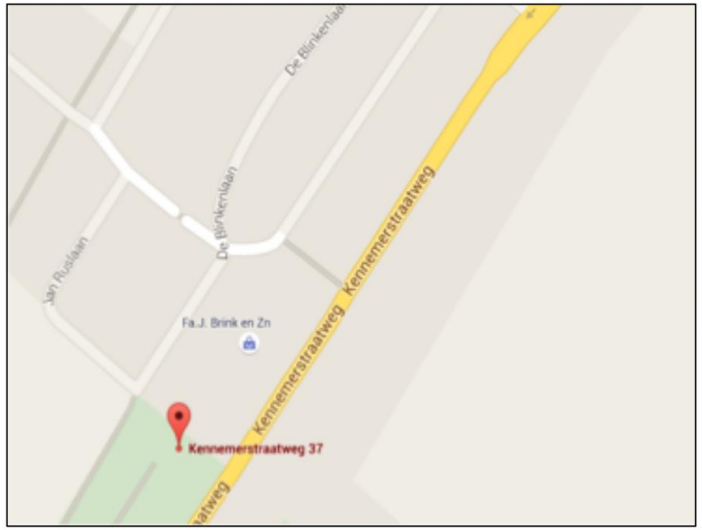


Twitter


Tweets 665
Following 173
Followers 100
Likes 4
Joffrey Bruin
@joffrey1981
Nu al weer zin in de volgende marathon!!!!
alkmaar
deflexwinkel.nl/mtbteam
Joined November 2010
Photos and videos
Tweets
Tweets & replies
Media
Joffrey Bruin Retweeted
Duchenne Heroes @Duchenne_Heroes · 24 Feb 2013
Het lijkt erop dat we blijven hangen op 394 deelnemers.. NEE TOCH!?!? Doe mee met #duchenne_heroes! Op naar minimaal 400 deelnemers! PL RT
Joffrey Bruin Retweeted
Jeroen van Melsen @Jeroenvanmelsen · 2 Feb 2013
Morgen laatste voorbereiding examen WFT Pensioen, daarna focus op fietsen en Duchenne Heroes! Nieuwsgierig? Check deflexwinkel.nl/mtbteam/
Joffrey Bruin Retweeted
IJsclub Koedijk @IJsclubKoedijk · 16 Jan 2013
Met dank aan @gijsleijen: Op het meertje aan de Achtergraft (achter Kanaaldijk 40) kan al geschaatst worden. Wees a.u.b. zuinig op het ijs!

Joffrey Bruin
@joffrey1981
Follow
Trots op haar nieuwe skeelers die ze heeft gehad voor haar vijfde verjaardag!
3:24 AM - 9 Jun 2012
Joffrey Bruin
@joffrey1981
Follow
@mjthvanleeuwen ja het was zwaar en zeer stoffig de #5vs
8:27 AM - 7 Apr 2012

Yellow Pages & Streetview



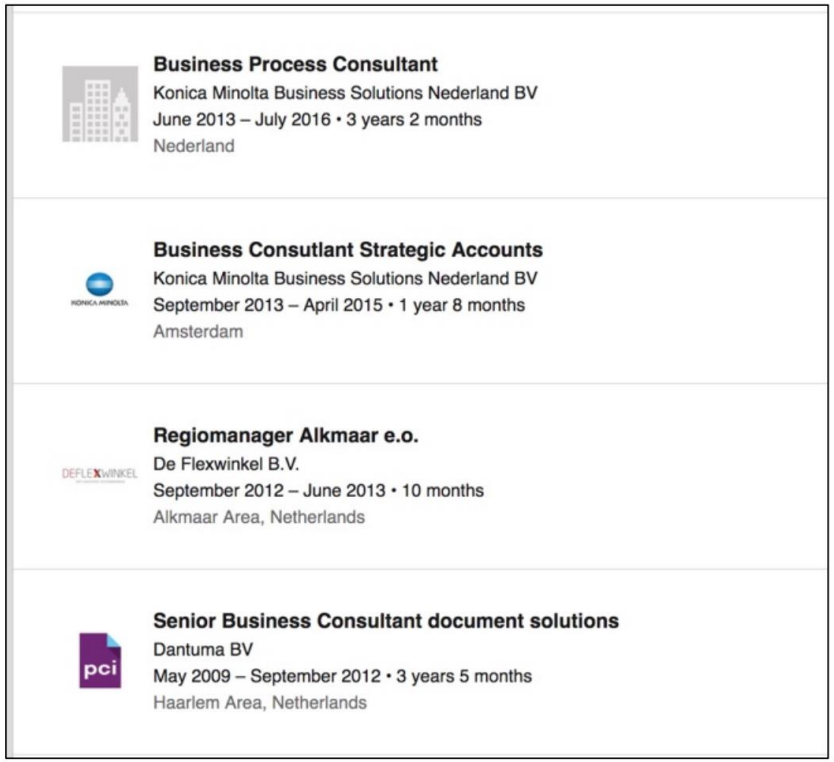
LinkedIn

- Past en Current jobs
- Education
- Validation on previous results

Joffrey Bruin
Solution Architect at Basware
Amsterdam Area, Netherlands
Information Technology and Services

500+ connections

Current	Basware
Previous	Konica Minolta Business Solutions Nederland BV, De Flexwinkel B.V., Dantuma BV
Education	Comptia
Recommendations	4 people have recommended **Joffrey Bruin**



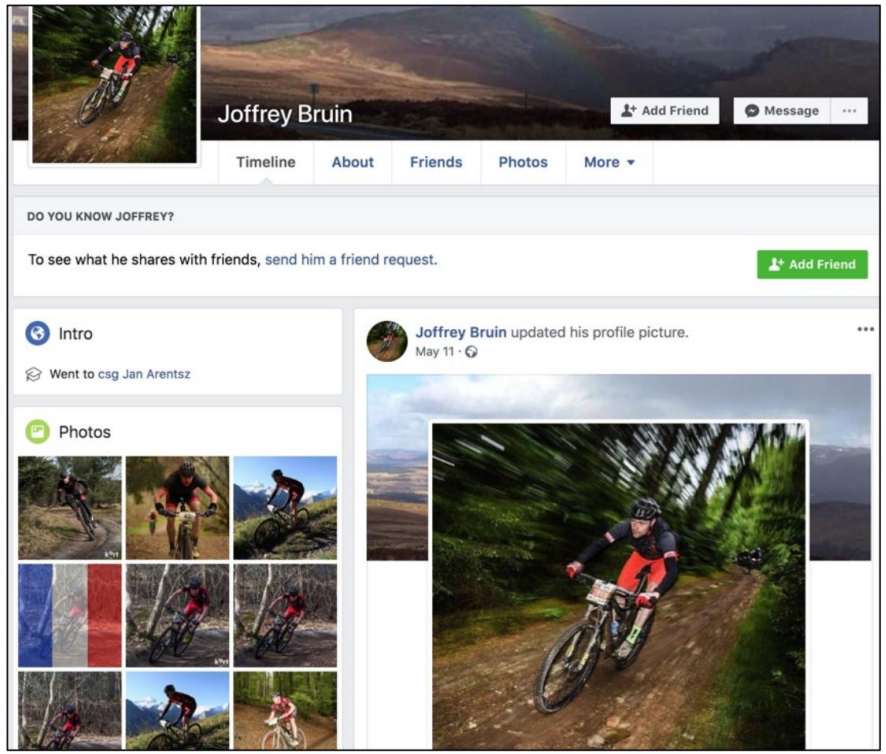
Business Process Consultant
Konica Minolta Business Solutions Nederland BV
June 2013 – July 2016 • 3 years 2 months
Nederland

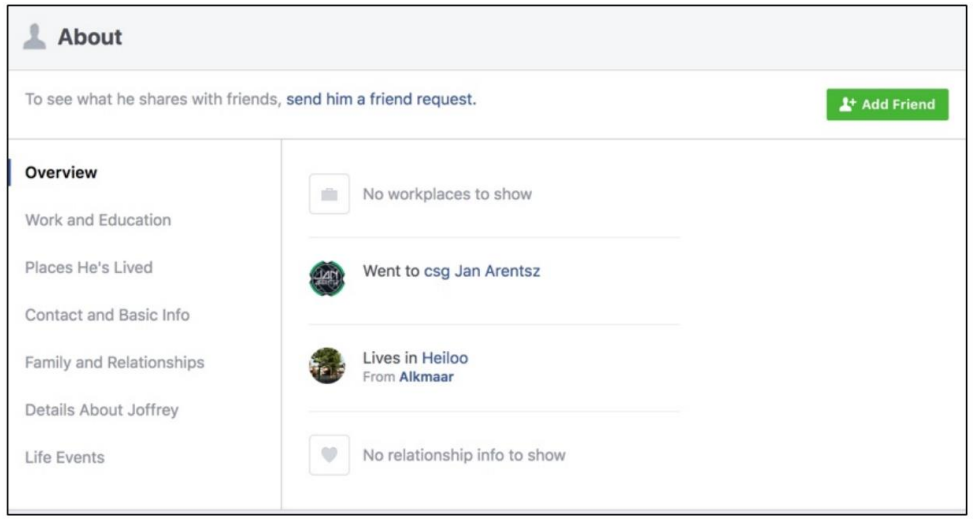
Business Consutlant Strategic Accounts
Konica Minolta Business Solutions Nederland BV
September 2013 – April 2015 • 1 year 8 months
Amsterdam

Regiomanager Alkmaar e.o.
De Flexwinkel B.V.
September 2012 – June 2013 • 10 months
Alkmaar Area, Netherlands

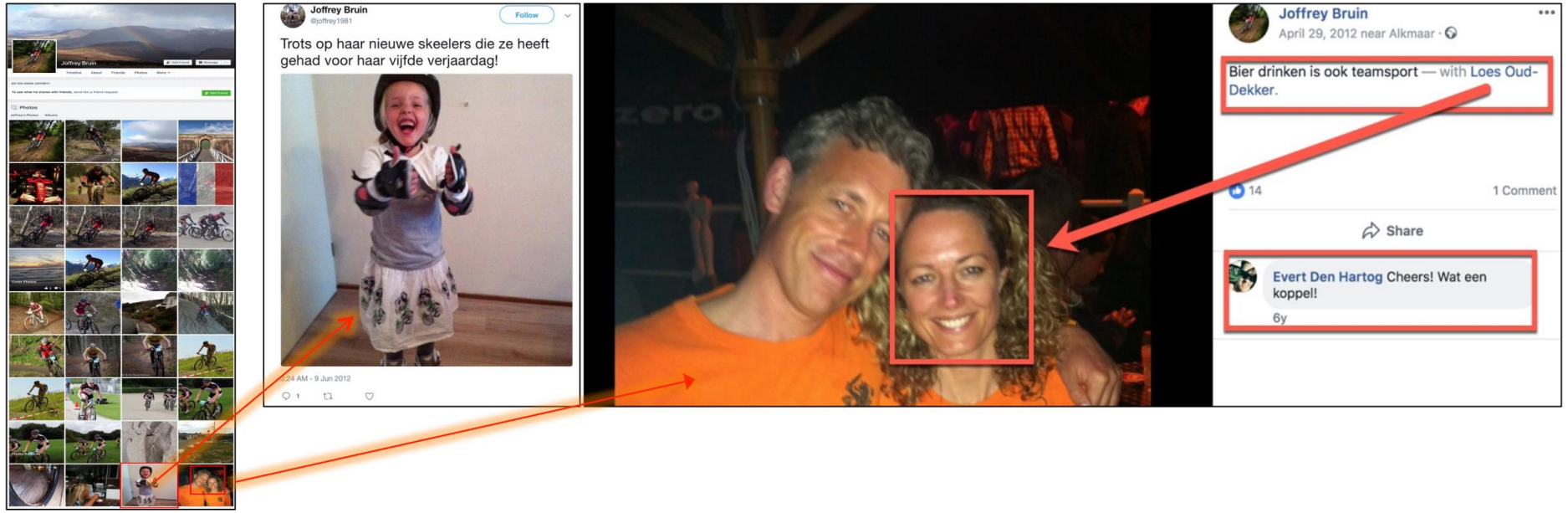
Senior Business Consultant document solutions
Dantuma BV
May 2009 – September 2012 • 3 years 5 months
Haarlem Area, Netherlands

Facebook

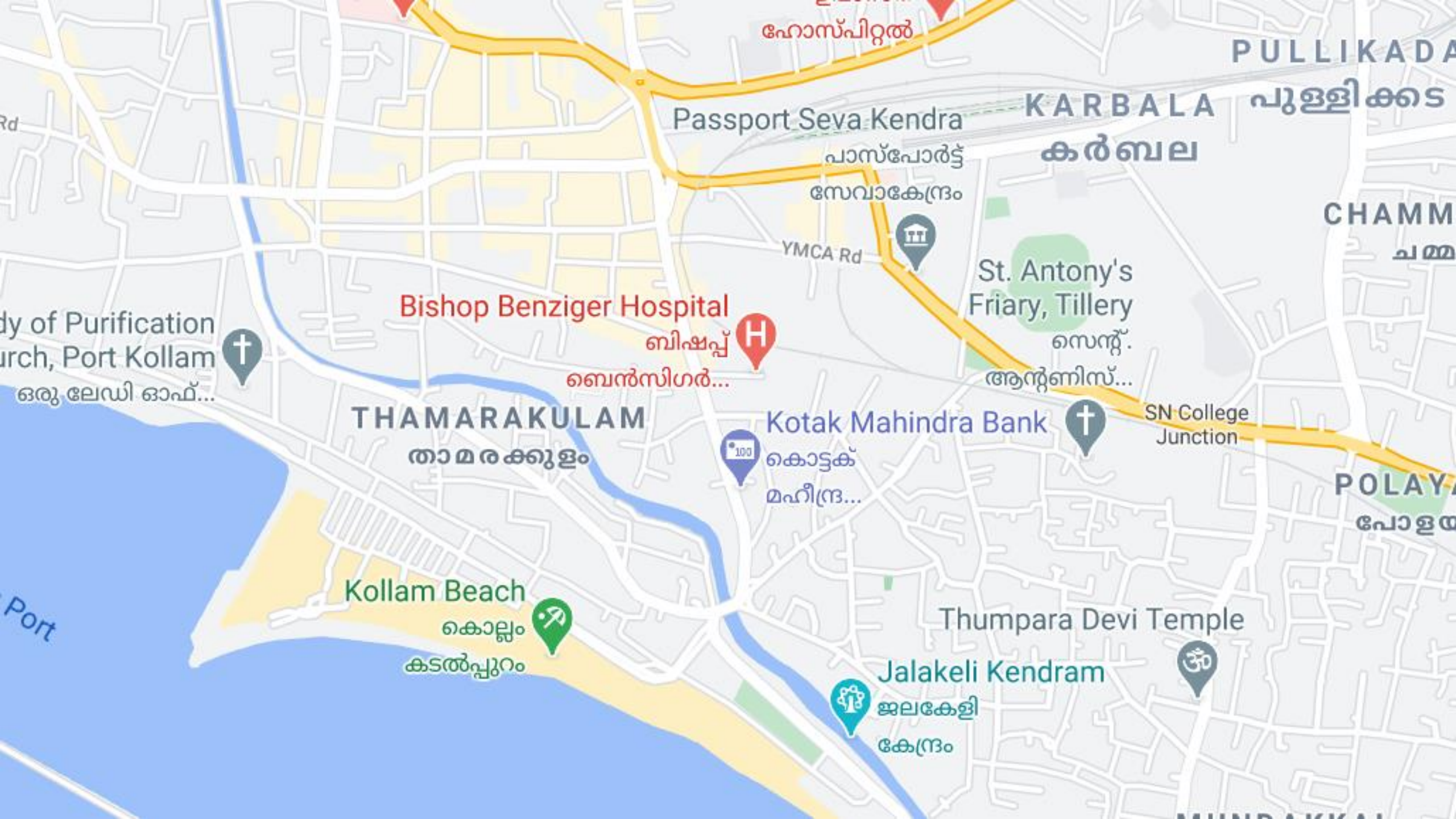

Joffrey Bruin
Add Friend
Message
Timeline
About
Friends
Photos
More
DO YOU KNOW JOFFREY?
To see what he shares with friends, send him a friend request.
Add Friend
Intro
Went to csg Jan Arentsz
Photos
Joffrey Bruin updated his profile picture.
May 11

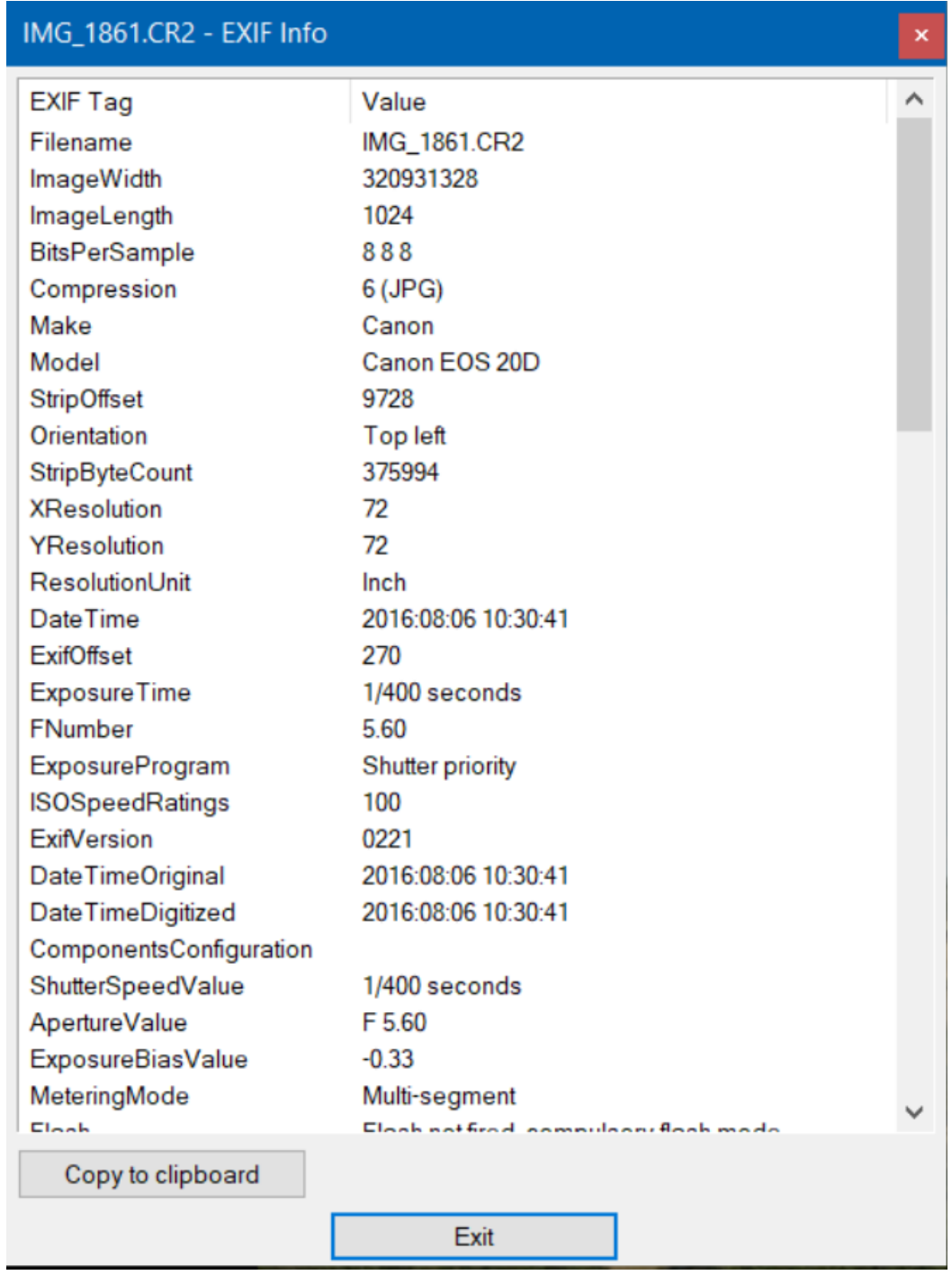

About
To see what he shares with friends, send him a friend request.
Add Friend
Overview
Work and Education
Places He's Lived
Contact and Basic Info
Family and Relationships
Details About Joffrey
Life Events
No workplaces to show
Went to csg Jan Arentsz
Lives in Heiloo
From Alkmaar
No relationship info to show

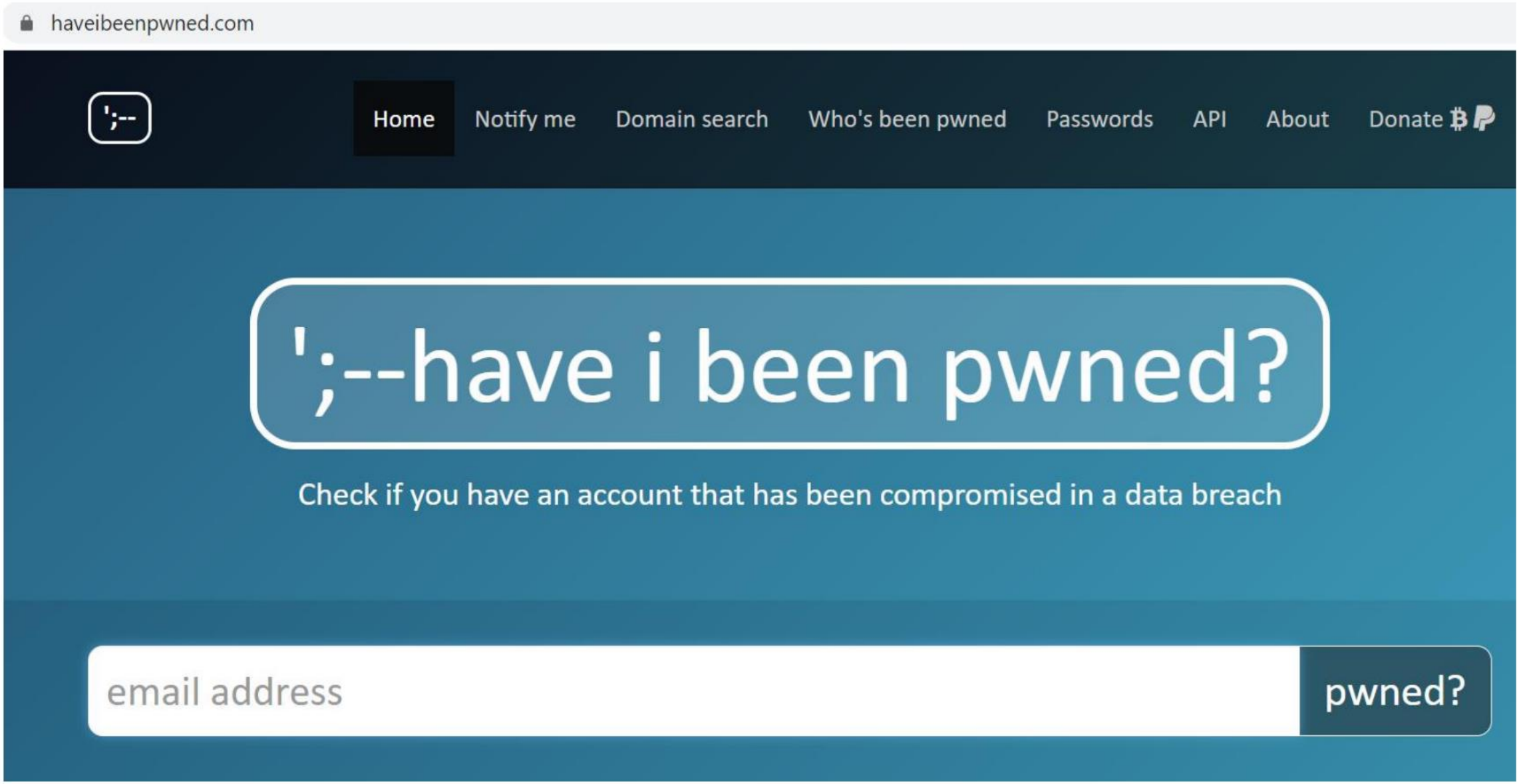
Facebook


Joffrey Bruin
Photos
Joffrey Bruin
@joffrey1981
Follow
Trots op haar nieuwe skeelers die ze heeft gehad voor haar vijfde verjaardag!
4:24 AM - 9 Jun 2012
Joffrey Bruin
April 29, 2012 near Alkmaar ·
Bier drinken is ook teamsport — with Loes Oud-Dekker.
14
1 Comment
Share
Evert Den Hartog Cheers! Wat een koppel!
6y

Pic2Map Photo Location Viewer
Can't remember the location where you took a picture with your camera or smartphone? Upload your photos and find out where they were taken. Pic2Map analyzes EXIF data embedded in the image to find the GPS coordinates and location. The result would be a map view of your photo with detailed address and additional EXIF information if available.
Drag and drop your images here to upload
or
Select Photo Files
Make the photos public?

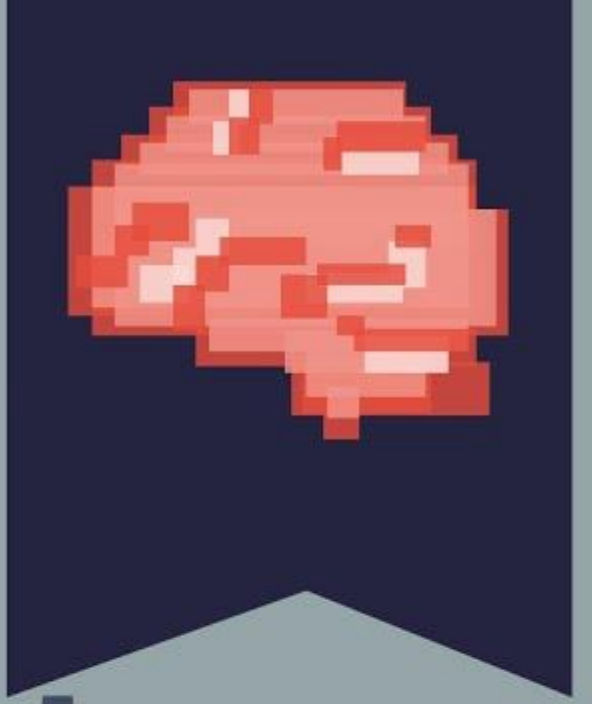

ഹോസ്പിറ്റൽ
PULLIKADA
പുള്ളിക്കട
KARBALA
കർബല
Passport Seva Kendra
പാസ്പോർട്ട്
സേവാകേന്ദ്രം
CHAMM
YMCA Rd
St. Antony's
Friary, Tillery
സെന്റ്.
ആന്റണിസ്...
Bishop Benziger Hospital
ബിഷപ്പ്
ബെൻസിഗർ...
dy of Purification
urch, Port Kollam
ഒരു ലേഡി ഓഫ്...
THAMARAKULAM
താമരക്കുളം
Kotak Mahindra Bank
കൊട്ടക്
മഹീന്ദ്ര...
SN College
Junction
POLAY
പോള
Port
Kollam Beach
കൊല്ലം
കടൽപ്പുറം
Thumpara Devi Temple
Jalakeli Kendram
ജലകേളി
കേന്ദ്രം


IMG_1861.CR2 - EXIF Info
EXIF Tag
Value
Filename
IMG_1861.CR2
ImageWidth
320931328
ImageLength
1024
BitsPerSample
8 8 8
Compression
6 (JPG)
Make
Canon
Model
Canon EOS 20D
StripOffset
9728
Orientation
Top left
StripByteCount
375994
XResolution
72
YResolution
72
ResolutionUnit
Inch
DateTime
2016:08:06 10:30:41
ExifOffset
270
ExposureTime
1/400 seconds
FNumber
5.60
ExposureProgram
Shutter priority
ISOSpeedRatings
100
ExifVersion
0221
DateTimeOriginal
2016:08:06 10:30:41
DateTimeDigitized
2016:08:06 10:30:41
ComponentsConfiguration
ShutterSpeedValue
1/400 seconds
ApertureValue
F 5.60
ExposureBiasValue
-0.33
MeteringMode
Multi-segment
Copy to clipboard
Exit


haveibeenpwned.com
';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?

FACEBOOK AI ENGINE

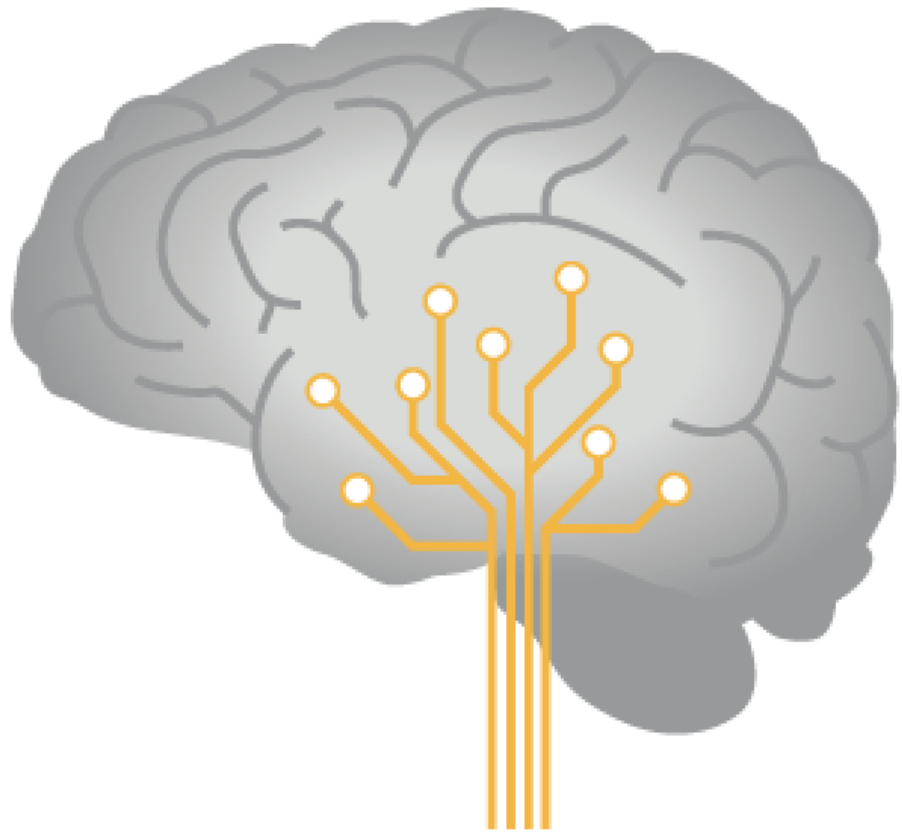
HOW DO HACKERS HACK ?



10100100 11011
110001 0110110
0011011 010101
1101010010 110

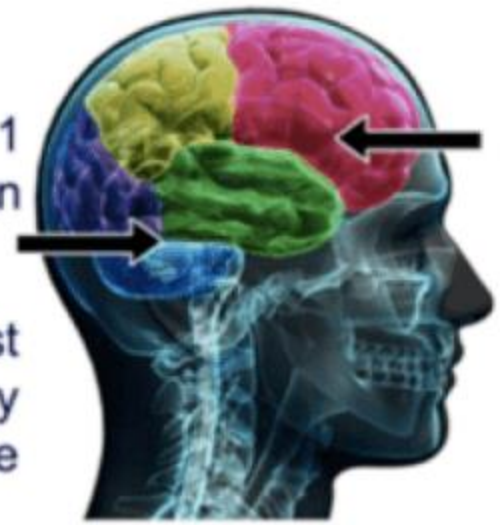
PRINCIPLE 1

THE HUMAN BRAIN IS NOT A COMPUTER



Human Decision Making: System 1 vs. System 2

Two Decision Making Routes



System 1
Unconscious Emotion

Very Fast
Involuntary
Associative

Implicit Responses

System 2
Conscious Thinking

Slow
Controlled
Rule Following

Explicit Responses

3M Pf14.0W Widescreen Privacy Filter(16:9)

Brand: 3M

4.4 out of 5 stars 595 ratings

| 20 answered questions

10 Days Replacement

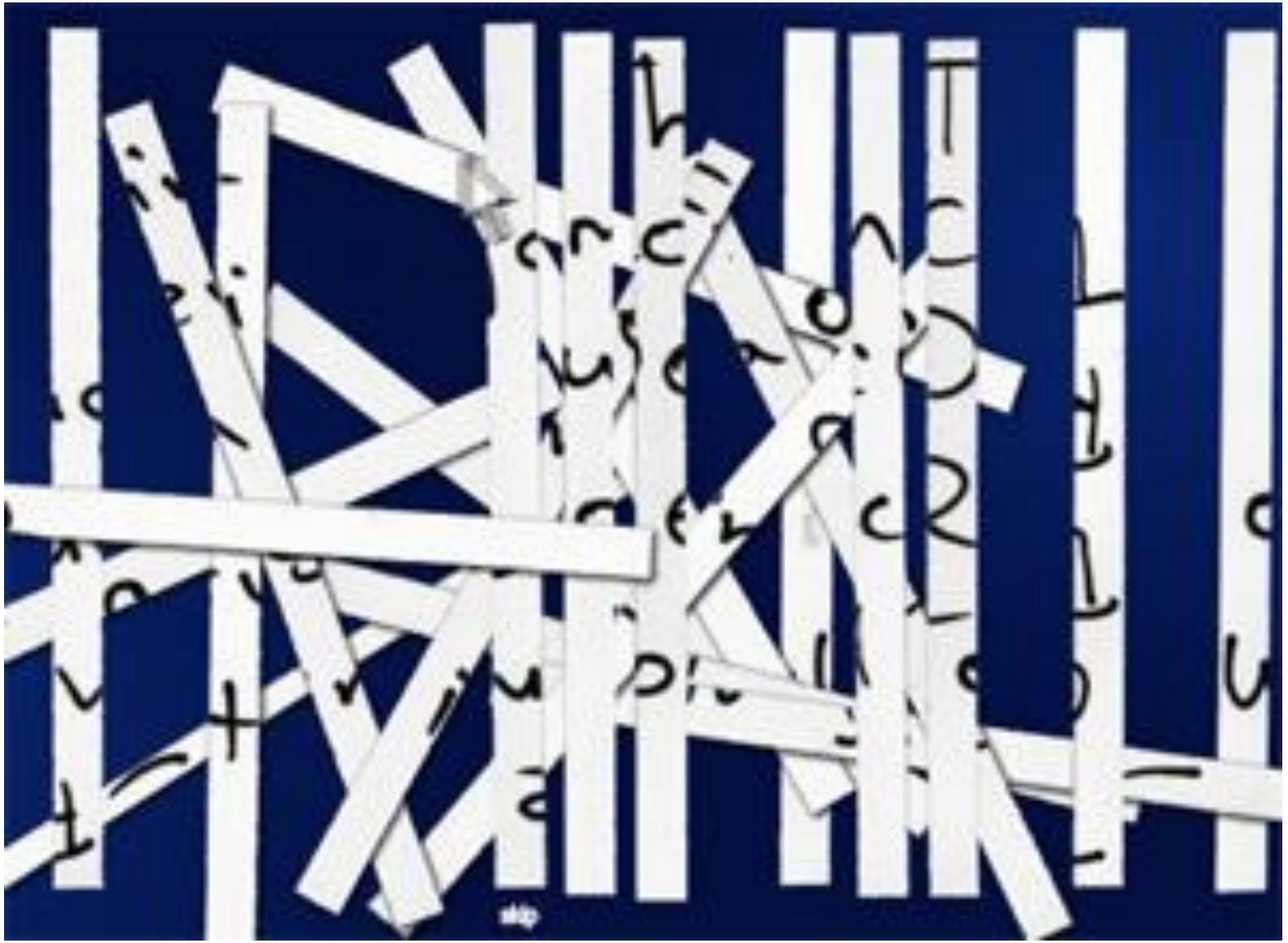
1 Year Warranty

Available from these sellers.

New (2) from ₹ 3,850.00 + FREE Shipping

- Fits screen sizes of 14" diagonaly measured (Width 12 3/16",Height 6 13/16")
- Protects on screen data when viewed from the side keeping your electronic information confidential making it excellent for use in high traffic areas.
- Provides 1.5 times more effective privacy than competitive models.
- Helps protect your fragile LCD screen from damage
- Reversible;Choose glossy or matte side

› See more product details

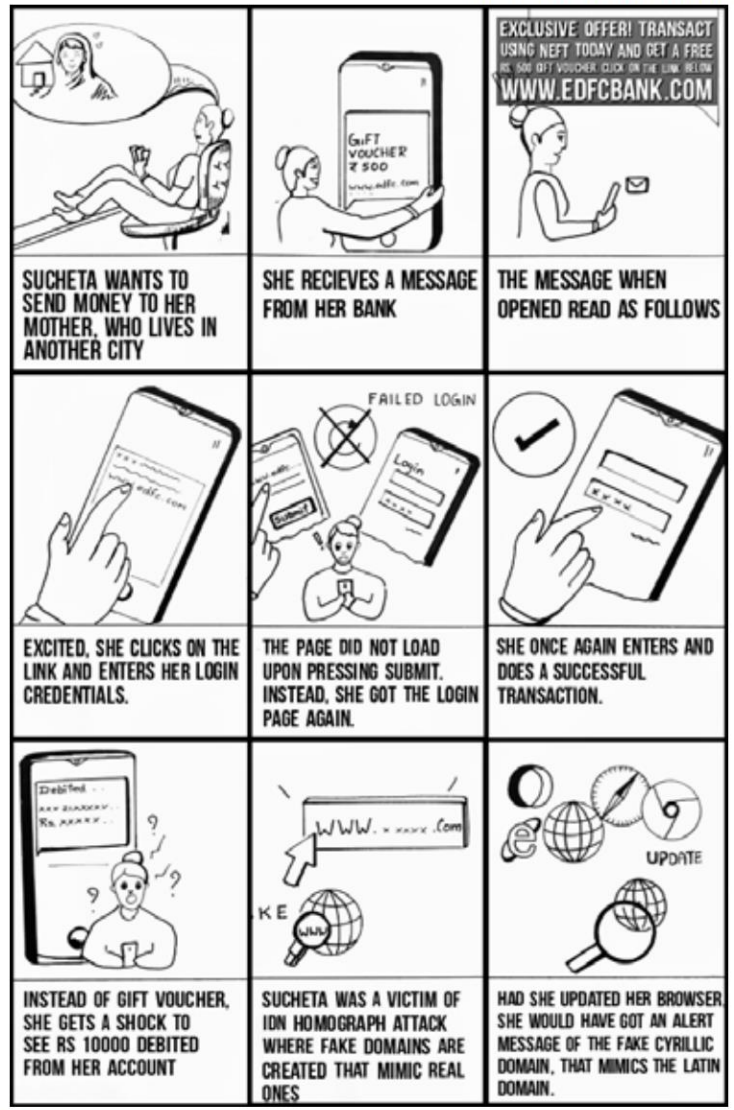


The First
Commercial
Document
Reconstruction
Tool in the World!

SURE PASS
CYBER PATRIOT
Indian Cyber Institute
Supported by
ISEA
Information Security Education & Awareness
Cyber Safe
Girl
4.0
40 eye-opening infotoons
to ensure online safety of girls
Ananth Prabhu G PhD, Post Doctoral Fellow
www.cybersafegirl.com
Co-Authors : Adv Prashant Jhala & Yashavantha Kumar KN DySP

Index

MOBILE RECHARGE SHOP
DEBIT CARD CLONING
KEYLOGGER
SMS SPOOFING
CALL SPOOFING
RANSOMWARE
CYBER STALKING
PICTURE MORPHING
PROFILE HACKING
ONLINE GAMES
JOB CALL LETTER
DEEPFAKES
DATING WEBSITE
CAMERA HACKING
SOCIAL TROLLING
PONZI SCHEME
FAKE MATRIMONIAL PROFILE
MOBILE REPAIR SHOP
FAKE REVIEWS
FAKE PROFILE WITH SEXTORTION
CYBER VULTURES
APP TRAPS
JUICE JACKING
WIFI HACKING
ONLINE RADICALIZATION
HONEY TRAP
QR CODE SCAM
RFID CLONING
DRONE SURVEILLANCE
SEARCH ENGINE RESULTS SCAM
IDN HOMOGRAPH ATTACK
SCRATCH CARD SCAM
SIM SWAP
CRYPTOJACKING
VIDEO CONFERENCE SCAM
KIDS MOBILE PHONE
SMART HOMES
MICRO LOANS
BLUE SNARFING
STOLEN PHONE



SUCHETA WANTS TO SEND MONEY TO HER MOTHER, WHO LIVES IN ANOTHER CITY

SHE RECIEVES A MESSAGE FROM HER BANK

THE MESSAGE WHEN OPENED READ AS FOLLOWS

EXCITED, SHE CLICKS ON THE LINK AND ENTERS HER LOGIN CREDENTIALS.

THE PAGE DID NOT LOAD UPON PRESSING SUBMIT. INSTEAD, SHE GOT THE LOGIN PAGE AGAIN.

SHE ONCE AGAIN ENTERS AND DOES A SUCCESSFUL TRANSACTION.

INSTEAD OF GIFT VOUCHER, SHE GETS A SHOCK TO SEE RS 10000 DEBITED FROM HER ACCOUNT

SUCHETA WAS A VICTIM OF IDN HOMOGRAPH ATTACK WHERE FAKE DOMAINS ARE CREATED THAT MIMIC REAL ONES

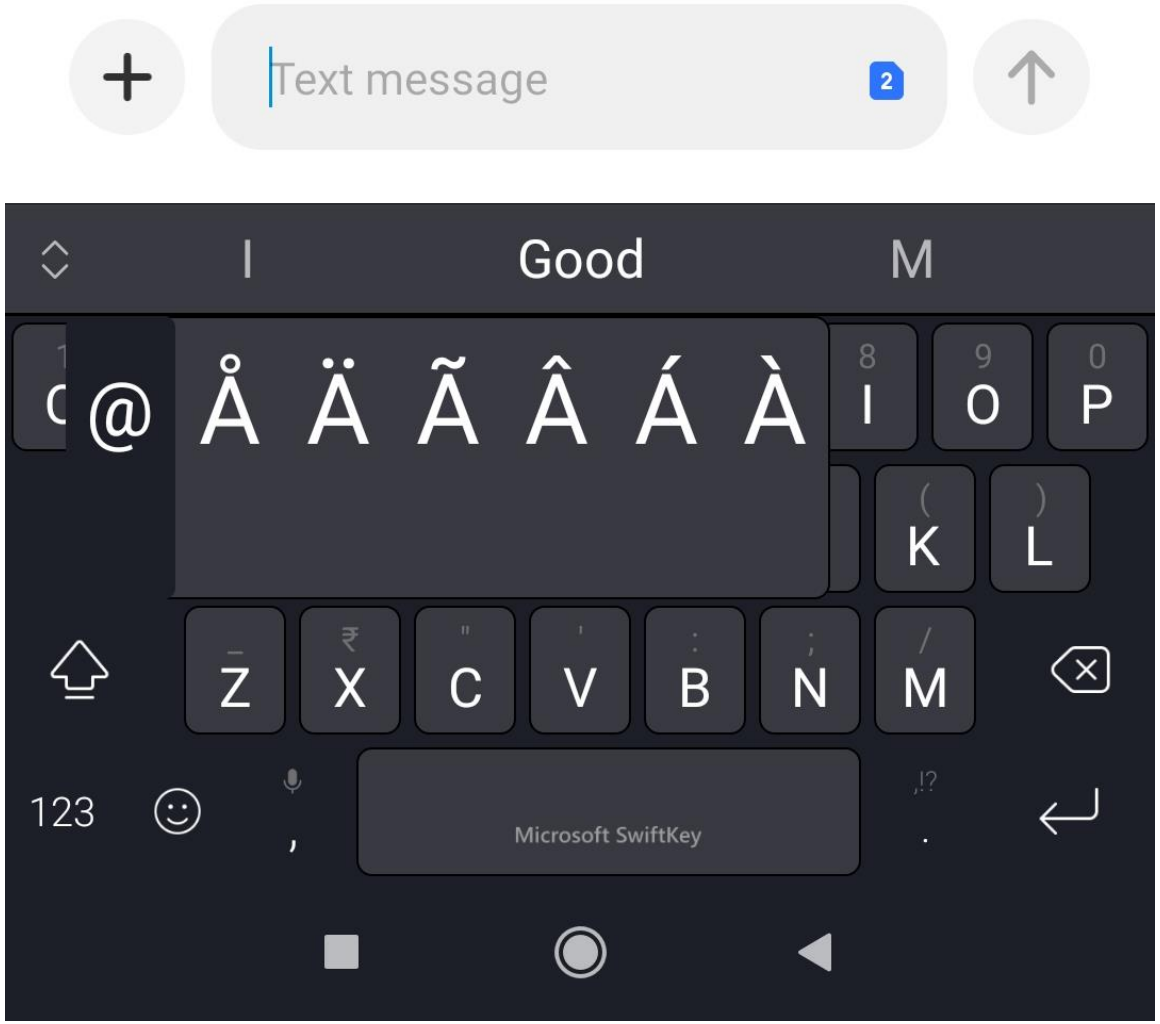
HAD SHE UPDATED HER BROWSER SHE WOULD HAVE GOT AN ALERT MESSAGE OF THE FAKE CYRILLIC DOMAIN, THAT MIMICS THE LATIN DOMAIN.

LUSTRE LIPSTICK ROUGE À LÈVRES
NET WT./ POIDS NET 3 g/0.1 US OZ
LUSTRE LIPSTICK/ROUGE À LÈVRES/ROSSETTO/LIPPENSTIFT/BARRA DE LABIOS
MAC

The Tale of Two Links

www.amazon.com

www.amazon.com


Text message
I
Good
M
@
Å
Ä
Ã
Â
Á
À
8
I
9
O
0
P
(
K
)
L
Z
X
C
V
B
N
M
123
Microsoft SwiftKey

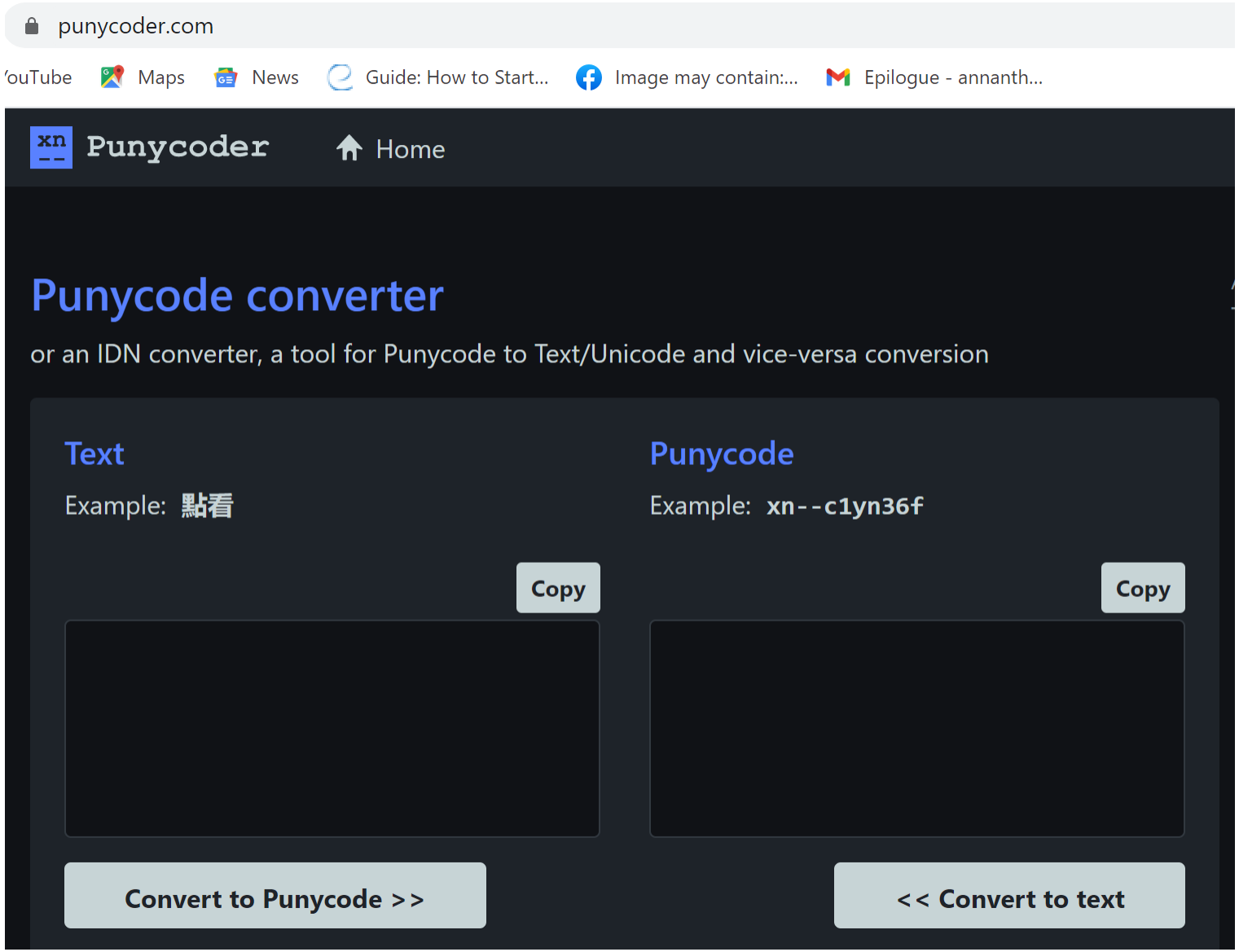
IDN HOMOGRAPH ATTACK

An IDN homograph attack is similar to another type of domain name spoofing known as typosquatting. Both techniques attempt to deceive users by using a new domain name that's similar to an established name, although they exploit different types of similarities.

Sections Applicable

IT Act Section 66 – Computer related offences
IT Act Section 66C – Punishment for Identity Theft
IT Act Section 66D – Punishment for cheating by personation using a computer resource

IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating


punycoder.com
ouTube
Maps
News
Guide: How to Start...
Image may contain:...
Epilogue - annanth...
Punycoder
Home
Punycode converter
or an IDN converter, a tool for Punycode to Text/Unicode and vice-versa conversion
Text
Example: 點看
Copy
Punycode
Example: xn--c1yn36f
Copy
Convert to Punycode >>
<< Convert to text

AMRIN IS IN FINANCIAL CRUNCH AND VERY MUCH WORRIED.
SHE WISHES FOR SOME MIRACLE TO HAPPEN WHERE SHE GETS INR 2 LAKHS.
SHE RECIEVES A SCRATCH CARD IN A WHATSAPP GROUP TO WIN UPTO 5 LAKHS.
AMRIN CLICKS ON THE LINK, SCRATCH CARD LOADS, SHE EAGERLY SCRATCHES THE CARD
You won Reward
Youve won
SHE WINS INR 3 LAKHS, SHE THANKS GOD FOR ANSWERING HER PRAYERS.
ENTER PIN
THE WALLET APP OPENS AND & IT PROMPTS FOR PIN NUMBER.
₹ 30,000
Pay from your bank
Pay ₹ 30,000
THE TRANSACTION WAS FOR PAY, INSTEAD OF RECEIVE WHICH AMRIN HADN'T CHECKED.
Debited
Sent
AMRIN ENTERS THE PIN ONLY TO LOOSE HER HARD EARNED INR 30,000.
ENTER PIN
SHE WAS UNAWARE THAT WALLETS DO NOT ASK PIN FOR RECEIVING MONEY.

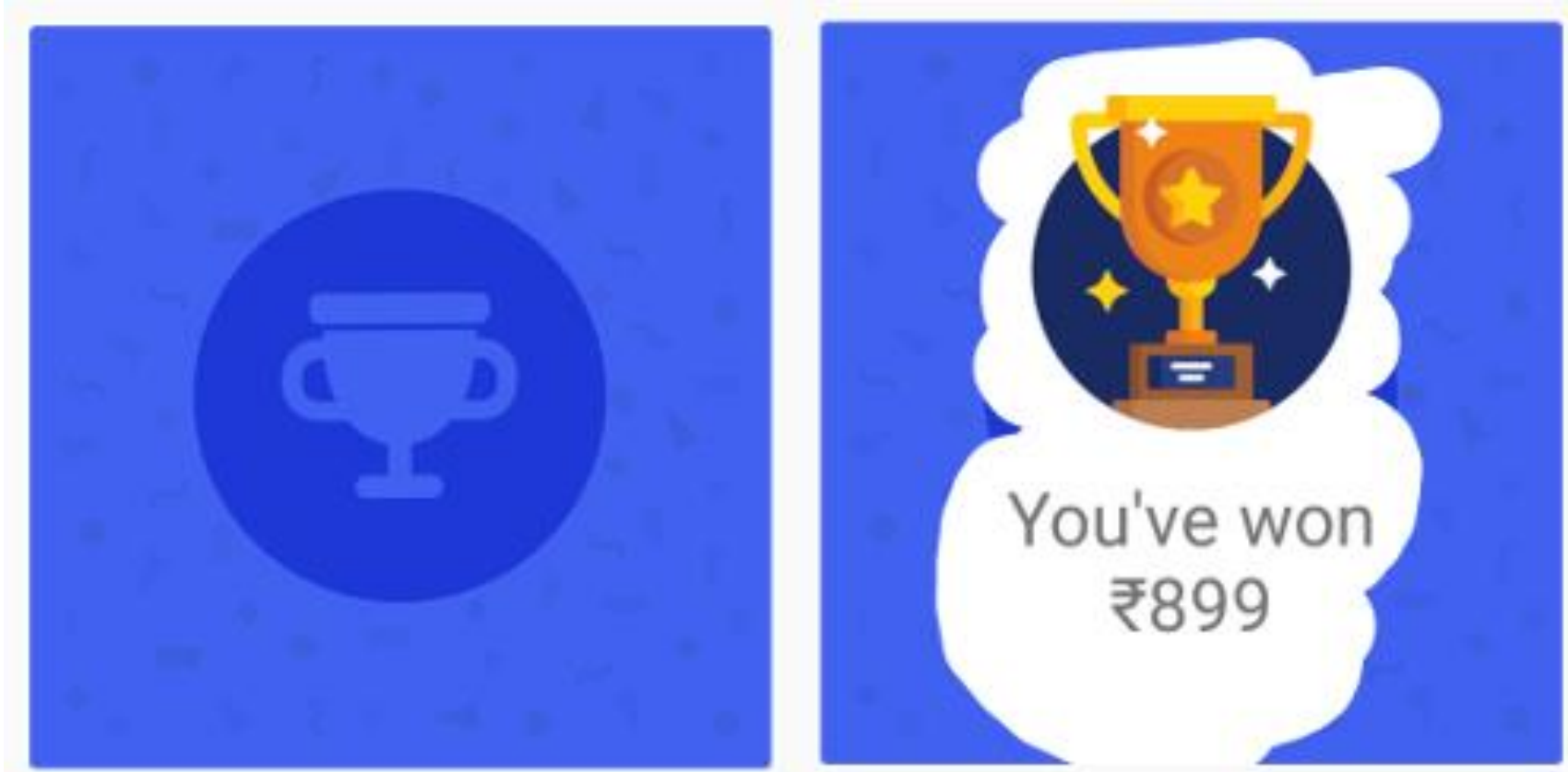
SCRATCH CARD SCAM

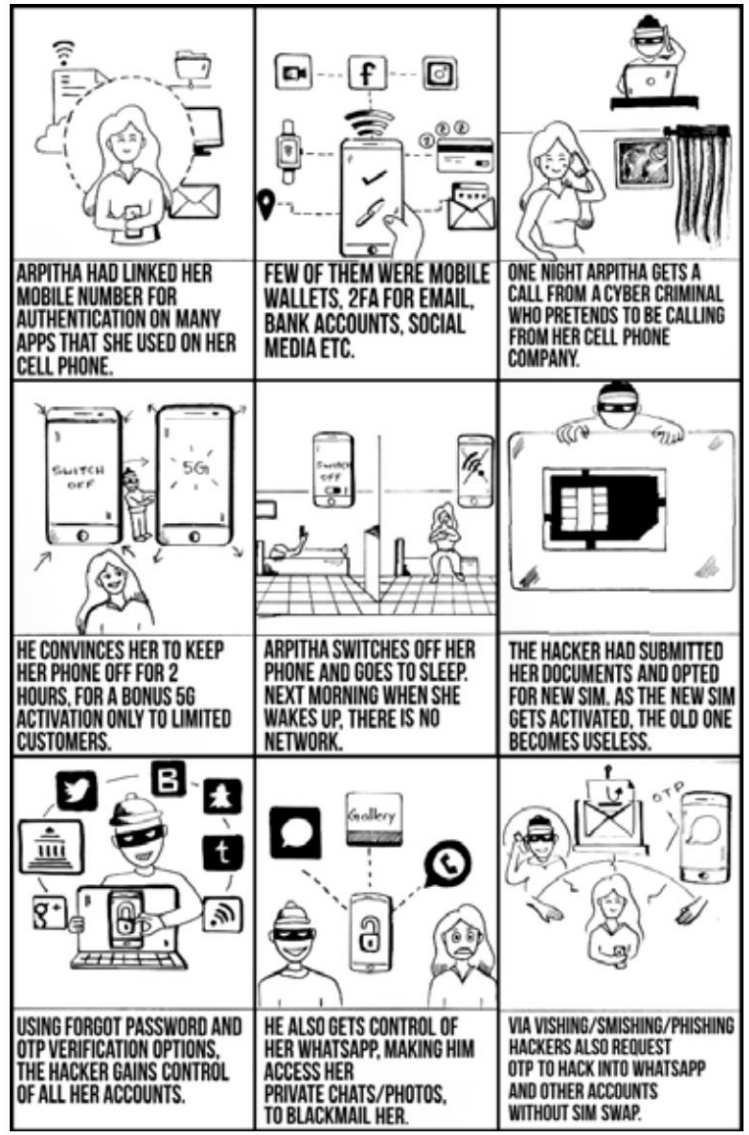
A user receives a message with a link to a third-party website with a promise of winning guaranteed money. When the user clicks on the link, it redirects to a website with a scratch card mimicking the design of popular Pay Wallets scratch card.

Sections Applicable

IT Act Section 66 - Computer related offences
IT Act Section 66C - Punishment for Identity Theft
IT Act Section 66D - Punishment for cheating by personation using a computer resource

IPC Section 419 - Punishment for cheating by personation
IPC Section 420 - Cheating


You've won
₹899


ARPITHA HAD LINKED HER MOBILE NUMBER FOR AUTHENTICATION ON MANY APPS THAT SHE USED ON HER CELL PHONE.
FEW OF THEM WERE MOBILE WALLETS, 2FA FOR EMAIL, BANK ACCOUNTS, SOCIAL MEDIA ETC.
ONE NIGHT ARPITHA GETS A CALL FROM A CYBER CRIMINAL WHO PRETENDS TO BE CALLING FROM HER CELL PHONE COMPANY.
SWITCH OFF
5G
HE CONVINCES HER TO KEEP HER PHONE OFF FOR 2 HOURS, FOR A BONUS 5G ACTIVATION ONLY TO LIMITED CUSTOMERS.
ARPITHA SWITCHES OFF HER PHONE AND GOES TO SLEEP. NEXT MORNING WHEN SHE WAKES UP, THERE IS NO NETWORK.
THE HACKER HAD SUBMITTED HER DOCUMENTS AND OPTED FOR NEW SIM. AS THE NEW SIM GETS ACTIVATED, THE OLD ONE BECOMES USELESS.
USING FORGOT PASSWORD AND OTP VERIFICATION OPTIONS, THE HACKER GAINS CONTROL OF ALL HER ACCOUNTS.
Gallery
HE ALSO GETS CONTROL OF HER WHATSAPP, MAKING HIM ACCESS HER PRIVATE CHATS/PHOTOS, TO BLACKMAIL HER.
OTP
VIA VISHING/SMISHING/PHISHING HACKERS ALSO REQUEST OTP TO HACK INTO WHATSAPP AND OTHER ACCOUNTS WITHOUT SIM SWAP.

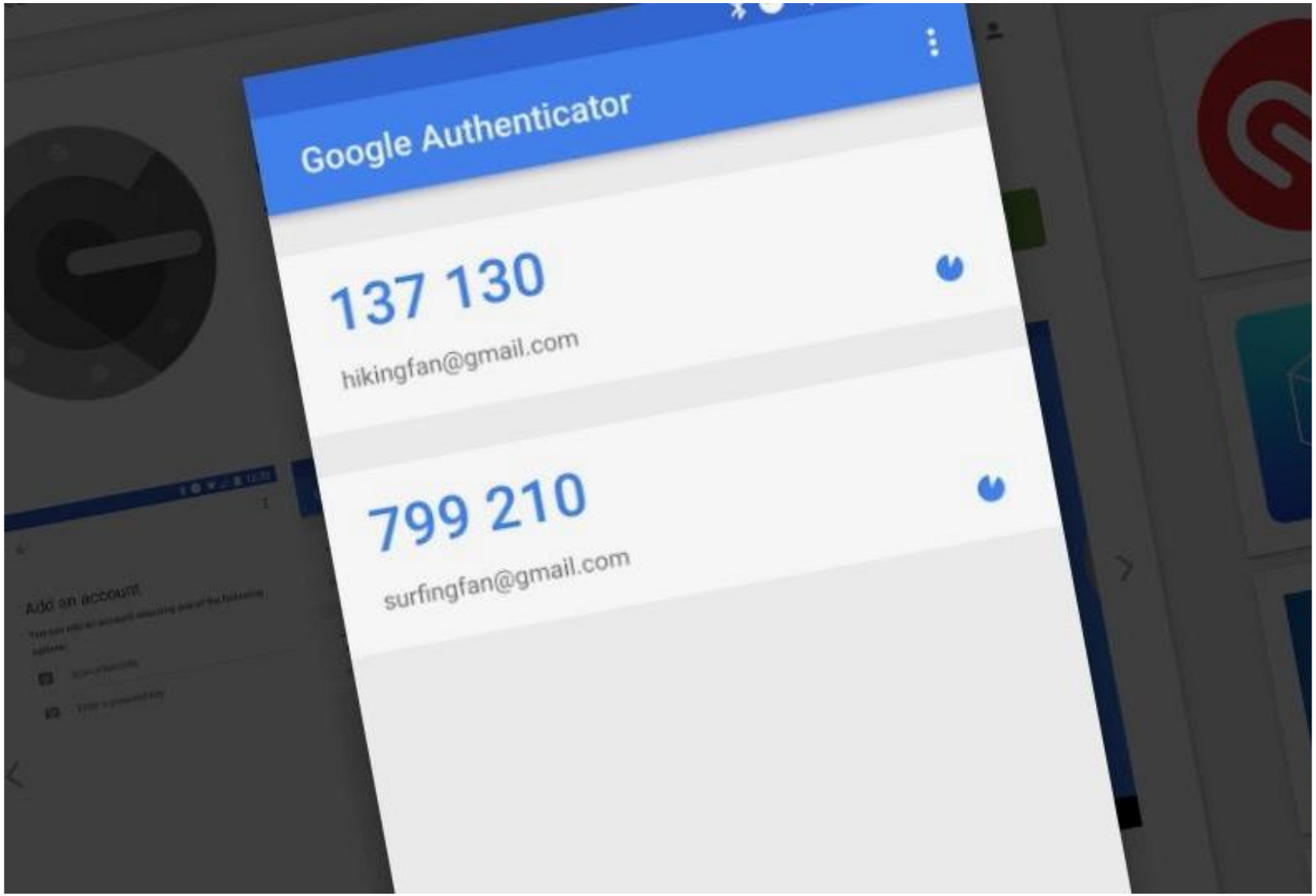
SIM SWAP

A SIM swap scam (also known as port-out scam, SIM splitting, Smishing and simjacking, SIM swapping) is a type of account takeover fraud. The fraud exploits a mobile phone service provider's ability to seamlessly port a telephone number to a device containing a different SIM. This feature is normally used when a customer has lost or had their phone stolen, or is switching service to a new phone.

Sections Applicable

IT Act Section 66 - Computer related offences
IT Act Section 66C - Punishment for Identity Theft
IT Act Section 66D - Punishment for cheating by personation using a computer resource

IPC Section 419 - Punishment for cheating by personation
IPC Section 420 - Cheating


Google Authenticator
137 130
hikingfan@gmail.com
799 210
surfingfan@gmail.com
Add an account

ROOPA IS A SOFTWARE DEVELOPER AND WORKS FROM HOME.
SHE USES 2 HIGH END LAPTOPS TO EXECUTE HER CODE WHICH ARE RESOURCE INTENSIVE.
OFF LATELY, SHE NOTICED HER SYSTEMS TO BE MUCH SLOWER THAN USUAL.
ALSO, THE POWER USAGE OF THE SYSTEM HAD GONE UP DRASTICALLY.
ctrl+alt+del
UPON OPENING THE PROCESS MANAGER, SHE COULD SEE SOME UNKNOWN APPS RUNNING.
DATA
THESE APPS WERE CRYPTOJACKING APPS THAT CONSUMED HER RESOURCES TO MINE BITCOINS.
http://www.
SHE HAD CLICKED ON AN UNKNOWN LINK THROUGH WHICH THIS APP WAS INSTALLED.
RAM
PROCESSOR
USING HER SYSTEMS RAM AND PROCESSOR, THE CYBER CRIMINAL EARNS A LOT OF MONEY BY MINING.
HAD SHE INSTALLED A GOOD PAID ANTIVIRUS AND BROWSER EXTENSION TO BLOCK COIN MINING, THE SYSTEM WOULD HAVE BEEN SAFE.

CRYPTOJACKING

It is a type of cyberattack in which a hacker co-opts a target's computing power to illicitly mine cryptocurrency on the hacker's behalf. Cryptojacking can target individual consumers, massive institutions, and even industrial control systems. It slows down infected computers, as the mining process takes priority over other legitimate activities.

Sections Applicable

IT Act Section 66 – Computer related offences
IT Act Section 66C – Punishment for Identity Theft
IT Act Section 66D – Punishment for cheating by personation using a computer resource

IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating

Section of Prevention of Money Laundering Act, 2002 (PMLA), may apply as per the facts of the case.

DETECTING CRYPTOJACKING

1. **Be aware of decrease in performance** in computing devices.
2. **Look for overheating of devices** and running fans for cooling.
3. **Monitor computer** for an increase in CPU usage.
4. **Check for coding** and file changes on your site.
5. **Scan for malware** to monitor your websites.
6. **Follow crypto-news** and look for parallels on your site.

VARONIS

PREVENTING CRYPTOJACKING

Train your IT Team to detect cryptojacking.

Use anti-cryptomining browser extensions.

Educate employees not to click on links in emails.

Disable JavaScript to block cryptoming code.

Use ad-blockers to block malicious code in online ads.

VARONIS

AMRITA WORKS FOR A MNC AS A TEAM LEAD. OFF LATELY, SHE HAD OPTED FOR WORK FROM HOME.
SHE USED TO REGULARLY HOST ONLINE MEETINGS TO COORDINATE WITH HER TEAM MEMBERS.
EVEN THE CLIENTS AT TIMES USED TO INTERACT VIA VIDEO CONFERENCE TO CHECK FOR PROGRESS AND SUGGEST CHANGES.
ONE MORNING, DURING THE CLIENT MEETING, A RANDOM USER LOGS IN AND POSTS A PORN CLIP.
EMBARRASSED BY THE EVENT, AMRITA LOGGED OFF.
Meeting ID
SHE HAD MADE THE MISTAKE OF POSTING THE MEETING ID AND PASSWORD IN THE SAME MESSAGE IN A DISCUSSION FORUM.
A DISGRUNTLED EMPLOYEE FROM THE CLIENTS SIDE LOGGED IN WITH A PROXY NAME.
WAITING ROOM
THE WAITING ROOM WAS NOT ENABLED TO SCREEN THE PARTICIPANTS.
Share Screen
File Share
PERMISSION TO SHARE SCREEN AND FILE SHARE WAS NOT DISABLED FOR ALL THE PARTICIPANTS.

VIDEO CONFERENCE SCAM

There has been a mass adaptation of online platforms to conduct meetings, online classes, conferences without giving much consideration to the security settings of these platforms. This has paved the way for cyber criminals to take advantage of loopholes for malicious purposes.

Sections Applicable

IT Act Section 66 – Computer related offences
IT Act Section 66C – Punishment for Identity
IT Act Section 67 – Publishing or transmitting obscene content
IT Act Section 67A – Publishing or transmitting sexually explicit acts or conduct

Theft
IT Act Section 66D – Punishment for cheating by personation using a computer resource
(as per the facts of the case)

IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating (as per the facts of the case)

1. Require passwords for all meetings

2. The chairperson joins first and enables waiting room

3. Lock calls after everyone joins

4. Do not reuse meeting ID

5. Set up alerts when meetings are forwarded

6. Limit file sharing and screen sharing.

7. Prevent Recording of meeting

8. Use business or enterprise license

9. Do not share meeting ID and password in the same message.

10. Update the software of the video conference

SUMAN IS A SINGLE MOTHER. LIVES WITH HER 9 YEAR OLD SON ARNAAV.
SHE WORKS AS A BEAUTICIAN AT A PARLOUR CLOSE TO HER HOUSE.
BECAUSE OF THE PANDEMIC, ALL THE CLASSES ARE ONLINE. ARNAAV ATTENDS CLASSES VIA HIS MOTHERS MOBILE PHONE.
GAME
INSTEAD OF ATTENDING CLASSES, ARNAAV PLAYS VIDEO GAMES.
DOWNLOAD
HE ALSO DOWNLOADS PAID APPS FROM THE PLAY STORE USING THE CREDIT CARD WHICH IS STORED.
GAME
₹ XXXX
SOMETIMES, HE EVEN BUYS COINS IN THE VIDEO GAMES TO COMPLETE THE LEVEL FASTER.
HE DELETES THE TRANSACTION MESSAGE RECEIVED VIA SMS SO THAT HIS MOTHER DOES NOT FIND OUT.
BILL
SUMAN WAS SHOCKED TO SEE RS 14000 SWIPED AT PLAY STORE IN HER MONTHLY CREDIT CARD BILL.
HAD SHE ENABLED PARENTAL CONTROLS ON IOS/ANDROID, ARNAAV COULD USE THE PHONE ONLY FOR ACADEMIC PURPOSES.

WANTIKNAS
Ricardo Indra
gerry wantikn...
Ismail Fahmi - D...
Toni W Adi Putr...
Burhand Telko...
tri sugiyarto
Ashwin Sasong...
Heni Susilowati
SUMARDIN (Uni...
Achmad djuhdi...
Muslim Iskandi...
Wantiknas_Adi...
Yermias J.I.Leu...
Quido Kainde_...
Rinna Fridiana
Muh. Nandi
Wanti Setianin...
Bin Laden
Muhammad Ya...
Rizka Dinkes Ja...
LIVE
zoom

KIDS MOBILE PHONE

Children are using devices at a younger age and it's a tricky situation for most parents since they do not want their child to come across adult, abusive, or violent content on the internet. Thus, it's important to consider setting controls on the devices they use. Responsible mobile phone use is about managing costs, sticking to family rules, keeping phones safe and being respectful.

Sections Applicable

If Gambling is involved:

The acts may attract Provisions of

Section 69A – IT Act for blocking illegal gambling websites.

The Public Gambling Act,1867.

The Foreign Exchange Management Act, 1999 (FEMA).

The Lotteries Regulation Act of 1998.

A few States have made provisions for laws on Gambling.

Exceptions:

1. Horse racing is legal in India
2. Lottery system (in few States)
3. The Public Gambling Act of 1867 exempts skill-based games from the definition of gambling.

PARENTAL
PASSWORD

SHAZIA IS A TECH SAVVY HOUSE WIFE. SHE LIKES TO INSTALL THE LATEST GADGETS AT HOME.
SHE HAD VISITED A SHADY MARKET, WHERE CHEAP INTERNET OF THINGS (IOT) SALE WAS GOING ON.
60%
SHE WAS EXCITED TO SEE MANY PRODUCTS ON SALE- UPTO 60% OFF
SHAZIA BUYS A SMART BULB AND INSTALLS IT IN HER BEDROOM
THE BULB CAN BE CONTROLLED FROM HER PHONE, WHERE SHE CAN CHANGE THE COLOR OF THE LIGHT AND ALSO SWITCH ON/OFF.
HARDLY DID SHE KNOW, THE WIFI CONNECTED BULB ALSO HAD A NANO CAMERA INSIDE IT.
100% SAFE
THE CAMERA RECORDED ALL THE ACTIVITIES IN HER BEDROOM AND UPLOADED IT TO THEIR SERVER.
BARELY DID SHE KNOW THAT IOT DEVICES SHOULD BE PROCURED ONLY FROM GENUINE VENDORS AND THE SECURITY SETTINGS SHOULD BE IN PLACE.
ANY DEVICE WHICH IS INTERNET ENABLED CAN BE USED FOR SNOOPING. TECHNOLOGY IS A DOUBLE EDGED SWORD.

SMART HOMES

Smart-home devices hold a treasure trove of personal information, from your birth date to credit card details, that cybercriminals can steal via hacking if the devices lack robust protections to thwart attacks. They can then use the stolen data to launch targeted attacks to rope you into shady deals.

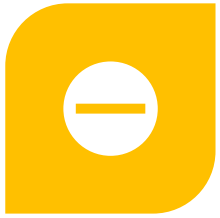
Sections Applicable

IPC Section 354 – Sexual harassment
IPC Section 354C – Voyeurism
IPC Section 509 – Outraging modesty of women

IT Act Section 66 – Computer related offences
IT Act Section 66E – Punishment for violation of privacy

1. ENABLE ROUTER SECURITY SETTINGS.

2. USE A STRONG ENCRYPTION METHOD FOR WI-FI.



3. DISABLE FEATURES YOU MAY NOT NEED.

4. KEEP YOUR SOFTWARE UP TO DATE.

5. DO THE TWO-STEP.

SAMANTHA IS A FINAL YEAR ENGINEERING STUDENT LIVING IN A PG NEAR TO HER COLLEGE.
HER PARENTS USED TO TRANSFER RS 5000 EVERY MONTH FOR HER EXPENSES.
SAMANTHA WAS UNABLE TO GET CAMPUS PLACED AS SHE HAD NO ADDITIONAL CERTIFICATIONS.
₹ 10,000
TO ENROL FOR AN ONLINE COURSE, SHE WANTED RS 10000 AND WAS HESITANT TO ASK HER PARENTS AS THEY WERE IN A FINANCIAL CRUNCH.
Ad
AN AD APPEARS WHILE BROWSING, WHICH PROMISES TO DISBURSE RS 10000 WITHOUT ANY DOCUMENTATION. HAPPILY SHE INSTALLS THE APP.
LOAN!!
IN SPITE OF COMPLETING THE COURSE, SHE DID NOT GET PLACED. THEREFORE, SHE WAS UNABLE TO REPAY THE LOAN.
HARDLY DID SHE KNOW, THE APP HAD REGULARLY ACCESSED HER FRIEND LIST, CONTACTS, LOCATION AND EVEN OTHER DATA FROM HER PHONE.
THE CUSTOMER CARE OF THE LOAN SHARK APP STARTED CALLING, ABUSING AND THREATENING HER AND HER FRIENDS FROM HER CONTACTS.
%
MANY LOAN SHARK APPS EVEN SEND BULLIES TO RECOVER THE AMOUNT AND ALSO LEVY HEAVY INTEREST ON THE LOAN AVAILED.

MICRO LOANS

Fly-by-night micro lending illegal app-based financiers are thriving. These moneylenders target younger customers who look for quick loans for consumption purposes. Those failing to pay up will have their photos shared in their family and workplace social media groups, a tactic that has driven many to desperation.

Sections Applicable

IPC Section 420 – Cheating
IPC Section 503/506 – Criminal Intimidation
IPC Section 383 – Extortion
IPC Section 306 – Abetment of Suicide
IPC Section 499/500 – Defamation
IPC Section 120B – Criminal Conspiracy
IPC Section 34 – Common Intention
Sections of Reserve Bank of India Act, 1934
(as per the facts of the case)

As per the official website of The Central Bank of India - RBI, the following 12 banks are listed

1. Bank of Baroda
2. Bank of India
3. Bank of Maharashtra
4. Canara Bank
5. Central Bank of India
6. Indian Bank
7. Indian Overseas Bank
8. Punjab and Sind Bank
9. Punjab National Bank
10. State Bank of India
11. UCO Bank
12. Union Bank of India

ALIA WANTED TO ATTEND ONLINE LECTURES. THEREFORE SHE BOUGHT A CHEAP TAB FROM A GREY MARKET.
SHE ALWAYS KEPT THE BLUETOOTH ON, AS HER EARPODS WERE ALWAYS CONNECTED TO THE TAB.
HER NEIGHBOR, ANUSH HAD MASTERED A FEW HACKING SKILLS BY GOING THROUGH THE COURSES IN THE DARK WEB.
HE DOWNLOADS A TOOLKIT WHICH CAN PAIR THE DIGITAL DEVICE WITH ANY DEVICE HAVING VULNERABILITIES.
REALIZING BLUETOOTH HAS A FAIRLY GOOD RANGE OF 10 METERS, HE COVERTLY HIDES IN HER GARDEN AND CONNECTS TO THE TAB.
UPON SUCCESSFUL PAIRING, HE GETS ACCESS TO HER FILES AND FOLDERS. ALSO HER IMEI.
HE THEREAFTER FORWARDS THE SMS AND CALLS TO HIS NUMBER.
ALIA FINDS MANY OF HER PHOTOS AND FILES MISSING FROM HER SIM ENABLED TAB. NEITHER SHE GETS ANY CALLS.
HAD SHE SET THE MAC ID OF HER BLUETOOTH AS HIDDEN INSTEAD OF DISCOVERABLE, SHE COULD HAVE BEEN SAFE.

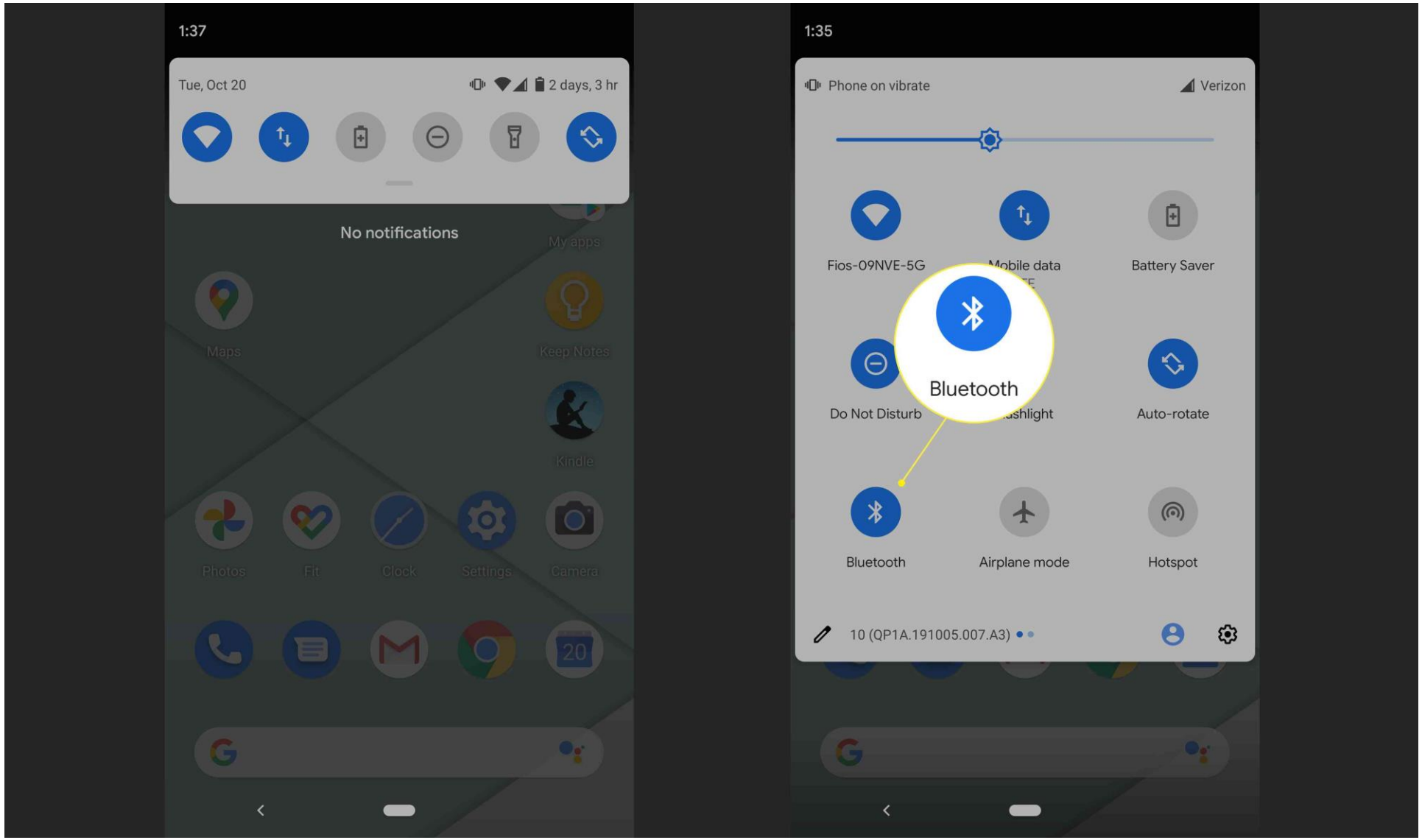
BLUE SNARFING

It is a device hack performed when a wireless, Bluetooth-enabled device is in discoverable mode. Bluesnarfing allows hackers to remotely access Bluetooth device data, such as a user's calendar, contact list, emails and text messages. This attack is perpetrated without the victim's knowledge.

Sections Applicable

IT Act Section 66 - Computer related offences
IT Act Section 66C - Punishment for Identity Theft
IT Act Section 66D - Punishment for cheating by personation using a computer resource
(as per the facts of the case)

IPC Section 419 - Punishment for cheating by personation
IPC Section 420 - Cheating (as per the facts of the case)


1:37
Tue, Oct 20
2 days, 3 hr
No notifications
My apps
Maps
Keep Notes
Kindle
Photos
Fit
Clock
Settings
Camera
1:35
Phone on vibrate
Verizon
Fios-09NVE-5G
Mobile data
Battery Saver
Bluetooth
Do Not Disturb
Auto-rotate
Bluetooth
Airplane mode
Hotspot
10 (QP1A.191005.007.A3)

ANAMIKA WAS A CELL PHONE ADDICT. SHE USED TO USE SNAPCHAT, WHATSAPP AND INSTAGRAM REGULARLY.
CARNIVAL
ALONG WITH HER FRIEND DIVYA, SHE GOES TO A CARNIVAL.
LOOKING AT THE FERRIS WHEEL, OUT OF EXCITEMENT, BOTH OF THEM BUY TICKETS AND HOP IN.
WITHOUT HER KNOWLEDGE, THE CELL PHONE FROM HER POCKET SLIPS OUT AND FALLS DOWN.
AT THE TOP, SHE PUTS HER HAND IN THE POCKET TO TAKE OUT THE PHONE TO CLICK A SELFIE.
SHELL SHOCKED, SHE REALIZES SHE LOST HER PHONE. SHE CALLS HER NUMBER FROM DIVYAS PHONE.
THE PERSON WHO STOLE HER PHONE CUTS THE CALL AND LATER SWITCHES IT OFF.
ANAMIKA COULD HAVE LOGGED INTO THE FIND MY DEVICE PORTAL AND TRACKED HER PHONE.
SHE COULD HAVE ALSO FORMATTED HER PHONE REMOTELY TO PROTECT HER DATA.

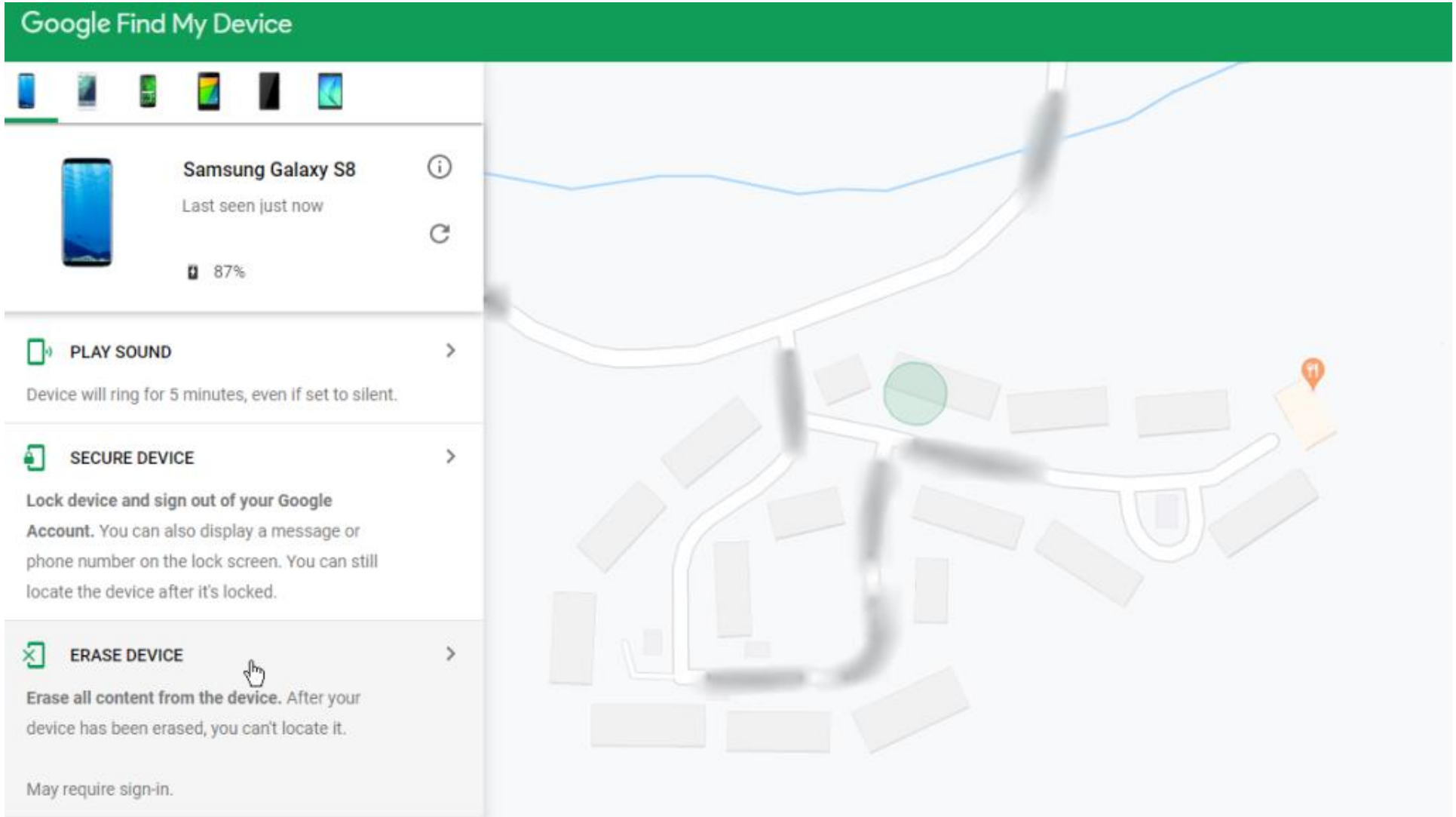
STOLEN PHONE

A stolen phone can leave you feeling helpless and scrambling. Mobile phones and the data they hold are very valuable to thieves. And for similar reasons - they hold so much important personal information of real and sentimental value - a theft can be a huge loss for the owner.

Sections Applicable

IPC Section 378/379 – Theft

IT Act Section 66 – Computer related offences


Google Find My Device
Samsung Galaxy S8
Last seen just now
87%
PLAY SOUND
Device will ring for 5 minutes, even if set to silent.
SECURE DEVICE
Lock device and sign out of your Google Account. You can also display a message or phone number on the lock screen. You can still locate the device after it's locked.
ERASE DEVICE
Erase all content from the device. After your device has been erased, you can't locate it.
May require sign-in.

CREDIT CARD

iParn RFID Aluminium Foil WiFi Credit Debit Card Cover Holder (ATM Card Sleeve 5 Pack_Silver)

5 RFID CREDIT CARD SLEEVE - atm cover card holder for men stylish,Our secure blocking credit debit card sleeves comes in a Silver Colour. Its smart design fits traditional size ... more »

₹299.00

+₹40.00 delivery

Amazon.in

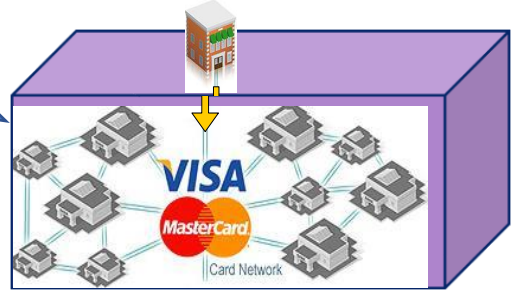
Visit site

PLASTIC CARDS PROCESS

FLOWCHART

1. Presents a card to purchase

2. Processes authorization from merchant bank



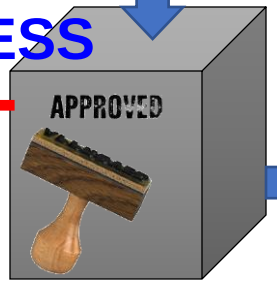
3. Merchant bank submits the authorization request to credit card network

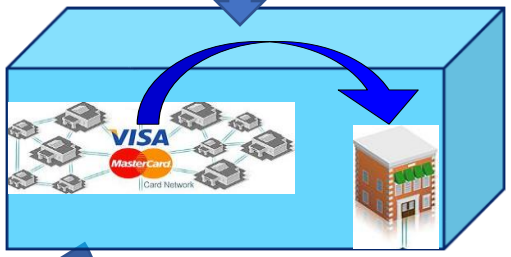
4. Credit card network sends the request to the card issuer

5. Card Issuer

Approves the transaction

Declines the transaction



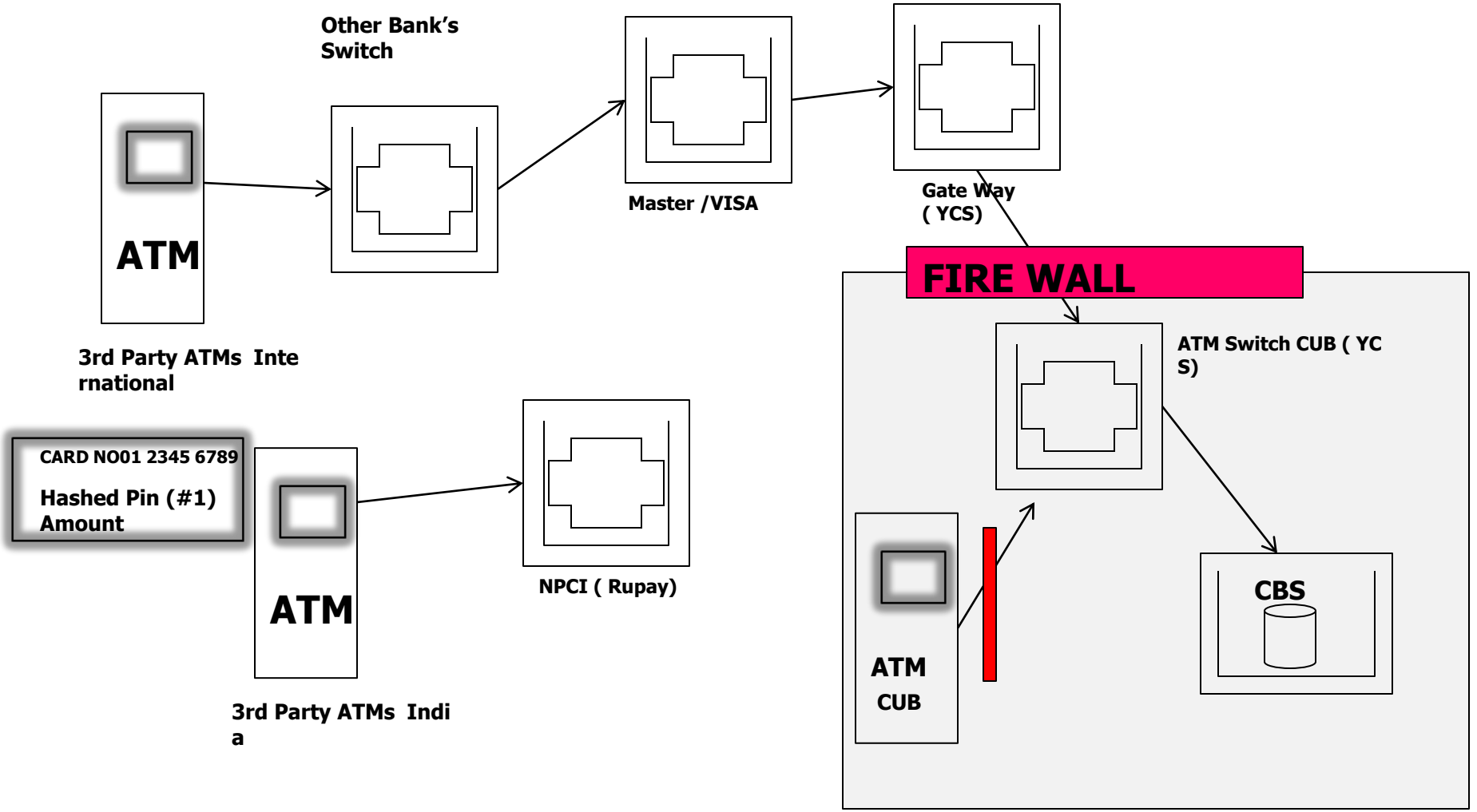


6. Credit card network forwards the card issuer's authorization response to the merchant bank

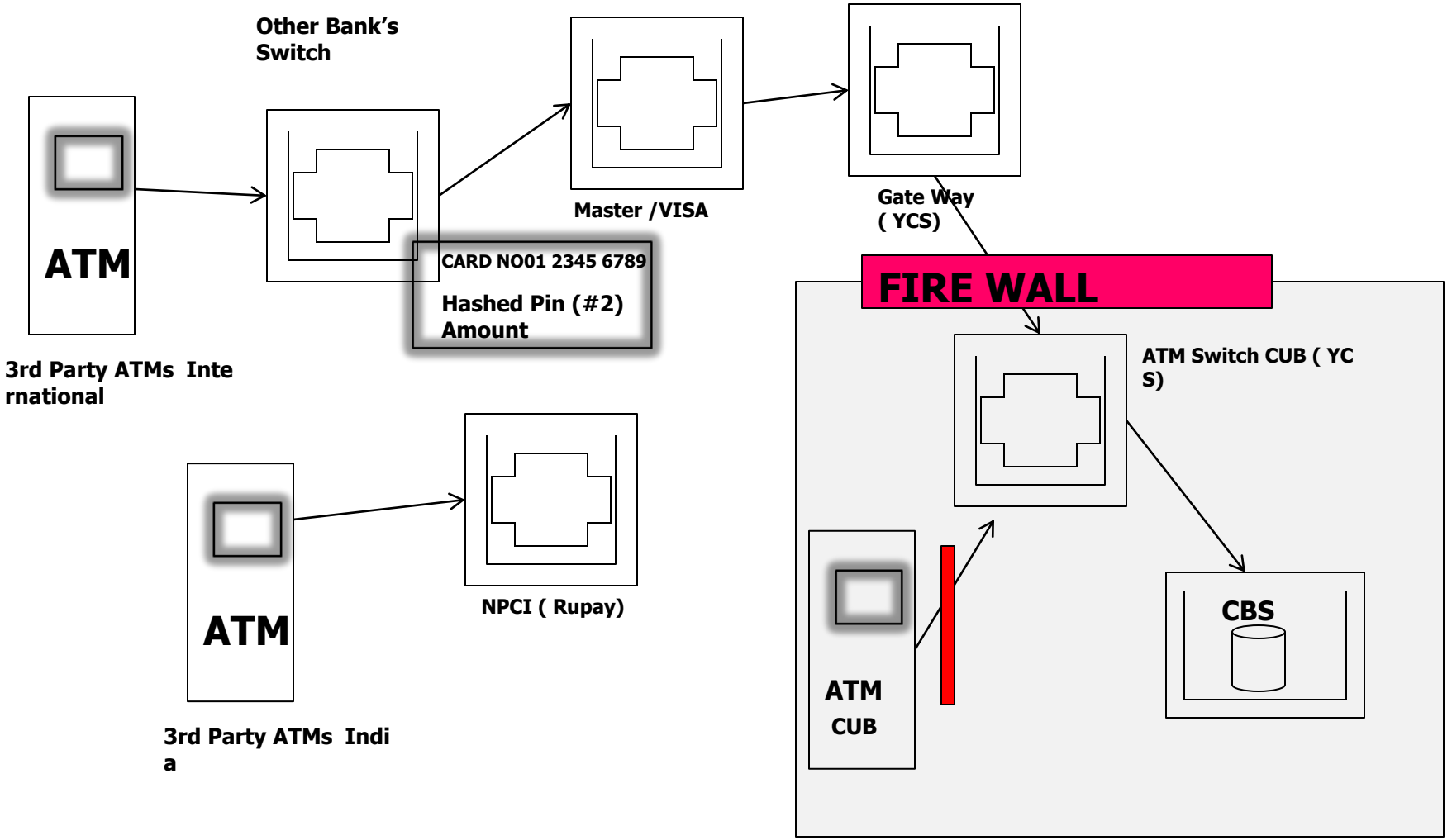
7. Merchant bank forwards the response to the merchant

8. Merchant receives the authorization response and completes the transaction

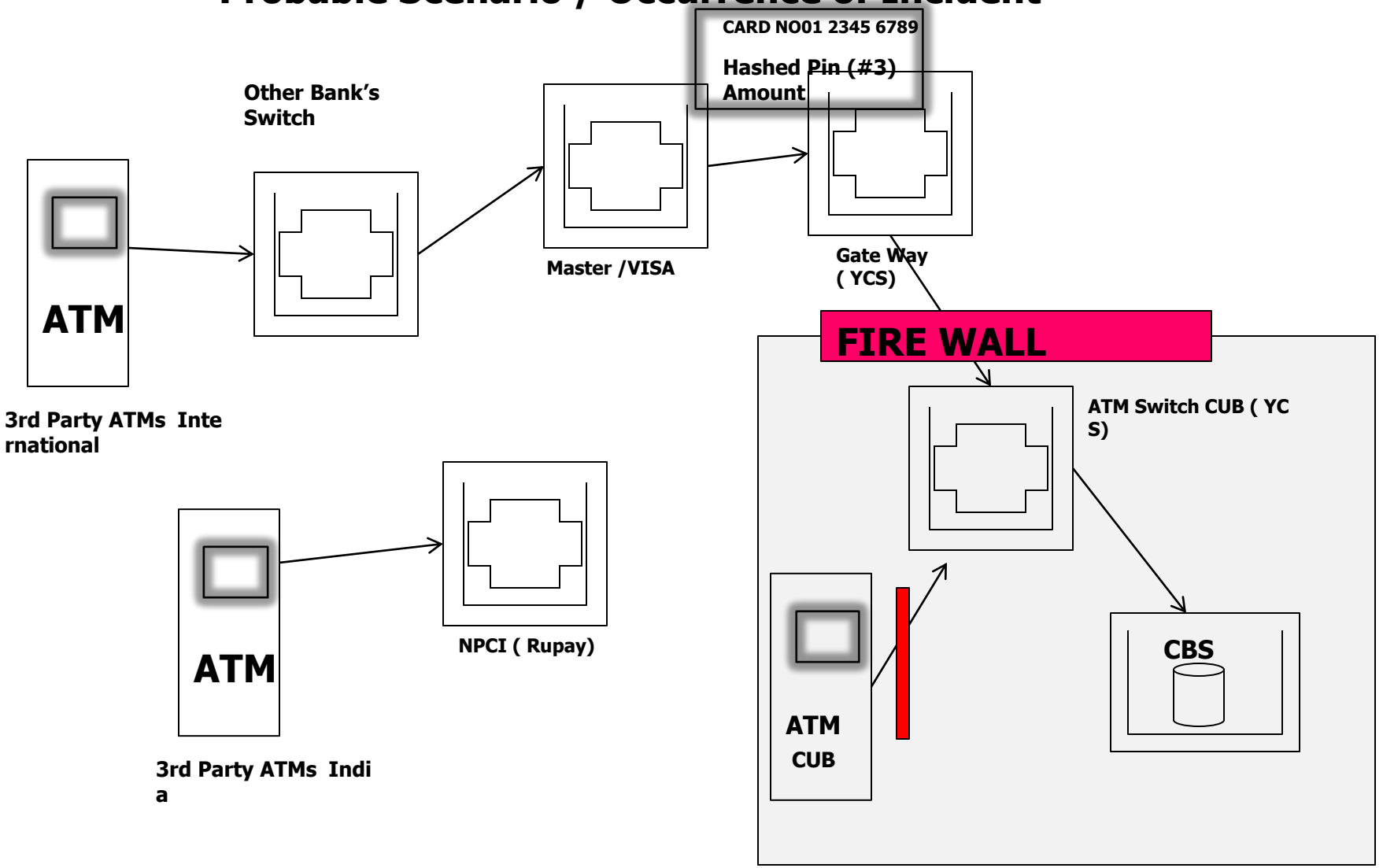
Probable Scenario / Occurrence of Incident



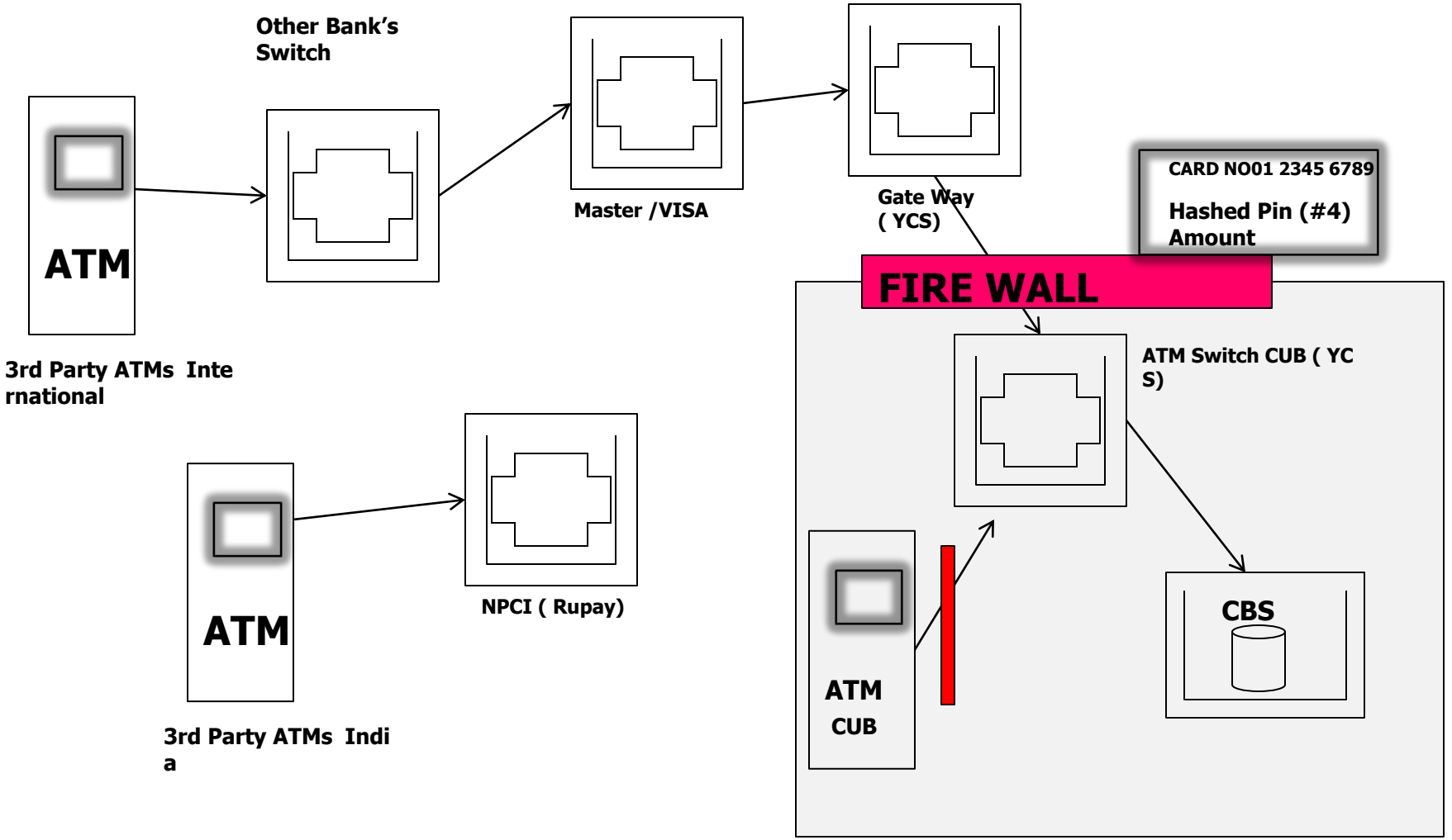
Probable Scenario / Occurrence of Incident



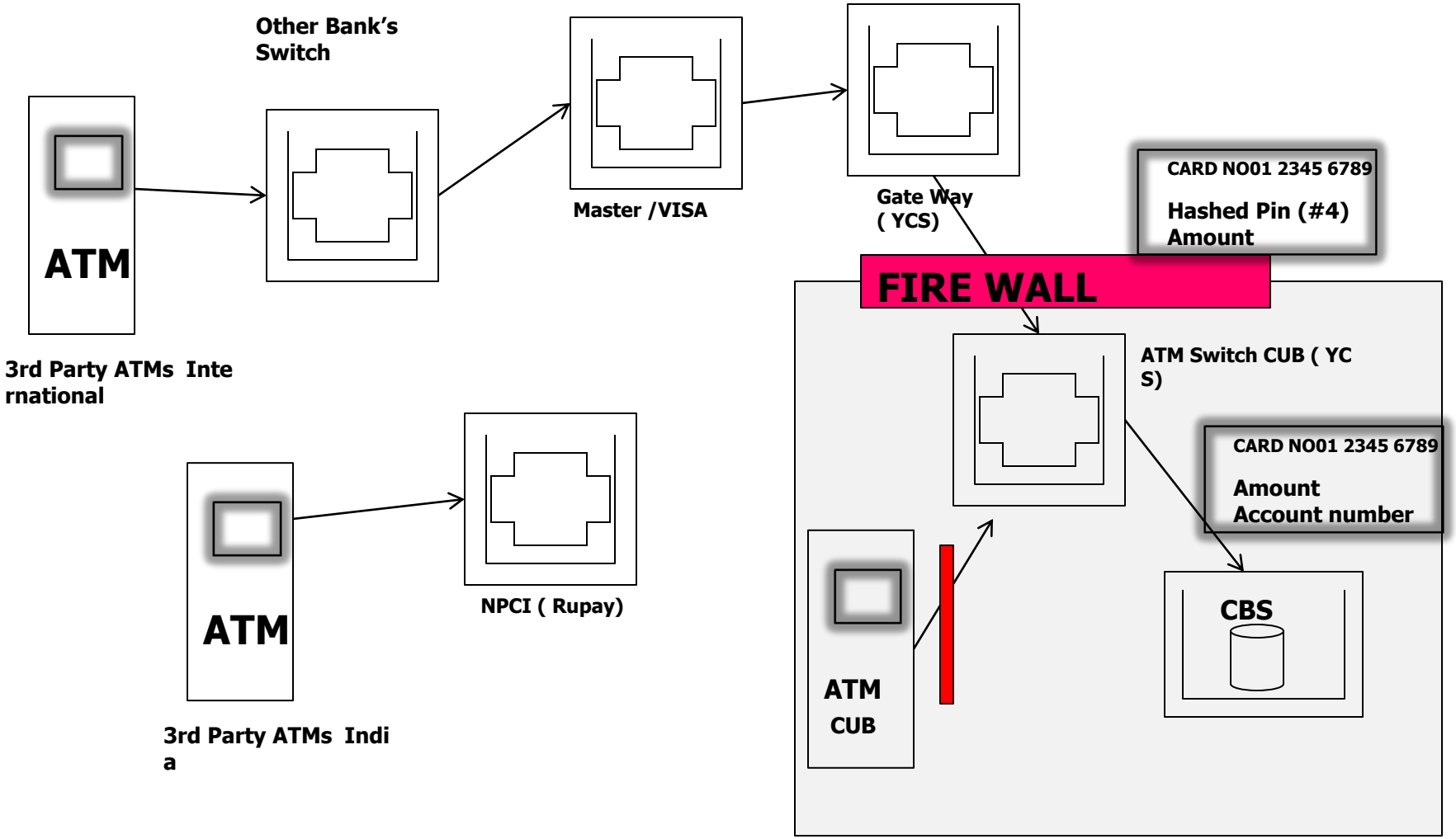
Probable Scenario / Occurrence of Incident



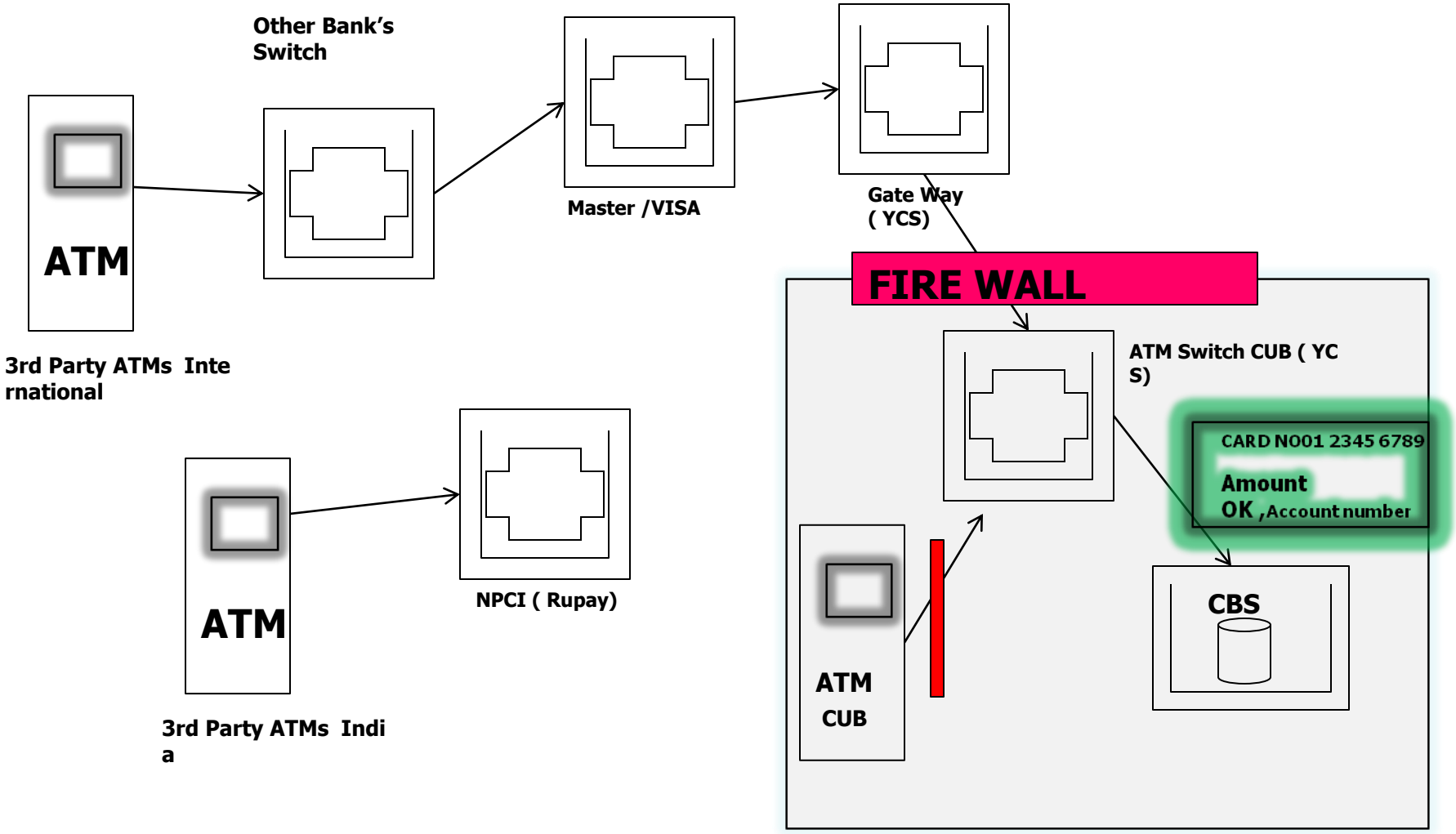
Probable Scenario / Occurrence of Incident



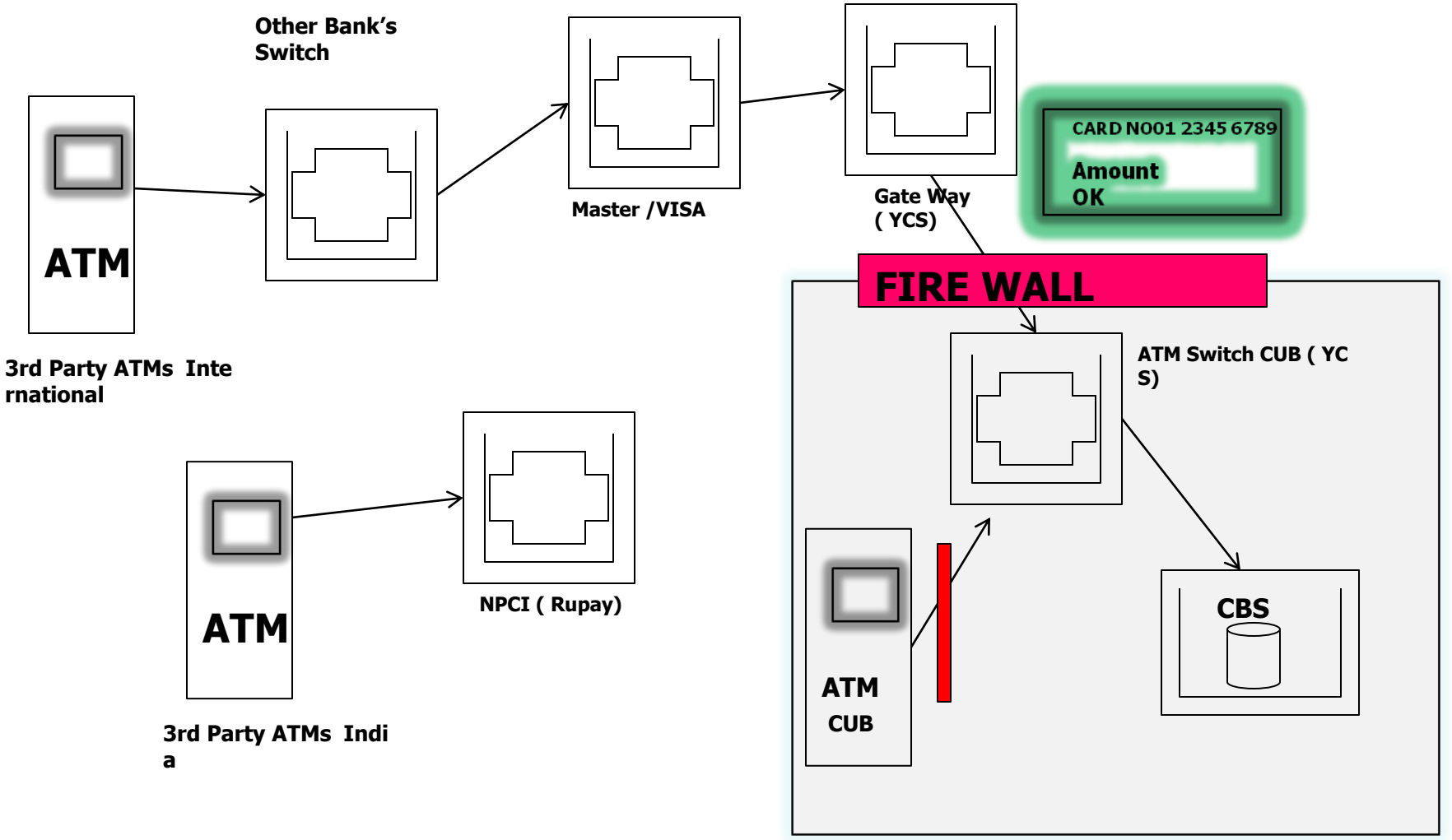
Probable Scenario / Occurrence of Incident



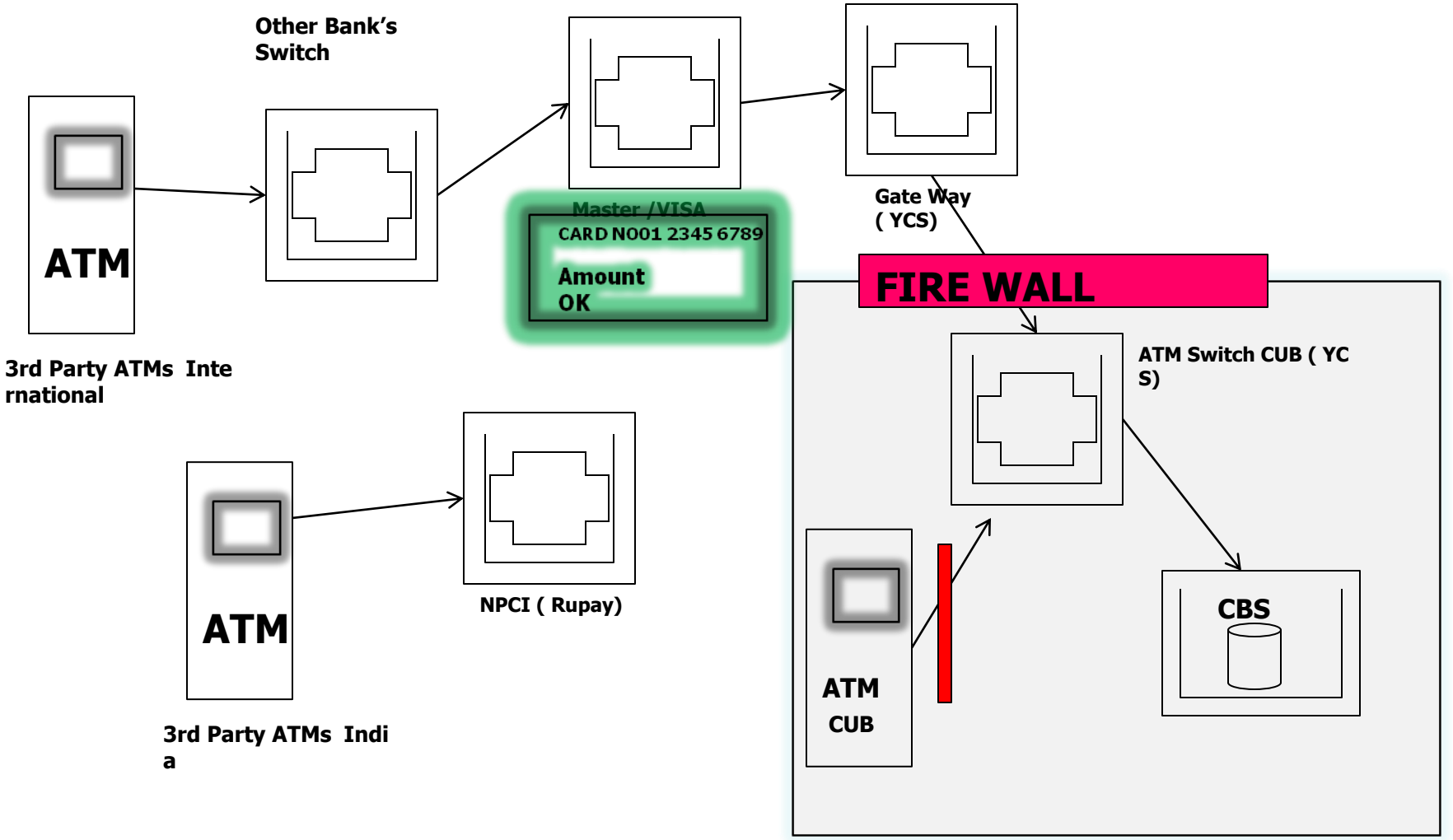
Probable Scenario / Occurrence of Incident



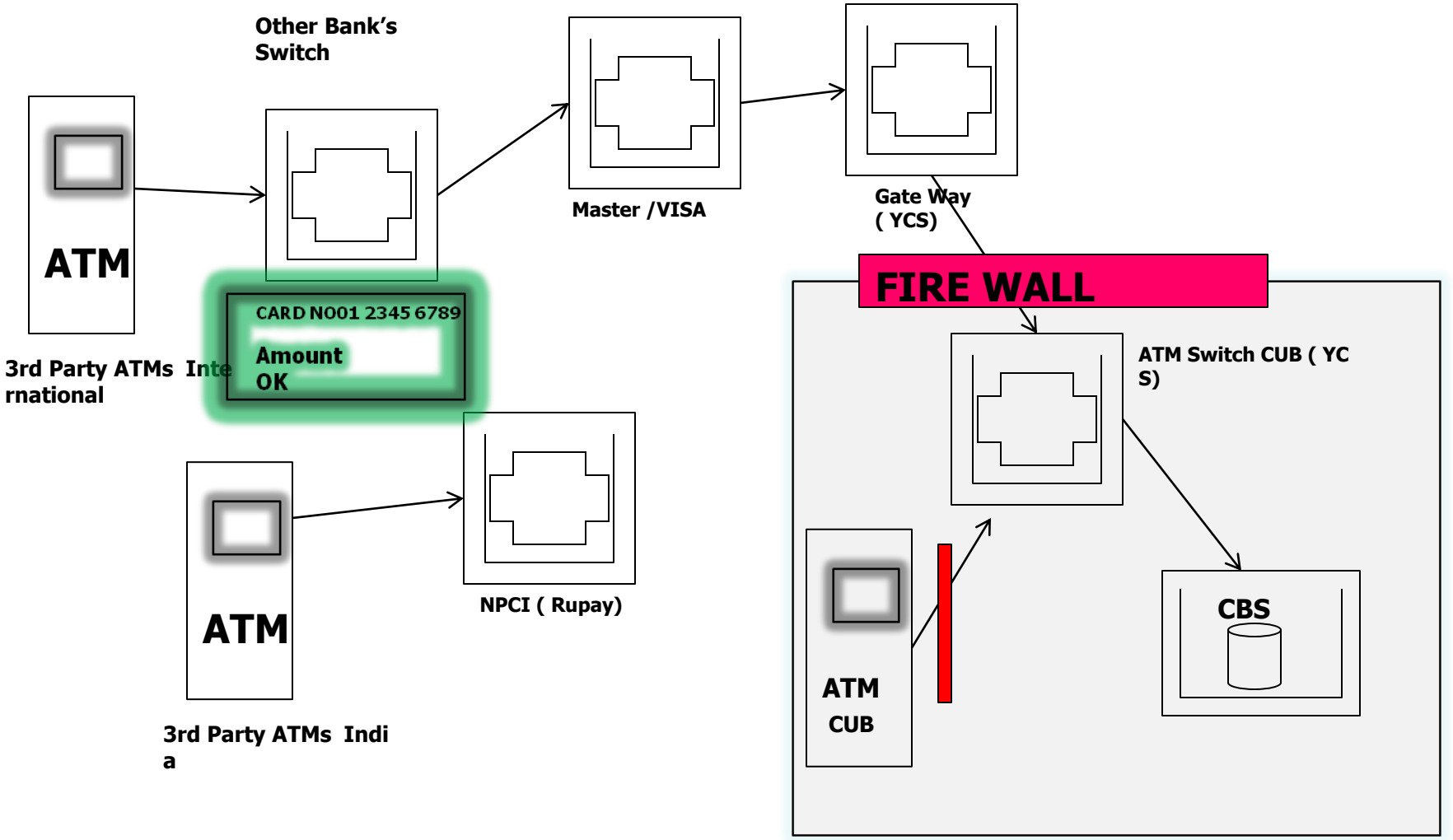
Probable Scenario / Occurrence of Incident



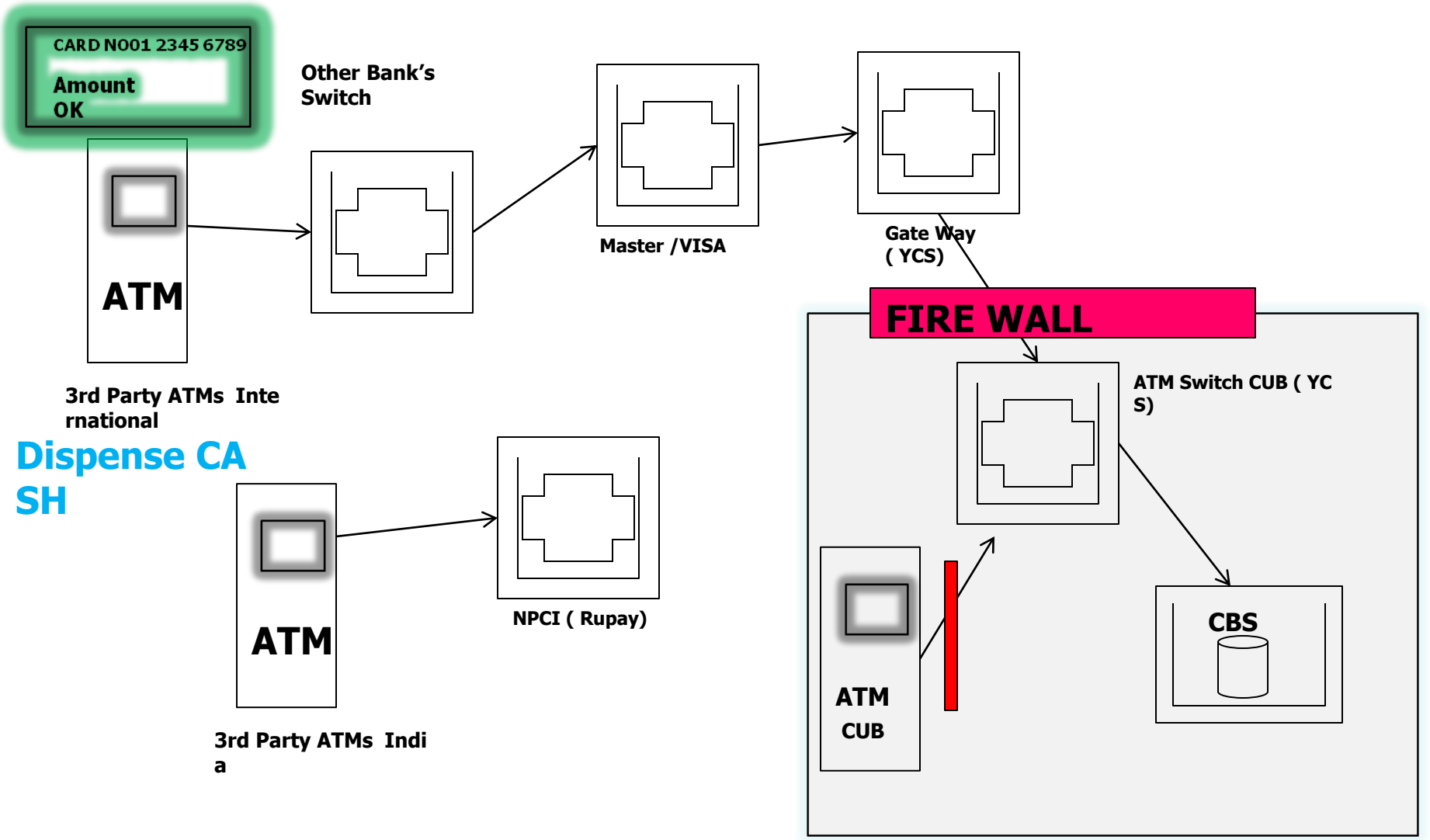
Probable Scenario / Occurrence of Incident



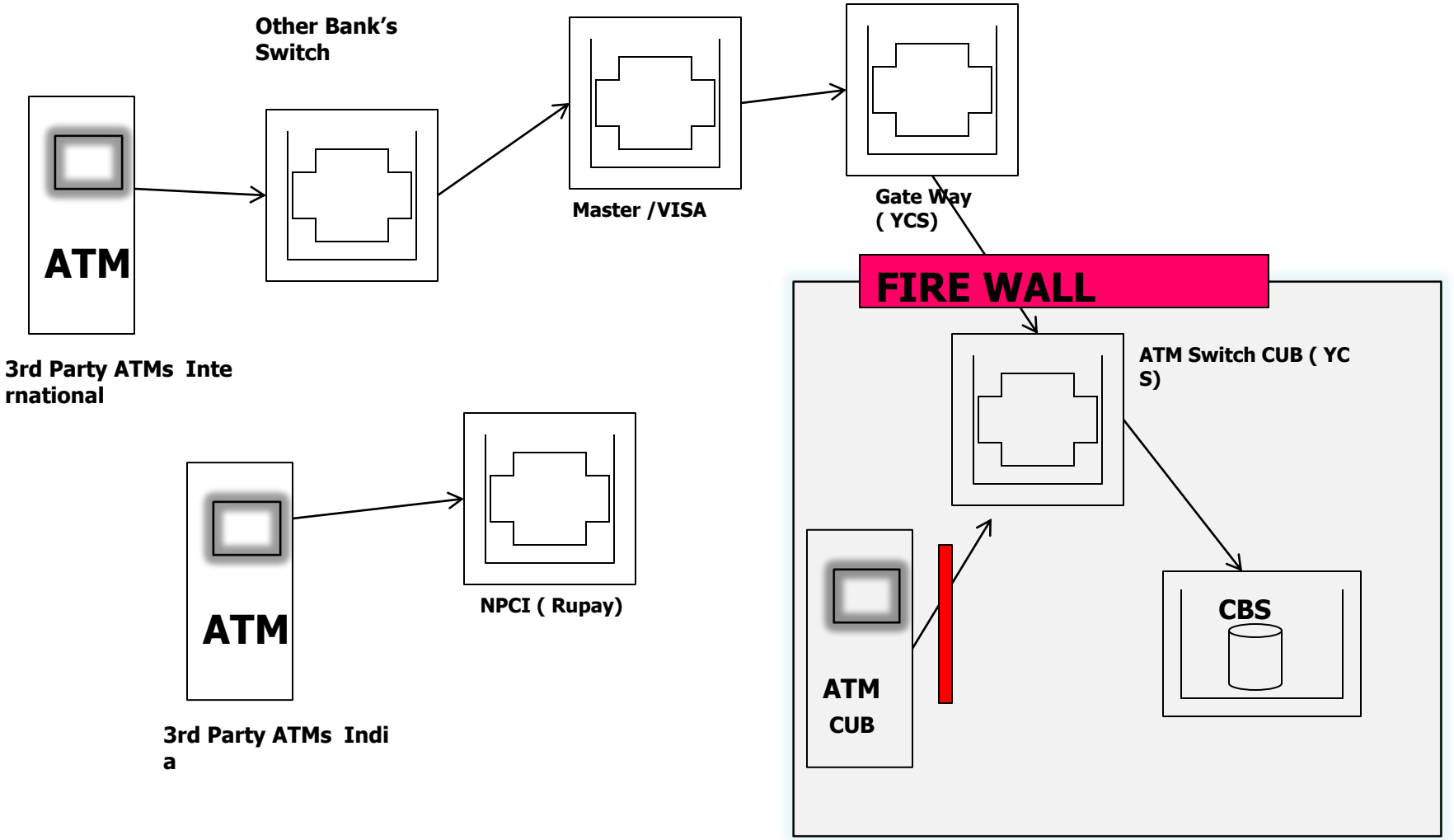
Probable Scenario / Occurrence of Incident



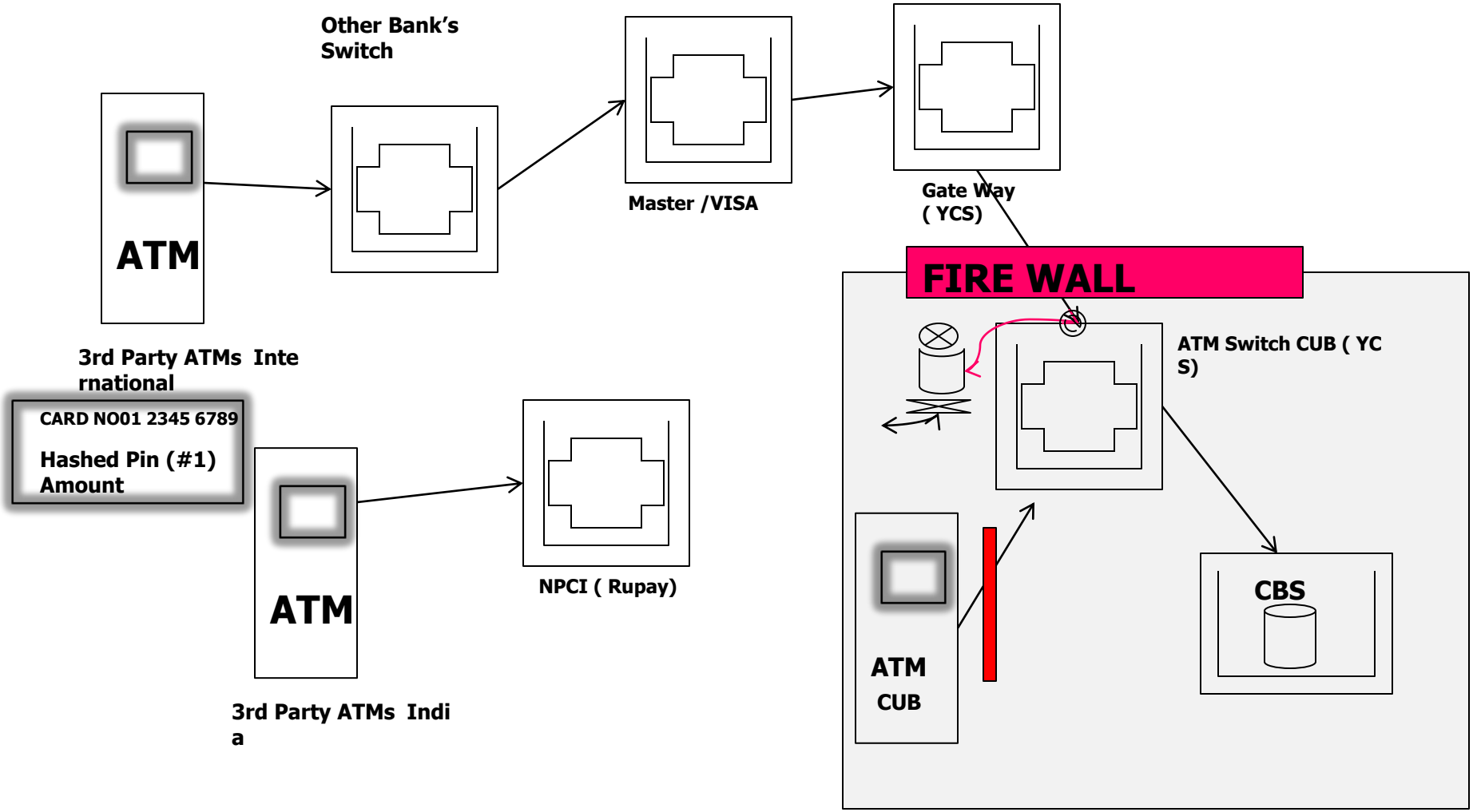
Probable Scenario / Occurrence of Incident



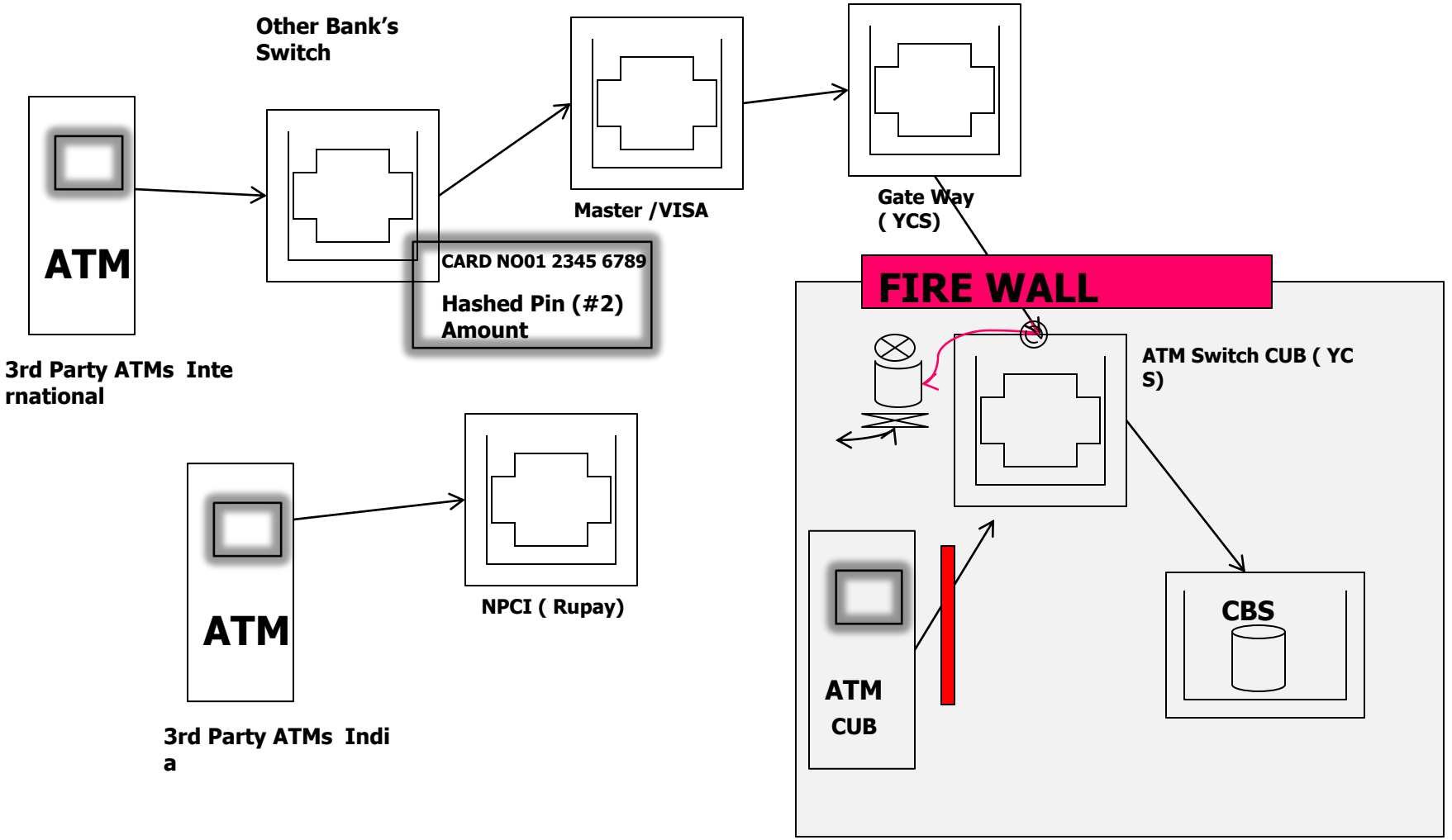
Probable Scenario / Occurrence of Incident



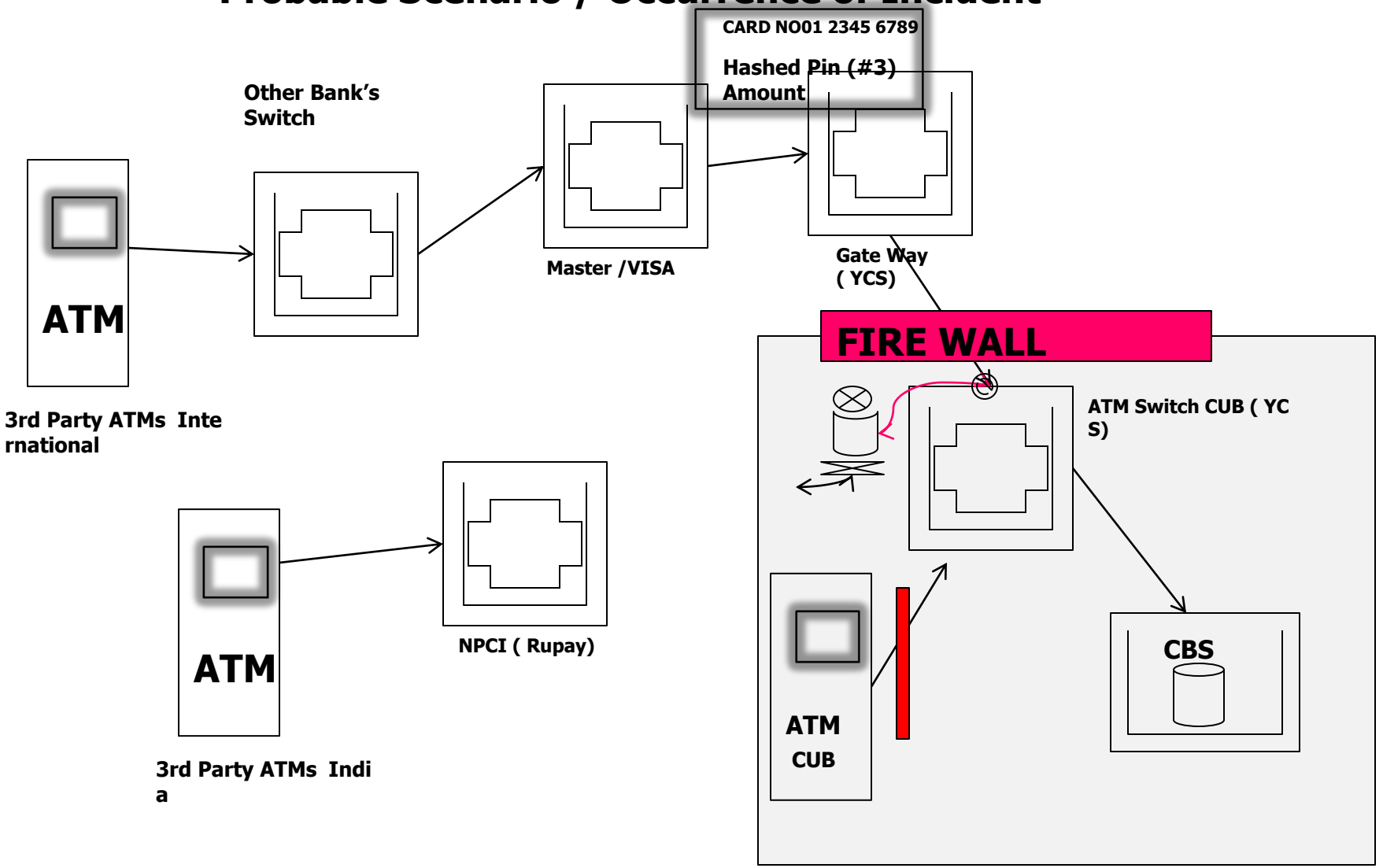
Probable Scenario / Occurrence of Incident



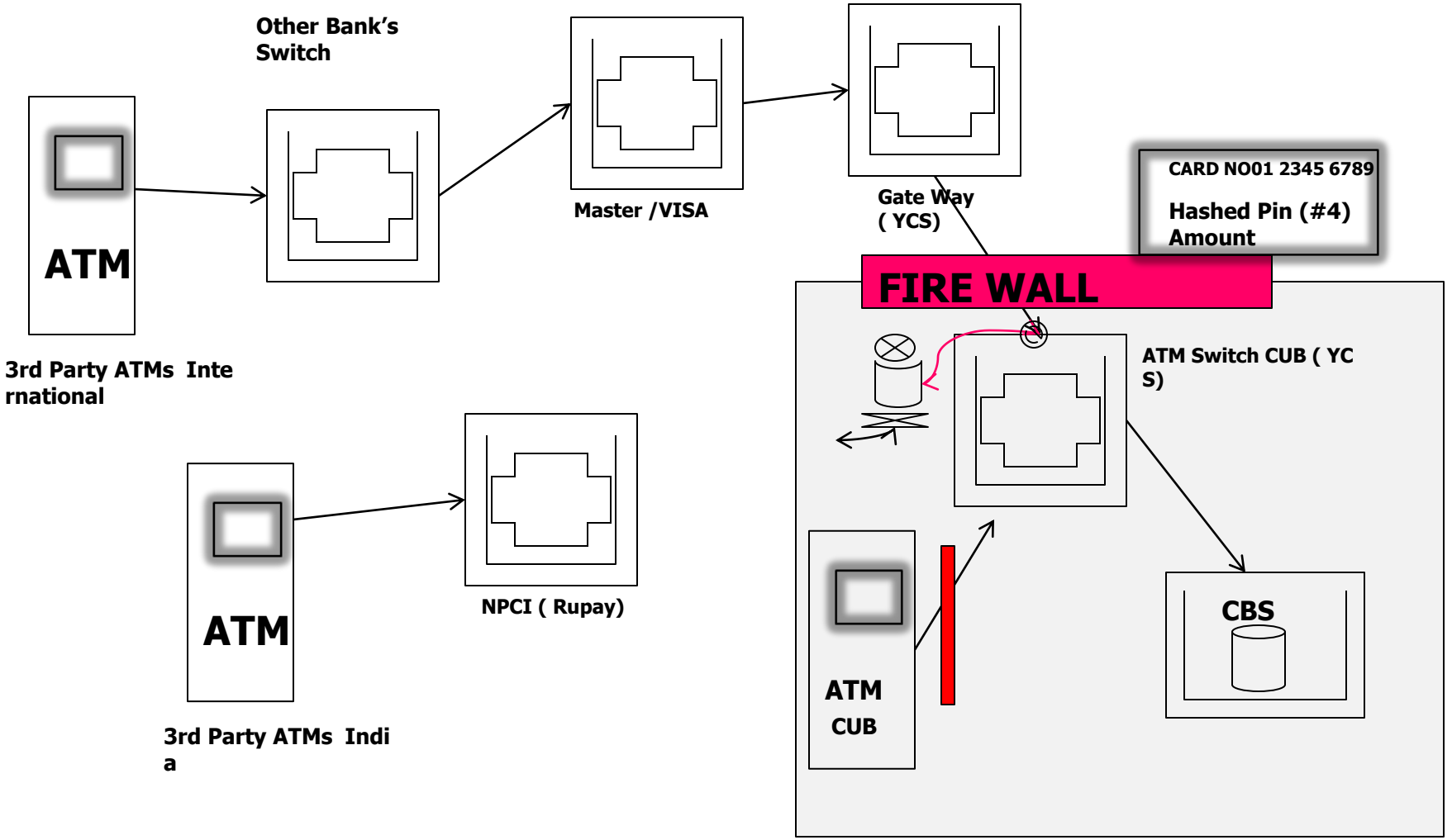
Probable Scenario / Occurrence of Incident



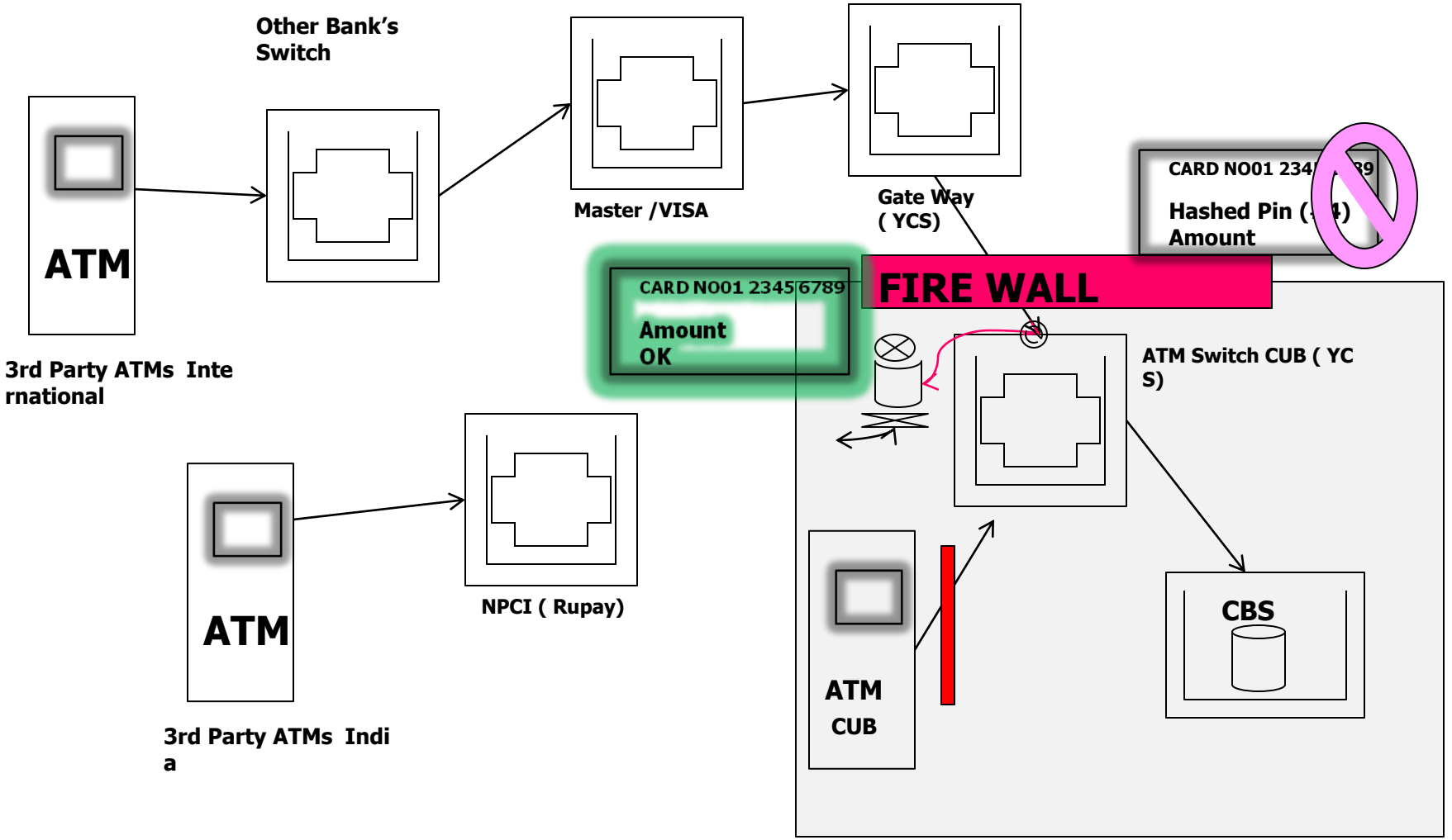
Probable Scenario / Occurrence of Incident



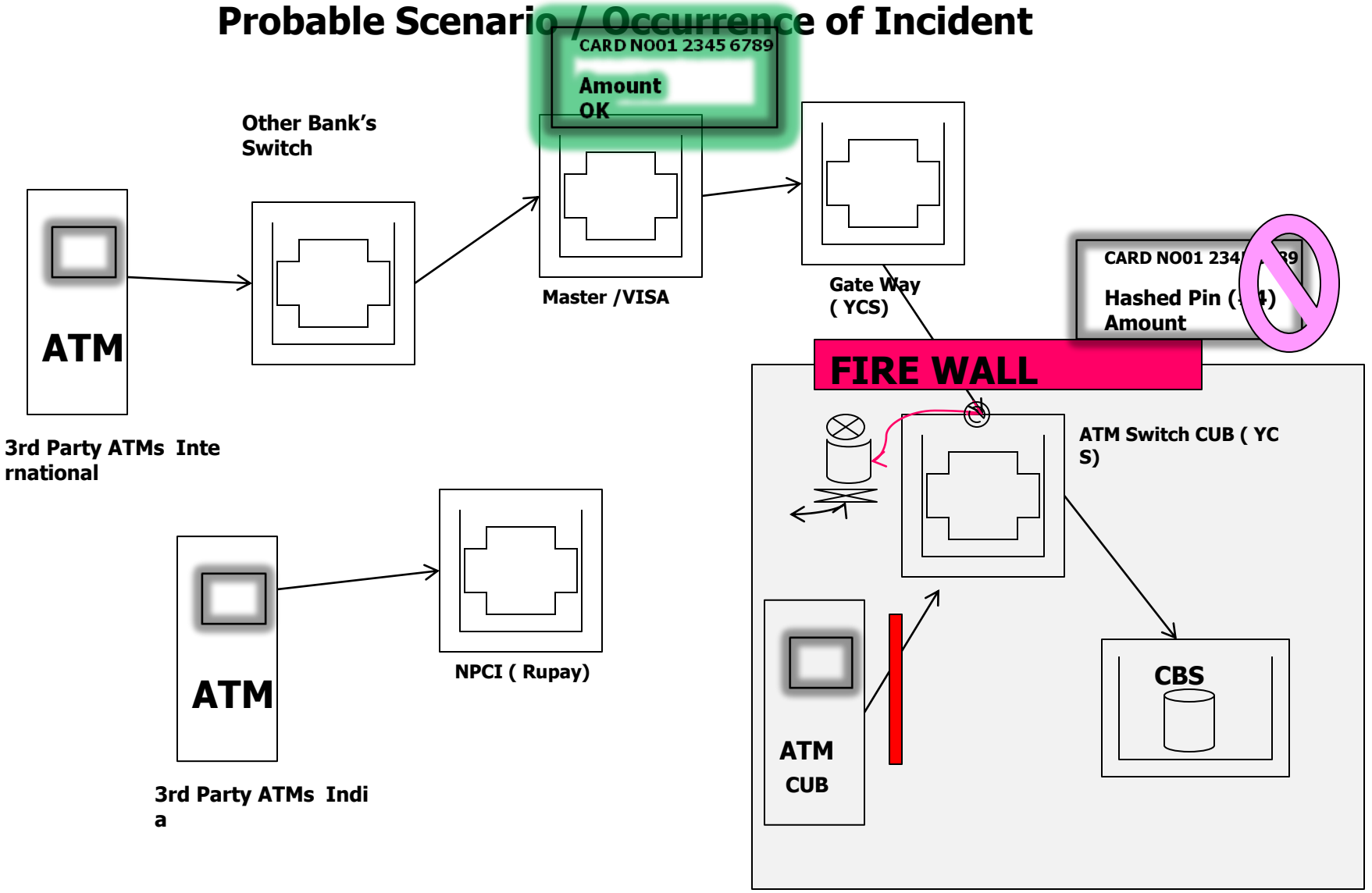
Probable Scenario / Occurrence of Incident



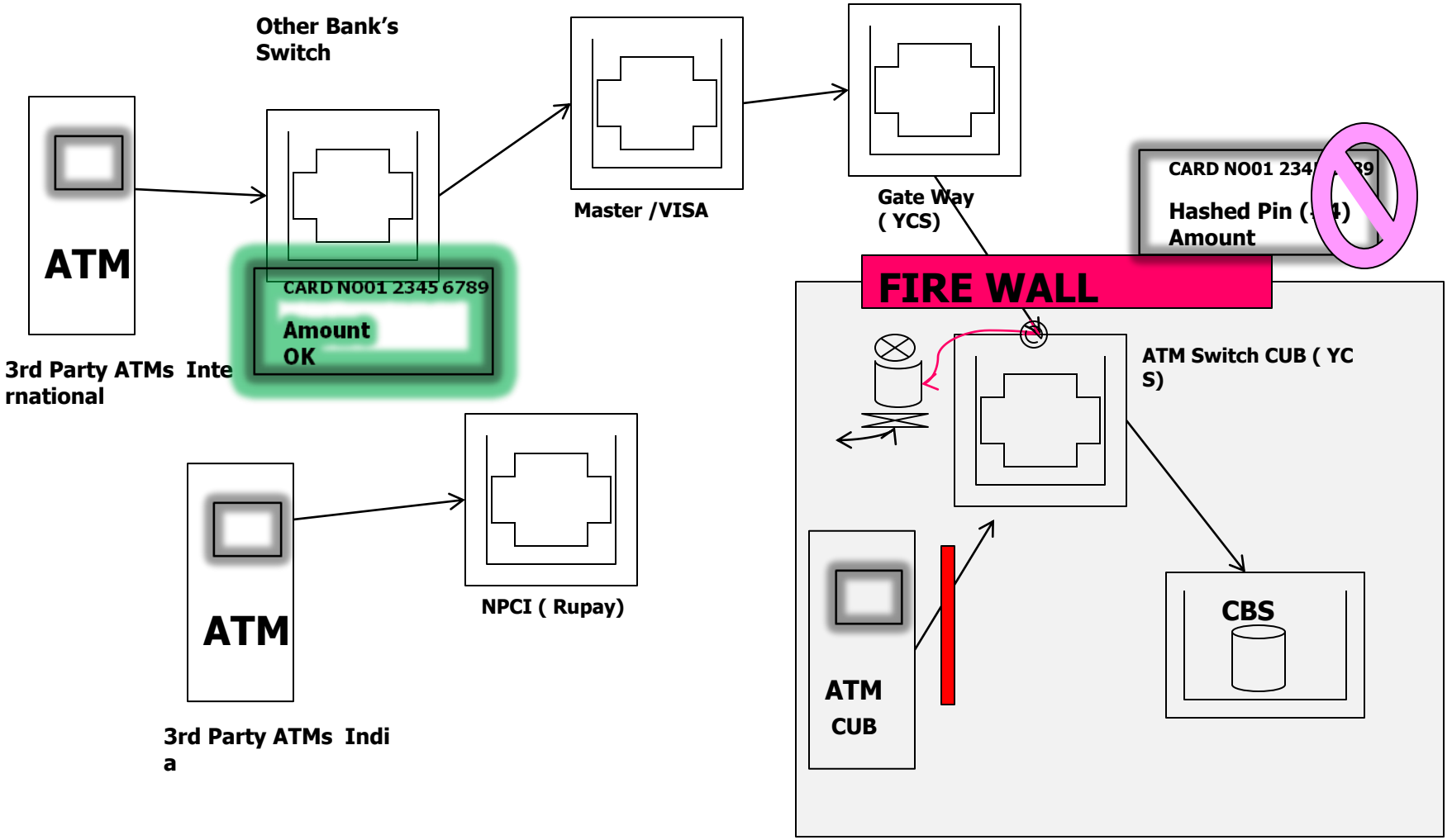
Probable Scenario / Occurrence of Incident



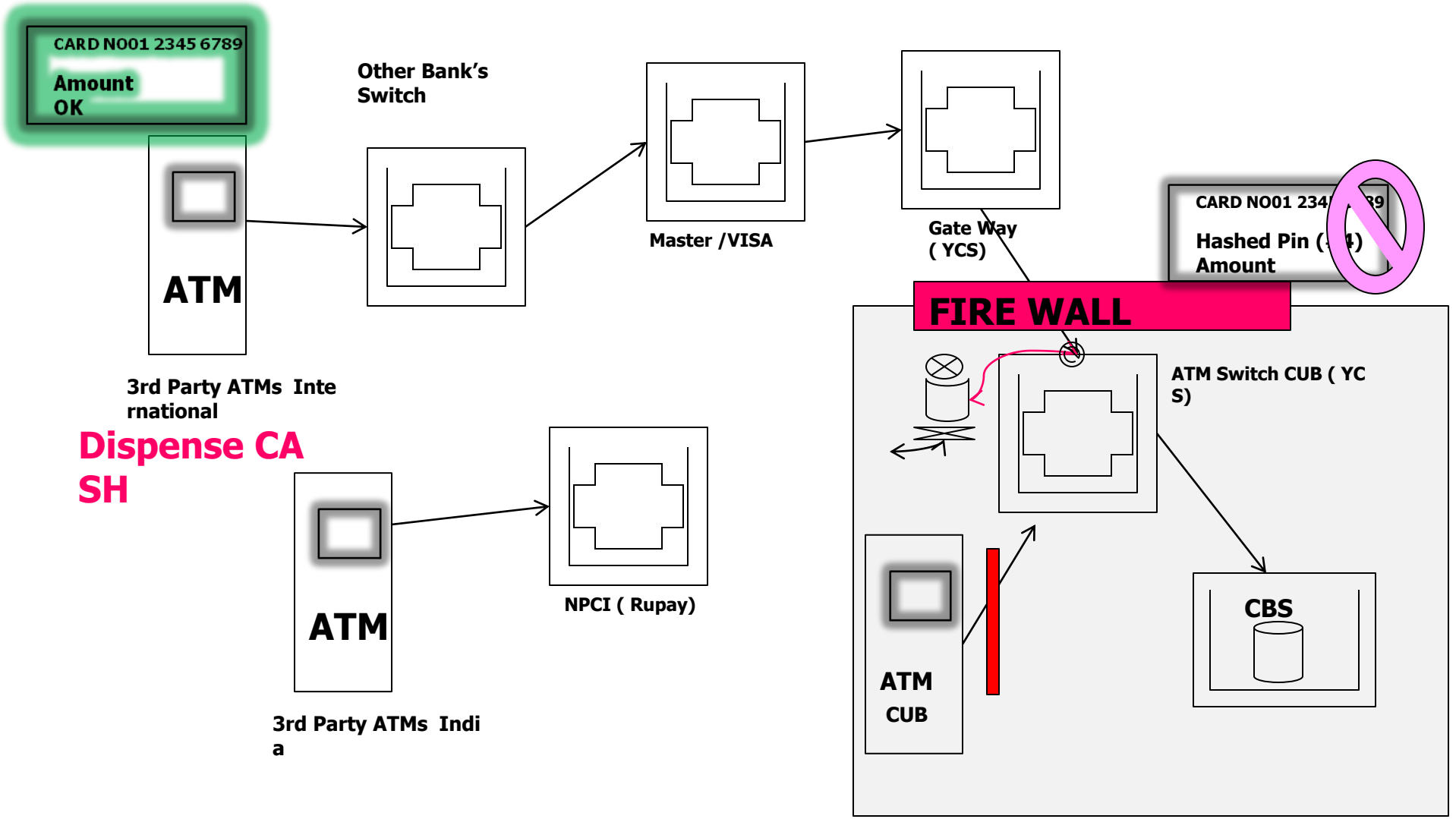
Probable Scenario / Occurrence of Incident



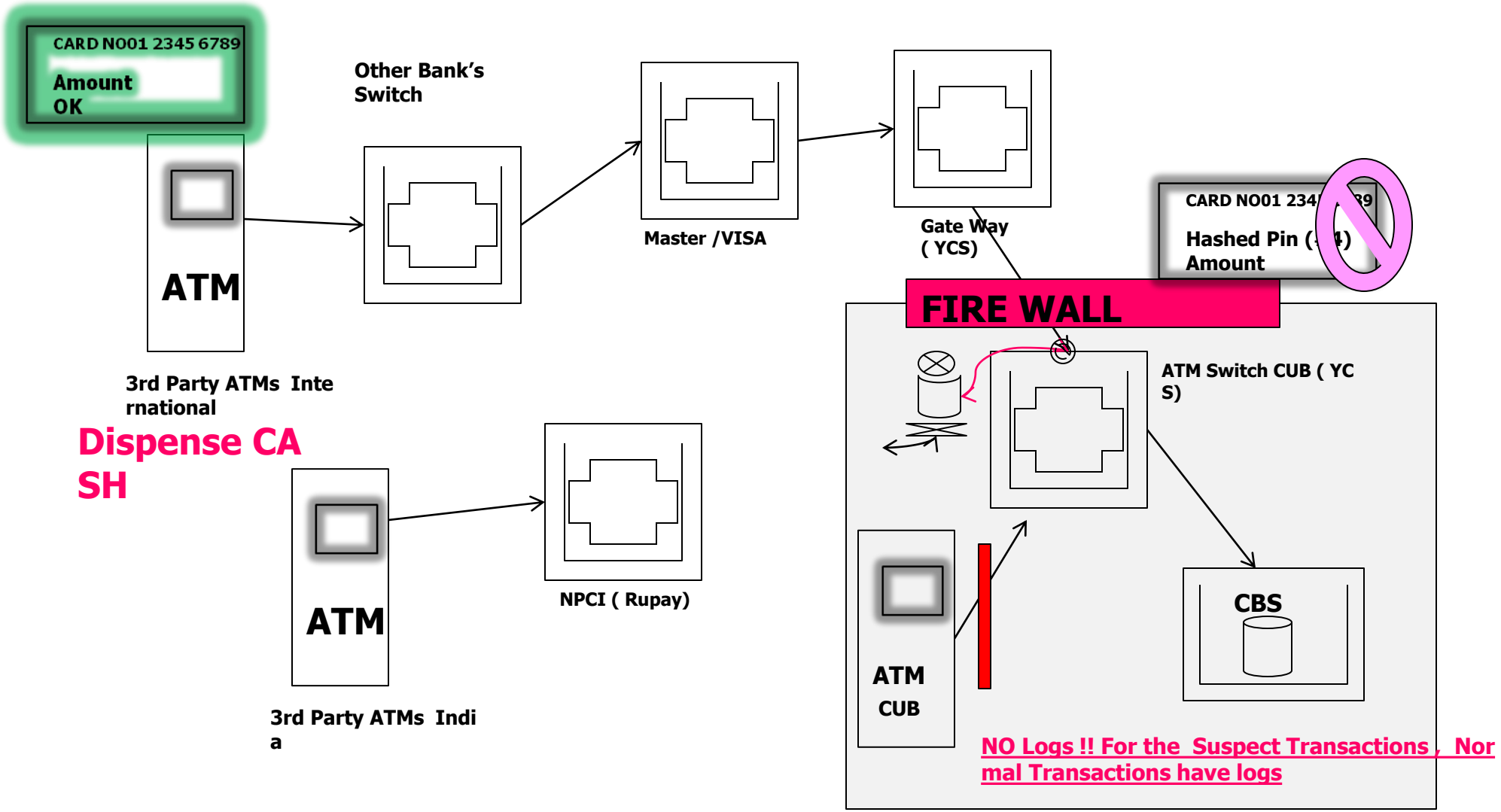
Probable Scenario / Occurrence of Incident



Probable Scenario / Occurrence of Incident



Probable Scenario / Occurrence of Incident



Countries in which transactions have been executed

S.No	Country
1	AUSTRALIA
2	BELARUS
3	BELIZE
4	BULGARIA
5	CANADA
6	CANADIAN - QUEBE
7	CYPRUS
8	CZECH REPUBLIC
9	UNITED STATES
10	DOMINICAN REPUBLIC
11	ESTONIA
12	FRANCE
13	SPAIN
14	UKRAINE
15	UNITED KINGDOM
17	INDIA

S.No	Country
16	GHANA
17	GREECE
18	INDONESIA
19	ISRAEL
20	ITALY
21	LATVIA
22	LITHUANIA
23	MEXICO
24	PHILIPPINES
25	POLAND
26	RUSSIA
27	TURKEY
28	UNITED ARAB EMIRATES

11

boisslockerroom

0 Posts

57 Followers

0 Following

Bois Locker Room 2.0

Let's start this again.

But this time join the group with fake accounts so no one can expose u.

-

/ri’kɑnɪsəns/ - re-con-nais-sance

reconnaissance

(noun) the act of reconnoitring (especially to gain information about an enemy or potential enemy)

Tip: you can create your own flashcards by adding this video to favourite list
Support me by liking / leaving a comment if it helped you

© learn2pronounce.com

WHENEVER YOU GET A FRIEND REQUEST FROM A **BEAUTIFUL GIRL**, DO NOT ACCEPT **HIM**

Privacy Settings and Tools

Your Activity	Who can see your future posts?	Friends	Edit
	Review all your posts and things you're tagged in		Use Activity Log
	Limit the audience for posts you've shared with friends of friends or Public?		Limit Past Posts
How People Find and Contact You	Who can send you friend requests?	Everyone	Edit
	Who can see your friends list?	Public	Edit
	Who can look you up using the email address you provided?	Everyone	Edit
	Who can look you up using the phone number you provided?	Friends	Edit
	Do you want search engines outside of Facebook to link to your profile?	Yes	Edit

Tips for avoiding a Social Engineering Attack

- [x] **LIMIT PUBLIC INFORMATION:**

  Limit the amount of personal information that you share online.

- [x] **BE SKEPTICAL:**

  Always question requests for sensitive information.

- [x] **TRUST BUT VERIFY:**

  Don't share information with people you don't know unless you can verify their identity.

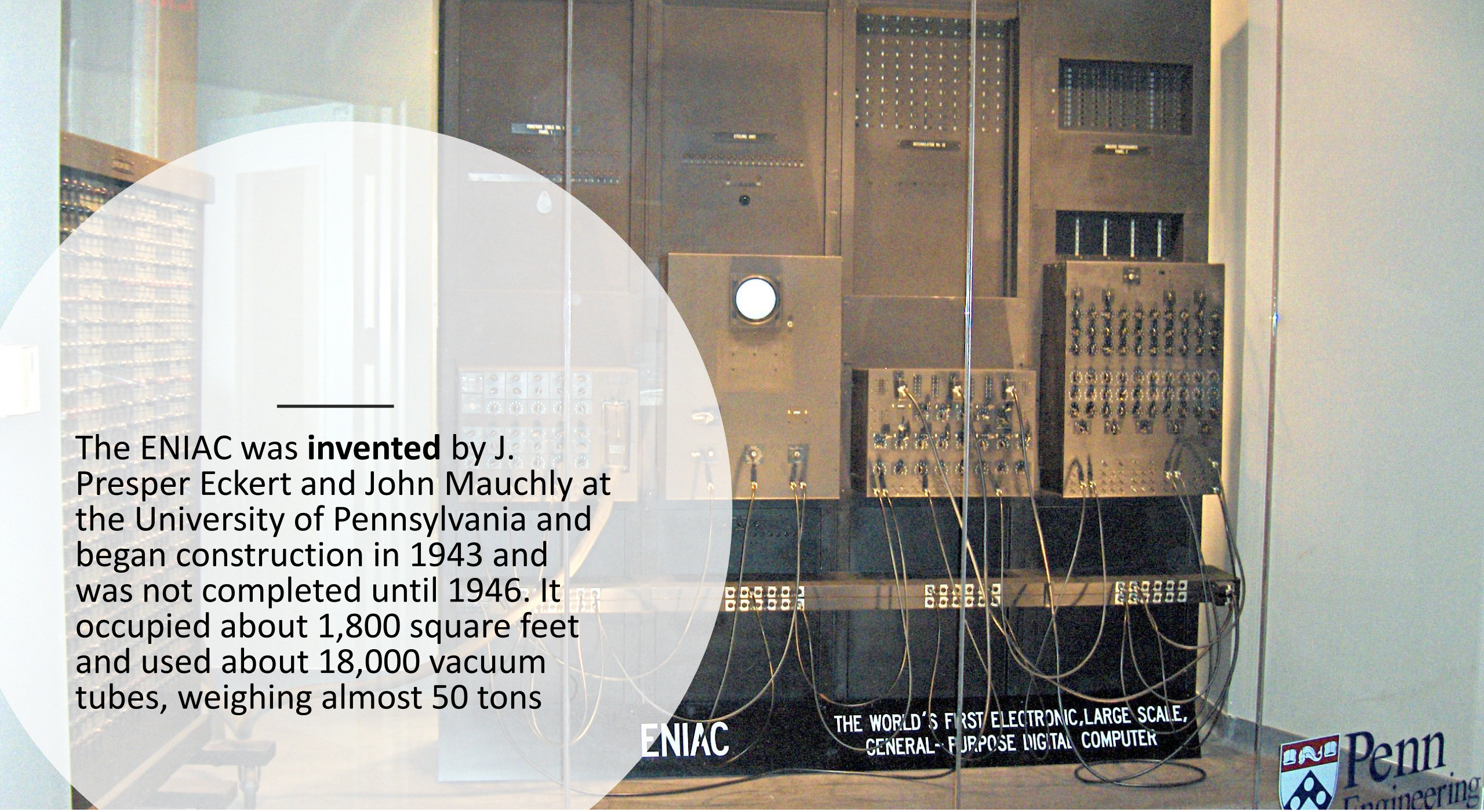
- [x] **CALL THEM BACK:**

  Through the main switchboard if possible.

- [x] **NO PASSWORDS OVER THE PHONE:**

  Never share your password with anyone over the phone.

Which was
the **first** programmable,
electronic, general-
purpose **digital computer** ?



The ENIAC was **invented** by J. Presper Eckert and John Mauchly at the University of Pennsylvania and began construction in 1943 and was not completed until 1946. It occupied about 1,800 square feet and used about 18,000 vacuum tubes, weighing almost 50 tons

Penn Engineering

Facebook
YouTube
Snapchat
Instagram
Pinterest

INTERNET – INSTALL MONITORING & FILTERING PROGRAMS

AntiSocial

Anti Social

Are you curious to find out how much you use your cell phone compared to other people? AntiSocial is designed to not only help you understand what 'normal usage' looks like, but to give you the tools to manage, block and control your cell phone usage so that you can unplug, minimize distractions and focus on the things that matter.

ONWARD

On Ward

We are on a mission to help restore Tech-Life Balance by developing scalable, affordable solutions that give each of us the ability to change our compulsive behaviors free of judgement and stigma.

(OFFTIME)

OFF TIME

(OFFTIME) helps you to focus and to unplug to be creative – thanks to smart app blocking, communications filter and insights into your smartphone usage.

QualityTime

Quality Time

Quality Time is a leading developer of family computing platforms. Cloud-based parental control and time management solutions for phones and tablets in this era of mobile hyper connectivity.

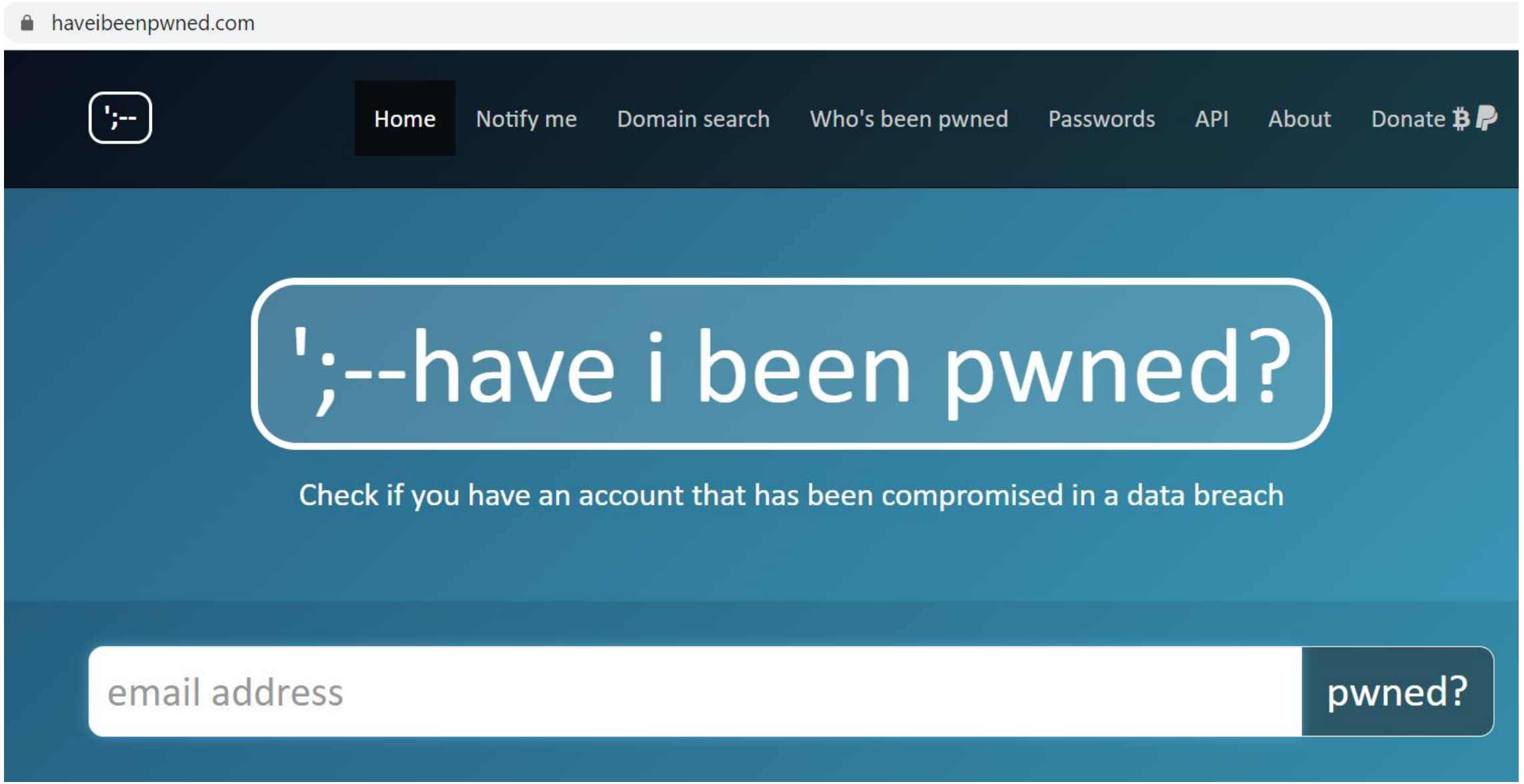
Period Prediction
Period
3 Days Left
Ovulation: 12 days left
Period Start?
100 MILLION
USER'S CHOICE
Accurate Calendar
June
15
Nov 13
High chance of pregnancy
Ovulation Day
Daily Health Notes
March 12
Symptoms
Moods
Drink Water
Cycle History
Average Value
5 Days
27 Days
History

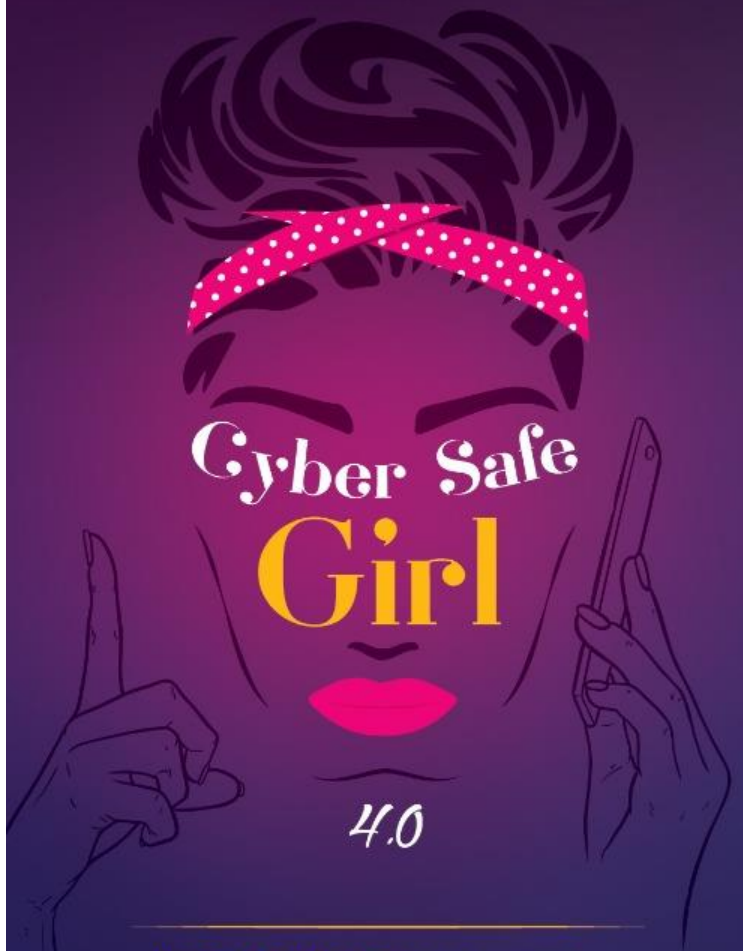
VIRUSTOTAL

Analyze suspicious files and URLs to detect types of malware, automatically share them with the security community

FILE | URL | SEARCH

By submitting data below, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.


haveibeenpwned.com
';--
Home
Notify me
Domain search
Who's been pwned
Passwords
API
About
Donate
';--have i been pwned?
Check if you have an account that has been compromised in a data breach
email address
pwned?



Cyber Safe Girl

4.0

Ananth Prabhu G PhD, Post Doctoral Fellow

Co-Authors : **Adv Prashant Jhala**

Yashavantha Kumar KN DySP

www.cybersafegirl.com

SURE PASS

CYBER PATRIOT

Indian Cyber Institute

Supported by

ISEA

Information Security Education & Awareness

Certificate of Completion

Certificate No : ..... Valid upto : .....

This is to certify that ..... has

successfully completed course on Cyber Safety

and has secured ..... Grade.

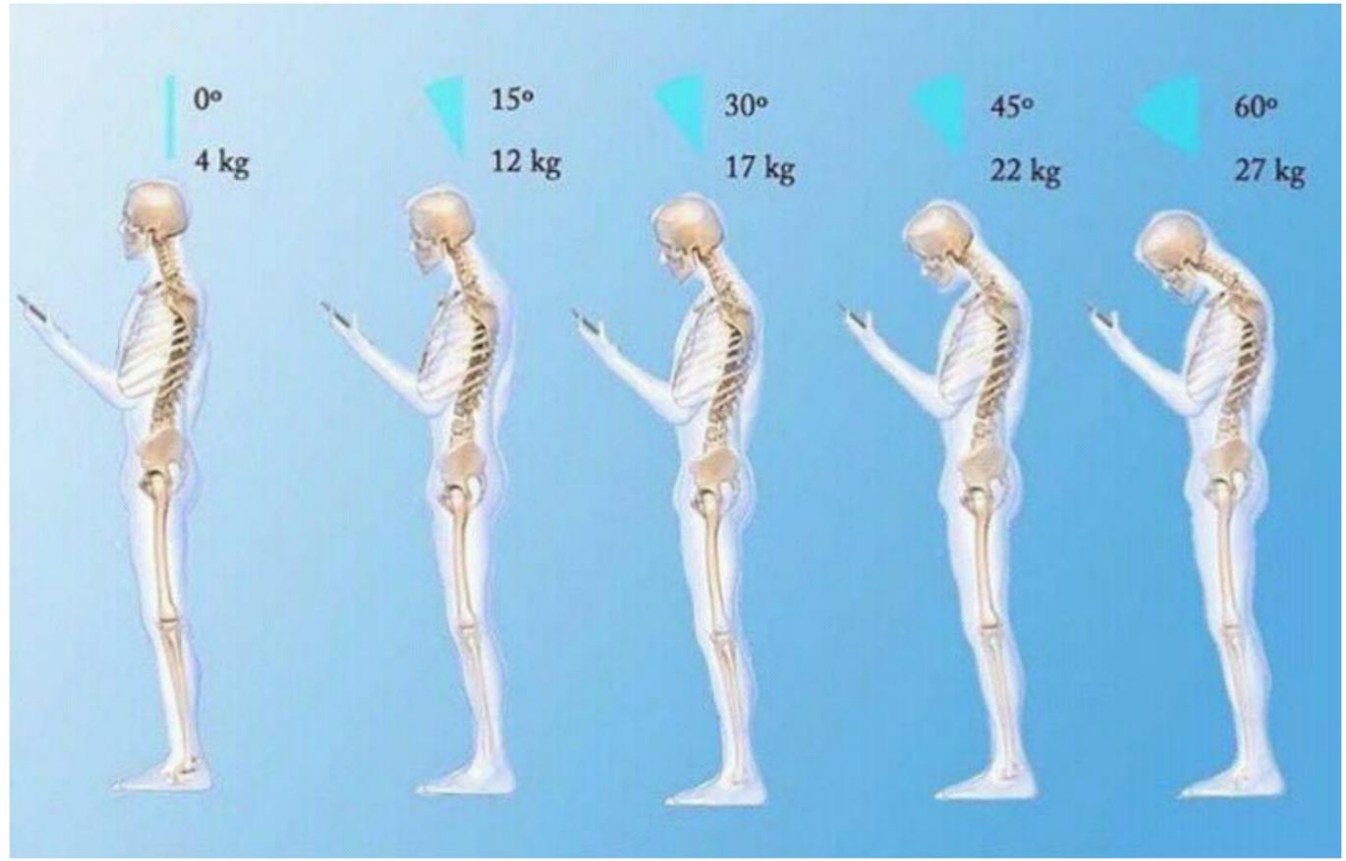
Date : .....

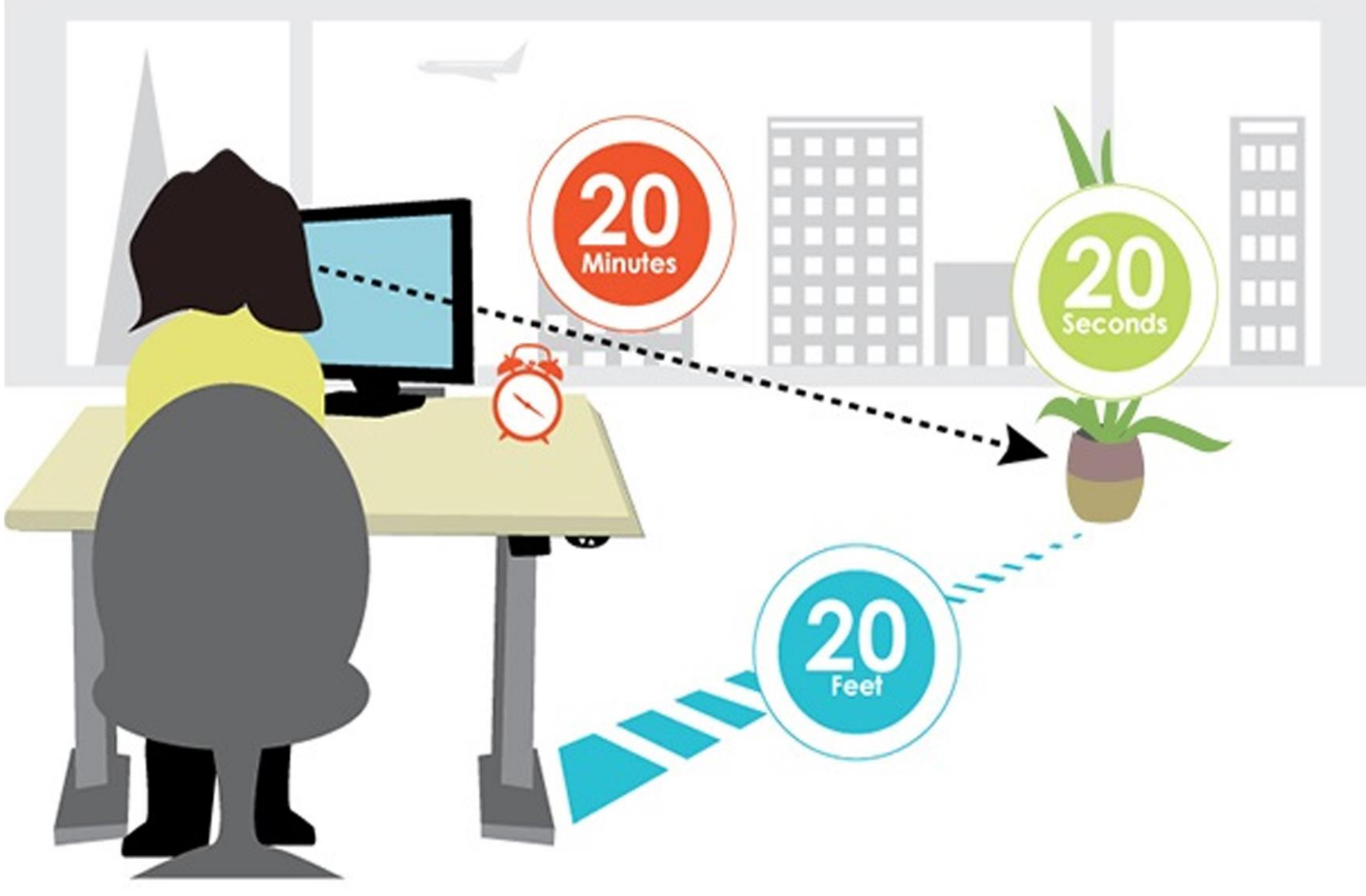
Authorized signatory

(Ananth Prabhu G)

Neck and Neck problem

- Did you know that your head weighs around 04 or 05 kg? All supported by some pretty small bones in your neck! A Quick look at biomechanic of the body shows that when you are slouched over a phone at 45 degree angle.its equivalent to placing 22kg of stress on the neck! This often translates into headache and pain down the back....consider your posture!


0°
4 kg
15°
12 kg
30°
17 kg
45°
22 kg
60°
27 kg


20
Minutes
20
Seconds
20
Feet

© Alamy

ANY
QUESTIONS?

Dr. Ananth Prabhu G

Professor- Sahyadri

Cyber Law Adjunct Faculty- Karnataka Judicial Academy

Cyber Security Trainer- Karnataka Police Academy

Director- SurePass Academy

+91 8951511111

www.fb.com/educatorananth

CYBER PATRIOT