SURE PASS

CYBER PATRIOT

Indian Cyber Institute

CYBER JAGRITHI

Supported by

ISEA

Information Security Education & Awareness

www.cybersafegirl.com

CYBER SAFE GIRL

Beti Bachao Cyber Crime Se... 5.0

50 EYE-OPENING INFOTOONS TO ENSURE ONLINE SAFETY OF NETIZENS

Ananth Prabhu G PhD, Post Doctoral Fellow

Co-Authors : **Adv Prashant Jhala** & **Yashavantha Kumar KN** DySP

Dr Ananth Prabhu G

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

is an Author, Software Engineer, Motivational Speaker and Cyber Security Expert. Currently serving as Professor and Principal Investigator of Digital Forensics and Cyber Security COE at Sahyadri College of Engineering and Management and Director of SurePass Academy. He is also the Cyber Law and Security Trainer at the Karnataka Judicial Academy and Karnataka Police Academy. Dr Prabhu was recognized by India Today magazine as one among the 30 unsung heroes of our country in 2019. Dr. Prabhu is a recipient of the Karnataka District Rajyotsava Award and Aryabhata International Award for the services rendered in the field of Cyber Security and Awareness.

+91 89515 11111
info@ananthprabhu.com
www.facebook.com/educatorananth

Co-Authors

Adv. Prashanth Jhala

He is the Founder of ICL Advocates (www.icladvocates.com) a Law Firm based out in Mumbai and also a Co-Founder of Indian Cyber Institute (indiancyberinstitute.com) which runs educational and training programs in the field of Cyber Crime Investigation, Computer Forensics, Ethical hacking and Information Security, Cyber Law etc. He has been instrumental in training the law enforcement agencies across the country. He is a regular speaker and trainer at various banking forums, the Defence Forces and workshops/events/seminars organised by Information and Technology stake holders.

+91 98691 84691
prashant@icladvocates.com

Yashavantha Kumar K N

He is a Police Officer in Karnataka State, Currently Serving as the Deputy Superintendent of Police in the CID. Mr Kumar has a MTech degree and is passionate in the field of Cyber Security and Forensics. He is an adjunct faculty in many training schools of the Law Enforcement Agencies of our country.

+91 94482 46483
yashvass@gmail.com

50 EYE-OPENING INFOTOONS
TO ENSURE ONLINE SAFETY OF NETIZENS

Title: Cyber Safe Girl

Version: Fifth

Publisher: Dr Ananth Prabhu G

Co-Authors: Adv Prashant Jhala and Yashavantha Kumar KN, DySP

First Published in India in 2018

Designed and printed by
Tarjani Communications Pvt. Ltd, Mangaluru

Credits

Sanjay Sahay
IPS (Rtd)

Ramachandra Rao
IPS

Arun Chakravarthy
IPS

Dr Murugan
IPS

Roopa D
IPS

Dr Vedamurthi
IPS

Ravi Kumar
IPS

Hariram Shankar
IPS

Hamza Hussain
Commandant

M C Kavitha
KSPS

Reena Suvarna
KSPS

Gopalkrishna K
KSP

Special Thanks to

Dr Manjunath Bhandary, MLC

Ch A S Murty
ISEA Team

Dr Varadraj G

Paritosh Vyas

Ravishankar B S

Vivek Shetty

CA Mohan Vishwa

Jagadish R Chandra

Naveen Kumar

Vaikunt Prabhu

Dr Mustafa B
Tech Resource

Rohan Don
Web Architect

Yashwanth A S

Vibha Puthran

Anudeep Karkera
Artist

Do you want to invite

Dr Ananth Prabhu G

to address the students of your school / college or employees of your organisation..?

contact

+91 89515 11111

educatorananth@gmail.com

to follow his regular updates
like the page

www.facebook.com/educatorananth

Topics

- 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
- EXAM MALPRACTICE
- CONNECTED CAR
- DRUG TRAFFICKING
- DOXXING
- CYBER GROOMING
- CRYPTO FRAUDS
- CYBER SEX TRAFFICKING
- CYBERWARFARE
- HACKTIVISM
- METAVERSE

FOREWORD

Cyber space today is the real world. Cyber identities are far more engrossing than real identities. With ever increasing trend of people staying connected in cyber space, of emoting in cyber space, of doing every possible transaction in cyber space, it is all the more important to be aware of vulnerability in cyber space.

In my long-standing stint in Bangalore city as Deputy Commissioner of Police of three law and order zones and subsequently as Commissioner of Police, Mangalore City, I have seen girls falling prey to various kinds of cyber offenses. With the changed landscapes where in majority of human relations also have cyber connect, the ramification of cyber offenses is much larger than loss of money or property, often affecting lives forever.

I am glad that cyber safe girl V 5.0 has made understanding of the vulnerability of girls in cyber space so simpler. The illustrations and infotoons have kept the content live and relevant. I am very sure this book would act as an SOP to follow for majority of the girls of new millennial generation. Let's hope that this book would help girls in becoming smart users of technology.

Warm Regards,

Dr Harsha PS, IPS
IGP and Commissioner
Department of Information and Public Relations
Govt of Karnataka

THE IMPORTANCE OF CYBER SAFETY!

Cyber safety is immeasurably an important set of rules/guidelines ideas to be followed while using the internet. When you use the internet, you are bound to make connections with strangers, unknown servers, etc.

If you are not responsible, you can very easily end up having your identity stolen, credit ruined and your files gone forever, to name a few.

Therefore, it is quintessential to follow the best practices to stay Cyber Safe and browse the internet responsibly.

I am glad that #CyberSafeGirl Version 5.0 has come out very well and it would definitely help millions of girls and netizens. The 50 infotoons are very simple and easy to comprehend. I am sure, it would benefit any one from 9 to 99 years of age!

I also promise to extend my full support for this noble cause.

Warm Regards,

Smt. Rekha Sharma
Chairperson
National Commision for Women, New Delhi

MOBILE RECHARGE SHOP

A Mobile Recharge Shop is a place where scamsters can gain access to your cellphone number because you have provided it to the recharge vendor. They will misuse your number to call or text you, exploit your ignorance or even emotionally manipulate you.

Sections Applicable

IPC Sections (to be applied to the Shop Keeper)

IPC Section 354A - Sexual Harassment and punishment for Sexual Harassment

IPC Section 354C - Voyeurism

IPC Section 383/384 - Extortion (IF ANY DEMAND)

IPC Section 503 - Criminal Intimidation

IPC Section 506 - Punishment for Criminal Intimidation

IPC Section 509 - Word, gesture or act intended to insult modesty of a woman

IT Act:

IT Act Section 66E – Punishment for violation of privacy

Mobile Number Sale to Stalkers by Recharge Shop:

IPC Sections (to be applied to the Shop Keeper)

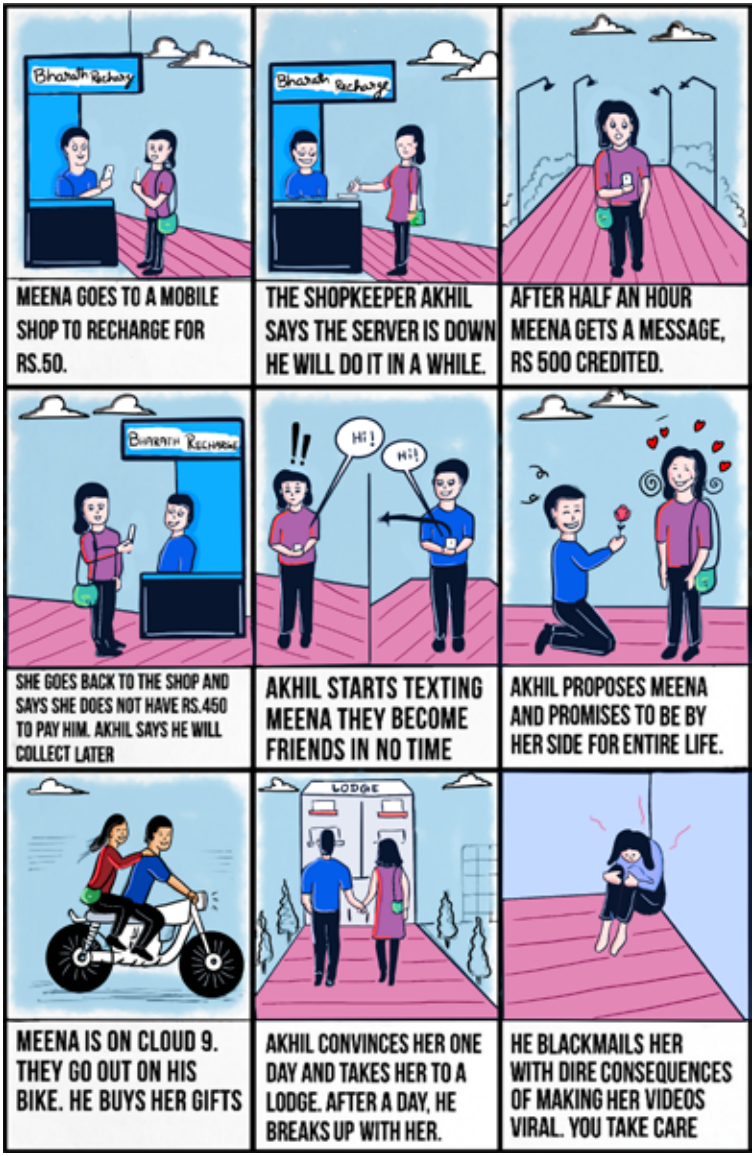
IPC Section 109 – Punishment for abetment

IPC Section 114 – Abettor present when offence is committed

IPC Section 120B – Punishment for Criminal Conspiracy

IPC Section 406 – Punishment for Criminal Breach of Trust

Everything comes for a Charge and in case of Recharge, there's no Free Charge!


Bharath Recharge
MEENA GOES TO A MOBILE SHOP TO RECHARGE FOR RS.50.
Bharath Recharge
THE SHOPKEEPER AKHIL SAYS THE SERVER IS DOWN HE WILL DO IT IN A WHILE.
AFTER HALF AN HOUR MEENA GETS A MESSAGE, RS 500 CREDITED.
Bharath Recharge
SHE GOES BACK TO THE SHOP AND SAYS SHE DOES NOT HAVE RS.450 TO PAY HIM. AKHIL SAYS HE WILL COLLECT LATER
!!
Hi!
Hi!
AKHIL STARTS TEXTING MEENA THEY BECOME FRIENDS IN NO TIME
AKHIL PROPOSES MEENA AND PROMISES TO BE BY HER SIDE FOR ENTIRE LIFE.
MEENA IS ON CLOUD 9. THEY GO OUT ON HIS BIKE. HE BUYS HER GIFTS
LODGE
AKHIL CONVINCES HER ONE DAY AND TAKES HER TO A LODGE. AFTER A DAY, HE BREAKS UP WITH HER.
HE BLACKMAILS HER WITH DIRE CONSEQUENCES OF MAKING HER VIDEOS VIRAL. YOU TAKE CARE

DEBIT CARD CLONING

Debit Card skimming happens when the PIN is revealed to another person. A scamster who knows the PIN and has possession of the card even for a short while can replicate the card with a skimming /schimming device and withdraw cash.

Sections Applicable

IT Act for cloning

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 computer resource

Money Transaction followed by cloning:

IPC Section 419 – Punishment for cheating by personation

IPC Section 420 – Cheating

IT Act

IT Act Section 66D – Punishment for cheating by personation by using computer resource

Cloning may blow up your Earnings!


MEENA AND REENA ARE FRIENDS STUDYING IN THE SAME COLLEGE.
MEENA'S BOYFRIEND ARJUN IS A DRUG ADDICT. HE ALWAYS ASKS HER FOR MONEY.
MEENA HOPED THAT ONE DAY ARJUN WOULD CHANGE. BUT HE CONTINUED TO BORROW MONEY BY THREATENING HER WITH A BREAKUP.
MEENA ASKS REENA FOR RS.500. REENA WITH UTMOST FAITH GIVES HER ATM CARD AND PIN.
MEENA COMES BACK AFTER FIFTEEN MINS. REENA GETS A RS. 500 DEBIT MESSAGE ON HER PHONE
A WEEK LATER, REENA GETS A DEBIT MESSAGE FOR RS.500. REENA IS IN SHOCK
ON THE DAY MEENA HAD BORROWED ATM CARD, ARJUN WAS WAITING OUTSIDE. HE TOOK THE ATM CARD
WITH A SKIMMING DEVICE HE REPLICATED THE CARD AND AFTER A WEEK WITHDREW MONEY FROM ATM AS HE HAD THE PIN
NEVER EVER GIVE YOUR ATM AND PIN TO ANYONE, NO MATTER HOW CLOSE THEY ARE TO YOU.

KEYLOGGER

It is a malicious program that may be installed on the victim's computer for recording computer user keystrokes to steal passwords and other sensitive information. With Keylogger a scamster will be able to collect login details and other matter saved in the computer and have them mailed to a designated email address.

Sections Applicable

Key logger installation: IT Act Section 66
- Computer Related Offences
Stealing personal information: IT Act Section 66C
- Punishment for Identity Theft

Creating fake profile & posting private conversation : IT Act
IT Act Section 66C **-** Punishment for Identity Theft
IT Act Section 66D **-** Punishment for cheating by personation by using computer resources
IT Act Section 67 **-** Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A **-** Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B **-** Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

IPC Sections:
IPC Section 354A **-** Sexual Harassment and punishment for Sexual **Harassment**
If in hard copy, IPC Sections 292, 293 & 294

Keylogger may empty your Coffer!


ANUSHA AND POOJA ARE BEST FRIENDS AND SHARE THE SAME ROOM IN THEIR PG. THEY WORK FOR THE SAME MNC
INCIDENTLY, BOTH OF THEM END UP HAVING A BIG TIME CRUSH ON THEIR BOSS VIVEK
WITHOUT WASTING ANY TIME, POOJA PROPOSES VIVEK AND HE ACCEPTS. THEY START DATING EACH OTHER.
ANUSHA IS HEART BROKEN. SHE WANTS TO TEACH POOJA A LESSON THAT SHE WOULD REMEMBER FOR LIFE.
ANUSHA INSTALLS KEYLOGGER SPYWARE ON POOJAS LAPTOP, TO SNOOP ON HER ACTIVITIES.
POOJA IS UNAWARE THAT HER PASSWORDS, PHOTOS SHARED, PRIVATE CHATS, EMAILS AND BROWSING HISTORY IS NOW AVAILABLE TO ANUSHA.
ANUSHA EMAILS THE PRIVATE CONVO TO POOJA'S PARENTS AND UPLOADS THEIR PRIVATE PHOTOS ON SOCIAL MEDIA VIA FAKE PROFILE.
VIVEK IS SHOCKED. THEY BREAK UP AND POOJA IS NOW ALL SHATTERED.
POOJA REGRETS FOR NOT LOCKING HER PC WITH A PASSWORD AND INSTALLING AN ANTI VIRUS PROGRAM WHICH WOULD HAVE PROTECTED HER.

SMS SPOOFING

Spoofing is being able to send a message by hiding or changing or using a completely different sender ID. Typically, when you send an SMS, your handheld device sends the message with your phone number as the originator where in you as the sender cannot alter that number.

Sections Applicable

Act of hoax or trick or deceive a communication
IPC Section
IPC Section 465 – Making a false document(FORGERY)
IPC Section 419 – Punishment for cheating by personation

IT Act
IT Act Section 66D – Punishment for cheating by personation by using computer resource

SMS are Spoofed by Cyber Crooks!


AISHWARIYA IS A SHOPOHOLIC. SHE WAS A PRIVILEGED MEMBER ON MANY ECOMMERCE SITES.
EVERYTIME SHE WOULD WAIT FOR THE RIGHT OFFERS AND MAKE PURCHASES. ALSO, WOULD REDEEM COUPON CODES.
ONE DAY SHE GETS AN EMAIL FROM WALLMART CONGRATULATING HER FOR WINNING A HANDBAG WORTH RS 5000 FOR ONLY RS 500
SHE ALSO GETS A TEXT FROM WALMART STATING, SHE COULD AVAIL THE OFFER TWO TIMES, PROVIDED SHE PAYS ONLINE AND NOT COD.
BANK
AISHWARYA RUSHES TO THE BANK AND DEPOSITS RS 1000 AND MAKES THE ONLINE TRANSACTION.
EVEN AFTER A MONTH, THE PRODUCTS ARE NOT DELIVERED. SHE CALLS THE HELPLINE TO FIND OUT.
SHE REALIZES THAT, THE LINK SHE HAD CLICKED WAS A FAKE URL AND IT WAS A CLEAR CASE OF PHISHING AND MESSAGE SPOOFING
DISCOUNT 90%
SHE REALIZED THAT, WHENEVER THE OFFERS ARE UNBELIEVABLE WITH MASSIVE DISCOUNTS, TO BE ALERT AND CROSS VERIFY
DANGER NIGERIAN -SCAM-
MANY NIGERIAN SCAM MESSAGES HAVE FLOODED THE INTERNET WHERE PEOPLE FALL PREY. YOU TAKE CARE.

CALL SPOOFING

Call spoofing happens through apps that enable a person with criminal intent to change his number and voice to impersonate another to defraud.

Sections Applicable

Act of hoax or trick or deceive a communication

IPC Section

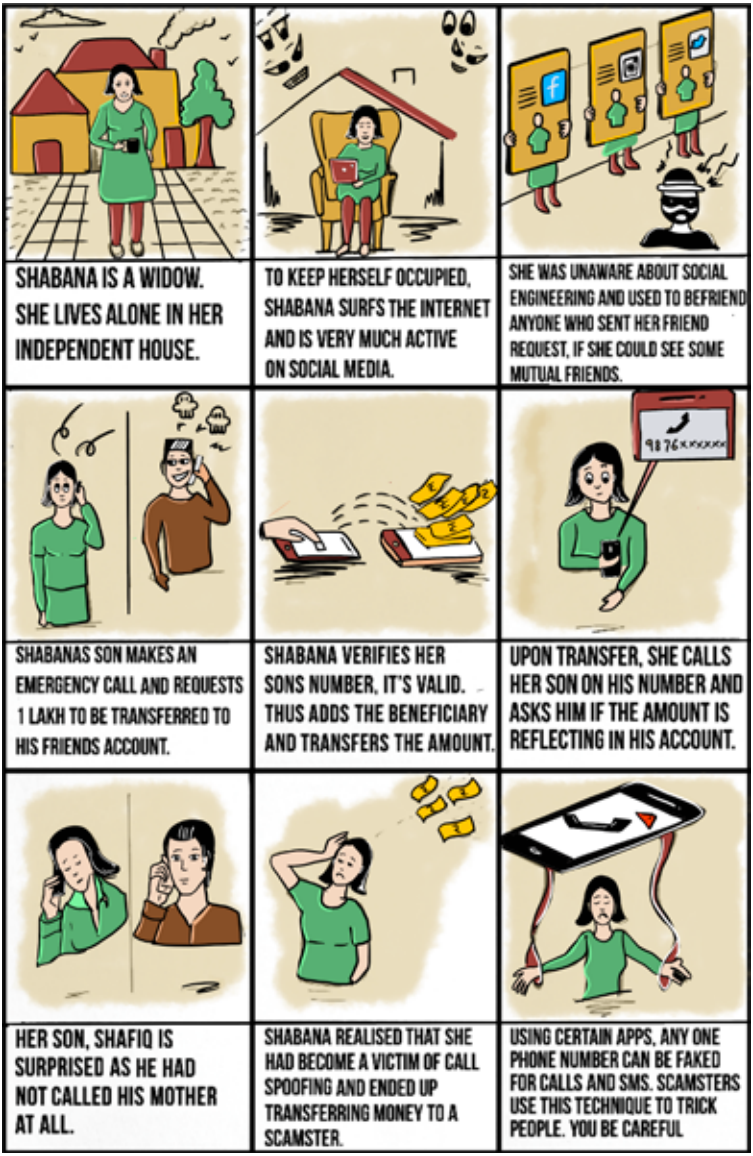
IPC Section 465 – Making a false document(FORGERY)

IPC Section 419 – Punishment for cheating by personation

IT Act

IT Act Section 66D – Punishment for cheating by personation by using computer resource

Call Spoofing is always with criminal intent!


SHABANA IS A WIDOW. SHE LIVES ALONE IN HER INDEPENDENT HOUSE.
TO KEEP HERSELF OCCUPIED, SHABANA SURFS THE INTERNET AND IS VERY MUCH ACTIVE ON SOCIAL MEDIA.
SHE WAS UNAWARE ABOUT SOCIAL ENGINEERING AND USED TO BEFRIEND ANYONE WHO SENT HER FRIEND REQUEST, IF SHE COULD SEE SOME MUTUAL FRIENDS.
SHABANAS SON MAKES AN EMERGENCY CALL AND REQUESTS 1 LAKH TO BE TRANSFERRED TO HIS FRIENDS ACCOUNT.
SHABANA VERIFIES HER SONS NUMBER, IT'S VALID. THUS ADDS THE BENEFICIARY AND TRANSFERS THE AMOUNT.
9876xxxxxx
UPON TRANSFER, SHE CALLS HER SON ON HIS NUMBER AND ASKS HIM IF THE AMOUNT IS REFLECTING IN HIS ACCOUNT.
HER SON, SHAFIQ IS SURPRISED AS HE HAD NOT CALLED HIS MOTHER AT ALL.
SHABANA REALISED THAT SHE HAD BECOME A VICTIM OF CALL SPOOFING AND ENDED UP TRANSFERRING MONEY TO A SCAMSTER.
USING CERTAIN APPS, ANY ONE PHONE NUMBER CAN BE FAKED FOR CALLS AND SMS. SCAMSTERS USE THIS TECHNIQUE TO TRICK PEOPLE. YOU BE CAREFUL

RANSOMWARE

Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data. Users are shown instructions as to how to pay a fee to get the decryption key. The costs can range from a few hundred rupees to thousands, payable to cybercriminals in bitcoin.

Sections Applicable

Unauthorised access, Denial, Encryption :

IT Act Section 66 – Computer related offences

Demand without payment :

IPC Section 384 – Extortion

IPC Section 511 – Punishment for attempting to commit offence punishable with imprisonment for life or other imprisonment

Demand & payment :

IPC Section 384 – Extortion.

Sensitize your Hardware and Software to avoid Ransomware!


ALISHA IS AN ENTREPRENEUR. HER COMPANY HAS 50 EMPLOYEES AND 60 SYSTEMS.
ONE DAY, SHE RECEIVES AN EMAIL FROM HER VENDOR HAVING AN ATTACHMENT.
ALISHA DOWNLOADS THE ATTACHMENT. HER ANTIVIRUS WAS NOT UPDATED, SO NO ALERTS.
UPON OPENING THE FILE, HER SYSTEM GETS LOCKED AND ALL FILES ARE ENCRYPTED. UNABLE TO ACCESS.
AN ALERT MESSAGE ON SCREEN DEMANDS RS. 1 LAKH TO BE PAID IN BITCOIN TO UNLOCK THE SCREEN.
ALISHA MAKES THE PAYMENT TO THE BITCOIN WALLET ADDRESS MENTIONED
THE HACKER DOES NOT SEND THE PRIVATE KEY. THE FILES REMAIN ENCRYPTED AND INACCESSIBLE.
HER MANAGER QUIPS THAT THE EMAIL SHE RECEIVED WAS A PHISHING EMAIL WITH RANSOMEWARE
ALISHA REGRETS FOR NOT DELETING THE EMAIL AND OPERATING HER SYSTEM BY NOT UPDATING HER ANTIVIRUS SOFTWARE. UPDATE ANTIVIRUS S/W ALWAYS

CYBER STALKING

Cyberstalking is the use of the Internet or other electronic means to stalk or harass another by misusing information uploaded on social networking sites.

Sections Applicable

Offline :
IPC Section 354 D – Stalking

Online :
IPC Section 354 D – Stalking

Cyber Stalking means some is keeping an eye on you remotely remotely!


JUVERIYA IS AN NRI, COMPLETED HER SCHOOLING FROM THE US AND IS NOW IN INDIA TO PURSUE HER ENGINEERING. SHE LIVES LIFE TO THE FULLEST
fb
Insta
Snapchat
WHATEVER SHE DOES, SHE WOULD UPLOAD ON SOCIAL MEDIA. OH YES! SHE HAD 10K PLUS FOLLOWERS.
SHE USED THE CHECK-IN FEATURE TO UPDATE HER WHERE ABOUTS. HER LIFE HAD MINIMUM PRIVACY
check in
ONE DAY SHE DECIDES TO GO TO GOA ON SOLO TRIP. SHE UPDATES HER PLANS ON HER WALL WITH ITINERARY.
KIRAN, A STALKER USED TO KEEP TRACK OF ALL HER DETAILS. HE WAS A HABITUAL OFFENDER AND WAS OUT ON BAIL RECENTLY.
HE TAKES A BUS TO GOA AND TEXTS JUVERIYA FROM HIS HOTEL ROOM AND EXPRESSES HIS DESIRE TO MEET HER.
AFTER CHECKING OUT HIS PROFILE, JUVERIYA BLOCKS HIM, UNAWARE ABOUT WHAT FATE HAD PLANNED FOR HER SHORTLY.
AS KIRAN HAD HER ITINERARY, HE FOLLOWS HER TO THE BEACH AND MOLESTS HER WHEN THERE WAS NO ONE AROUND, KIRAN ESCAPES.
JUVERIYA IS FEELING TERRIBLE AND REGRETS FOR UPLOADS, UPDATES AND POSTS ON SOCIAL MEDIA. YOU TAKE CARE.

PICTURE MORPHING

Morphing the face of a person to the body of another and publishing it to blackmail or otherwise intimidate the person is one of the ways by which people who upload photos on social networking sites can be exploited.

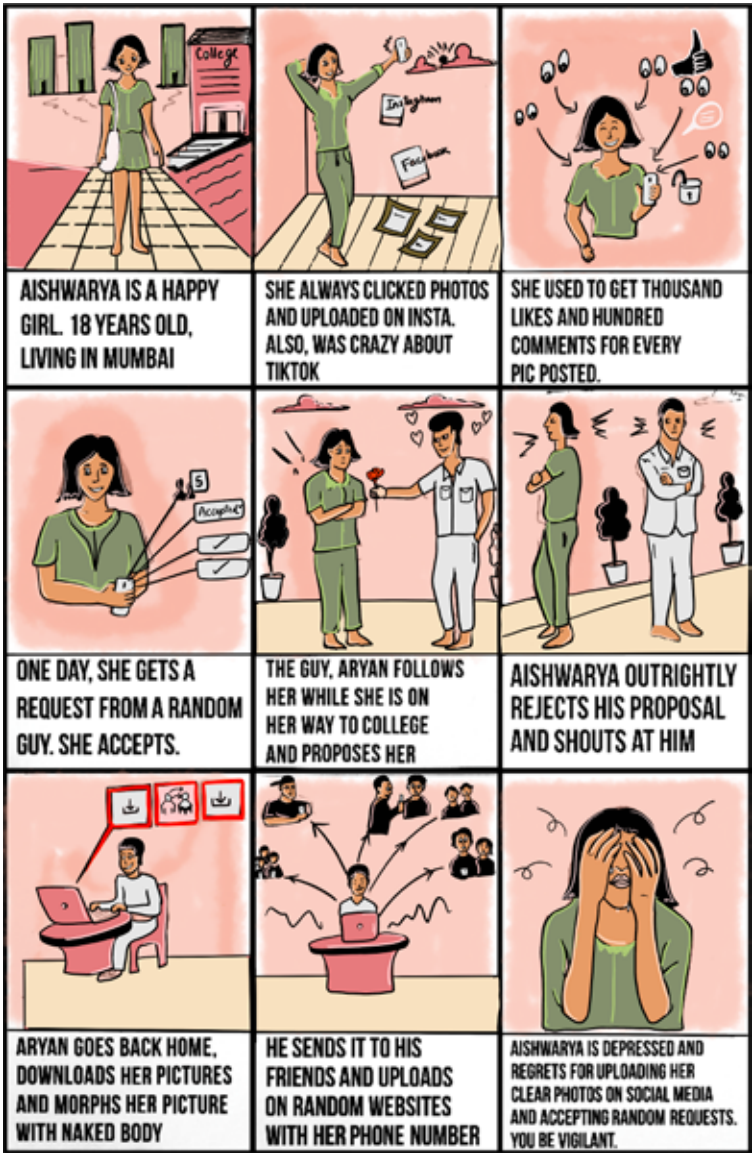
Sections Applicable

IPC Sections
IPC Section 292 – Sale etc of Obscene books etc (if in hardcopy)
IPC Section 465 – Morphing photographs and creating a false electronic record
IPC Section 469 – Making false electronic document for causing defamation
IPC Section 507 – Criminal Intimidation by an Anonymous communication
IPC Section 509 – Word, guesture or act intended to insult modestyof a woman

IT Act
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

For publishing photos containing indecent representation of women:
Section 4 R/W Section 6 of Indecent Representation of Women's Act, 1986

Morphing is used for Defaming!


College
AISHWARYA IS A HAPPY GIRL. 18 YEARS OLD, LIVING IN MUMBAI
SHE ALWAYS CLICKED PHOTOS AND UPLOADED ON INSTA. ALSO, WAS CRAZY ABOUT TIKTOK
SHE USED TO GET THOUSAND LIKES AND HUNDRED COMMENTS FOR EVERY PIC POSTED.
5
Accepted
ONE DAY, SHE GETS A REQUEST FROM A RANDOM GUY. SHE ACCEPTS.
THE GUY, ARYAN FOLLOWS HER WHILE SHE IS ON HER WAY TO COLLEGE AND PROPOSES HER
AISHWARYA OUTRIGHTLY REJECTS HIS PROPOSAL AND SHOUTS AT HIM
ARYAN GOES BACK HOME, DOWNLOADS HER PICTURES AND MORPHS HER PICTURE WITH NAKED BODY
HE SENDS IT TO HIS FRIENDS AND UPLOADS ON RANDOM WEBSITES WITH HER PHONE NUMBER
AISHWARYA IS DEPRESSED AND REGRETS FOR UPLOADING HER CLEAR PHOTOS ON SOCIAL MEDIA AND ACCEPTING RANDOM REQUESTS. YOU BE VIGILANT.

PROFILE HACKING

Profile Hacking happens when your email or social networking profile is accessed by a probable stalker who then compromises it.

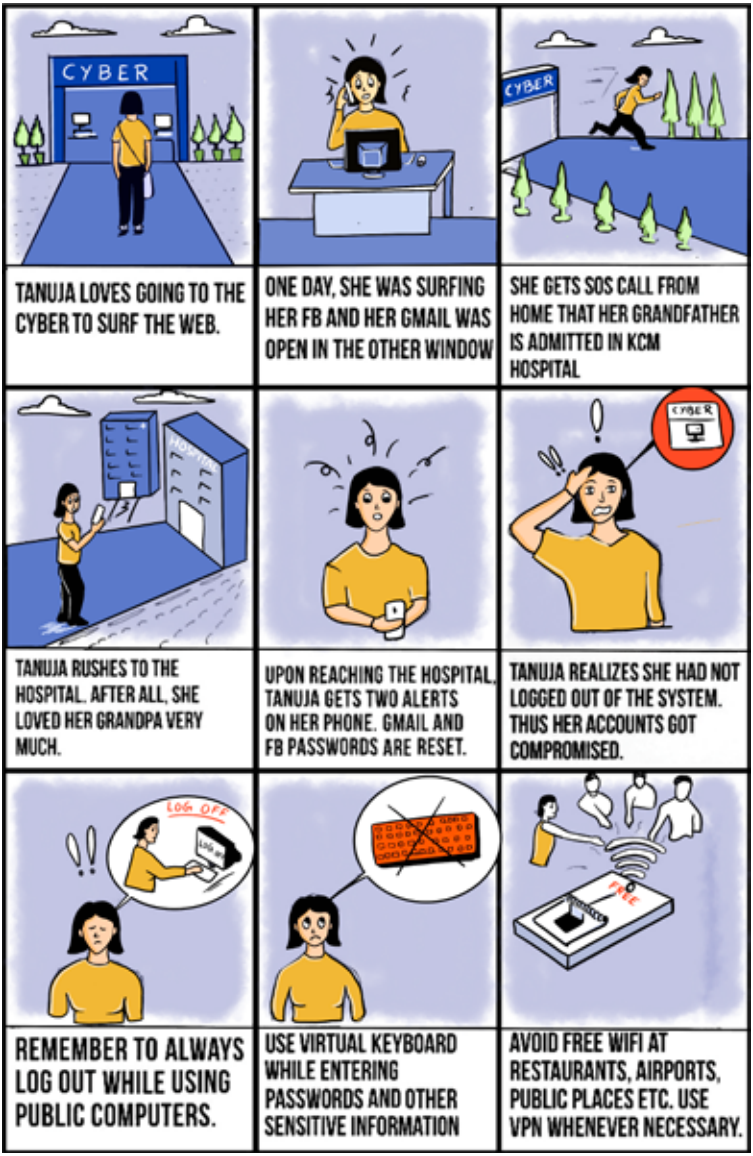
Sections Applicable

IT Act

IT Act Section 66 – Computer related offences

IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using password)

Profile Hacking means Security is Lacking!


CYBER
TANUJA LOVES GOING TO THE CYBER TO SURF THE WEB.
ONE DAY, SHE WAS SURFING HER FB AND HER GMAIL WAS OPEN IN THE OTHER WINDOW
CYBER
SHE GETS SOS CALL FROM HOME THAT HER GRANDFATHER IS ADMITTED IN KCM HOSPITAL
HOSPITAL
TANUJA RUSHES TO THE HOSPITAL. AFTER ALL, SHE LOVED HER GRANDPA VERY MUCH.
UPON REACHING THE HOSPITAL, TANUJA GETS TWO ALERTS ON HER PHONE. GMAIL AND FB PASSWORDS ARE RESET.
CYBER
TANUJA REALIZES SHE HAD NOT LOGGED OUT OF THE SYSTEM. THUS HER ACCOUNTS GOT COMPROMISED.
LOG OFF
REMEMBER TO ALWAYS LOG OUT WHILE USING PUBLIC COMPUTERS.
USE VIRTUAL KEYBOARD WHILE ENTERING PASSWORDS AND OTHER SENSITIVE INFORMATION
FREE
AVOID FREE WIFI AT RESTAURANTS, AIRPORTS, PUBLIC PLACES ETC. USE VPN WHENEVER NECESSARY.

ONLINE GAMES

Girls who are vulnerable to loneliness, low self-esteem and clinical depression can fall prey to dangerous online games that may become addictive and further harm them. some dangerous online games like the blue whale challenge even end in the victim ending her life. This is a personal as well as social challenge for the others around.

Sections Applicable

IPC Sections
The site

IPC Section 299 – Culpable homicide
IPC Section 305 – Abetment of suicide of Child or Insane Person
IPC Section 306 – Abetment of suicide
IPC Section 321 – Voluntarily causing hurt
IPC Section 335 – Voluntarily causing grievous hurt on provocation
IPC Section 336 – Act endangering life or personal safety of others

Before it becomes a game changer of your child's Future, keep track what they do on their personal Computers (laptops, iPads, mobile phones, tabs, desktop etc).


DEVIKA IS A FIRST YEAR ENGINEERING STUDENT, HAILING FROM A REMOTE VILLAGE IN KARNATAKA.
FRIENDS
HER CLASSMATES USED TO IGNORE HER BECAUSE SHE WAS TOO SIMPLE TO GEL AMONG THE GROUP OF GIRLS. SHE HAD NO ONLINE FRIENDS EITHER.
GAME
BECAUSE OF LONELINESS, SHE ENDED UP CLICKING A LINK THAT SHE RECEIVED IN HER EMAIL, WHICH READ- THE BLUE WHALE GAME. ARE YOU READY?
DEVIKA WAS EXCITED TO PLAY THIS GAME. IT HAD FIFTY LEVELS. EACH LEVEL HAD A TASK TO BE EXECUTED.
COMPLETING EACH TASK GAVE HER A BROWNIE POINT. SHE FELT GOOD. THE DOPAMINE RUSH GOT HER ADDICTED TO IT.
DANGEROUS TASKS LIKE TATTOOING ON BODY WITH KNIFE,GRAVEYARD WALKS WERE ASSIGNED.
NO ONE BOTHERED INSPITE OF SEEING CHANGES IN HER.
TASK
FINAL TASK WAS TO COMMIT SUICIDE BY HANGING. SHE WROTE AN APOLOGY TO HER PARENTS AND HANGED.
THE LETTER READ- I WISH PEOPLE LOVED ME. I WAS IGNORED. WHAT'S THE POINT IN LIVING.

JOB CALL LETTER

Websites offering jobs need to be checked for veracity and authenticity. Mails need to be double-checked and verified before one responds and acts on instructions provided, especially if one is asked to put in a personal appearance.

Sections Applicable

Fake account / ID:
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

Impersonation for cheating:
IT Act Section 66D – Punishment for cheating by personation by using computer resource
IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating
IPC Section 465 – Making a false document (DEFINITION SECTION)
IPC Section 468 – Forgery for cheating
IPC Section 471 – Using forged document as genuine
IPC Section 474 – Procession of forged document
IPC Section 120-B – Punishment for Criminal Conspiracy
IPC Section 34 – Acts done by several persons in furtherance of Common Intention

Abatement for offence
a. On the spot : IPC Section 114 – Abettor present when offence is committed
b. Remotely: IPC Section 109 – Punishment for abetment

Such fake call letters may see you out of your existing job sooner or later!


NISHITA COMPLETED HER ENGINEERING WITH FIRST CLASS. BUT SHE WAS NOT ABLE TO SECURE CAMPUS PLACEMENT
SHE USED TO ALWAYS UPLOAD HER RESUME ON NAUKRI.COM AND OTHER JOB CLASSIFIED WEBSITES, HOPING TO GET A GOOD JOB
ONE DAY SHE RECEIVES A CALL LETTER FROM A REPUTED COMPANY. THE PAY PACKAGE READ 7 FIGURES.
HOTEL
THE INTERVIEW WAS SCHEDULED AT A 5STAR HOTEL IN THE CITY. NISHITA TOOK AN AUTO AND REACHED THE HOTEL.
INTERVIEW
SHE WAS DIRECTED TO A SUITE ROOM, WHERE SHE SAW MANY JOB ASPIRANTS DOING THEIR LAST MINUTE PREPARATIONS
IT WAS NISHITAS TURN. BEFORE THE INTERVIEW BEGAN, SHE WAS OFFERED A DRINK BY THE BUTLER. SHORTLY, SHE FELT DIZZY.
NISHITA DOES NOT REMEMBER ANYTHING THAT HAPPENED AFTER SHE DRANK. SHE WAS ON BED WITHOUT CLOTHES. SHE WAS EXPLOITED.
FAKE
SHE LATER REALIZED THAT, IT WAS A PHISHING MAIL WHICH SHE RECEIVED. SHE DID NOT VERIFY THE DETAILS.
LIKE NISHITA, IN THE PRETEXT OF GETTING JOBS, LAKHS OF WOMEN GET EXPLOITED AND MANY GET ROBBED OF MONEY.
YOU TAKE CARE.

DEEPFAKES

Deepfake is a technique that is used to combine and superimpose new images and videos onto source images or videos. It is used to create videos where the voice or face of another is superimposed on the original in such a way that the viewer or listener cannot distinguish or doubt the veracity of it.

Sections Applicable

Fake account / ID: IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)
Impersonation for cheating :
IT Act Section 66D – Punishment for cheating by personation by using computer resource
IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating
Publishing online:
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO
IPC Section 354A – Sexual Harassment and punishment for Sexual Harassment
IPC Section 465 – Making a false document
Section 507 – Criminal Intimidation by an Anonymous communication
SEC 509 – Insulting modesty of women
Stalking: : IPC Section 354 D – Stalking Offline
: IPC Section 354 D – Stalking Online
IPC Section 120-B – Punishment for Criminal Conspiracy
IPC Section 34 – Acts done by several persons in furtherance of Common Intention
Abatement for offence:
a. On the spot: IPC Section114 – Abettor present when offence is committed
b. Remotely: IPC Section109 – Punishment for abetment

Deep Fakes are not noticeable easily and hence have High Stakes!


JANET IS A FINAL YEAR MBBS STUDENT. SHE AND JOHN ARE IN A RELATIONSHIP SINCE 3 YEARS.
SHE WAS A REGULAR CONTENT CREATOR ON TIKTOK AND INSTAGRAM. USED TO UPLOAD AT LEAST TWO POSTS A DAY.
JANET HAD A FIGHT WITH JOHN AND BROKE UP. HER SENIOR ARJUN GETS TO KNOW.
ARJUN TAKES THE OPPORTUNITY AND PROPOSES TO JANET. SHE AGREES. BUT LATER REGRETS FOR DUMPING JOHN.
WITHIN A WEEK, SHE BREAKS UP WITH ARJUN AND GETS BACK TO JOHN AFTER SEEKING FORGIVENESS.
INFURIATED ARJUN WANTS TO TEACH JANET A LESSON FOR PLAYING WITH HIS FEELINGS.
WITH INSTAGRAM PHOTOS AND TIKTOK VIDEOS AS INPUT, ARJUN CREATES DEEPFAKES USING ARTIFICIAL INTELLIGENCE AND OTHER TOOLS
THE DEEPFAKES VIDEO CREATED SHOWED JANET INDULGING IN ADULTERY WITH MULTIPLE PARTNERS. IT WAS MADE VIRAL ON SOCIAL MEDIA.
MOST OF THEM WHO RECEIVED THE VIDEO BELIEVED IT. JANET IS NOW TERRIFIED, FOR UPLOADING CLEAR PHOTOS AND VIDEOS ON SOCIALMEDIA.

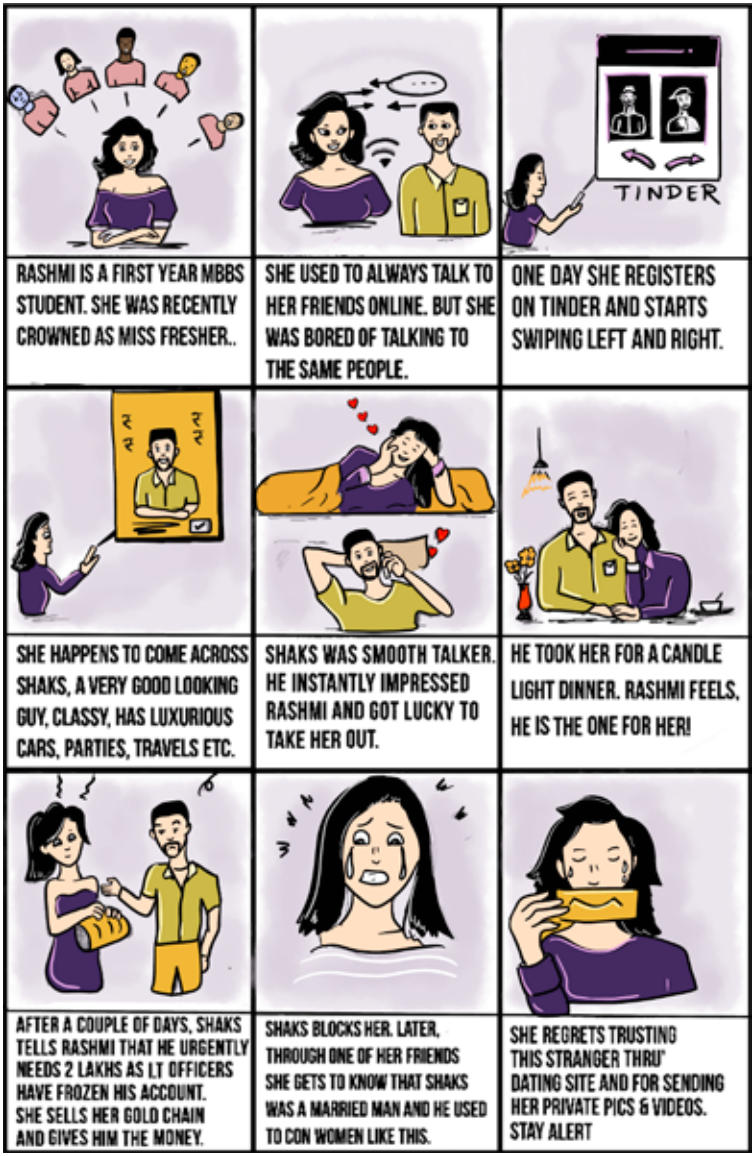
DATING WEBSITE

Females can be emotionally manipulated by smooth talkers on dating sites. Any private pictures or texts that they send across to probable dating companions on such sites are fair game for unscrupulous persons who can then blackmail them.

Sections Applicable

IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)
IT Act Section 66D – Punishment for cheating by personation by using computer resource
IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating
IPC Section 354A – Sexual Harassment and punishment for Sexual Harassment
IPC Section 354C – Voyeurism
Stalking : Offline : IPC Section 354 D – Stalking
Online : IPC Section 354 D – Stalking
Publishing online
IT Act Section 67– Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A– Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B– Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO
IPC Section 507 – Criminal Intimidation by an Anonymous communication
IPC Section 509 – Word, gesture or act intended to insult modesty of a woman
IPC Section 465 – Making a false document

Looking out for a Date, be careful that you don't get Check-Mate!


TINDER
RASHMI IS A FIRST YEAR MBBS STUDENT. SHE WAS RECENTLY CROWNED AS MISS FRESHER..
SHE USED TO ALWAYS TALK TO HER FRIENDS ONLINE. BUT SHE WAS BORED OF TALKING TO THE SAME PEOPLE.
ONE DAY SHE REGISTERS ON TINDER AND STARTS SWIPING LEFT AND RIGHT.
SHE HAPPENS TO COME ACROSS SHAKS, A VERY GOOD LOOKING GUY, CLASSY, HAS LUXURIOUS CARS, PARTIES, TRAVELS ETC.
SHAKS WAS SMOOTH TALKER. HE INSTANTLY IMPRESSED RASHMI AND GOT LUCKY TO TAKE HER OUT.
HE TOOK HER FOR A CANDLE LIGHT DINNER. RASHMI FEELS, HE IS THE ONE FOR HER!
AFTER A COUPLE OF DAYS, SHAKS TELLS RASHMI THAT HE URGENTLY NEEDS 2 LAKHS AS IT OFFICERS HAVE FROZEN HIS ACCOUNT. SHE SELLS HER GOLD CHAIN AND GIVES HIM THE MONEY.
SHAKS BLOCKS HER. LATER, THROUGH ONE OF HER FRIENDS SHE GETS TO KNOW THAT SHAKS WAS A MARRIED MAN AND HE USED TO CON WOMEN LIKE THIS.
SHE REGRETS TRUSTING THIS STRANGER THRU' DATING SITE AND FOR SENDING HER PRIVATE PICS & VIDEOS. STAY ALERT

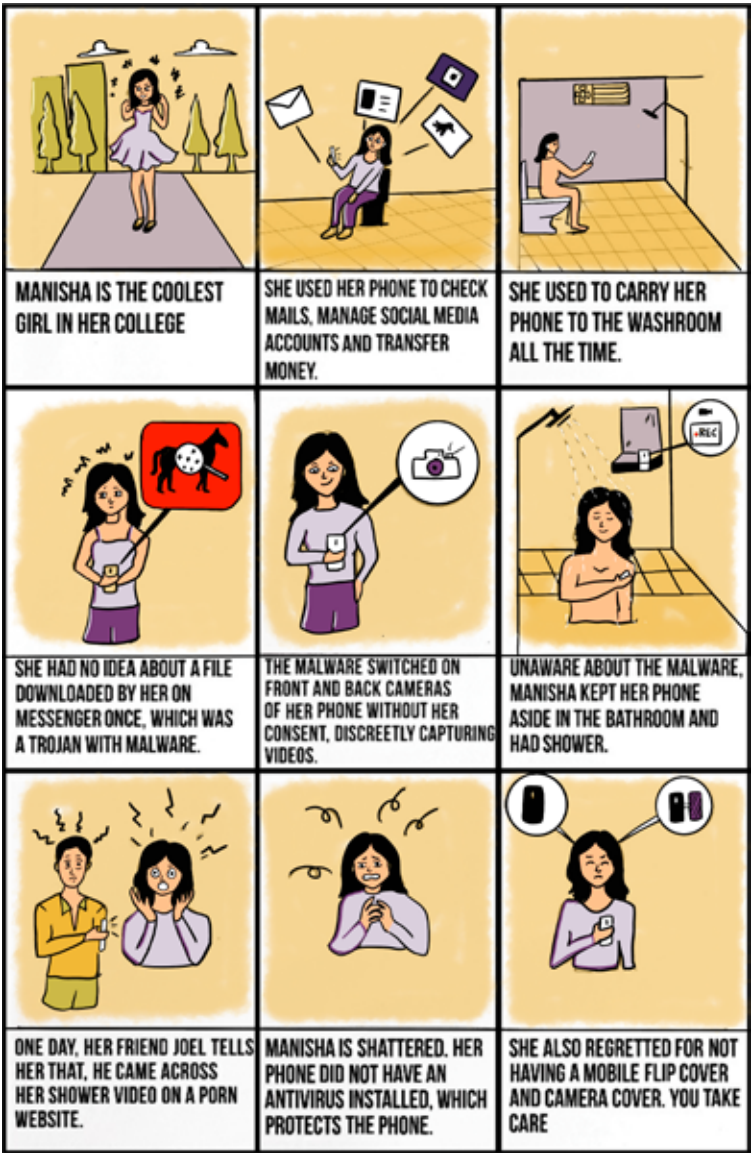
CAMERA HACKING

Camera hacking happens when photographs of a person are taken without consent, through malware that got downloaded with an attachment. Phones with no camera guard can be exploited for such criminal activities.

Sections Applicable

Hacking–
IPC Section 66 – Computer related offences
Capturing photograph/video:
IPC Section 354C – Voyeurism
IT Act Section 66E – Punishment for violation of privacy
Creating Fake ID in social media
IT Act Section 66D – Punishment for cheating by personation by using computer resource
IPC Section 419 – Punishment for cheating by personation
Online Sexual harassment to a woman
IPC Section 354A – Sexual Harassment and punishment for Sexual Harassment
Stalking : Offline : IPC Section 354 D – Stalking
Online : IPC Section 354 D – Stalking
Publishing online
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO
IPC Section 507 – Criminal Intimidation by an Anonymous communication
IPC Section 509 – Word, gesture or act intended to insult modesty of a woman

Think before taking your cell phones while using the restroom. Your privacy may have no room to rest!


MANISHA IS THE COOLEST GIRL IN HER COLLEGE
SHE USED HER PHONE TO CHECK MAILS, MANAGE SOCIAL MEDIA ACCOUNTS AND TRANSFER MONEY.
SHE USED TO CARRY HER PHONE TO THE WASHROOM ALL THE TIME.
SHE HAD NO IDEA ABOUT A FILE DOWNLOADED BY HER ON MESSENGER ONCE, WHICH WAS A TROJAN WITH MALWARE.
THE MALWARE SWITCHED ON FRONT AND BACK CAMERAS OF HER PHONE WITHOUT HER CONSENT, DISCREETLY CAPTURING VIDEOS.
REC
UNAWARE ABOUT THE MALWARE, MANISHA KEPT HER PHONE ASIDE IN THE BATHROOM AND HAD SHOWER.
ONE DAY, HER FRIEND JOEL TELLS HER THAT, HE CAME ACROSS HER SHOWER VIDEO ON A PORN WEBSITE.
MANISHA IS SHATTERED. HER PHONE DID NOT HAVE AN ANTIVIRUS INSTALLED, WHICH PROTECTS THE PHONE.
SHE ALSO REGRETTED FOR NOT HAVING A MOBILE FLIP COVER AND CAMERA COVER. YOU TAKE CARE

SOCIAL TROLLING

Social Trolling is posting inflammatory messages or visuals about a person or organisation in an online community with the sole intention of causing humiliation or nuisance to that person.

Sections Applicable

IPC Section 507 – Criminal Intimidation by an Anonymous communication

IPC Section 509 – Word, gesture or act intended to insult modesty of a woman

Stalking:

Offline: IPC Section 354 D – Stalking

Online : IPC Section 354 D – Stalking

Are you Trolling, the law may be soon following!


COLLEGE
COLLEGE
meme
meme
TROLL PAGE
fb
SHRUTHI IS A SIMPLE GIRL, HAILING FROM A MIDDLE CLASS FAMILY. SHE BELIEVES IN MORALS AND ETHICS.
THE STUDENTS IN COLLEGE WHERE SHE STUDIED WERE MOSTLY CAREFREE TYPES AND FASHION FREAKS
EVERY DAY THEY WOULD PULL HER LEGS, CALL HER BY NAMES AND MAKE HER FEEL MISERABLE.
ROHAN, THE MOST FAMOUS BOY IN THE COLLEGE CALLED SHRUTHI A GAWAR AND TOLD HER TO GO BACK TO HER VILLAGE.
SHRUTHI DECIDED TO PUT A FULL STOP TO THIS MENACE. SHE GAINS COURAGE AND ASKS HIM TO GET LOST AND MIND HIS BUSINESS.
IRRITATED ROHAN GOES BACK HOME AND EDITS ADULTS JOKES WITH SHRUTHI'S NAME AND FORWARDS IT TO HIS FRIENDS.
ALSO MAKES A TROLL PAGE OF SHRUTHI, UPLOADS MEMES AND FUNNY VIDEOS OF HER
SHRUTHI BECOMES A LAUGHING STOCK AND NOW WISHES TO DISCONTINUE HER STUDIES.
SHRUTHI LATER REALIZES SHE SHOULD HAVE INFORMED THE AUTHORITIES IN COLLEGE AND LODGED A COMPLAINT IN THE WOMENS POLICE STATION

PONZI SCHEME

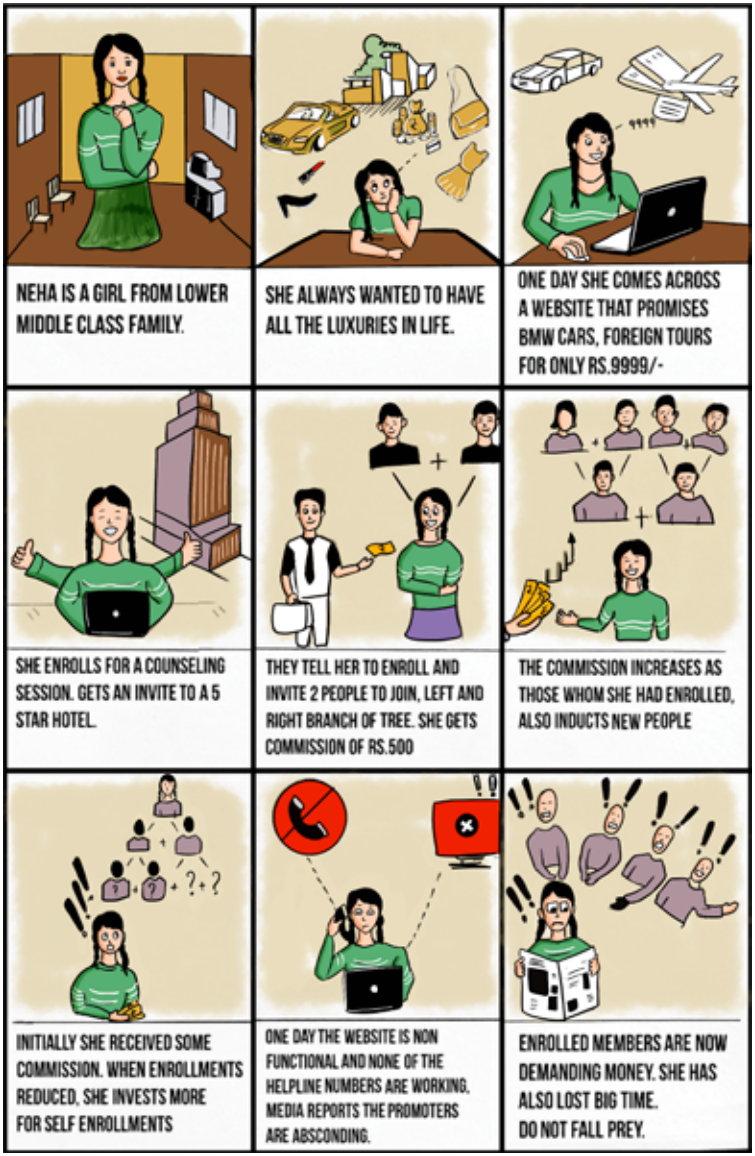
A Ponzi scheme is a fraudulent investing scam promising high rates of return with little risk to investors. Victims of such schemes are vulnerable to hackers with malicious intent and fall prey to their promises of recovery of their losses.

Sections Applicable

Sections 3, 4, 5, 6 of Prize Chits and Money Circulation Schemes (Banning) Act, 1978
Also look up at State Acts eg
Section 9 of the Karnataka Protection of Interest of Depositors In Financial Establishments Act, 2004
Section 3, 4 of Maharashtra Protection of Interest of Depositors In Financial Establishments Act, 1999 etc.

IPC Section 120-B – Punishment for Criminal Conspiracy
IPC Section 406 – Punishment for Criminal Breach of Trust
IPC Section 420 – Cheating
R/W IPC Section 34 – Acts done by several persons in furtherance of Common Intention

Investing in Ponzi schemes may make you run out of all other Schemes of life!


NEHA IS A GIRL FROM LOWER MIDDLE CLASS FAMILY.
SHE ALWAYS WANTED TO HAVE ALL THE LUXURIES IN LIFE.
ONE DAY SHE COMES ACROSS A WEBSITE THAT PROMISES BMW CARS, FOREIGN TOURS FOR ONLY RS.9999/-
SHE ENROLLS FOR A COUNSELING SESSION. GETS AN INVITE TO A 5 STAR HOTEL.
THEY TELL HER TO ENROLL AND INVITE 2 PEOPLE TO JOIN, LEFT AND RIGHT BRANCH OF TREE. SHE GETS COMMISSION OF RS.500
THE COMMISSION INCREASES AS THOSE WHOM SHE HAD ENROLLED, ALSO INDUCTS NEW PEOPLE
INITIALLY SHE RECEIVED SOME COMMISSION. WHEN ENROLLMENTS REDUCED, SHE INVESTS MORE FOR SELF ENROLLMENTS
ONE DAY THE WEBSITE IS NON FUNCTIONAL AND NONE OF THE HELPLINE NUMBERS ARE WORKING. MEDIA REPORTS THE PROMOTERS ARE ABSCONDING.
ENROLLED MEMBERS ARE NOW DEMANDING MONEY. SHE HAS ALSO LOST BIG TIME.
DO NOT FALL PREY.

FAKE MATRIMONIAL PROFILE

A fraudster may have registered on a matrimonial site with a fake profile. The details and profile pic may not be his. He can dupe a naive girl who falls for his practised charm and believes in the authenticity of supportive material that he provides to back up his identity.

Sections Applicable

IPC Section 465 – Making a false document
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)
IT Act Section 66D – Punishment for cheating by personation by using computer resource
IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating
IPC Section 507 – Criminal Intimidation by an Anonymous communication

Marriages are made in Heaven but in the virtual world you end up paying the cost of messing with Heavenly Affairs!


FATHIMA A SPINSTER WORKS AS AN ENGINEER. HER PARENTS ARE ON THE LOOKOUT FOR A GROOM
SHE HAD REGISTERED ON MANY MATRIMONIAL SITES, HOPING TO FIND A GROOM.
SHE GETS AN INBOX MESSAGE FROM A 30 YEAR OLD MALE, EXPRESSING INTEREST
HER SEARCH REVEALS HIM AS AN INDIAN, IRS OFFICER WORKING IN BANGALORE AND HAILING FROM A WEALTHY FAMILY
THEY START EXCHANGING TEXTS, THEN CALL EACH OTHER. HE WAS A CHARMER AND SHE FALLS FOR HIM
TO MAKE HER BELIEVE, HE SHOWED HER HIS ID, LOGIN DETAILS ON THE WEBSITE, PHOTOS OF HIS FAMILY, FRIENDS ETC.,
ONE DAY HE TOLD HER, HE HAS GOT SUSPENDED FROM JOB BECAUSE SOME POLITICIANS NEVER LIKED HIM. HE WANTED MONEY TO GET BACK HIS JOB.
HE HANDS OVER HIS PASSPORT, ID AND OTHER DOCUMENTS FOR SAFE KEEPING. SHE TRANSFERS 5LAKHS TO HIS ACCOUNT, TO HELP HIM DURING HIS DIFFICULT TIMES.
A WEEK LATER, SHE READS IN THE NEWSPAPER, HE WAS ARRESTED FOR CHEATING MANY WOMEN THROUGH MATRIMONIAL WEBSITE. YOU BE SURE.

MOBILE REPAIR SHOP

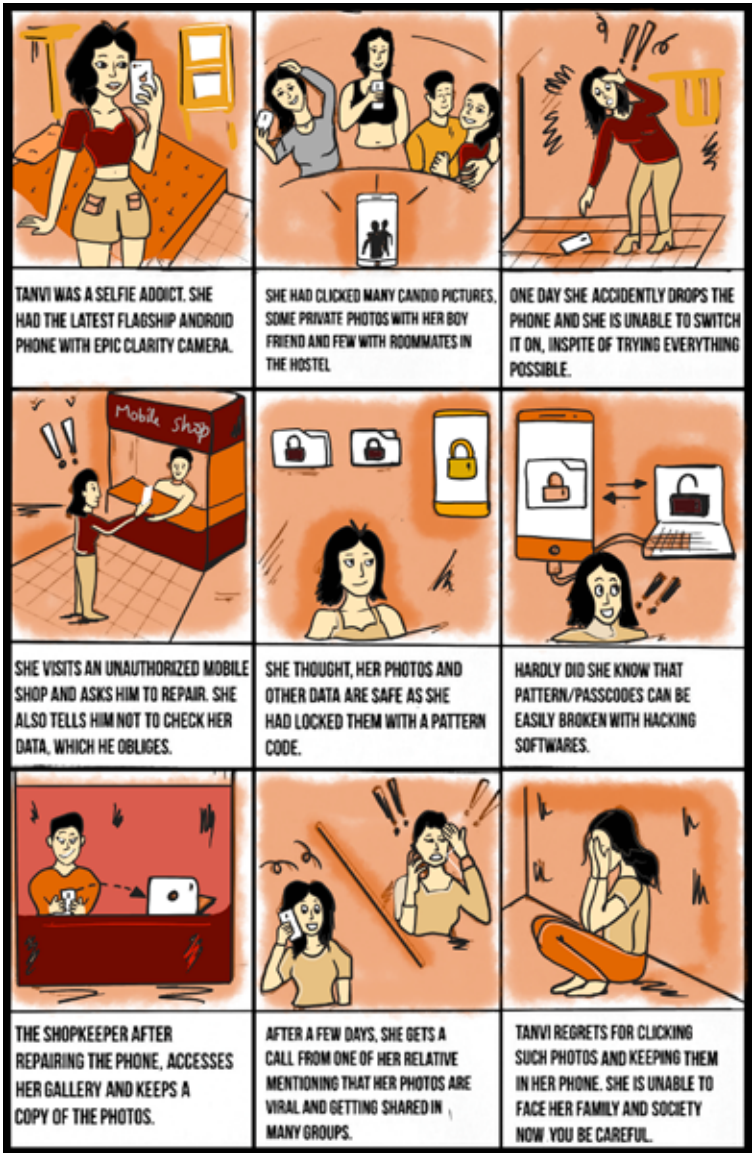
Pictures and videos stored in the phone's gallery can be accessed by any person once the phone is in his possession. A mobile repair shop may have a criminal who accesses private pictures or other data and uploads them on shady sites to make them viral. He may also use them for blackmailing.

Sections Applicable

IT Act Section 66 – Computer Related Offences
IPC Section 406 – Punishment for Criminal Breach of Trust

Publishing online
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO
IPC Section 506 – Punishment for Criminal Intimidation
IPC Section 507 – Criminal Intimidation by an Anonymous communication
IPC Section 509 – Word, gesture or act intended to insult modesty of a woman

If caution not adhered at such Shops, get ready to take big Hops!


TANVI WAS A SELFIE ADDICT. SHE HAD THE LATEST FLAGSHIP ANDROID PHONE WITH EPIC CLARITY CAMERA.
SHE HAD CLICKED MANY CANDID PICTURES, SOME PRIVATE PHOTOS WITH HER BOY FRIEND AND FEW WITH ROOMMATES IN THE HOSTEL
ONE DAY SHE ACCIDENTLY DROPS THE PHONE AND SHE IS UNABLE TO SWITCH IT ON, INSPITE OF TRYING EVERYTHING POSSIBLE.
Mobile Shop
SHE VISITS AN UNAUTHORIZED MOBILE SHOP AND ASKS HIM TO REPAIR. SHE ALSO TELLS HIM NOT TO CHECK HER DATA, WHICH HE OBLIGES.
SHE THOUGHT, HER PHOTOS AND OTHER DATA ARE SAFE AS SHE HAD LOCKED THEM WITH A PATTERN CODE.
HARDLY DID SHE KNOW THAT PATTERN/PASSCODES CAN BE EASILY BROKEN WITH HACKING SOFTWARES.
THE SHOPKEEPER AFTER REPAIRING THE PHONE, ACCESSES HER GALLERY AND KEEPS A COPY OF THE PHOTOS.
AFTER A FEW DAYS, SHE GETS A CALL FROM ONE OF HER RELATIVE MENTIONING THAT HER PHOTOS ARE VIRAL AND GETTING SHARED IN MANY GROUPS.
TANVI REGRETS FOR CLICKING SUCH PHOTOS AND KEEPING THEM IN HER PHONE. SHE IS UNABLE TO FACE HER FAMILY AND SOCIETY NOW YOU BE CAREFUL.

FAKE REVIEWS

A website may dupe customers by putting up fake reviews of products. They plant glowing reviews and pay for perfect ratings that attract customers, especially backed by discounted prices. These products from dubious sites may cause untold harm if used.

Sections Applicable

IPC Section 406 – Punishment for Criminal Breach of Trust
IPC Section 420 – Cheating

Fake Reviews may give you wrong Overviews!


COLLEGE
NIKITA IS AN UNDERGRADUATE STUDENT AND ALSO AN UPCOMING MODEL.
SHE USED TO ATTEND A LOT OF PAGE 3 PARTIES TO MAKE SURE SHE WAS IN LIMELIGHT.
THE COSMETICS AND PERFUMES THAT SHE WORE WERE VERY EXPENSIVE, WHICH LASTED LONG TILL THE END OF THE PARTY.
AS SHE STARTED ATTENDING MORE PARTIES, THE COSMETICS GOT OVER SOON. SHE STARTS EXPLORING OPTIONS TO BUY THEM ONLINE FOR CHEAP.
LESS 50%
SHE COMES ACROSS A WEBSITE WHICH OFFERS THE SAME PRODUCTS AT 50% DISCOUNT
REVIEWS
THOUGH IT LOOKS UNBELIEVABLE, SHE CHECKS THE VERIFIED REVIEWS. IT WAS 4 STARS ON AN AVERAGE
SHE DECIDES TO BUY THE PERFUME AND COSMETICS. PAYS ONLINE .GETS AN SMS FOR ORDER CONFIRMATION.
SHE GETS THE PRODUCTS HOME DELIVERED. UPON USING THEM SHE GETS RASHES ON HER SKIN, WHICH WERE SO ACUTE, THAT SHE GOT ADMITTED TO THE HOSPITAL.
REAL
FAKE
NIKITA GOT CARRIED AWAY BY FAKE REVIEWS. MANY WEBSITES ARE KNOWN TO PLANT GLOWING REVIEWS. YOU TAKE CARE OF WEBSITE & REVIEWS, ELSE WOULD PAY FOR THE MISTAKE.

FAKE PROFILE WITH SEXTORTION

Public changing rooms may have strategically placed cameras that capture pics of the users, naturally with criminal intent. These pics can then be uploaded on a duplicate social media account with the intention of extortion.

Sections Applicable

Capturing photograph/video:

IPC Section 354C – Voyeurism

IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

IT Act Section 66D – Punishment for cheating by personation by using computer resource

IPC Section 419 – Punishment for cheating by personation

IPC Section 354A – Sexual Harassment and punishment for Sexual

IPC Section 507 – Criminal Intimidation by an Anonymous communication

Publishing online

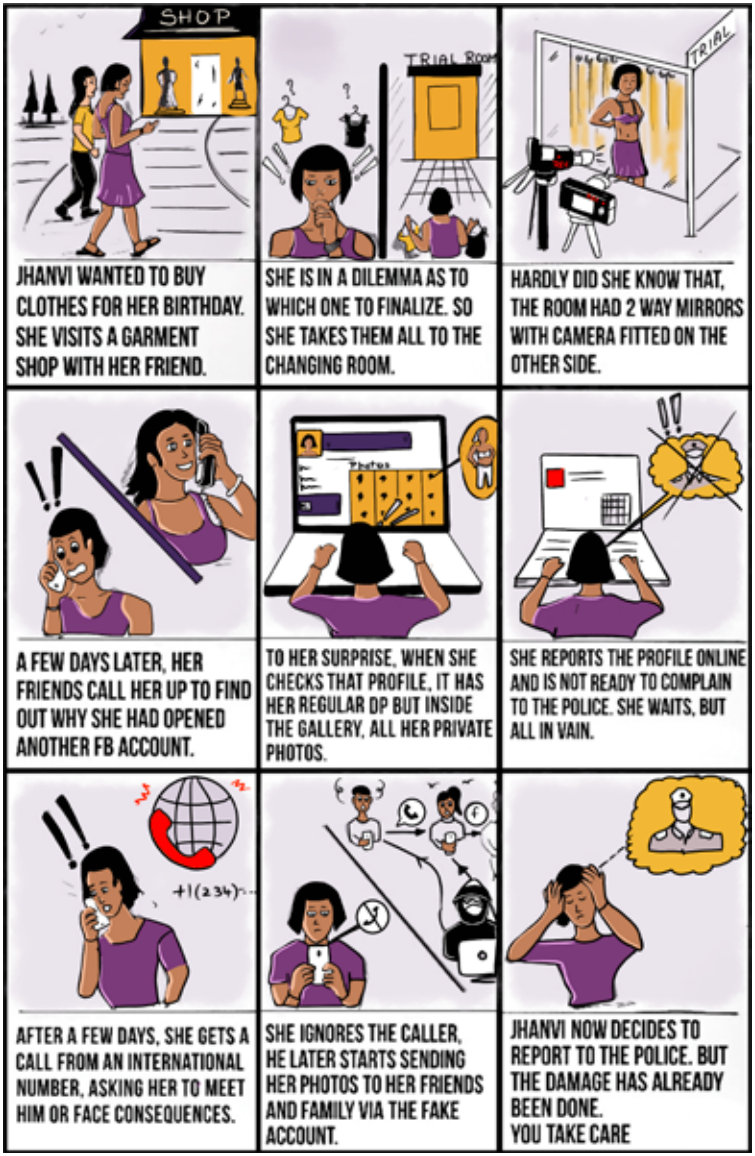
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form

IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

IPC Section 509 – Word, gesture or act intended to insult modesty of a woman

A Fake Profile can cause unimaginable consequences!


SHOP
TRIAL Room
TRIAL
JHANVI WANTED TO BUY CLOTHES FOR HER BIRTHDAY. SHE VISITS A GARMENT SHOP WITH HER FRIEND.
SHE IS IN A DILEMMA AS TO WHICH ONE TO FINALIZE. SO SHE TAKES THEM ALL TO THE CHANGING ROOM.
HARDLY DID SHE KNOW THAT, THE ROOM HAD 2 WAY MIRRORS WITH CAMERA FITTED ON THE OTHER SIDE.
A FEW DAYS LATER, HER FRIENDS CALL HER UP TO FIND OUT WHY SHE HAD OPENED ANOTHER FB ACCOUNT.
Photos
TO HER SURPRISE, WHEN SHE CHECKS THAT PROFILE, IT HAS HER REGULAR DP BUT INSIDE THE GALLERY, ALL HER PRIVATE PHOTOS.
SHE REPORTS THE PROFILE ONLINE AND IS NOT READY TO COMPLAIN TO THE POLICE. SHE WAITS, BUT ALL IN VAIN.
+1(234)
AFTER A FEW DAYS, SHE GETS A CALL FROM AN INTERNATIONAL NUMBER, ASKING HER TO MEET HIM OR FACE CONSEQUENCES.
SHE IGNORES THE CALLER, HE LATER STARTS SENDING HER PHOTOS TO HER FRIENDS AND FAMILY VIA THE FAKE ACCOUNT.
JHANVI NOW DECIDES TO REPORT TO THE POLICE. BUT THE DAMAGE HAS ALREADY BEEN DONE.
YOU TAKE CARE

CYBER VULTURES

Cyber-vultures are a merciless breed of hackers who like to feast on consumers and businesses suffering from any type of attack. They use this scenario as an opportunity to trick them and swindle more money.

Sections Applicable

IT Act Section 66 – Computer related offences
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

Impersonation as financial company:
IT Act Section 66D – Punishment for cheating by personation by using computer resource
Fetching personal/ Banking/wallet details:
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature/password/electronic signature)
IPC Section 420 – Cheating

Vultures live on dead bodies, cyber vultures live on people who have already lost their money (who are dead financially).


MRS LOBO IS A WIDOW HAILING FROM A MIDDLE CLASS FAMILY. SHE HAS 2 DAUGHTERS.
ONE OF HER RELATIVES CONVINCED HER TO INVEST ALL HER SAVINGS AMOUNT INTO A PONZI SCHEME FOR HIGHER RETURNS.
SHE ALSO ENDED UP INVESTING HER HUSBAND'S INSURANCE AMOUNT INTO THE SCHEME.
Fraud
SCAM
ONE DAY SHE REALIZES THE COMPANY DIRECTORS HAVE FLED AND SHE BELIEVES SHE HAS LOST ALL HER MONEY.
A HACKER MANAGES TO GET THE DATABASE OF ALL THOSE WHO HAD INVESTED BY GAINING ACCESS TO THE SERVER.
HE CALLS INVESTORS INDIVIDUALLY, ASSURES THEM THEY WIL GET THE AMOUNT BACK IF THEY GIVE HIM 30% OF THE AMOUNT RECEIVED.
MRS LOBO AGREES FOR THE OFFER. HE REQUESTS FOR UPI CODE, ATM AND ACCOUNT NUMBER.
2***** Debited
MRS LOBO WAS SHOCKED TO SEE THE ONLY AMOUNT SHE HAD, RS 2 LAKHS WAS DEBITED BY THE HACKER, IN NO TIME.
THE AMOUNT WAS TRANSFERRED TO A SHADY EWALLET COMPANY, WHICH REFUSES TO COMPLY WITH THE INVESTIGATION AGENCIES. BE SURE OF RANDOM CALLERS.

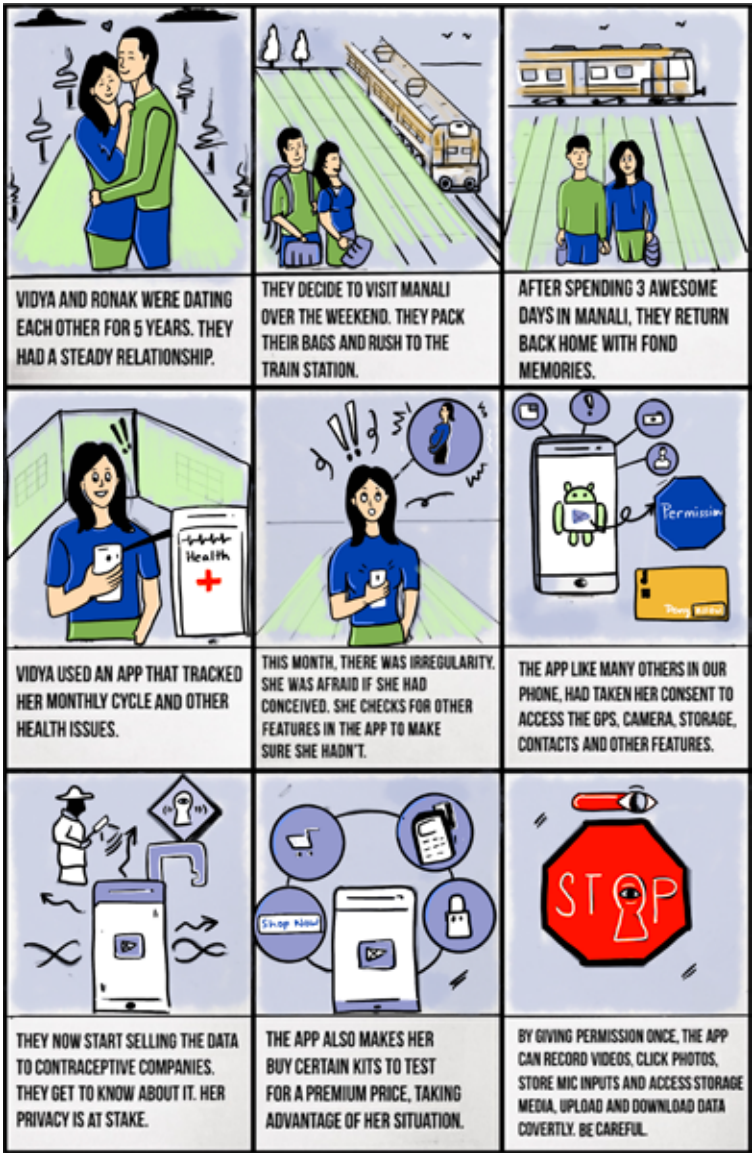
APP TRAPS

The internet could come with a hidden cost. One of these is preloaded apps that harvest users' data without their knowledge. These apps ask for permission to access files and once given, they may use videos, photos and storage media not only to be mined by marketers but also for other nefarious purposes.

Sections Applicable

IPC Section 406 – Punishment for Criminal Breach of Trust
IPC Section 420 – Cheating

These traps give you a silent rap and take away your sensitive personal data.


VIDYA AND RONAK WERE DATING EACH OTHER FOR 5 YEARS. THEY HAD A STEADY RELATIONSHIP.
THEY DECIDE TO VISIT MANALI OVER THE WEEKEND. THEY PACK THEIR BAGS AND RUSH TO THE TRAIN STATION.
AFTER SPENDING 3 AWESOME DAYS IN MANALI, THEY RETURN BACK HOME WITH FOND MEMORIES.
Health
VIDYA USED AN APP THAT TRACKED HER MONTHLY CYCLE AND OTHER HEALTH ISSUES.
THIS MONTH, THERE WAS IRREGULARITY. SHE WAS AFRAID IF SHE HAD CONCEIVED. SHE CHECKS FOR OTHER FEATURES IN THE APP TO MAKE SURE SHE HADN'T.
Permission
THE APP LIKE MANY OTHERS IN OUR PHONE, HAD TAKEN HER CONSENT TO ACCESS THE GPS, CAMERA, STORAGE, CONTACTS AND OTHER FEATURES.
THEY NOW START SELLING THE DATA TO CONTRACEPTIVE COMPANIES. THEY GET TO KNOW ABOUT IT. HER PRIVACY IS AT STAKE.
Shop Now
THE APP ALSO MAKES HER BUY CERTAIN KITS TO TEST FOR A PREMIUM PRICE, TAKING ADVANTAGE OF HER SITUATION.
STOP
BY GIVING PERMISSION ONCE, THE APP CAN RECORD VIDEOS, CLICK PHOTOS, STORE MIC INPUTS AND ACCESS STORAGE MEDIA, UPLOAD AND DOWNLOAD DATA COVERTLY. BE CAREFUL.

JUICE JACKING

Juice Jacking is a type of cyber attack involving a charging port that doubles as a data connection, typically over USB. This often involves either installing malware or copying sensitive data from a smart phone or other computer devices. Charging ports at public places are prime areas for juice jacking.

Sections Applicable

IT Act Section 66 – Computer Related Offences
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature/password/electronic signature)

You may end up giving your data by way of Lottery to the fraudster as against the life of your Battery.


NIDHI IS A WEDDING PLANNER. HER LIFE WAS ALL ABOUT COORDINATING WITH HER VENDORS.
SHE ALWAYS MADE SURE THAT EVERY WEDDING THAT SHE PLANNED, WAS FLAWLESS AND MEMORABLE.
SHE USED TO CALL HER VENDORS TWICE TO CROSS CHECK IF EVERYTHING WAS IN PLACE.
HER WORK INVOLVED A LOT OF TRAVELLING. THEREFORE, SHE USED TO SPEND A LOT OF TIME IN THE AIRPORT.
WHENEVER SHE RAN OUT OF CHARGE IN HER PHONE, SHE USED TO CHARGE IT AT THE FREE CHARGING STATIONS AT THE AIRPORT.
SHE COULD FIGURE OUT THAT, HER PHONE GOT SLOWER AND HOTTER.
SCAN
SCANNING WITH ANTIVIRUS SHOWED PRESENCE OF DANGEROUS MALWARE THAT REDUCED PERFORMANCE.
MALWARE WAS INJECTED INTO HER PHONE VIA CHARGING CABLE AT CHARGING STATIONS.
CONFIDENTIAL PHOTOS AND VIDEOS WERE STOLEN FROM THE PHONE VIA JUICE JACKING. YOU TAKE CARE.

WIFI HACKING

Wifi hacking is essentially cracking the security protocols in a wireless network, granting full access for the hacker to view, store, download, or abuse the wireless network. Weak passwords to wifi networks may enable a hacker to log into the net through the wifi connection in the vicinity.

Sections Applicable

IT Act Section 66 – Computer Related Offences

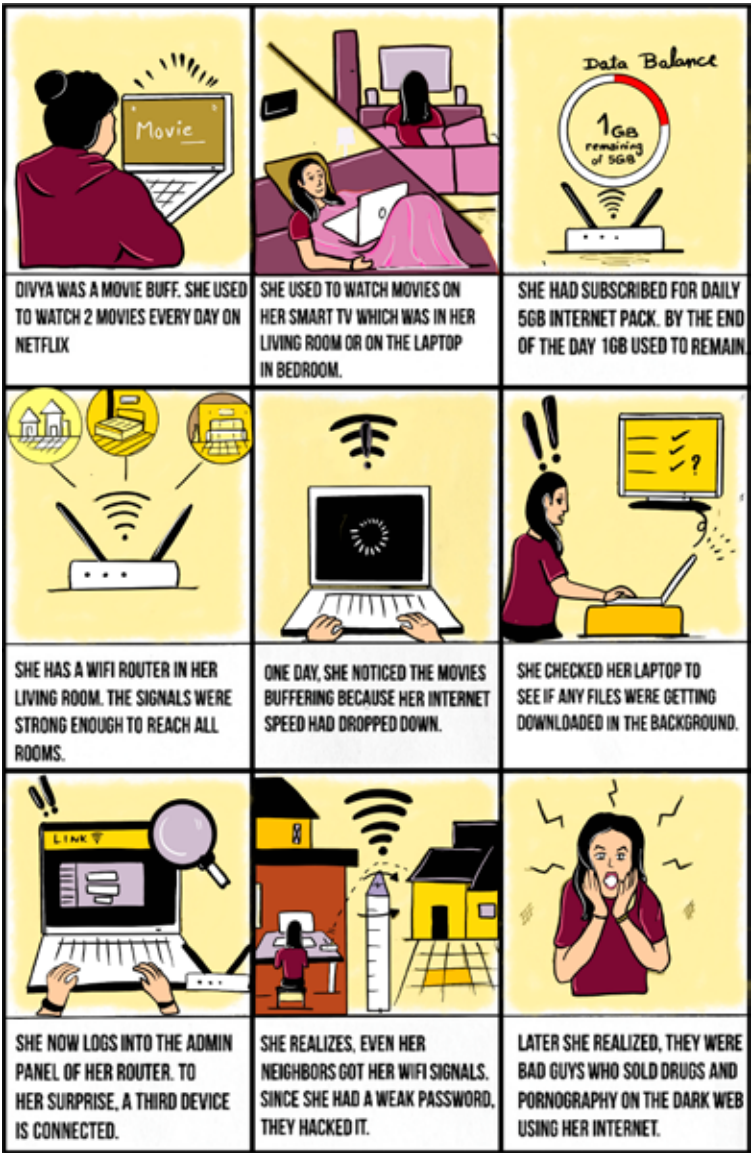
Wrongful gain, wrongful loss of internet data:
IPC Section 420 – Cheating

Mischief by internet utility:
IPC Section 425/426 – Mischief

Publishing online
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

Other provisions of Narcotic Drugs and Psychotropic Substances Act, 1985.

To live a highfy virtual life, better secure your Wi-Fi!


Movie
Data Balance
1GB remaining of 5GB
DIVYA WAS A MOVIE BUFF. SHE USED TO WATCH 2 MOVIES EVERY DAY ON NETFLIX
SHE USED TO WATCH MOVIES ON HER SMART TV WHICH WAS IN HER LIVING ROOM OR ON THE LAPTOP IN BEDROOM.
SHE HAD SUBSCRIBED FOR DAILY 5GB INTERNET PACK. BY THE END OF THE DAY 1GB USED TO REMAIN.
SHE HAS A WIFI ROUTER IN HER LIVING ROOM. THE SIGNALS WERE STRONG ENOUGH TO REACH ALL ROOMS.
ONE DAY, SHE NOTICED THE MOVIES BUFFERING BECAUSE HER INTERNET SPEED HAD DROPPED DOWN.
SHE CHECKED HER LAPTOP TO SEE IF ANY FILES WERE GETTING DOWNLOADED IN THE BACKGROUND.
LINK
SHE NOW LOGS INTO THE ADMIN PANEL OF HER ROUTER. TO HER SURPRISE, A THIRD DEVICE IS CONNECTED.
SHE REALIZES, EVEN HER NEIGHBORS GOT HER WIFI SIGNALS. SINCE SHE HAD A WEAK PASSWORD, THEY HACKED IT.
LATER SHE REALIZED, THEY WERE BAD GUYS WHO SOLD DRUGS AND PORNOGRAPHY ON THE DARK WEB USING HER INTERNET.

ONLINE RADICALIZATION

Young, vulnerable individuals can fall prey to terrorists' propaganda while spending time online and browsing the net. The targets of such extremists are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

Sections Applicable

IT Act Section 66F – Punishment for Cyber Terrorism
IPC Section 120B – Punishment of Criminal Conspiracy
IPCSection121 – Waging or attempting to wage war, or abetting waging of war, against the Government of India
IPC Section 121A – Conspiracy to commit offences punishable under Section 121A
IPC Section122 – Collecting arms, etc., with intention of waging war against the Government of India
IPC Section 124A – Sedition

Don't get Radicalized, rather be Rationalized!


RESHMA WAS A SIMPLE GIRL. SHE HAD COMPLETED HER ENGINEERING.
HER PARENTS DID NOT WANT HER TO WORK AFTER HER STUDIES. THEY GOT HER MARRIED TO AN ENGINEER IN AFRICA
HER HUSBAND TOOK HER ALONG WITH HIM TO AFRICA. BUT SHE DID NOT GET A JOB THERE.
SHE WAS AT HOME ALL THE TIME WITH NO WHERE TO GO AROUND. SO SHE SPENT MOST OF HER TIME ONLINE.
ONCE SHE CAME ACROSS A POST. UPON CLICKING, SHE ENTERED INTO A WEBSITE WITH WEIRD IMAGES AND POSTS.
SHE RECEIVED EMAILS FROM THAT WEBSITE AND LATER STARTED REGULAR CONVERSATIONS WITH THEIR LEADER.
HE WAS SUCCESSFUL IN PLANTING THEIR IDEOLOGY INTO HER INNOCENT MIND. ALSO, DELIVERED THE WEAPONS TO HER HOME.
MALL
AFTER RECITING THE PRAYERS, THE NEXT DAY SHE EXPLODES HERSELF IN A MALL, IN SEEK OF HEAVEN.
HER HUSBAND AND FAMILY WERE SHELL SHOCKED. THEY WERE CLUELESS ABOUT THIS COVERT ONLINE RADICALISATION

HONEY TRAP

Honey trapping is an investigative practice that uses romantic or intimate relationships for an interpersonal, political or monetary purpose to obtain sensitive information. In today's cyber world, "Honey Trap" has gained a new dimension on social media platforms like Facebook, Twitter etc to trap targets by blackmailing them.

Sections Applicable

Capturing Picture/Video Over Online:

IPC Section 354C – Voyeurism

IPC Section 509 – Word, gesture or act intended to insult modesty of a woman

IT Act Section 66E – Punishment for violation of privacy

IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form

IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

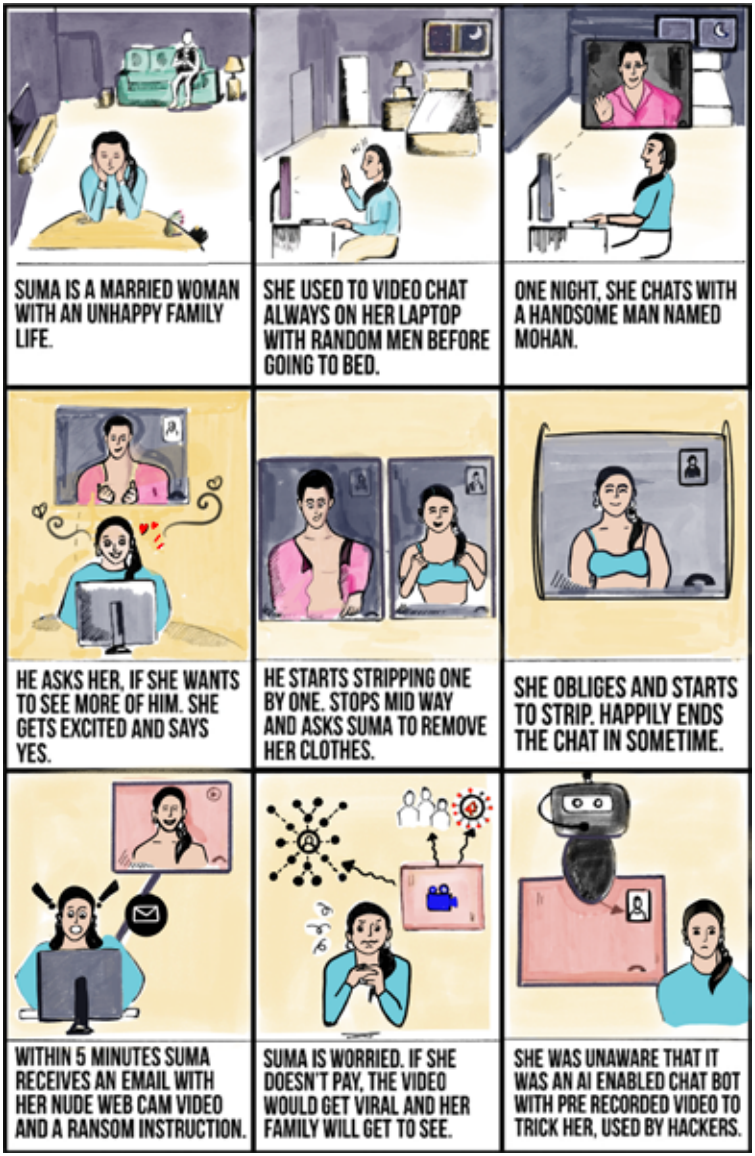
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

Demand for ransom (attempt):

IPC Section 385– Putting person in fear of injury in order to commit extortion

IPC Section 511 – Punishment for attempting to commit offence punishable with imprisonment for life or other imprisonment

With AI, it becomes almost difficult if not impossible to make out the real from surreal.


SUMA IS A MARRIED WOMAN WITH AN UNHAPPY FAMILY LIFE.
SHE USED TO VIDEO CHAT ALWAYS ON HER LAPTOP WITH RANDOM MEN BEFORE GOING TO BED.
ONE NIGHT, SHE CHATS WITH A HANDSOME MAN NAMED MOHAN.
HE ASKS HER, IF SHE WANTS TO SEE MORE OF HIM. SHE GETS EXCITED AND SAYS YES.
HE STARTS STRIPPING ONE BY ONE. STOPS MID WAY AND ASKS SUMA TO REMOVE HER CLOTHES.
SHE OBLIGES AND STARTS TO STRIP. HAPPILY ENDS THE CHAT IN SOMETIME.
WITHIN 5 MINUTES SUMA RECEIVES AN EMAIL WITH HER NUDE WEB CAM VIDEO AND A RANSOM INSTRUCTION.
SUMA IS WORRIED. IF SHE DOESN'T PAY, THE VIDEO WOULD GET VIRAL AND HER FAMILY WILL GET TO SEE.
SHE WAS UNAWARE THAT IT WAS AN AI ENABLED CHAT BOT WITH PRE RECORDED VIDEO TO TRICK HER, USED BY HACKERS.

QR CODE SCAM

A QR (Quick Response) code is nothing more than a two-dimensional barcode. This type of code was designed to be read by robots that keep track of produced items in a factory. As a QR code takes up a lot less space than a legacy barcode, its usage soon spread and Hackers took it to their advantage! QR codes are easy to generate and hard to tell apart from one another. To most human eyes, they all look the same.

Sections Applicable

IPC Section 406 – Punishment for Criminal Breach of Trust
IPC Section 420 – Cheating

Unauthorised Access by installing malware in the background:
IT Act Section 66 – Computer related offences

Your money may be at stake because the codes or apps downloaded by you can be fake.


KIARA IS A TECH SAVVY GIRL AND VOUCHES FOR DIGITAL PAYMENTS.
SHE TRANSACTS WITH CREDIT, DEBIT CARDS AND EWALLETS ON HER PHONE.
500
ONE DAY SHE SCANS A REQUEST PAYMENT QR CODE. THE VALUE IS RS 500. THE AMOUNT APPEARS ON HER PHONE.
THE QR CODE SCANNED WAS MALICIOUS. INSTEAD OF RUPEES, THE DENOMINATION WAS DOLLARS.
KIARA HAD OVERLOOKED THE CURRENCY AND EXCHANGE VALUE.
NO REFUND
THE SERVICE PROVIDER DID NOT REFUND THE MONEY, AS SHE HAD VOLUNTARILY INITIATED TRANSACTION.
KIARA'S FRIEND TANYA TOO HAD SCANNED QR CODE AND GOT HER PHONE INFECTED.
BY A TECHNIQUE CALLED DRIVE BY DOWNLOAD, CODE GETS DOWNLOADED AND INSTALLED IN THE BACKGROUND.
SCANNING QR CODE CAN GIVE AWAY APP CONTROL TO THE ATTACKERS.

RFID CLONING

Radio frequency identification, or RFID often abbreviated Radio Frequency IDentification is method for automatic identification of objects, where the object IDs read or write data using radio waves. Each chip contains an identifier stored inside, with unique number and antenna. Most of these cards can be cloned, easily!

Sections Applicable

IT Act Section 66 – Computer Related Offences

Stealing RFID data / RFID Cloning:

IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature/password/electronic signature)

Retaining stolen data & Selling Credit Card Details:

IT Act Section 66B – punishment for dishonestly receiving stolen computer resource or communication device

IPC Section 420 – Cheating

Creating Replica of Digital ID & accessing server by impersonation:

IT Act Section 66 – Computer Related Offences

IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

IT Act Section 66D – Punishment for cheating by personation by using computer resource

IPC Section 419 – Punishment for cheating by personation

Use technology only if you can imbibe Cyber Hygiene in your Genes.


AYESHA IS AN IT EMPLOYEE. SHE USED HER RFID TAG FOR DOOR ACCESS.
RFID
SHE USED TO PLACE THE RFID CARD IN HER WALLET AND FLASH THE WALLET AT THE READER.
SHE HAD A HABIT OF KEEPING HER WALLET ON THE DESK, EVERYTIME.
ONE DAY, SHE FORGOT TO TAKE THE WALLET WITH HER WHILE SHE LEFT HER DESK TO GO TO THE WASHROOM
RFID READER
A COLLEAGUE, JOHN WHO WAS JEALOUS OF AYESHAS SUCCESS SCANS HER WALLET USING A RFID READER.
JOHN COLLECTS HER OFFICE ID DETAILS AS WELL AS HER CONTACTLESS CREDIT CARD DETAILS.
SOLD
THE CREDIT CARD DETAILS ARE SOLD IN THE DARK WEB FOR MONEY BY JOHN.
REAL
REPLICA
JOHN CREATES A REPLICA OFFICE ID OF AYESHA USING THE DETAILS COLLECTED.
USING THAT ID, JOHN ENTERS THE SERVER ROOM AND HACKS THE SYSTEMS. AYESHA GETS BLAMED FOR NO FAULT OF HERS.

DRONE SURVEILLANCE

In aviation and in space, a drone refers to an unpiloted aircraft or spacecraft. Drones can be equipped with various types of surveillance equipment that can collect high definition video and still images day and night. Drones can be equipped with technology allowing them to intercept cell phone calls, determine GPS locations, and gather license plate information.

Sections Applicable

Following/Stalking/Capturing any PRIVATE AREA pic /video of a women by DRONE without her consent:

IPC Section 354A – Sexual Harassment and punishment for Sexual Harassment

IPC Section 354C – Voyeurism

IPC Section 354D – Stalking

IPC Section 509 – Word, gesture or act intended to insult modesty of a woman

IT Act Section 66E – Punishment for violation of privacy

Unauthorised access to WI FI by DRONE:

IT Act Section 66 – Computer Related Offences

Stealing personal information via WI FI Cracker:

IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

Dropping hazardous materials to house via DRONE:

IPC Section 436 – Mischief by fire or explosive substance with intent to destroy house, etc.

You are profiled day in and day out without doubt.


ANURADHA, A MEDICAL STUDENT LIVED IN THE 33RD FLOOR OF HER APARTMENT.
SHE USED TO KEEP ALL HER WINDOWS OPEN AS THERE WERE NO TALLER BUILDINGS NEARBY WHO COULD VIEW HER PLACE.
SHE USED TO ROAM INDOORS WITH MINIMAL CLOTHES AS SHE NEVER SHARED HER HOME WITH ANYONE.
AKSHAY, HER EX BOYFRIEND USED A DRONE TO SNOOP ON HER IN MANY WAYS.
HE SENT THE DRONE ALL THE WAY UP TO RECORD HER BEDROOM AND LIVING ROOM VIDEOS COVERTLY.
THE DRONE USED TO KEEP TRACK OF IN AND OUT MOVEMENTS FROM HER HOUSE.
IT ALSO HAD A WIFI CRACKER IN IT, TO INTERCEPT ALL THE DATA, TO SNOOP ON HER.
HE COULD ALSO DROP HAZARDOUS MATERIALS/ WEAPONS TO HER HOUSE USING THE DRONE.
SHE COULD HAVE TRACKED THE DRONE IN THE VERY BEGINNING HAD SHE INSTALLED A CC CAMERA WITH MOTION SENSOR

SEARCH ENGINE RESULTS SCAM

A hacker can create a legitimate-looking website and get it indexed by various search engines, making it appear in search results based on the keywords you type. This way, misleading results, fake help line numbers etc can be displayed, making the user believe them and fall prey to this Search Engine Optimization (SEO) scam.

Sections Applicable

IT Act Section 66 – Computer Related Offences

Replacing Original Contact Details by Fraudster Details:
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)
IT Act Section 66D – Punishment for cheating by personation by using computer resource
IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating
IPC Section 465 – Making a false document
IPC Section 468 – Forgery for the purpose of cheating

Fake numbers of customer care may put you under intensive care.


AKSHATA HAD BOOKED A FLIGHT TICKET TO MANGALORE.
TWO DAYS BEFORE THE JOURNEY SHE GETS AN EMAIL STATING HER TICKETS ARE CANCELLED.
SHE GOOGLES THE HELPLINE NUMBER AND CALLS THE NUMBER WHICH APPEARED IN THE RESULTS.
THE CUSTOMER CARE ASKS HER CARD DETAILS FOR VERIFICATION. SHE GIVES ALONG WITH CVV.
SHE LOSES RS 10000 FOR 5 CONSECUTIVE TIMES. TOTAL RS 50000.
THE MAIL SHE HAD RECEIVED WAS SPOOFED. NOT FROM THE AIRLINE.
THE CALL CENTER NUMBER IN THE SEARCH WAS INJECTED BY HACKERS. A FAKE NUMBER TO TRICK PEOPLE.
THOUGH SHE HADN'T SHARED OTP, FOREIGN GATEWAYS DO NOT NEED OTP FOR TRANSACTION.
AKSHATA HAD NOT DISABLED INTERNATIONAL USAGE ON HER CREDIT AND DEBIT CARD.

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

Crackers replacing Letters & Characters to commit frauds.


GIFT VOUCHER
₹ 500/-
EXCLUSIVE OFFER! TRANSACT USING NEFT TODAY AND GET A FREE RS. 500 GIFT VOUCHER. CLICK ON THE LINK BELOW
WWW.EDFCBANK.COM
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
FAILED LOGIN
Login
Submit
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.
DEBITED
₹18000
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
UPDATE
HAD SHE UPDATED HER BROWSER, SHE WOULD HAVE GOT AN ALERT MESSAGE OF THE FAKE CYRILLIC DOMAIN, THAT MIMICS THE LATIN DOMAIN.

SCRATCH CARD SCAM

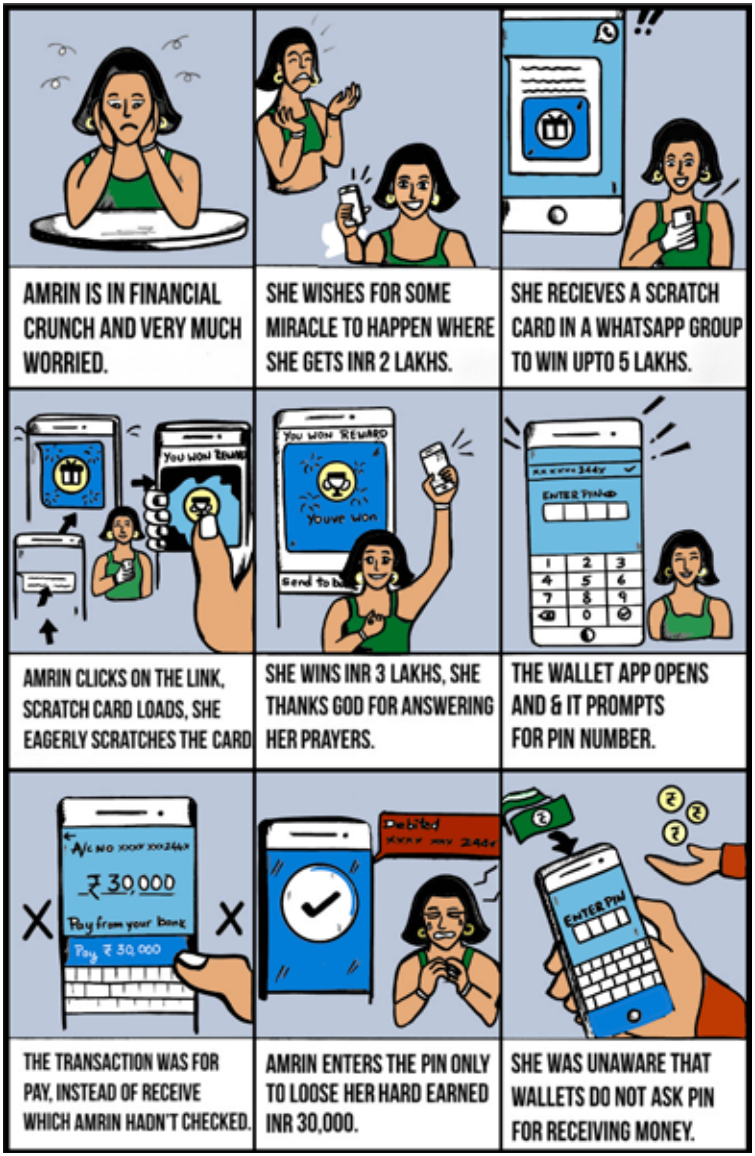
A user receives a message with a link to a third-party website with a promise of winning guaranteed money. When the user clicks on the link, it redirects to a website with a scratch card mimicking the design of popular Pay Wallets scratch card.

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

Sharing sensitive Credentials will bring about losses that would be Substantial


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
You've won
SHE WINS INR 3 LAKHS, SHE THANKS GOD FOR ANSWERING HER PRAYERS.
ENTER PINNO
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
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.

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

Swapping of Sim could lead you to a situation thats Dim


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.

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.

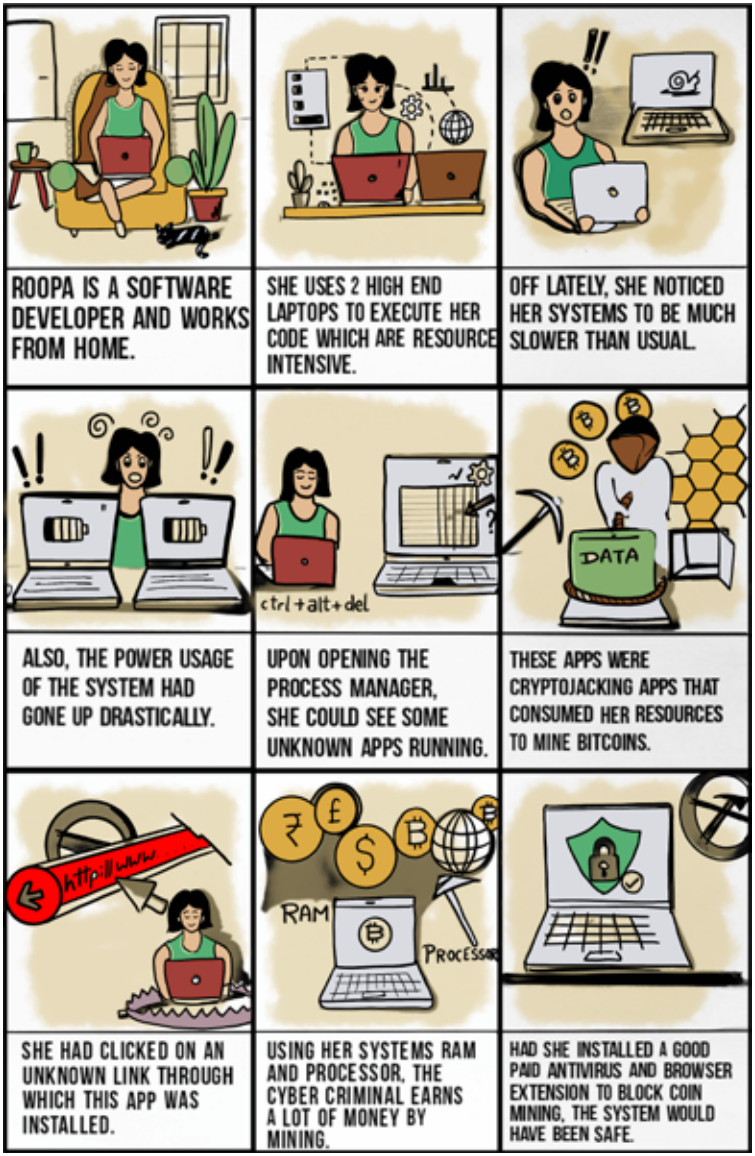
Sections Applicable

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.

Cryptojacking helps hackers in Money Making


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.

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)

Inference of who's attending such virtual Conference needs to made


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.
WAITING ROOM
ADMIT
Share Screen
File Share
A DISGRUNTLED EMPLOYEE FROM THE CLIENTS SIDE LOGGED IN WITH A PROXY NAME.
THE WAITING ROOM WAS NOT ENABLED TO SCREEN THE PARTICIPANTS.
PERMISSION TO SHARE SCREEN AND FILE SHARE WAS NOT DISABLED FOR ALL THE PARTICIPANTS.

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).

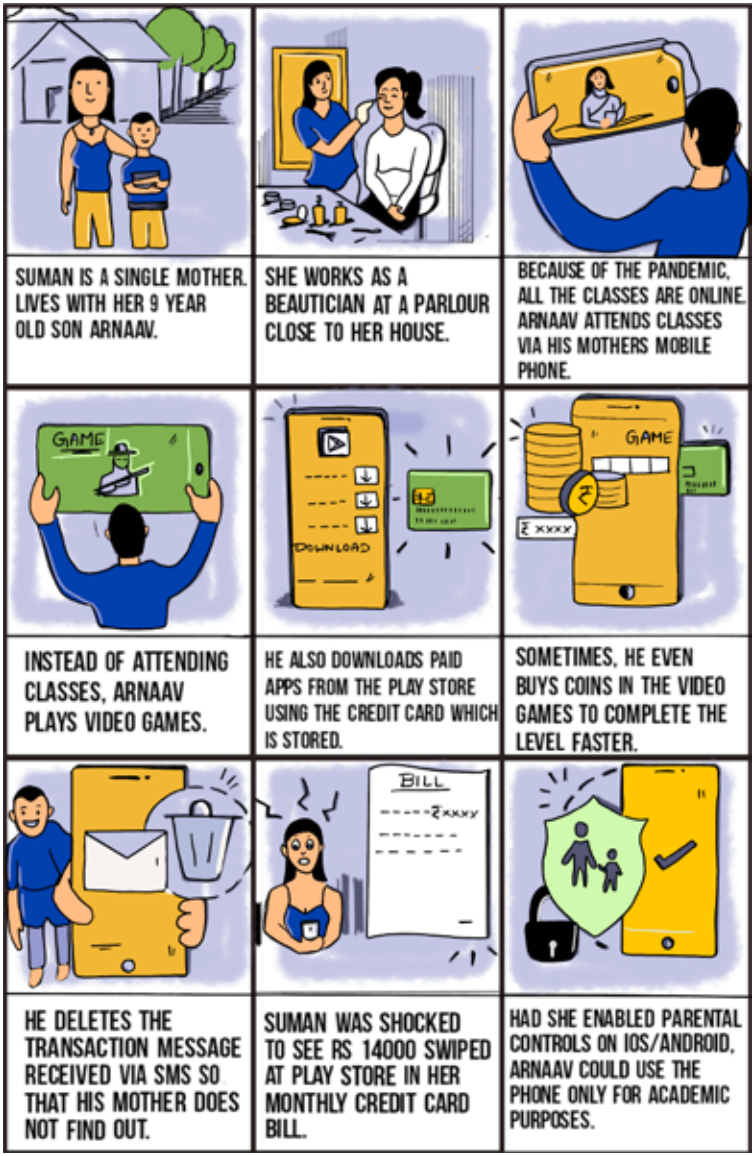
The Lotteries Regulation Act of 1998.

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.

Online games may bring about losses, disrepute and shame


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
-----₹XXXX
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.

SMART HOMES

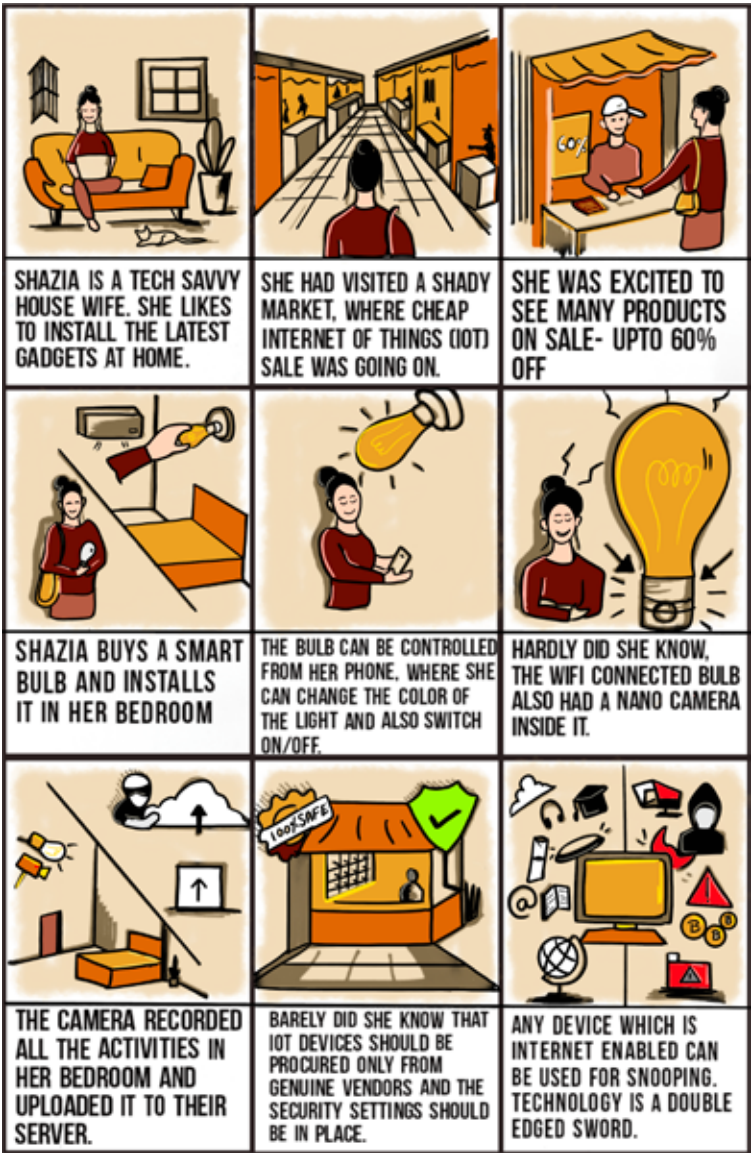
Smart-home devices hold a treasure trove of personal information, from your birth date to credit card details, that cybercriminals can steal via hacking if the devices lack robust protections to thwart attacks. They can then use the stolen data to launch targeted attacks to rope you into shady deals.

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

Digital outreach may lead to Privacy Breach


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.
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.
THE CAMERA RECORDED ALL THE ACTIVITIES IN HER BEDROOM AND UPLOADED IT TO THEIR SERVER.
100%SAFE
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.

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)

App based micro loans are Unsecured and the borrower becomes Insecure


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.

BLUE SNARFING

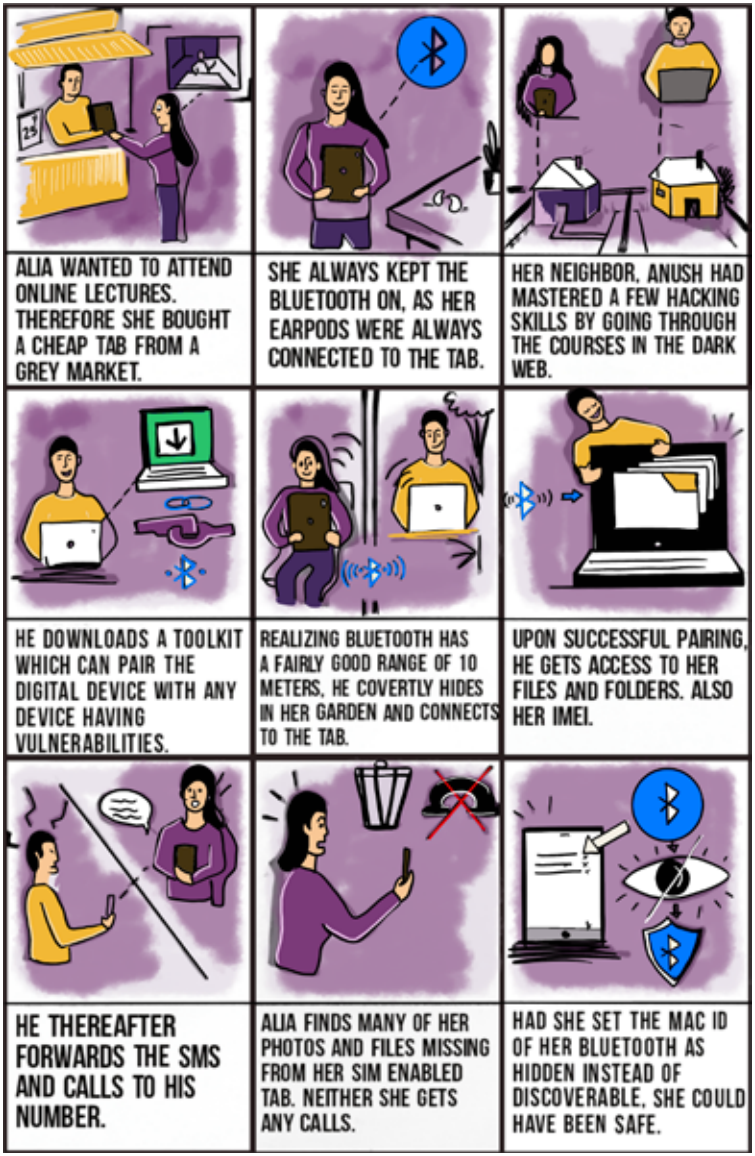
It is a device hack performed when a wireless, Bluetooth-enabled device is in discoverable mode. Bluesnarfing allows hackers to remotely access Bluetooth device data, such as a user's calendar, contact list, emails and text messages. This attack is perpetrated without the victim's knowledge.

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)

Hacker may use your Bluetooth to route your information and cause you blues


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.

STOLEN PHONE

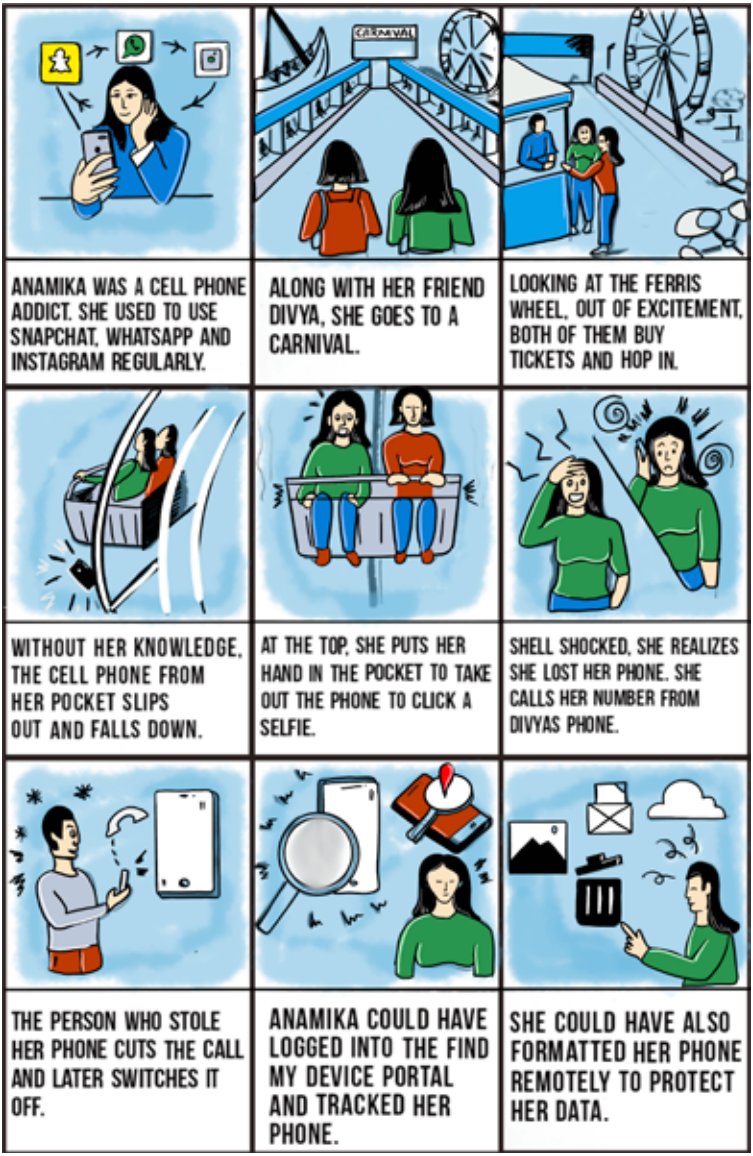
A stolen phone can leave you feeling helpless and scrambling. Mobile phones and the data they hold are very valuable to thieves. And for similar reasons - they hold so much important personal information of real and sentimental value - a theft can be a huge loss for the owner.

Sections Applicable

IPC Section 378/379 – Theft

IT Act Section 66 – Computer related offences

Lost cell phone, it may affect your cells and hormone


ANAMIKA WAS A CELL PHONE ADDICT. SHE USED TO USE SNAPCHAT, WHATSAPP AND INSTAGRAM REGULARLY.
ALONG WITH HER FRIEND DIVYA, SHE GOES TO A CARNIVAL.
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.

EXAM MALPRACTICE

Examination malpractice is defined as any deliberate act of wrongdoing, contrary to the rules of examinations designed to give a candidate an undue advantage. Also known as cheating, these days students resort to hi-tech examination malpractice (otherwise called e-cheating or digital cheating) in various levels of the educational system.

Sections Applicable

420 IPC, 66 R/W 43(c) IT Act – Cheating

Short cuts may cut short your career.


EXAMS
NITARA IS AN ACADEMICALLY PROFICIENT STUDENT .
UNFORTUNATELY, SHE GETS INFECTED WITH COVID & IS UNABLE TO TO ATTEND CLASSES.
NITARA IS WORRIED ABOUT HER UPCOMING EXAMS.
HER BEST FRIEND NITYA SUGGESTS HER A DEVICE TO COPY IN THE EXAMS.
THE DEVICE IS A SPY BLUETOOTH EARPIECE DESIGNED TO ASSIST FOR CHEATING.
NITARA IMPLANTS THE DEVICE IN HER EAR . NITYA COMMUNICATES BY SITTING OUTSIDE THE EXAM HALL.
SHE ALSO WEARS SMART GLASSES HAVING CAMERA, MIC & INTERNET.
THE INVIGILATOR NOTICES NITARA'S STRANGE BEHAVIOUR & SUBJECTS HER TO FRISKING .
NITARA IS DEBARRED FOR 3YEARS, HER ACADEMIC FUTURE IS RUINED .

CONNECTED CAR

Connected cars are part of the 'internet of things', a phrase that refers to everyday items being connected to the internet with the intention of making life easier. The connected car is becoming software-defined, network-aware, and ultra-connected, transmitting data and "interacting" with the road and every other vehicle around it, increasing the chances of getting hacked!

Sections Applicable

354D IPC – This Section also covers online stalking that is to say monitoring her use of the internet, email or other forms of electronic communications & 66 R/W 43 (a), if he causes DOS then 43(f)

While using IoT-Internet of Things also use your IoT-Intelligence of Thinking.

DISHA VISITS A CAR SHOWROOM TO BUY HER 1ST CAR.

SHE'S IMPRESSED WITH THE CONNECTED CAR .

MOST OF THE FEATURES OF THE CAR CAN BE CONTROLLED FROM THE MOBILE PHONE REMOTELY.

HER EX-BOYFRIEND ARUSH USED TO ALWAYS SPY & SNOOP ON HER.

HE REALISES THE SECURITY LOOPHOLES IN HER CONNECTED CAR & HACKS IT.

ARUSH GETS ACCESS TO HER LOCATION, AND OTHER DETAILS OF HER JOURNEY.

DISHA HAD NOT REGULARLY UPDATED HER CARS FIRMWARE AND SOFTWARE PATCHES.

VEHICLE THEFT, MANIPULATION OF SAFETY CRITICAL SYSTEMS, TEST OF PERSONAL DATA ARE THE EFFECTS OF HER SLACKNESS.

MAL-CONFIGURATION ISSUES AND DENIAL OF SERVICE ARE SOME OF THE SECURITY RISKS INVOLVED IN CONNECTED CARS.

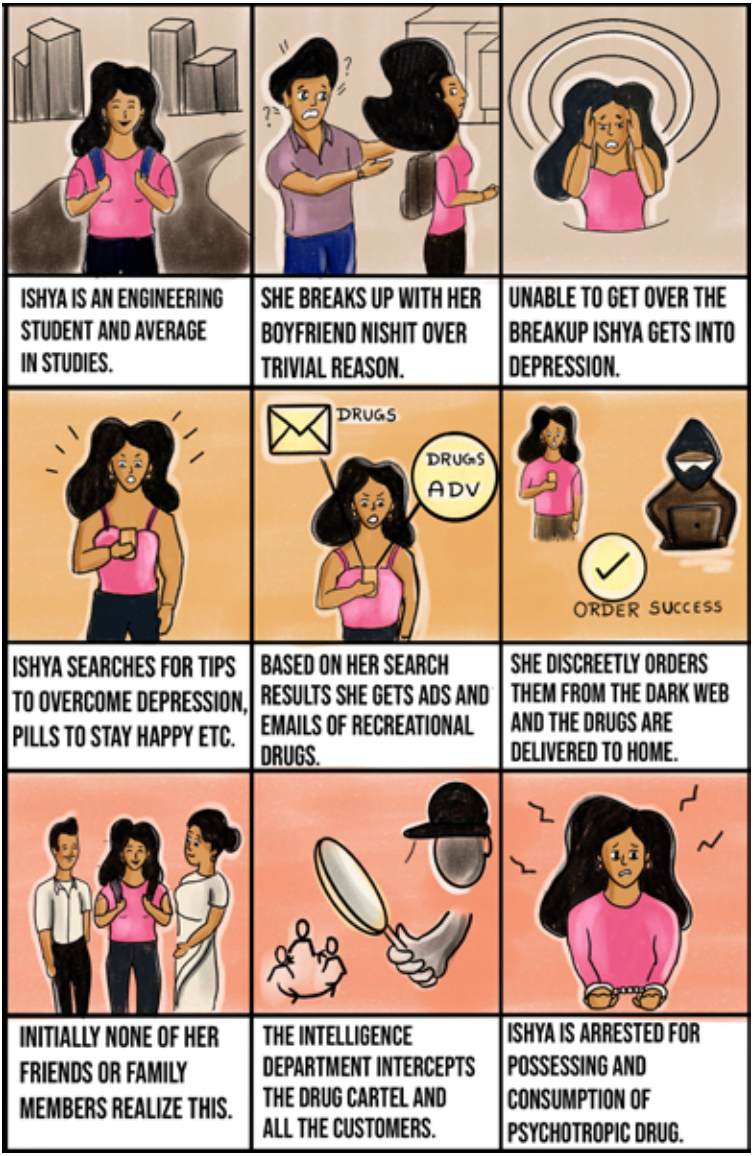
DRUG TRAFFICKING

The last decade has seen the emergence of new internet technologies that have acted as important facilitators of online drug markets. The internet now hosts a range of virtual marketplaces (both on the surface and deep web) for selling and buying illicit substances. Greater connectivity, global outreach and easily accessible forums are some of the reasons for their popularity.

Sections Applicable

Sections of NDPS (sections would apply depending upon the quantity that she was in possession of at the time of the raid, it could be for personal consumption or commercial quantity, and sections would also apply as to whether she was also supplying or trading/dealing/facilitating of the banned substances)

Use of prohibited drugs when depressed, you may have your freedom to right to life and right to personal liberty get suppressed.


ISHYA IS AN ENGINEERING STUDENT AND AVERAGE IN STUDIES.
SHE BREAKS UP WITH HER BOYFRIEND NISHIT OVER TRIVIAL REASON.
UNABLE TO GET OVER THE BREAKUP ISHYA GETS INTO DEPRESSION.
ISHYA SEARCHES FOR TIPS TO OVERCOME DEPRESSION, PILLS TO STAY HAPPY ETC.
DRUGS
DRUGS ADV
BASED ON HER SEARCH RESULTS SHE GETS ADS AND EMAILS OF RECREATIONAL DRUGS.
ORDER SUCCESS
SHE DISCREETLY ORDERS THEM FROM THE DARK WEB AND THE DRUGS ARE DELIVERED TO HOME.
INITIALLY NONE OF HER FRIENDS OR FAMILY MEMBERS REALIZE THIS.
THE INTELLIGENCE DEPARTMENT INTERCEPTS THE DRUG CARTEL AND ALL THE CUSTOMERS.
ISHYA IS ARRESTED FOR POSSESSING AND CONSUMPTION OF PSYCHOTROPIC DRUG.

DOXXING

To dox someone means to release their personal or private information that may prove harmful or embarrassing. This can happen in the real world, but the internet has made it easier both to find and release this information to a wide audience. Doxxing may reveal someone's personal information like their home address or workplace, social security or phone number, private correspondence or pictures, criminal history, IP address, or other details.

Sections Applicable

In India, there is no law specifically prohibiting or punishing doxxing, while there are laws prohibiting voyeurism (Section 354C IPC and Information Technology Act, 2000), disclosing sexually explicit or filthy content (Section 292 IPC), defamation (Section 499 IPC), and online stalking (Section 354D IPC). Disclosing banking details and phone numbers (PII) 72A. Sharing private chats if objectionable in nature then 67 IT Act, disclosing sexually explicit or filthy content Section 292 IPC, defamation Section 499 IPC, outraging women's modesty 509 IPC.

As in Boxing, in Doxxing too an accused could launch a knockout punch causing irreparable injury to the victim.


RABYA IS IN A LIVE-IN RELATIONSHIP WITH KARTHIK.
SHE GETS A VERY GOOD JOB OFFER WHICH SHE ALWAYS DREAMT OF FROM UNITED KINGDOM.
RABYA DECIDES TO END HER FOUR-YEAR-OLD RELATIONSHIP WITH KARTHIK AND START A NEW LIFE.
KARTHIK IS DEVASTATED. HE DECIDES TO TEACH HER A LESSON FOR LIFE.
xx99xxxxx
HE POSTS HER PERSONAL CELL PHONE NUMBER.
HE ALSO SHARES SCREENSHOTS OF THEIR PRIVATE CONVERSATION, EMBARRASSING PERSONAL DETAILS AND BANK ACCOUNT DETAILS.
RABYA STARTS RECEIVING HARASSING CALLS FROM UNKNOWN NUMBERS.
STALKERS ALSO HOUND HER BY COMING NEAR HER HOUSE.
RABYA BECOMES A VICTIM OF DOXXING AND CYBER STALKING.

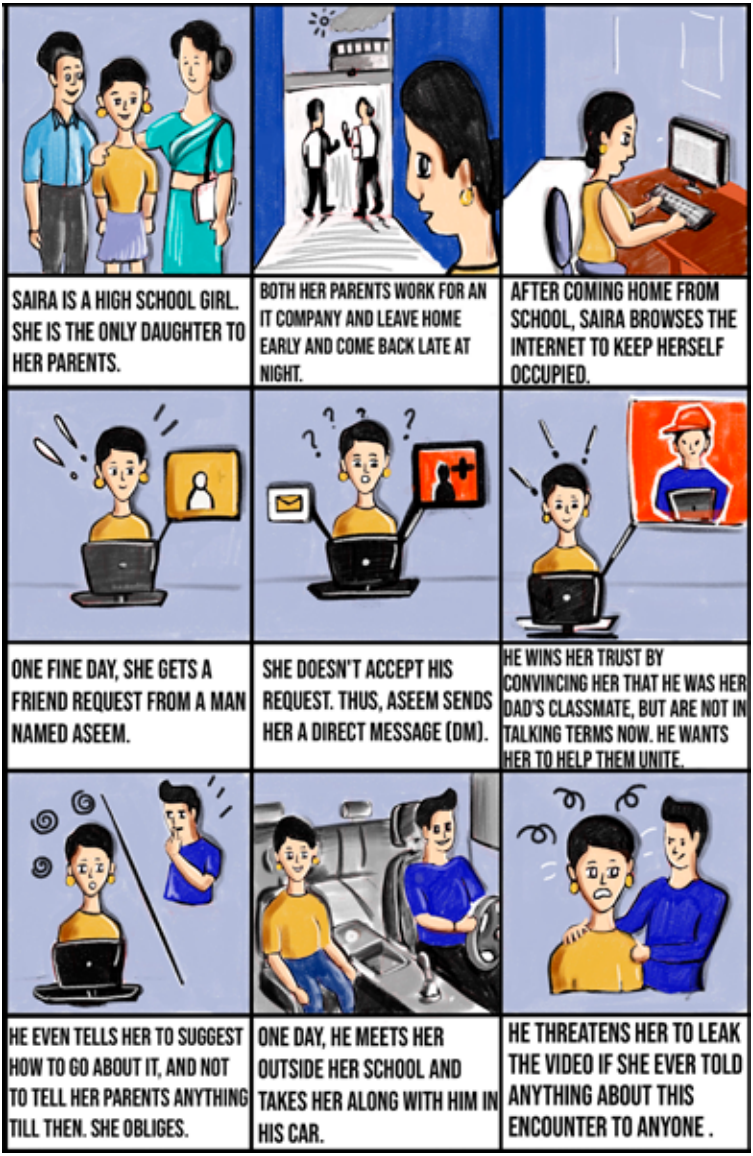
CYBER GROOMING

Cyber grooming is the process of 'befriending' a young person online "to facilitate online sexual contact and/or a physical meeting with them with the goal of committing sexual abuse. Cyber grooming is when someone (often an adult) befriends a child online and builds an emotional connection with future intentions of sexual abuse, sexual exploitation or trafficking. The main goals of cyber grooming are: to gain trust from the child, to obtain intimate and personal data from the child (often sexual in nature—such as sexual conversations, pictures, or videos) in order to threaten and blackmail for further inappropriate material.

Sections Applicable

Sections of POCSO, 67B IT Act & disclosing sexually explicit or filthy content Section 292 IPC

Browse the internet with utmost Morality (principles concerning the distinction between right and wrong or good and bad behaviour) else you are sure to be encountered with cyber crimes with Mathematical Certainty.


SAIRA IS A HIGH SCHOOL GIRL. SHE IS THE ONLY DAUGHTER TO HER PARENTS.
BOTH HER PARENTS WORK FOR AN IT COMPANY AND LEAVE HOME EARLY AND COME BACK LATE AT NIGHT.
AFTER COMING HOME FROM SCHOOL, SAIRA BROWSES THE INTERNET TO KEEP HERSELF OCCUPIED.
ONE FINE DAY, SHE GETS A FRIEND REQUEST FROM A MAN NAMED ASEEM.
SHE DOESN'T ACCEPT HIS REQUEST. THUS, ASEEM SENDS HER A DIRECT MESSAGE (DM).
HE WINS HER TRUST BY CONVINCING HER THAT HE WAS HER DAD'S CLASSMATE, BUT ARE NOT IN TALKING TERMS NOW. HE WANTS HER TO HELP THEM UNITE.
HE EVEN TELLS HER TO SUGGEST HOW TO GO ABOUT IT, AND NOT TO TELL HER PARENTS ANYTHING TILL THEN. SHE OBLIGES.
ONE DAY, HE MEETS HER OUTSIDE HER SCHOOL AND TAKES HER ALONG WITH HIM IN HIS CAR.
HE THREATENS HER TO LEAK THE VIDEO IF SHE EVER TOLD ANYTHING ABOUT THIS ENCOUNTER TO ANYONE .

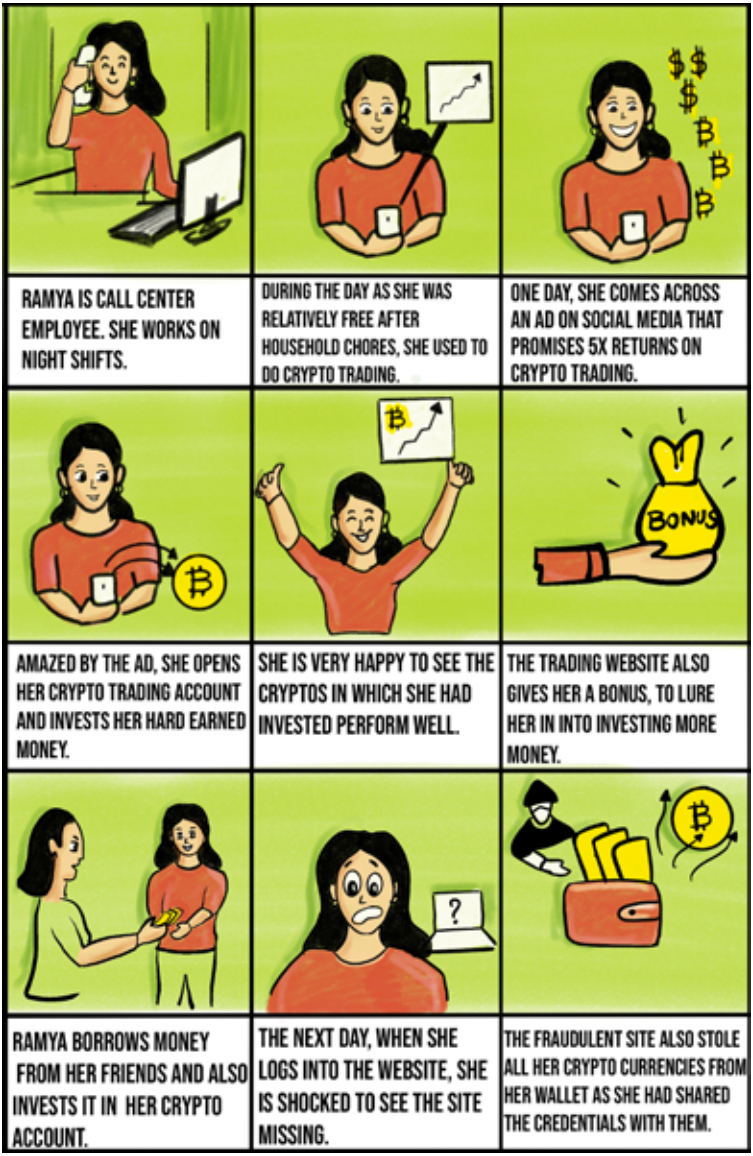
CRYPTO FRAUDS

Scammers are always looking for new ways to steal your money, and the massive growth of cryptocurrency in recent years has created plenty of opportunities for fraud. There are many types of crypto scams. Some of the most common include: Fake Websites, Pump and Dump Scams, Phishing Scams, Fake Apps, Fake celebrity endorsements, Giveaway scams, cloud mining scams and initial offering scams.

Sections Applicable

Cheating 420 IPC, Criminal Breach of Trust 409, section 421- Dishonest or fraudulent removal or concealment of property to prevent distribution among creditors. Section 90- Consent known to be given under fear or misconception.

Check your Avenues (a strategy for making money, a financial approach or method) else there could be reduction in your Revenues.


RAMYA IS CALL CENTER EMPLOYEE. SHE WORKS ON NIGHT SHIFTS.
DURING THE DAY AS SHE WAS RELATIVELY FREE AFTER HOUSEHOLD CHORES, SHE USED TO DO CRYPTO TRADING.
ONE DAY, SHE COMES ACROSS AN AD ON SOCIAL MEDIA THAT PROMISES 5X RETURNS ON CRYPTO TRADING.
AMAZED BY THE AD, SHE OPENS HER CRYPTO TRADING ACCOUNT AND INVESTS HER HARD EARNED MONEY.
SHE IS VERY HAPPY TO SEE THE CRYPTOS IN WHICH SHE HAD INVESTED PERFORM WELL.
BONUS
THE TRADING WEBSITE ALSO GIVES HER A BONUS, TO LURE HER IN INTO INVESTING MORE MONEY.
RAMYA BORROWS MONEY FROM HER FRIENDS AND ALSO INVESTS IT IN HER CRYPTO ACCOUNT.
?
THE NEXT DAY, WHEN SHE LOGS INTO THE WEBSITE, SHE IS SHOCKED TO SEE THE SITE MISSING.
THE FRAUDULENT SITE ALSO STOLE ALL HER CRYPTO CURRENCIES FROM HER WALLET AS SHE HAD SHARED THE CREDENTIALS WITH THEM.

CYBER SEX TRAFFICKING

Cybersex trafficking, or online sexual exploitation, is a cybercrime and a form of modern slavery. Cybersex trafficking is when a victim is forced into sexual exploitation using coercion, force, or fraud, and their abuse is streamed live on the internet via webcam, video, photography, or other digital media.

Sections Applicable

499, 506, 509, 354A, 370, 347, 357 IPC

Disclosing sexually explicit or filthy content Section 292. Sections of Immoral Traffic (Prevention) Act 1956 also known as PITA (Prevention of Immoral Trafficking Act). 67 & 67A IT Act

While surfing the internet and making connections, be Mindful else it could take you from Sublime to Ridicule (from something that is very good or very serious to something very bad or silly).


AMARA IS AN UNDERGRADUATE. BECAUSE OF HER LOW GRADES IN COLLEGE, SHE DID NOT GET CAMPUS PLACED.
EVERY MORNING, SHE USED TO GET READY AND GO TO DIFFERENT COMPANIES TO GIVE OFF CAMPUS INTERVIEWS.
SALIL, A LOCAL ROWDY WHO LIVES NEAR HER HOUSE, KNEW THAT AMARA NEEDED MONEY.
USING A SOCK PUPPET ACCOUNT, HE CONNECTS TO AMARA ON A DATING WEBSITE.
HE SHOWERS HER WITH LOADS OF GIFTS- PERFUMES, COSMETICS, HANDBAGS, AND EVERYTHING ELSE SHE WANTS.
HE INVITES HER HOME ONE DAY, WHICH IN FACT IS A CYBERSEX DEN, THAT AMARA WASN'T AWARE OF.
HE COERCES HER AND RECORDS HER EXPLOITATION AND LIVE STREAMS OVER THE INTERNET. ALSO PAYS HER TO KEEP QUIET.
THE SAME ORDEAL IS REPEATED MANY TIMES WITH HIS FRIENDS AND LIVE STREAMED. FEARING SOCIAL STIGMA, SHE REFRAINS FROM COMPLAINING.
SALIL AND HIS FRIENDS LEAD A LUXURIOUS LIFE. THEY EARN A LOT OF MONEY BY SUCH ILLEGAL SEX TRADES ON DARK WEB.

CYBERWARFARE

Cyberwarfare is the use of cyber attacks against an enemy state, causing comparable harm to actual warfare and/or disrupting vital computer systems. Some intended outcomes could be espionage, sabotage, propaganda, manipulation or economic warfare.

Sections Applicable

121 IPC. 66E, 66 R/W 43(a) (c) (e) (f)

Sections of Unlawful Activities (Prevention) Act, 1967 (UAPA). In Maharashtra- Sections of The Maharashtra Control of Organised Crime Act, 1999 (MCOCA). Sections of Prevention of Terrorism Act, 2002.

Right to Remedy shall be Rejected if for the offence of Hacking an accused gets Convicted.


RUHI IS AN ENGINEERING STUDENT. INTROVERT AND A TECHNOLOGY WIZARD.
AFTER COLLEGE SHE GOES HOME AND SITS IN FRONT OF HER LAPTOP! SHE LOVES CODING.
SHE WAS ALSO A MEMBER OF MANY CODERS FORUMS. HER COMMENTS AND DEBUGGING SKILLS WERE APPRECIATED BY ALL.
ONE DAY, SHE GETS A MESSAGE IN HER INBOX TO CARRY OUT AN ATTACK ON RUSSIA, FOR WHICH SHE WOULD BE PAID A BIG BOUNTY.
TASK
THE PERSON ALSO TELLS HER, SHE WOULD NEVER EVER HAVE TO WORK UPON COMPLETING THIS TASK AND SHE WOULD GET SO MUCH MONEY TO RETIRE IMMEDIATELY.
RUHI CARRIES OUT DDOS ATTACKS ON RUSSIAN SERVERS USING PROXY AND OTHER STEALTH TECHNIQUES.
BANK
SHE ALSO ATTACKS THEIR POWER GRID AND BANKING SYSTEMS.
THE INTELLIGENCE TEAM OF RUSSIA IDENTIFIES THE PREPARATOR AS RUHI.
SHE IS NOW ARRESTED AND MUST UNDERGO LIFE IMPRISONMENT.

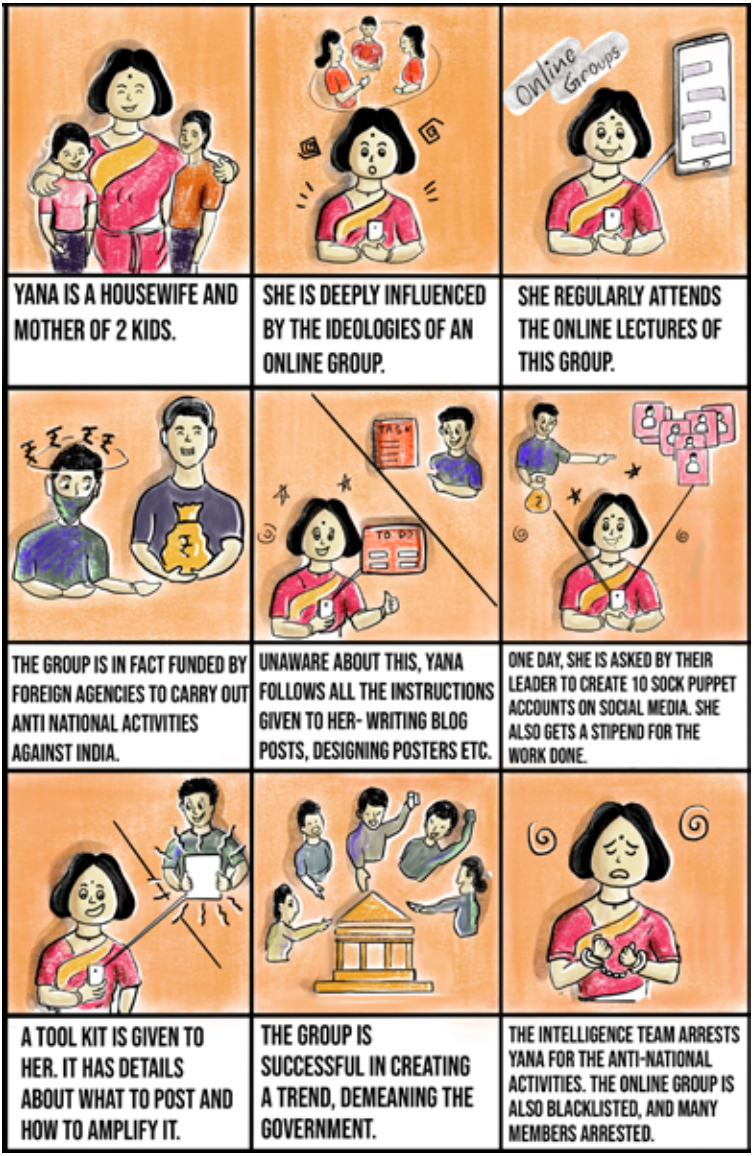
HACKTIVISM

Derived from combining the words 'Hack' and 'Activism', hacktivism is the act of hacking, or breaking into a computer system, for politically or socially motivated purposes. The individual who performs an act of hacktivism is said to be a hacktivist. The hacktivist who does such acts, such as defacing an organization's website or leaking that organization's information, aims to send a message through their activities and gain visibility for a cause they are promoting.

Sections Applicable

120A, 121, 122, 153, 153A, 107 IPC
For creating fake accounts- 66C & 66F IT Act

Think about you and do not allow someone else to think for you.



YANA IS A HOUSEWIFE AND MOTHER OF 2 KIDS.

SHE IS DEEPLY INFLUENCED BY THE IDEOLOGIES OF AN ONLINE GROUP.

SHE REGULARLY ATTENDS THE ONLINE LECTURES OF THIS GROUP.

THE GROUP IS IN FACT FUNDED BY FOREIGN AGENCIES TO CARRY OUT ANTI NATIONAL ACTIVITIES AGAINST INDIA.

UNAWARE ABOUT THIS, YANA FOLLOWS ALL THE INSTRUCTIONS GIVEN TO HER- WRITING BLOG POSTS, DESIGNING POSTERS ETC.

ONE DAY, SHE IS ASKED BY THEIR LEADER TO CREATE 10 SOCK PUPPET ACCOUNTS ON SOCIAL MEDIA. SHE ALSO GETS A STIPEND FOR THE WORK DONE.

A TOOL KIT IS GIVEN TO HER. IT HAS DETAILS ABOUT WHAT TO POST AND HOW TO AMPLIFY IT.

THE GROUP IS SUCCESSFUL IN CREATING A TREND, DEMEANING THE GOVERNMENT.

THE INTELLIGENCE TEAM ARRESTS YANA FOR THE ANTI-NATIONAL ACTIVITIES. THE ONLINE GROUP IS ALSO BLACKLISTED, AND MANY MEMBERS ARRESTED.

METAVERSE

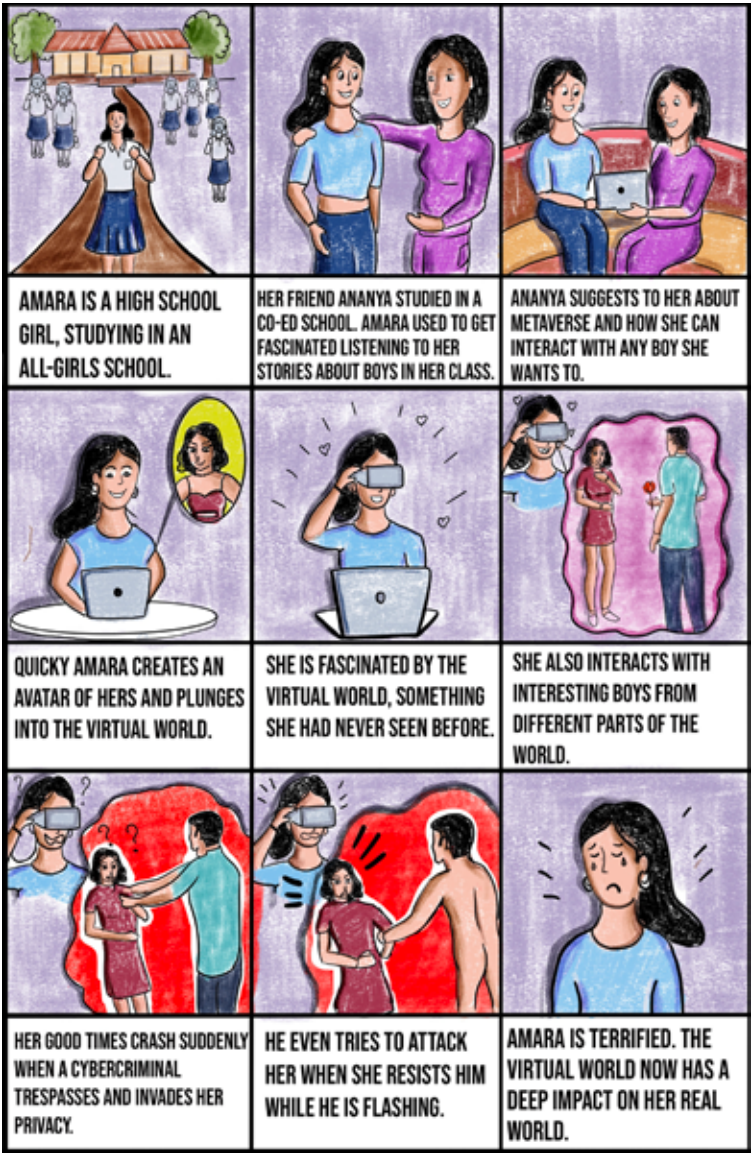
The metaverse is a 3D version of the Internet and computing at large. The metaverse is "an integrated network of 3D virtual worlds." These worlds are accessed through a virtual reality headset - users navigate the metaverse using their eye movements, feedback controllers or voice commands. The headset immerses the user, stimulating what is known as presence, which is created by generating the physical sensation of actually being there.

Sections Applicable

354, 506 IPC, sections of POCSO, section 67B IT Act

Right to Privacy is now a Fundamental Right under Article 21 of the Constitution of India.

Be well versed that Metaverse is not the real Universe.


AMARA IS A HIGH SCHOOL GIRL, STUDYING IN AN ALL-GIRLS SCHOOL.
HER FRIEND ANANYA STUDIED IN A CO-ED SCHOOL. AMARA USED TO GET FASCINATED LISTENING TO HER STORIES ABOUT BOYS IN HER CLASS.
ANANYA SUGGESTS TO HER ABOUT METAVERSE AND HOW SHE CAN INTERACT WITH ANY BOY SHE WANTS TO.
QUICKY AMARA CREATES AN AVATAR OF HERS AND PLUNGES INTO THE VIRTUAL WORLD.
SHE IS FASCINATED BY THE VIRTUAL WORLD, SOMETHING SHE HAD NEVER SEEN BEFORE.
SHE ALSO INTERACTS WITH INTERESTING BOYS FROM DIFFERENT PARTS OF THE WORLD.
HER GOOD TIMES CRASH SUDDENLY WHEN A CYBERCRIMINAL TRESPASSES AND INVADES HER PRIVACY.
HE EVEN TRIES TO ATTACK HER WHEN SHE RESISTS HIM WHILE HE IS FLASHING.
AMARA IS TERRIFIED. THE VIRTUAL WORLD NOW HAS A DEEP IMPACT ON HER REAL WORLD.

INFOTOONS EXPLAINED!

By Adv. Prashanth Jhala

TIPS TO STAY CYBER SAFE

1. MOBILE RECHARGE:

Precautions: While recharging your mobile prepaid card account you have to give your mobile number to the vendor. Though ideally one should go to the Customer Care Centre of the Mobile Service Provider to get the recharge done but as a matter of convenience people approach a local vendor who keeps prepaid vouchers of practically all the mobile service providers and of all denominations. Thereby for recharging they end up giving their cell numbers and hence the scope of misuse. It is advisable to get the recharge done online or through the Customer Care Centre or one should take the voucher and key in the digits by themselves or ask some trusted person to do it for them. Purchasing sim cards from local vendors also warrants you to give your id proofs and photos which could possibly be duplicated and misused. Then again, the convenience of getting a recharge done on credit, if the local vendor is known to you, is also an attractive deal. Use now Pay later may cost you greater.

2. DEBIT CARD CLONING:

Precautions: A skimmer is a device which is used for copying the data on the card on to that device which can be retrieved later and the data thereafter is implanted or embedded on a blank card thus a clone (duplicate) copy of a card is ready for use. While using an ATM kiosk, look out for suspicious fittings on the machine itself. Skimmer comes in different sizes and shapes which are hard to identify and locate. They are fitted precisely at a place where you insert your debit/credit cards into the machines so that they can capture the data residing on the card. Look out for those protruding or extra layer of fittings by physically

checking and actually pulling the exact slot where you insert the card. Sounds inhuman but needs to be done. Then again to record the pin number that you are going to type on the keypad after insertion of your card, small cameras are fitted in obscure or concealed places so that they can clearly record your key strokes. Thus, your card data and your pin number are now with the fraudster and a cloned card is ready for use. Pin numbers can be recorded by also placing pin overlay pads (an extra layer of pin pad which is the replica of original pin pad and is attached to the original pin pad) which in actual would be a keylogger that would log the keystrokes. Therefore, also check the pin pad of that machine. Always cover the pin pad with your hand while keying in the pin number for extra safety. Yet another way would be to send a phishing mail, collect card information from unsuspecting victims, collecting CVV number by use of Social Engineering and make a clone card. Pin number and OTP is collected later while using the cloned card. Thus, look out for suspicious mails and never click on the links appearing in an email. Never share your card details, CVV number and OTP with anyone. Learn more about the modus operandi of Social Engineering.

3. KEYLOGGER:

Precautions: Keyloggers may in the form of a hardware that could be attached to your computer system or to an ATM Machine actual key pad, or it could be a software that could be implanted into your computer system. Difficult to trace them out because generally they are in stealth mode and even best of antivirus used by your systems may not be able to block them. A cyber security expert or a malware analyst's would be able to find out its presence upon thorough investigation of the system. Keep your antivirus updated, update your operating system to latest versions through timely patches released by the provideers, use licensed software's, do not click on suspicious links and the links that originate from unknown source, do not download free songs, movies, videos,

software's, applications, games etc., for a keylogger could be embedded in them and you may end up downloading one for free. Make sure to enable Two Factor Authentication for an additional layer of security, use virtual keyboard to enter the username and password and install a good antivirus on your system to stay cyber safe.

4. SMS SPOOFING:

Precautions: No proper solution for this because a hacker may clone your sim and use your cell number to send SMS's. There are websites, software's and apps that allow a fraudster to send spoofed SMS's to cheat, deceive or defame someone. A Remote Access Trojan if implanted into your cell phone can allow the implanter to send SMS's using your device. Furthermore, such spoofed SMS's are difficult to trace and track. Anonymity is greater when a fraudster uses techniques to spoof.

5. CALL SPOOFING:

Precautions: No proper solution for this because a hacker may clone your sim and use your cell number to make calls. They may also use VOIP (Voice Over Internet Protocol) for spoofing. There are websites, software's and apps that allow a fraudster to make spoofed calls to cheat, deceive or defame someone and they also have the facility to change the modulation, depth, pitch, decibel and quality of voice, a male's voice can be changed to a female's voice or to a voice of a kid and vice a versa. A Remote Access Trojan if implanted into your cell phone can allow the implanter to make calls using your device. Furthermore, VOIP calls are difficult to trace and track and thus anonymity is at its peak in such spoofed calls. To stay protected, Don't place all your trust in the caller ID information presented to you. Now that you know that Caller ID can be easily spoofed by the use of third-party caller ID spoofing services and other tools, that you won't be trusting the technology as you have been in the past. This should help you in the quest to scam-proof your brain.

Also, never give credit card information to someone who calls you. You may also use Google reverse lookup or Truecaller for assistance.

6. RANSOMWARE:

Precautions: Do not click on links that appear from unknown sources. Do not trust the friends you have made on social networking sites. A few cases were reported wherein the so-called friends on social networking sites, sent provocative and/or suggestive pictures embedded with malwares that affected the computer systems and the unsuspected victims clicked on the picture and downloaded malware and got affected in the process. Since different algorithms are used to create ransomwares, the encryption level also changes and hence there is no tailor-made approach to these crimes. Various breeds of ransomware are on prowl but ideally the aim of the hacker would be to deny access to your own computer/network or data. One fit suit all, does not work here as a solution. Remember to take real-time backups. Updating the information and cyber security policies and practices should be an ongoing and proactive endeavour. Patch management has to be in real time right from firewalls, antivirus, intrusion detection alarms etc., and should be upgraded timely. Vulnerability Assessment and Penetration Testing (VAPT) has to be carried out periodically. In the year 2017, WannaCry ransomware affected approximately 150 countries at one go.

7. CYBER STALKING:

Precaution: Cyberstalking is a serious crime, and no one wants to become a victim. One way to help protect yourself is to keep your personal information private on the internet. That's a start. Be careful about allowing physical access to your computer and other web-enabled devices like smartphones. Cyberstalkers can use software and hardware devices (sometimes attached to the back of your PC without you even

knowing it) to monitor their victims. Be sure you always log out of your computer programs when you step away from the computer and use a screensaver with a password. Delete or make private any online calendars or itineraries — even on your social network — where you list events you plan to attend. That information could allow a cyberstalker to know where and when you're planning to be somewhere. A lot of personal information is often displayed on social networks, such as your name, date of birth, where you work, and where you live. Use the privacy settings in all your online accounts to limit your online sharing with those outside your trusted circle. You can use these settings to opt out of having your profile appear when someone searches for your name. You can block people from seeing your posts and photos, too. If you post photos online via social networks or other methods, be sure to turn off the location services metadata in the photo. The metadata reveals a lot of information about the photo — where and when it was taken, what device it was taken on, and other private information. Most often, metadata comes from photos taken on a mobile phone. You can turn this off — it's usually a feature called geo-tagging — in your phone's settings.

8. PICTURE MORPHING:

Precautions: Morphing has become a child's play with tools, apps, software's and technology made available by the internet for free. Various apps allow photo editing and high-end software's allows the act of morphing very easy. High end filters are available for free which can be used to enhance the quality of the pictures. With Drag and Drop and Cut, Copy and Paste options, super imposing or replacing the body and/or body parts of one individual with that of another can be done with considerable ease. Thus, porn and obscene contents are easily created to defame someone by using the victims face and other identification features that are similar to the victims and a lookalike picture of the victims can be uploaded online thereby shaming them. Do not share

your pictures with unknown people or strangers and while uploading on social networking sites like Fb, Instagram, Snapchat etc, one should have an appropriate privacy setting in place before sharing. Very recently a girl committed suicide when she learnt that a morphed vulgar pictures of her were circulated online by an accused. Care before you Share.

9. PROFILE HACKING:

Precaution: Identity theft is the prime motive of Hackers especially when they would want to defame or cheat a woman. Once unauthorized access is gained to a women's social networking sites account, these hackers would invite her friends to like stuffs that are prohibited or filthy in nature. Vulgar, obscene and morphed pictures are posted and people start commenting on them. Messages that invite people for having good time are posted so as to defame that women because her own friends and the new one which the hacker adds from his side would think that this woman herself is posting messages and photos on her own account and hence these would be factual. Hence never click on unknown links, social networking sites password should be strong and needs to be changed often. Your social networking sites are linked to an email account so the password of that mail account should never be revealed to anyone and if you suspect it to be compromised, you need to change the password immediately. Always log out from all the accounts you have logged in. For apps on your mobile, it is advisable to have them password protected as an extra layer of security. Do not reveal your passwords to best of your friends because you never know when they would turn out to be your foe.

10. ONLINE GAMES:

Precautions: Very recently it was reported that fake versions of online games (including Temple Run, Free Flow and Hill Climb Race) that are popular and have huge number of downloads were uploaded on play stores

as free downloads. Innocent people not able to distinguish between the real and the fake versions, downloaded the fake version and ended up in sharing entirepersonal data that resided on their devices. The hacker can also infect the devices with malwares and thereby causing financial losses and also commit identity theft. Addiction to play online games is again a drawback and cases where young children using their parents credit/debit cards without their consent or knowledge to play online games have been reported. Children use their parents high end mobile phones to play such games. The OTP that is sent by the bankers are received by these children and the parents come to know only when they get the card account statement. Many parents do not see the details of the statements and pays up the amount online thereby giving their children a good cover for their forbidden acts. A few games were allegedly displaying inappropriate pictures that could cloud the innocent minds of children. Parents need to keep a tab on what their children are downloading or playing online by examining their browsing history and it is a point to worry if the browsing history is cleared regularly by children because that means they are hiding their footprints. Parental controls should come into play.

11. JOB CALL LETTER:

Precautions: With the advent of high-end printers/copiers and scanners, it is far easier to forge logos, water marks, letter heads, signatures, companies' seals, governments seals etc., and entire set off documents to cheat innocent victims. They are made to believe that they are being offered a high pay package by way of salary either in their own country or somewhere in the western world for which the victims are asked to deposit money on various pretext to get that job call letter. Even telephonic interviews are facilitated to make the victims believe that they are interacting with right entities. Money maybe asked as security deposit, visa facilitation charges, RBI clearance, insurance for travel, opening of bank accounts abroad, for facilitating staying facilities, federal charges etc., Fake and forged documents duly signed under seal

are reduced on the forged letterheads of the companies are sent to the victims to trick them into believing that the offer that they have is for real. Check and recheck before paying anything against such job calls. Do your research, find out more about the company, lookup for its website, call if necessary and ask them if they have floated such requirements in actual. Never pay upfront.

12. DEEP FAKES:

Precautions: Since the advent of high-end filters, photo editors, printers, scanners, apps and software's, creation of any form of content is a child's play. With a little knowledge of technology and the requisite tools that are available for free on internet, one can do wonders using their imagination in the virtual world. Artificial Intelligence (AI) has just added speed, sharpness, ease, convenience, cost effectiveness in the sphere of creation of contents. Superimposing of images and mixing them with high-end filters, makes it extremely difficult for anyone to distinguish the original from the copy (fake). Before trusting any content, be it audio clips, video clips, photos, songs, documents, movies etc, one should verify the source from where it originated. The file sizes of the fakes differ from that of the original ones and that needs to be verified. Metadata (data's data) if available of both the contents may reveal the facts. Forensic examination may also reveal the facts of the contents. Ideally speaking, it becomes almost impossible to distinguish the original content from the fakes.

13. DATING WEBSITES:

Precautions: Before creating an account on dating sites one should keep in mind about frauds being played by the sites and its users. Be careful before swiping Left or Right because your act may swipe you outright and you may have not much left before you could ever realize your mistake. Fake profiles are uploaded on such sites, false

information is provided and old pictures are uploaded by the users to lure the victims. A male may think that he is dating online with a beautiful female but chances are high that the beautiful female may turn out to be an awful male in real. It could be a visa versa case as well. Cases have been reported wherein males were asked to undress and post their pictures on the site and later on those pictures were used to extort money to get them deleted from the site by the accused or were threatened that they would publish them online. Often it has been reported that the reality is far from real as against that which has been mentioned in the profile and the pictures also do not confirm or match or resemble to the ones uploaded. Personal information is gathered by these sites while registering people as clients with them and may be used to one's disadvantage. In a particular case, a dating website was hacked into and the hacker threatened to make all the names of the clients public together with their personal profiles and private pictures if that site did not shut its business online as their privacy policy was not acceptable to that hacker. That site had a few hundred users who were Indians. A couple of suicides were reported because of that breach. Scary isn't that!

14. CAMERA HACKING:

Precautions: Cases have been reported wherein a trojan (which gives privileges and remote access to the implanter) was activated without the knowledge of the owner of a laptop and their pictures and moments of privacy were clicked and uploaded online on porn sites. A small sized file sent to your mobile phone via an attachment can grant access to the implanter and It may allow them to take photos, videos, record sounds, turn on your location services, receive and make calls, send and receive SMS's, access your phone book, your email account, pop up obscene images and much more. Thus, the implanter can start taking pictures and videos without your knowledge and there could be a huge privacy

breach. Always use a masking tape on the webcam of your laptops to avoid breach of your privacy. As for mobile phones, put a piece of cloth on it when you are not using it. Remember that the mobile phones have cameras on both the side so precaution has to be adopted accordingly.

15. SOCIAL TROLLING:

Precaution: Do not indulge in trolling at all. Moreover, when you do not have the facts of the matter, you shouldn't be paddling false or fake information, be it for some news, views or a person concerned. Remember that whatever appears in the virtual world need not necessarily be true. False and fake information can be made viral easily online and people like to share such contents without verifying the facts. Trolling may spread hatred, cause to defame someone, make someone an object of shame, make someone to go into self-shame or depression or could end up defaming someone and it could have a punitive effect on that person being trolled if the actual facts differed from the ones that have been circulated in the trolls. Be discreet while posting or endorsing!

16. PONZI SCHEMES:

Precautions: Schemes that offers to make you rich and wealthy without much efforts are often dubious. Remember such schemes offer high returns on your investment and may never return the money that you had invested. Unfortunately, both literate and illiterate people fall prey to such schemes. The greed to make money without efforts or to adopt a shortcut to become rich and wealthy may reduce your hard-earned savings and make you poor. There have been enough Ponzi schemes being reported and investigated by the law enforcement agencies but despite that new Ponzi schemes are floated and people fall prey to such schemes. Study the entire project and cross verify, make your own research before entrusting your money to someone or investing it into any such schemes. Do not trust agents who promotes such schemes

because they are appointed to paddle wrong information and paint a fake picture of the scheme that would attract your attention and make you not think rationally.

17. FAKE MATRIMONIAL SITES:

Precautions: Such sites not only collect important credentials like your age, your citizenship, your caste, your employment details or the professional services that you offer, your address, your mobile number, your email id, your income, your likes and dislikes in regards prospective brides or bride grooms that you are looking out to match for yourselves, your educational qualifications, your pictures that you upload, your hobbies etc. Fake sites would collect all such details and create a profile of yours and may use it to your disadvantage. False entities are matched and even people already married are shown as prospective clients looking out for life partners and thereby clients stands cheated and deceived thus harming their reputation and honour which creates a deep psychological impact on their minds. Cases have been reported wherein the prospective grooms collects money, ornaments etc., from the prospective brides on various pretext by giving dubious reasons and by giving false promise of marriage and dupes the victims. Physical abuses have also been reported.

18. MOBILE REPAIR SHOP:

Precautions: This one is tricky. When you give your phones for minor repairs to a local vendor for the sake of convenience and also it is supposed to be cost effective, you actually hand over the entire contents and privacy of yours to that vendor. Your phones sim card is a veritable key to financial and sensitive personal data or information. An unscrupulous vendor may make a copy of your entire phones data and retain and save a copy on his laptop and you would even not come to know that fact. People give their phones to vendors for formatting and that also gives a

chance to them to copy your data. While selling away your used phones in exchange of a new or a used one, you may format your phones and hand it over to the vendors. It takes a simple software to retrieve the formatted phones data and here again the vendor may have a copy of your data. So is with your Memory and SD cards. Never give away your Memory or SD cards, instead destroy them and trash them. While disposing or selling off the used phones, first encrypt the entire phone data, then format it. Now if the vendor wants to retrieve the formatted data, he will need a key to decrypt which he wouldn't have for sure. Buying a used phone from a local vendor has another challenge, the vendor may implant a trojan in the phone before selling and thus this preloaded trojan or a malware, will grant him remote access of your entire phone.

19. FAKE REVIEWS:

Precaution: Reviews for a particular site, online activity, hotels, food stuffs, products, services etc., can be manipulated and the reader of those fake reviews may be tricked into buying or taking up products that are fake or spurious or services that are par below excellence. Never trust reviews because they can be manipulated and may show a wrong picture of that product or service which may be factually incorrect. One should do more research before buying or engaging any services. Remember, reviews can be manipulated, do not trust them.

20. FAKE PROFILES WITH SEXTORTION:

Precautions: An upward trend in these crimes have been observed. Pictures and videos clicked with or without consent in the moments of privacy are used later to blackmail and or extort females for further gratification, to extort money or to get them indulged into commission of other crimes or getting them involved in criminal activities. Pictures and Videos clicked in your good times comes to haunt you when the relationship turns sour. Never ever allow anyone to click a picture or a video that you may feel

would go against you someday. Also called Revenge Porn.

21. CYBER VULTURES:

Precautions: Any financial schemes that appears to be too good to be true, should not be entered into. Avoid being lured into by false claims of the providers of such schemes. Do not get carried away by false information spread by these cheats who would by uploading their pictures having political clouts and claiming themselves to be rich and powerful and thereby deceive your rational thinking. There are no freebies mind you. When you lose money and then someone promises to make good the loss, is a bait in itself. You are sure to end up losing more money in that event for trying to recover the money that you already have lost. The situation thereafter would be hopeless. Caution! Your need and your greed should be agreed and balanced by your own prudence.

22. APP TRAPS:

Precautions: Trackers and smart watches are enabled with Health Care utilities and are now capable of recording your heart betas, pulse rates, sleeping patterns, calories burnt, miles walked by way of number of footsteps you walked throughout the day, water consumed in a day etc. Personal medical profiles are uploaded by the users to maintain a record and give them real time information on their medical condition and hygiene. Fake apps may pick up this information, keep a record of the same and may use it to your disadvantage. Very recently it was allegedly reported that Google's Play Store had about 2,000 fake apps being uploaded for the users to download for free. Apart from that, several apps are reported to transmit data to unknown servers without your permission. Beware!

23. JUICE JACKING:

Precautions: Try not to use Kiosks that provide free charging (at Malls, Airports, Public places etc.,) to the batteries of your cell phones. The charging port and the data transfer cable is one and the same for all smart phones. A small chip residing clandestinely in the Kiosk can drain your phone data while boosting up your drained batteries. Use of Power Banks is a safe bet.

24. WIFI HACKING:

Precautions: Check the level of your security by having strong password that needs to be changed often (some users still use the default password set by the providers). The most current security protocol that is in use is WPA2 (Wi-Fi Protected Access2) which implements the latest security standards which includes high grade encryption. If possible, maintain a log of people to whom you have granted access to your Wi-Fi network. Companies have their own information security policies for the use of Wi-Fi. If due to weak security/password, if a criminal manages to hack your wi-fi and commit a crime, the IP address of your router will be reflected and the police will begin enquiry from your house where you have your wi-fi router placed. In a particular case, a terrorist used an open and unprotected wi-fi of a college to send a mail to a media house, claiming responsibility for the blasts that were carried out in a city. That's dangerous, isn't it!

25. ONLINE RADICALIZATION:

Precautions: Gullible girls and women are either lured of brainwashed to join groups in the name of religion, ideology or a cause that suits the goals and ambitions of those groups. This may be done in the name of religion, for political gains, false hopes that the group members will earn name and fame in the society or may earn rewards in the eyes of God. Baits like receiving huge money, power, status, cadres, sacrifice for

a good cause etc., are used to motivate the victims. Use of fake/false information through audio/video clips are shown to provoke the victims to join the group. Cult practices are used to entice innocent and ignorant victims. By causing harm to others, one cannot do good to the society. Basic principles of humanity should be strongly imbibed in you so as to not to get carried away by such fake/false information. Avoid visiting such sites/blogs. Use prudence before falling prey to such groups. Check whether your online and offline values match.

26. HONEY TRAP

Accepting friends request from strangers and chatting with them and also putting your own privacy at risk as mentioned in the case study as above and thereafter being victimized for ransom or extortion has been on the rise. Your attitude of being casual and thinking that it's fair to share on internet may prove to be unfair and you may fall in the criminals net.

Most of such dating sites and sites which offer free chatting services claim to guard the privacy of subscribers but in actual they record your sessions, be it chat or photos or videos, and send it to servers in unknown locations and they may be used against you for extortion or for granting favors. These criminals have a simple modus operandi and that is to lure soft targets and victims especially the ones who are in depression or are going through heart break or are widows and having children or are having troubled marriage etc. These vulnerabilities are exploited by the criminals to reach their targets and crimes as mentioned here in above are committed.

27. QR HACK

Use technology that your brains can comprehend. The 'on the go' payment systems through QR code's scan, tap n pay, pull n push money etc., should be enabled on your phone only if you conceptually understand the procedure that involves in these kind of payment facilities.

Technology such as Drive by downloads etc., are making things complex for a layman to understand but in the urge to display that we are tech savvy, we fail to read the fine prints that gives away our access privileges by way of permissions and we use such payment systems freely and usually end up loosing money. Numerous frauds have been reported by use of UPI platforms. The pull and push concept of payments are being misused and the criminals are taking advantage of lack of knowledge of victims in regards UPI system. Victims are asked to download QR code's that are fake, lookalike apps that are fake and which gives away remote access of your phones and thereafter swindling victims money becomes easy.

It is better to transact money by using tested ways rather than trying fancy and untrusted ways.

Let us keep one thing in mind that an 'OTP is generated only when You have to make a payment' and hence never share your OTPs.

For receiving money, no OTP is ever generated.

One more fact is that two factor authentication is available in India. For international transactions, OTP is not generated.

28. RFID CLONING

Let us understand by breaking up the word technology 'Tech-No-Logy(let us read it as Logic). Hence if you are desirous to use 'Tech' but have 'No Logic' than privacy and security breaches are but obvious. The more tech you use in day to day life, the more logic should be used to protect yourself from misuses.

With high end scanners and readers and copiers, it is easy to copy data or make a clone of your Debit/Credit/Access cards etc., Leaving such cards unattended could cause immense problems to you if someone is revengeful. Recently it was reported that a criminal got into a stared hotel and gained entry into a room of a guest which was enabled by keyless entry ie. Card Key. CCTV cams helped to nail the culprit and he

confessed that he had a device which could store 10 virtual keys and that copying the data of the keys was as easy as tapping on the actual key.

Recently crimes were reported by use of Fast Tag that is used to pay tolls at toll plazas by the use of RFID. Reports of receiving messages by owners of the car that toll has been deducted even though the car was with the owner and had not crossed that toll plaza ever were highlighted by the media.

All our data dump is allegedly available on dark web and it is a fertile place to buy and sell such data.

29. DRONE SURVEILLANCE

Advancement in Future Technologies and its products thereof will play a dominant role in our lives.

Murphy's law says that 'When something has to go wrong, it will'. In the above case, privacy breach just cannot be avoided.

Though surveillance equipment's and CCTV cams could have detected the drones but it would be a guess if this entire incidence was avoidable.

New generation Drones are as small as a butterfly but can fly high and collect data. They are enabled with multiple payloads and can deliver, tamper, collect, snoop, block and sniff data or internet facilities and also capture, record, publish, transmit and stream live contents to the base receiver.

With Internet of Things (IoT) and Home Assistance devices like Amazons Echo and Alexa etc. our privacy is at stake all the time. Even when not commanded, these devices listen to what is being said in your house or office and the recording is uploaded onto a server without your permission and knowledge. Anything that is put up on the Internet is archived for lifetime hence your data remains on those servers.

In the world of internet, privacy breaches are very common and guarding your data is an unfathomable task.

30. SEARCH ENGINE FRAUD

This is a new age crime and trending all over. Hackers have become very ingenious and are adopting new modus operandi to fleece money from victims.

They insert/inject codes on the pages of a website and post their contact details. Unsuspecting victims looking for help would lookup at Google search and would trust the numbers of customer care/help line appearing on those sites and calls that number for help. The criminals happily agree to help them out to solve their problems and by way of social engineering gets the victims card details together with CVV (Card Verification Value- 3 digit at the back side of your card). Money is transferred or spent on international platforms and online services so no OTP is required as two factor authentication is only for transactions done within Indian boundaries. Such international transactions are done in quick successions and before the victim understands the gravity of the fraud, huge amount of money is lost.

Sometimes the criminals asks the victims to download apps or links send by them so that refund amount can be transferred, but in actual it gives away remote access of you device to them. This is far more dangerous.

As per the guidelines of RBI, if customers shares their pins/OTPs/ passwords, the banks are not liable to reimburse the money lost. It's like giving away to a stranger, your keys of a locker where your money lies.

Abstain from trusting the numbers so appearing in the search results. Take some time and lookup for other helpline or customer care numbers. Check whether as per the mail sent, the flight tickets was canceled in actual.

RBI has now provided and enabled an added feature as a Security measure for Cards wherein you can now only make use of your cards at ATMs and on Point of Sale (POS) devices within the Country.

Thus in the new debit and credit cards, features like international transactions, online transaction and contactless transactions will be disabled and a customer will have to opt for the same if they want such services by requesting the issuing bank.

31. IDN HOMOGRAPH ATTACK

The Internationalised Domain Name (IDN) homograph attack is a way a malicious party may deceive computer users about what remote system they are communicating with, by exploiting the fact that 26 alphabets of English language have different look alike representation and carries different relevance as against the actual 26 alphabet in English language.

For example, a regular user of example.com may be lured to click a link where the English alphabet "a" is replaced with the Cyrillic character

Attackers can register their own domain names that are similar to the existing web addresses using the above technique.

Attackers can send "ɑ" homographic URLs via email and social networks and they will look legitimate until the link is clicked on.

In order to best protect your device and network against phishing and malware, it is advised to use solutions that protect against IDN homograph attacks such as supporting web browsers (e.g., Firefox or Chrome) and carefully inspecting domain names for suspicious lookalike characters. Moreover, the use of network security solutions that scan traffic to identify and block IDN homograph attacks is another layer of defense that reduces the risk of accidentally accessing these potentially malicious domains.

The above mentioned frauds are very sophisticated and needs browsers to be updated and extensions to be in place. Sucheta would have been incapacitated to recognise and avert this crime as this one requires minute observations and tech support.

32. SCRATCH CARD SCAM:

This modus operandi has been in use for quite some time now but people who are not tech savvy or not literate enough to understand how technology works fall prey to such crimes.

By use of Wallets, either one can pay/transfer money (also known as push money) or alternatively one can call/request money (also known as pull money) from the person to whom such request could be sent via QR Codes.

Amrin failed to understand that the money that she thought would be paid to her was in fact a request for her to pay to the criminal.

Logically, you do not need your pin to receive money into your own account. The fraudsters do ask victims to use pin to send the money that they have sent (which actually is a request to pay money to the criminal) to transfer the amount show in the QR Code.

Golden Principle:

If you apply or use your wallets pin for any transactions, that logically means that you are making a payment to someone.

For receiving money into your account, you do not require to use your wallets pin.

So also if an OTP is generated and sent to you by your bank on your registered mobile number, that ideally means that you are going to make a payment. For receiving money, no OTP is required.

33. SIM SWAP:

SIM swap lets you move your number to a replacement SIM if your old SIM is lost, stolen or damaged, or if you need a different size SIM for your new device.

A sim is a veritable key to all your online transactions and is linked to

your banks and all your apps as well.

This fraud displays human weakness which justifies this statement, 'When ones Greed overpower ones Need', one may end up loosing something in bargain.

In order to avail the benefits of 5G connection meant only for privileged few as projected by the criminal, Arpitha fell for that bait/trap and shut her mobile for a couple of hours. The fraud was committed within that time and a new sim with forged documents was procured by the criminals. Naturally when criminal have the newly procured sim, all related and linked activities can be controlled by the criminal as the original sim is blocked. A criminal can gain unauthorised access in an authorised manner due to the new sim that's available with him.

Practically all accounts (banks, social media, apps, email etc) can be accessed and used by the criminals post initiation of 'reset password or pins'.

Despite users adopting best practices for information security, this modus operandi defeats all those purposes.

'Due Diligence' needs to adhered to by these mobile service providers before blocking the original sim and issuing a duplicate or new sim and verification should be done with the sim owner before processing any request. Time and again authorities have lambasted the acts of mobile service providers but SIM cards are yet being issued without proper verification.

Control on WhatsApp also can be initiated because now the 6 digit verification code will be sent to the new sim which the criminals have.

Sim Swap also can be initiated through IVR (Interactive Voice Response) facilities that the mobile service providers use for services. The sim owner is asked to key in digits that will allow Sim Swap through the use of IVRs and thus they loose control over their sim.

34. CRYPTOJACKING

Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. The unsuspecting victim's system may get compromised by clicking on malicious links or by infecting a website or online ad that may be loaded in victims browser with execution codes.

These crypto mining activities happen in background n hence are in a stealth mode.

Cryptojacking allows the infected machines to work for the hacker to mine cryptocurrency.

Raid consumption of power or electricity, excessive use of RAM and CPUs compared to regular usage are symptomatic and indicators that mining may be happening in the background.

Preventions:

Not clicking on links in an email or SMS originating from unknown source. Keeping an eye on processing speed of the system and also on rising electricity bills.

Install an ad-blocking or anti-cryptomining extension on web browsers.

Keep your web filtering tools up to date.

Use anti malware protection that is capable of detecting known crypto miners. Many of the anti malware vendors have added crypto miner detection to their products.

Use a mobile device management (MDM) solution to better control what's on users' devices.

35. VIDEO CONFERENCE SCAM

Preventions:
Neither host nor attendees of such meetings should share the meeting credentials in public or unknown forms.

Enable file sharing, screen sharing, video and audio communication mode and session recording option to required set of meeting participants and not all meeting participants.

In case if the number of meeting participants is high, ensure to provide a standard naming method to easily identify and avoid unwanted people from getting into the meeting.

In case of back to back meeting's enable waiting room to keep the meeting sessions separated and thereby avoid participants from entering into any session not meant for them.

36. KIDS MOBILE PHONE:

Due to pandemic, we have all been introducted to a new concept of working ie. Work From Home and so also children have to attend online lectures arranged by their schools.

This culture has forced quite a few families to share their device's, mostly mobiles, with their immediate family members for logging on to internet to attend meetings, transact business, do online banking and also children use these devices for attending online classes. After a point of time, children tend to deviate from their studies and start playing online games that give them enjoyment and thrill. The games are designed to be played for free for certain time by the providers and then once a child gets addicted, he/she would want to continue by paying for playing such games.

These games offer the winner points, stars, coins etc that could be won or bought and used to play further advance levels of those games, also would make the winner eligible to play other new games. Most of the parents have their debit/credit cards or wallets linked directly to their online bank accounts which makes it easier for a child to make payments using those links and because they have the control on the mobiles at that time, they would get the OTP for those transactions which they would smartly delete from logs after use.

Only when the parents get a bill or a bank statement, they would come to know their children's deeds.

Preventions:

Do not keep your banks accounts linked to debit/credit cards or wallets.

Opt the features of 'enable or disable' available on your devices very meticulously.

Disable features available on your cards to make international transactions and also disable it for use on POS machines (Point Of Sale) or ATM machines outside India.

Do use parental control software's and privacy settings available on Android/IOS devices.

Parents may prohibit/restrict access to particular sites by setting up filters on their devises.

Apart from virtual security, human surveillance and checks & balances should be adopted to control child's activity.

37. SMART HOMES

Ensure that you do not share the device credentials with strangers.

Always ensure to change the default device credentials.

Device firmware needs to be updated to latest versions.

Hidden cameras in bulbs etc could breach privacy of the user who would be unaware of such a crime being committed against them.

Buy products from trusted sources/platforms/portals/dealers to avoid commission of such crimes.

Privacy is a Fundamental Right and is an integral part of the right to life and liberty which is guaranteed under the Constitution.

38. MICRO LOAN

Also know as App based instant-loan or online-loaning firms through which small amounts of loans are provided for short term without documents or verification of the borrower and involves high or exorbitant interest rates that are payable.

In December 2020, 3 centres in Hyderabad who had employed nearly 600 tele-callers were raided, these companies took instructions from their heads in Jakarta.

In a swift action, the police of Hyderabad and Cyberabad arrested 17 people, including several heads of app-based instant loan companies, for their role in lending money at a high interest rate and harassing the defaulters through coercive methods.

Tele-callers were used to persuade, harass and intimidate loan defaulters at various stages.

Loan collection agents or even rowdy recovery agents were sent to threaten, bully, manhandle or insult the defaulters.

Amongst others who were arrested, a CEO of an app-based instant loan company was arrested too for 'illegal' operation and cheating borrowers.

In Hyderabad, in a case of harassment by micro loan app organisers, a 28 year old techie died by suicide. When he could not repay the loan, they began harassing him and his family members by demanding repayment and even circulated his pictures and details to all his contacts, branding him as a fraud. He could not endure the humiliation and thus ended his life.

When you apply for such loans, they ask you to install their app as it is an app based instant-loan that is being offered.

Once you install, the app asks for certain permissions and in the guise of doing so, they gain access to lots of information in the background.

The app companies also collect sensitive data such as contacts, photos,

locations and phone memory from the mobile phones of the customers and are used to defame or blackmail the customers to get the repayment. Failing to repay will encourage these providers of loans to defame the defaulter by calling up his contacts, friends, families and also post defamatory statements on their social media platforms.

Preventions: Never download personal loan apps which are unauthorised and always check users rating and review before downloading. Before signing or accepting the terms of the loan, check your EMI using a personal loan EMI calculator and compare it with the EMI amount given by the lender.

These loan providers are not registered with the RBI. The App may be unverified and fake. Terms & Conditions may be vague or misleading. They do not verify borrowers credentials and asks for processing fees before disbursement of the loan amount. Customers should not be lured by scams and instead should opt for well-known and reputed financial institutions to ensure that they are not a victim of personal loan scams.

39. BLUESNARFING

Preventions: Always keep the Bluetooth of your devices in 'Switched Off' mode when not required. In case of frequent usage of the Bluetooth, manually configure the discovery of your Bluetooth device so that the in other nearby Bluetooth devices your device name is not exhibited.

Keep your Bluetooth software's and drivers updated. Bluetooth device should be titled in a way that would not reveal your identity.

Ensure to verify every incoming request on your bluetooth device rather than accepting all incoming requests.

40. STOLEN PHONE

Remember: Our cell phone has become as important as other cells in our body. Upon realising that either you have misplaced your cell phone,

forgot your phone or maybe it got stolen, there are a few actions that one needs to take.

Firstly Block you SIM card. Inform the local police, in case your phone is lost, forgotten or misplaced, the police will issue a Loss Certificate mentioning relevant details of your cell phone.

If the phone has been stolen and if there are enough proofs and evidence to that fact, the police will register an FIR of Theft.

On your phone, always keep the Phone Finder facility 'On', so in case of above mentioned circumstances, you may be able to locate your device by logging into your computer and using the app you may be able to track down where your phone is currently located. Though accuracy differs when it comes to location finding and not all phones are to be found by such technology easily. The other way is to use your computer and remotely delete data or block access to your phone.

Approaching the police and informing them is required to absolve yourself from any liabilities originating from that device once it was out of your possession.

41. EXAM MALPRACTICE

One should not use such devices for cheating in an examination. It may put one's career at stake by indulging in such unlawful acts. There are several spy wares and surveillance devices that are available in the open market and using the same for gaining unauthorised access to commit offences or if someone provides assistance in facilitating to gain unauthorised access by use of such devise and wares, the law catches up to punish the implanter or the offender. The Information Technology Act punishes insertion of computer contaminants, spy ware are included within that definition of a contaminant. Dishonest or Fraudulent intentions for such insertion provides for imprisonment and fines.

Attention: Short cuts may cut short your career.

42. CONNECTED CAR

Internet of Things (IoT) is used by consumers or end-users. Purpose of IoT is to connect smart devices to help improve the lives of consumers. The Industrial Internet of Things (IIoT) is used for industrial purposes such as manufacturing, monitoring and supply chain management. Using smart connected devices (IoT- Internet of Things or IIoT- Industrial Internet of Things) without understanding their potential could prove to be a risk of gargantuan (colossal or huge) proportions. Fail to update or upgrade these devices and you fail to protect your data which could be hazardous and could breach or infringe upon your right to privacy and personal life and liberty. Dangers of being exposed to criminals who could gain unauthorised access to such interconnected systems through the internet, puts you at high risk.

43. DRUG TRAFFICKING

Carelessly surfing the internet and especially dark web may lead someone to be indulged in criminal activities. The Narcotic Drugs and Psychotropic Substances Act, 1985, (NDPS Act) prohibits production/manufacturing/ cultivation, possession, sale, purchasing, transport, storage, and/or consumption of any narcotic drug or psychotropic substance. Ishya has ventured into unlawful activity and depending on the type of substance and the quantity that she procured, she would be entitled to get punished under the stringent provisions of NDPS Act.

44. DOXXING

In India, disclosing of personal information or sensitive personal data or information without the consent of that person is punished under IT Act. Voyeurism is punished under IPC and IT Act and stalking is punished under IPC. Sharing of personal information or sensitive personal data or information in good times with friends or colleagues may go against the victim when times go sour. Such information could be used to defame and harass the victim and cause misery and dent future prospects of life of the victims.

45. CYBER GROOMING

Strict adherence to the principles of Cyber Hygiene is the key to save oneself from any untoward incident or an event being caused. Believing and trusting what is claimed by strangers, using the virtual world, goes against such principles of due diligence. Impetuous (careless) browsing and connecting with strangers exposes the risk of being faced with cyber crimes that could tarnish the image of the victims and also cause a dent in victims personal life, especially when the victims are of tender age (a time in one's life when they are still young and lack experience).

46. CRYPTO FRAUDS

Believing and accessing advertisements and laying trust on unverified websites (fake websites with fake reviews) and non adherence to principles of cyber security and thereafter investing huge amounts of money is an all time high risk factor. By offering freebies and/or bonus, the bait only gets stronger as laid by the criminals.

47. CYBER SEX TRAFFICKING

Misrepresentation (Identity theft or impersonation) and Misconceptions (a view or opinion that is incorrect because based on faulty thinking or understanding) prevails in cyber space in epic proportions. Victims are more vulnerable when they are facing a low self esteem while negotiating with competitive times that life puts forth as a challenge. Getting carried away or swayed away by opportune cyber criminals is high on stakes at that point of time when the victims are facing a downturn in their careers.

48. CYBERWARFARE

Such acts could be termed as Cyber Terrorism. In order to get an easy life committing such acts of cyber crimes, the offender would face a term of imprisonment and fines. Hackers who carry out such Distributed Denial of Service Attack (DDoS) on Power installations and Banking industry

which is so critical for finance and economy of a country may attract imprisonment and fines. Hackers form a syndicate to carry out such attacks which needs high sophistication to penetrate computer systems or infrastructure which has data of critical nature, which can be also called Critical Information Infrastructure (CII). Such attacks on a nations computer infrastructure would have serious repercussions and would lead to turmoil and may cause irreparable injury and losses of humungous nature to such nations. Cyber Terrorism as per the Information Technology Act, 2000 provides imprisonment which may extend to imprisonment for Life.
Attention: Right to Remedy shall be Rejected if for the offence of Hacking an accused gets Convicted.

49. HACKTIVISM

This is a case of Online Radicalisation. Wherein a particular ideology or a narrative is driven into the brains of persons and the brain washing is so enormous that the victim gets convinced with whatever information is supplied to them and they would go all out to execute the tasks allotted and thereby the victims end up committing cognizable offences. Rational thinking stops once a person gets radicalised. In such cases a victim ends up being a criminal.

50. METAVERSE

This is an age old crime transpiring in the new age virtual world, though the modus and the resultant act of offence remains the same and the experience of the victims are as bad as in real world. With Web 3.0, 5G, 3D, Artificial Intelligence (AI), Virtual Reality (VR), Augmented Reality (AR), Mixed Reality (MR) etc paving way for the participants to experience a new virtual world or a universe (Metaverse) the crimes originating in that world needs to be addressed and laws needs to be framed or interpreted to provide a logical conclusion and thereby punish the offender or the one who is guilty of committing crimes.

Where to Report Cyber-Crimes

1. Report all your cyber-crimes to your local police station that has the jurisdiction over your residence or your office premises, as the case maybe.
2. Cities having a Cyber Police Station established, cyber-crimes may be reported there and they generally have jurisdiction over the entire city (to be checked and verified before filing).
3. Online portals are also available in mega cities to register cyber-crimes complaints. At the national level, we have https://cybercrime.gov.in/
4. Districts and Mofussil areas where cyber police stations are not established, would ideally have a Cyber Cell which would register such complaints of cyber-crimes.
5. In absence of a cyber police station or a cyber cell, victims may approach a high-ranking police officer in a District or a City (Superintendent of Police or Deputy Commissioner of Police, as the case may be) to take directions with regards to registration of a cyber-crimes.
6. Every State, City, District may have a different mechanism available to register the complaints of cyber-crimes which needs to be checked with appropriate authorities.

GOOGLE ANDROID HARDENING CHECKLIST

By Yashavantha Kumar K.N, DySP

Basic Security

1 Update operating system to the latest version
2 Do not Root the device
3 Do not install applications from third party app stores
4 Enable device encryption
5 Disable 'Developer Actions'
6 Use an application/service to provide remote wipe functionality
7 Enable Android Device Manager
8 Erase all data before return, repair, or recycle

Authentication Security

9 Set a PIN and automatically lock the device when it sleeps
10 Set an alphanumeric password
11 Set Auto-Lock Timeout
12 Disable 'Make Passwords Visible'
13 Erase data upon excessive passcode failures

Browser Security

14 Show security warnings for visited sites
15 Disable 'Form Auto-Fill'
16 Do not automatically remember passwords
17 Disable browser plug-ins
18 Turn on Do Not Track

Network Security

19 Turn off Bluetooth when not in use
20 Disable network notification
21 Forget Wi-Fi networks to prevent automatic rejoin

Additional Security Settings1

22 Turn off Location Services
23 Use a third party application to password protect applications with sensitive data
24 Limit the number of text (SMS) and multimedia messages (MMS) saved
25 Disallow cookies in Chrome browser
26 Disable JavaScript in Chrome browser
27 Use TextSecure to encrypt SMS messages

APPLE IOS HARDENING CHECKLIST

Basic Security

1 Update operating system to the latest version
2 Do not Jailbreak iOS to sideload applications
3 Enable Automatic Downloads of App Updates
4 Enable remote wipe functionality
5 Enable Find My iPhone
6 Encrypt device backups through iTunes
7 Erase all data before return, repair, or recycle

Authentication Security

8 Require a passcode or password
9 Enable TouchID with a complex password
10 Set Auto-Lock Timeout
11 Disable Grace Period for Screen Lock
12 Erase data upon excessive passcode failures
13 Enable Data Protection

Browser Security

14 Enable Fraud Warning in Safari
15 Disable AutoFill for sensitive information
16 Block cookies from third parties
17 Turn on Do Not Track

Network Security

18 Turn off Ask to Join Networks
19 Turn off AirDrop when not in use
20 Turn off Bluetooth when not in use
21 Turn off Personal Hotspot when not in use
22 Forget Wi-Fi networks to prevent automatic rejoin

Additional Security Settings1

23 Turn off Location Services
24 Restrict access to Location Services, Contacts, Photos, etc.
25 Disable access to Control Center on Lock Screen
26 Disable TouchID
27 Enable Private Browsing in Mobile Safari as needed
28 Disable JavaScript in Mobile Safari

These security settings are proactive in nature but are intended for devices where there exists a very high need for security, as they may negatively impact the user experience and interfere with the functionality and utility of many applications.

OFFENCES AND RELEVANT PENAL SECTIONS

Cyber Crimes Mapping with Information Technology Act, 2000, Information Technology (Amendment) Act, 2008, IPC and Special and Local Laws.

Sl. No	Nature of complaint	Applicable section(s) and punishments under ITA 2000 & ITAA 2008	Applicable section(s) under other laws and punishment
1	Mobile phone lost/stolen	-	Section 379 IPC 3 years imprisonment or fine or both
2	Receiving stolen computer/ mobile phone/data (data or computer or mobile phone owned by you is found in the hands of someone else.)	Section 66 B of ITAA 2008 3 years imprisonment or Rupees one lakh fine or both	Section 411 IPC 3 years imprisonment or fine or both
3	Data owned by you or your company in any form is stolen	Section 66 of ITAA 2008 3 years imprisonment or fine up to rupees five lakh or both	Section 379 IPC 3 years imprisonment or fine or both
4	A password is stolen and used by someone else for fraudulent purpose.	Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh Section 66D ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC 3 years imprisonment or fine Section 420 IPC 7 years imprisonment and fine
6	An e-mail is read by someone else by fraudulently making use of password	Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	
7	A biometric thumb impression is misused	Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	
8	An electronic signature or digital signature is misused	Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	
10	A Phishing e-mail is sent out in your name, asking for login credentials	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC 3 years imprisonment or fine or both
11	Capturing, publishing, or transmitting the image of the private area without any person's consent or knowledge	Section 66E of ITAA 2008 3 years imprisonment or fine not exceeding Rupees two lakh or both	Section 292 IPC 2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction
12	Tampering with computer source Documents	Section 65 of ITAA 2008 3 years imprisonment or fine up to Rupees two lakh or both Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both	
13	Data Modification	Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both	

14	Sending offensive messages through communication service, etc.		Section 500 IPC 2 years or fine or both Section 504 IPC 2 years or fine or both Section 506 IPC 2 years or fine or both — if threat be to cause death or grievous hurt, etc. — 7 years or fine or both Section 507 IPC 2 years along with punishment under section 506 IPC Section 508 IPC 1 year or fine or both Section 509 IPC 1 years or fine or both of IPC as applicable
15	Publishing or transmitting obscene material in electronic form	Section 67 of ITAA 2008 first conviction — 3 years and 5 lakh Second or subsequent conviction— 5 years and up to 10 lakh	Section 292 IPC 2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction
16	Publishing or transmitting of material containing sexually explicit act, etc., in electronic form	Section 67A of ITAA 2008 first conviction —5 years and up to 10 lakh Second or subsequent conviction— 7 years and up to 10 lakh	Section 292 IPC 2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction
17	Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form	Section 67B of ITAA 2008 first conviction —5 years and up to 10 lakh Second or subsequent conviction— 7 years and up to 10 lakh	Section 292 IPC 2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction
18	Misusing a Wi-Fi connection for acting against the state	Section 66 3 years imprisonment or fine up to Rupees five lakh or both Section 66F— life imprisonment of ITAA 2008	
19	Planting a computer virus that acts against the state	Section 66 3 years imprisonment or fine up to Rupees five lakh or both 66F— life imprisonment	
20	Conducting a denial of service attack against a government computer	Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both Section 66F of ITAA 2008— life imprisonment of	
21	Stealing data from a government computer that has significance from national security perspective	Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both, 66F — life imprisonment	
22	Not allowing the authorities to decrypt all communication that passes through your computer or network.	Section 69 of ITAA 2008 imprisonment up to 7 years and fine	
23	Intermediaries not providing access to information stored on their computer to the relevant authorities	Section 69 of ITAA 2008 imprisonment up to 7 years and fine	

24	Failure to Block Web sites, when ordered	Section 69A of ITAA 2008 imprisonment up to 7 years and fine	
25	Sending threatening messages by e-mail		Section 506 IPC 2 years or fine or both
25	Word, gesture or act intended to insult the modesty of a woman		Section 509 IPC 1 years or fine or both – IPC as applicable
26	Sending defamatory messages by e-mail		Section 500 IPC 2 years or fine or both
27	Bogus Web sites, cyber frauds	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC 3 years imprisonment or fine Section 420 IPC 7 years imprisonment and fine
28	E-mail Spoofing	Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC 2 years or fine or both Section 468 IPC 7 years imprisonment and fine
29	Making a false document	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC 2 years or fine or both
30	Forgery for purpose of cheating	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC 7 years imprisonment and fine
31	Forgery for purpose of harming reputation	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section. 469 IPC 3 years and fine
32	E-mail Abuse		Sec. 500 IPC 2 years or fine or both
33	Punishment for criminal intimidation		Sec. 506 IPC 2 years or fine or both – if threat be to cause death or grievous hurt, etc. – 7 years or fine or both
34	Criminal intimidation by an anonymous communication		Sec. 507 IPC 2 years along with punishment under section 506 IPC
35	Copyright infringement	Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both	Sec. 63, 63B Copyrights Act 1957
36	Theft of Computer Hardware		Sec. 379 IPC 3 years imprisonment or fine or both
37	Online Sale of Drugs		NDPS Act
38	Online Sale of Arms		Arms Act

Disclaimer: The above-mentioned explanations made herein are to the best of our knowledge and interpretations and are purely for academic and information purpose only. They may be used as a guiding force. They should not be construed as legal opinion by any stretch of imagination. We are thankful to all the stake holders for uploading information which we may have used for education purpose only.

GLOSSARY

A

Antivirus

Antivirus software is used to monitor a computer or network, to detect cyber security threats ranging from malicious code to malware. As well as alerting you to the presence of a threat, antivirus programs may also remove or neutralise malicious code.

Artificial Intelligence (AI)

(AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. Unfortunately, that same technology can be deployed by cybercriminals, which has forced cybersecurity experts to work even harder to stay ahead of the latest attack strategies.

Authentication

The process of verifying the identity or other attributes of a user, process or device.

B

Backdoor

An undocumented, private, or less-detectible way of gaining remote access to a computer, bypassing authenticiation measures, and obtaining access to plaintext.

Bitcoin

Cryptocurrency, a form of electronic cash created by Satoshi Nakamoto.

Blacklist

A list of entities (users, devices) that are either blocked, denied privileges or access.

Blockchain

A blockchain is a write-only database, dispersed over a network of interconnected computers, that uses cryptography to create a tamperproof public record of transactions. Because blockchain technology is transparent, secure and decentralized, a central actor cannot alter the public record.

Bot

A computer connected to the Internet that has been compromised with malicious logic to undertake activities under the command and control of a remote administrator.

Botnet

A network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge.

Breach

The unauthorised access of data, computer systems or networks.

Bring your own device (BYOD)

A strategy or policy whereby an organisation permits employees to use their personal devices for work purposes.

Brute force attack

An attack in which computational power is used to automatically enter a vast quantity of number combinations in order to discover passwords and gain access.

Bug

A relatively minor defect or flaw in an information system or device.

C

CAPTCHA

A test that distinguishes between robots and humans using a website where you have to "prove you're human".

Catfishing

Creating a fake identity on a social network account, usually a dating website, to target a specific victim for deception.

CISO

Acronym for Chief Information Security Officer is a senior-level executive job in a company, in the IT or cyber security department. A CISO's responsibilities include ensuring and maintaining adequate protection for the company's assets and technology, in terms of both strategy and development, to mitigate and manage cyber security risks. CSO (Chief Security Officer) is another name used for the same job.

Cookie

A segment of data sent by an Internet server to the browser that is returned to the browser every time it accesses the server. This is used to identify the user or track their access to the server. Initially, cookies were used to stay logged in but are now commonly used for tracking.

Cryptography

The study of encoding. Also, the use of code/cipher/mathematical techniques to secure data and provide authentication of entities and data.

Cyber attack

Deliberate and malicious attempts to damage, disrupt or gain access to computer systems, networks or devices, via cyber means.

Cyber incident

A breach of a system or service's security policy.

D

Data breach

The unauthorised movement or disclosure of information, usually to a party outside the organisation.

Data integrity

The quality of data that is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

Data loss

No longer having data, whether because it has been stolen, deleted, or its location forgotten

Data security

The measures taken to protect confidential data and prevent it from being accidentally or deliberately disclosed, compromised, corrupted or destroyed.

Darkweb

The dark web refers to websites and online content that exists outside the reach of traditional search engines and browsers. This content is hidden by encryption methods (in most cases, these sites use the Tor encryption tool to hide their identity and location) and can only be accessed with specific software, configuration settings or pending approval from their admins. The dark web is known for being a hub for illegal activities (drug and crime transactions, dark hat hacking and so on).

Decryption

The process of deciphering coded text into its original plain form.

Denial of service (DoS)

This is a type of cyber attack that prevents the authorised use of

information system services or resources, or impairs access, usually by overloading the service with requests.

Dictionary attack

Known dictionary words, phrases or common passwords are used by the attacker to gain access to your information system. This is a type of brute force attack.

Digital Signature

A digital signature is a technique used to encrypt and validate the authenticity and integrity of a message, software or digital document. The digital signature is difficult to duplicate by a hacker, that's why it is important in information security.

Distributed denial of service (DDoS)

A denial of service technique where multiple systems are used to perform the attack, overwhelming the service.

Download attack

Malicious software or a virus that is installed on a device without the user's knowledge or consent – sometimes known as a drive-by download.

E

Electronic warfare (EW)

The use of energy, such as radio waves or lasers, to disrupt or disable the enemy's electronics. An example would be frequency jamming to disable communication equipment.

Encode

The use of a code to convert plain text to cipher text.

Encryption

The use of a cipher to protect information, making it unreadable to anyone who doesn't have the key to decode it.

Endpoint

A collective term for internet-capable computer devices connected to a network – for example, modern smartphones, laptops and tablets are all endpoints.

Ethical hacking

The use of hacking techniques for legitimate purposes – i.e. to identify and test cyber security vulnerabilities. The actors in this instance are sometimes referred to as 'white hat hackers'.

Exfiltration

The transfer of information from a system without consent.

Exploit

The act of taking advantage of a vulnerability in an information system. Also used to describe a technique that is used to breach network security.

F

Firewall

A virtual boundary surrounding a network or device that is used to protect it from unwanted access. Can be hardware or software.

G

Gateway

An intermediate system that is the interface between two computer

networks. A gateway can be a server, firewall, router, or other device that enables data to flow through a network.

GDPR

General Data Protection Regulations. European legislation designed to prevent the misuse of data by giving individuals greater control over how their personal information is used online.

H

Hacker

Someone who breaks into computers, systems and networks.

Hashing

Using a mathematical algorithm to disguise a piece of data.

Honeypot (honeynet)

A decoy system or network that serves to attract potential attackers, protecting actual systems by detecting attacks or deflecting them. A good tool for learning about attack styles. Multiple honeypots form a honeynet.

I

Incident

Any breach of the security rules for a system or service. This includes attempts to gain unauthorised access, the unauthorised use of systems for the processing or storing of data, malicious disruption or denial of service, and changes to a system's firmware, software or hardware without the owner's consent.

Incident response plan

A predetermined plan of action to be undertaken in the event of a cyber incident.

Indicator

A signal that a cyber incident may have occurred or is in progress.

Insider threat

A malicious threat to a group or organization that comes from someone within, like an employee, contractor, or business associate, who has insider information regarding the organization's data, computer systems, or security measures.

Internet of things (IoT)

The ability of everyday objects, such as kettles, fridges and televisions, to connect to the internet.

Intrusion Detection System/Intrusion Detection and Prevention (IDS/IDP)

Hardware or software that finds and helps prevent malicious activity on corporate networks.

IP address

Also known as an Internet Protocol address, is the string of numbers used to identify each computer using the internet on a network.

IP spoofing

A tactic used by attackers to supply a false IP address in an attempt to trick the user or a cyber security solution into believing it is a legitimate actor.

J

Jailbreak

The removal of a device's security restrictions, with the intention of installing unofficial apps and making modifications to the system. Typically applied to a mobile phone.

Javascript

A language used to create and control the content on a website, allowing you to program the behavior of web pages to do a specified action.

K

Key

The numerical value used to encrypt and decrypt cipher text.

Keylogger

A type of software or hardware that tracks keystrokes and keyboard events to monitor user activity.

L

Logic bomb

A piece of code that carries a set of secret instructions. It is inserted in a system and triggered by a particular action. The code typically performs a malicious action, such as deleting files.

M

Malicious code

Program code designed for evil. Intended to hurt the confidentiality,

integrity or availability of an information system.

Malvertising

The use of online advertising to deliver malware.

Malware

Short for malicious software. Any viruses, Trojans, worms, code or content that could adversely impact organisations or individuals.

Man-in-the-middle Attack (MitM)

Cyber criminals interpose themselves between the victim and the website the victim is trying to reach, either to harvest the information being transmitted or alter it. Sometimes abbreviated as MITM, MIM, MiM or MITMA.

Mitigation

The steps taken to minimise and address cyber security risks.

Mobile Device Management (MDM)

Mobile device management (MDM) is a type of security software, specifically for monitoring, managing and securing mobile, tablet and other devices, allowing remote administration and management of the device.

N

Netiquette

(short for network etiquette) is a collection of best practices and things to avoid when using the Internet, especially in communities such as forums or online groups. This is more of a set of social conventions that aim to make online interactions constructive, positive and useful. Examples include: posting off-topic, insulting people, sending or posting spam, etc.

O

Obfuscation

In cyber security, obfuscation is a tactic used to make computer code obscure or unclear, so that humans or certain security programs (such as traditional antivirus) can't understand it. By using obfuscated code, cyber criminals make it more difficult for cyber security specialists to read, analyze and reverse engineer their malware, preventing them for finding a way to block the malware and suppress the threat.

P

Packet sniffer

Software designed to monitor and record network traffic. It can be used for good or evil – either to run diagnostics and troubleshoot problems, or to snoop in on private data exchanges, such as browsing history, downloads, etc.

Passive attack

Attackers try to gain access to confidential information in order to extract it. Because they're not trying to change the data, this type of attack is more difficult to detect – hence the name 'passive'.

Password sniffing

A technique used to harvest passwords by monitoring or snooping on network traffic to retrieve password data.

Patching

Applying updates (patches) to firmware or software, whether to improve security or enhance performance.

Paylad

The element of the malware that performs the malicious action – the cyber security equivalent of the explosive charge of a missile. Usually spoken of in terms of the damaging wreaked.

Penetration testing

A test designed to explore and expose security weaknesses in an information system so that they can be fixed.

Personally Identifiable Information (PII)

The data that enables an individual to be identified.

Pharming

An attack on network infrastructure where a user is redirected to an illegitimate website, despite having entered the right address.

Phishing

Mass emails asking for sensitive information or pushing them to visit a fake website. These emails are generally untargeted.

Proxy server

A go-between a computer and the internet, used to enhance cyber security by preventing attackers from accessing a computer or private network directly.

Q

Quantum computing

A quantum computer can process a vast number of calculations simultaneously. Whereas a classical computer works with ones and zeros, a quantum computer will have the advantage of using ones, zeros and "superpositions" of ones and zeros. Certain difficult tasks

that have long been thought impossible for classical computers will be achieved quickly and efficiently by a quantum computer.

R

Ransomware

Ransomware is a type of malware (malicious software) which encrypts all the data on a PC or mobile device, blocking the data owner's access to it.

ReCAPTCHA

A service from Google that works to protect websites from spam and abuse caused by robots. A user is presented with a Turing test to distinguish them from a robot.

Red team

A group authorised and organised to emulate a potential adversary's attack or exploitation capabilities against an enterprise's cyber security posture.

Redundancy

Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

Remote Access Trojan (RAT)

Remote Access Trojans (RATs) use the victim's access permissions and infect computers to give cyber attackers unlimited access to the data on the PC.

Rootkit

A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence

of the tools, maintain the access privileges, and conceal the activities conducted by the tools

S

Secret key

A cryptographic key that is used for both encryption and decryption, enabling the operation of a symmetric key cryptography scheme.

Security Operations Center (SOC)

A central unit within an organisation that is responsible for monitoring, assessing and defending security issues.

Smishing

Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.

Social engineering

Manipulating people into carrying out specific actions or divulging information that is of use to an attacker. Manipulation tactics include lies, psychological tricks, bribes, extortion, impersonation and other type of threats. Social engineering is often used to extract data and gain unauthorised access to information systems, either of single, private users or which belong to organisations.

Software as a service (SaaS)

Describes a business model where consumers access centrally-hosted software applications over the Internet.

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spear phishing

Spear phishing is a cyber attacks that aims to extract sensitive data from a victim using a very specific and personalised message designed to look like it's from a person the recipient knows and/or trusts.

Spoofing

Faking the sending address of a transmission to gain unauthorised entry into a secure system.

Spyware

Spyware is a type of malware designed to collect and steal the victim's sensitive information, without the victim's knowledge.

SQL injection

This is a tactic that uses code injection to attack applications that are data-driven. The maliciously injected SQL code can perform several actions, including dumping all the data in a database in a location controlled by the attacker. Through this attack, malicious hackers can spoof identities, modify data or tamper with it, disclose confidential data, delete and destroy the data or make it unavailable. They can also take control of the database completely.

SSL / Secure Sockets Layer

This is an encryption method to ensure the safety of the data sent and received from a user to a specific website and back. Encrypting this data transfer ensures that no one can snoop on the transmission and gain access to confidential information, such as card details in the case of online shopping. Legitimate websites use SSL (start with https). Users should avoid inputting their data in websites that don't use SSL.

Steganography

A way of encrypting data, hiding it within text or images, often for malicious intent.

Symmetric key

A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt plain text and decrypt cipher text, or create a message authentication code and to verify the code.

T

Threat analysis

The detailed evaluation of the characteristics of individual threats.

Threat assessment

The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.

Threat hunting

Cyber threat hunting is the process of proactively searching across networks and endpoints to identify threats that evade existing security controls.

Threat management

There is no silver bullet to prevent 100% of cyber threats. Successful threat management requires a multi-layered approach encompassing prevention, detection, response and recovery.

Threat monitoring

During this process, security audits and other information in this category are gathered, analysed and reviewed to see if certain events in the information system could endanger the system's security. This is a continuous process

Tracking cookie

This type of cookies are places on users' computers during web browsing sessions. Their purpose is to collect data about the user's browsing preferences on a specific website, so they can then deliver targeted advertising or to improve the user's experience on that website by delivering customized information.

Trialware

Software that can only be run for a limited amount of time before it expires.

Trojan horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program.

Two-factor authentication (2FA)

The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

U

Unauthorised access

Any access that violates the stated security policy.

URL injection

A URL (or link) injection is when a cyber criminal creates new pages on a website owned by someone else that contain spam words or links. Sometimes, these pages also contain malicious code that redirects your users to other web pages or makes the website's web server contribute to a DDoS attack. URL injection usually happens because of vulnerabilities in server directories or software used to operate the website, such as an outdated WordPress or plugins.

V

Virtual Private Network (VPN)

An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

Virus

Programs that can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.

Visual Hacking

Also called "shoulder surfing" or "screen snooping," visual hacking occurs when someone steals sensitive information or credentials by physically looking at someone's screen. This could involve glancing at a computer monitor or picking up an unattended smartphone or tablet. While there are many security measures designed to combat conventional cyberattacks, visual hacking requires innovative strategies like screen protectors or continuous biometric authentication.

Vulnerability

A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.

W

Wabbits

A wabbit is one of four main classes of malware, among viruses, worms and Trojan horses. It's a form of computer program that repeatedly replicates on the local system. Wabbits can be programmed to have malicious side effects. A fork bomb is an example of a wabbit: it's a form

of DoS attack against a computer that uses the fork function. A fork bomb quickly creates a large number of processes, eventually crashing the system. Wabbits don't attempt to spread to other computers across networks.

Water-holing (watering hole attack)

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling

Highly targeted phishing attacks (masquerading as a legitimate emails) that are aimed at senior executives.

White team

A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

Whitelist

A list of entities that are considered trustworthy and are granted access or privileges.

Worm

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread

X

Xafecopy

Malware particularly found embedded in a variety of mobile apps, most commonly in battery optimizers, without the knowledge or consent of the user, ultimately subscribing the phone to a number of services which charge money directly to the user's mobile phone bill.

XSS Attack

An abbreviation of cross-site scripting, Cross-Site Scripting attacks is a method in which malicious scripts are injected into an otherwise trusted web site. An attacker can use XSS to send a malicious script to an unsuspecting user.

The user's browser has no way to know that the script should not be trusted, and will execute the script since it thinks the script came from a trusted source.

Y

Y2K

Stands for "year 2000". This abbreviation is well known today because of the term "the Y2K problem" or "the millennium bug". The Y2K problem stemmed from fears of computer programs that store year values as two-digits figures-"97" to mean the year 1997, for example—would cause problems as the year 2000 rolls in.

Z

Zero-day

Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

Zombie

A zombie computer is one connected to the Internet that, in appearance, is performing normally, but can be controlled by a hacker with remote access to it who sends commands through an open port. Zombies are mostly used to perform malicious tasks, such as spreading spam or other infected data to other computers, or launching DoS (Denial of Service) attacks, with the owner being unaware of it.

HELPLINE NUMBERS

Cyber Crime Helpline	: 1930
National Emergency Number	: 112
Police	: 100
Women Helpline	: 1091
Mental Health Helpline	: 1800-599-0019
iCall Suicide Helpline	: 9152987821
Fire	: 101
Ambulance	: 102
Disaster Management Service	: 108

Are you Certified?

Now that you have gone through the Cyber Safe Girl book, its time to learn a little more about all the Cyber Crimes and take the grand test!

Upon successfully completing, you get "I Am Cyber Safe" Certificate which is valid for 1 year!

www.cybersafegirl.com

SURE PASS

CYBER PATRIOT

Indian Cyber Institute

CYBER JAGRITHI

Supported by

ISEA

Information Security Education & Awareness

Beti Bachao Cyber Crime Se...

9 789353 820305

Don't be a victim of cyber crime.

www.cybersafegirl.com

Be a #CyberSafeGirl