SURE PASS

CYBER PATRIOT

Indian Cyber Institute

CYBER JAGRITI

trescon

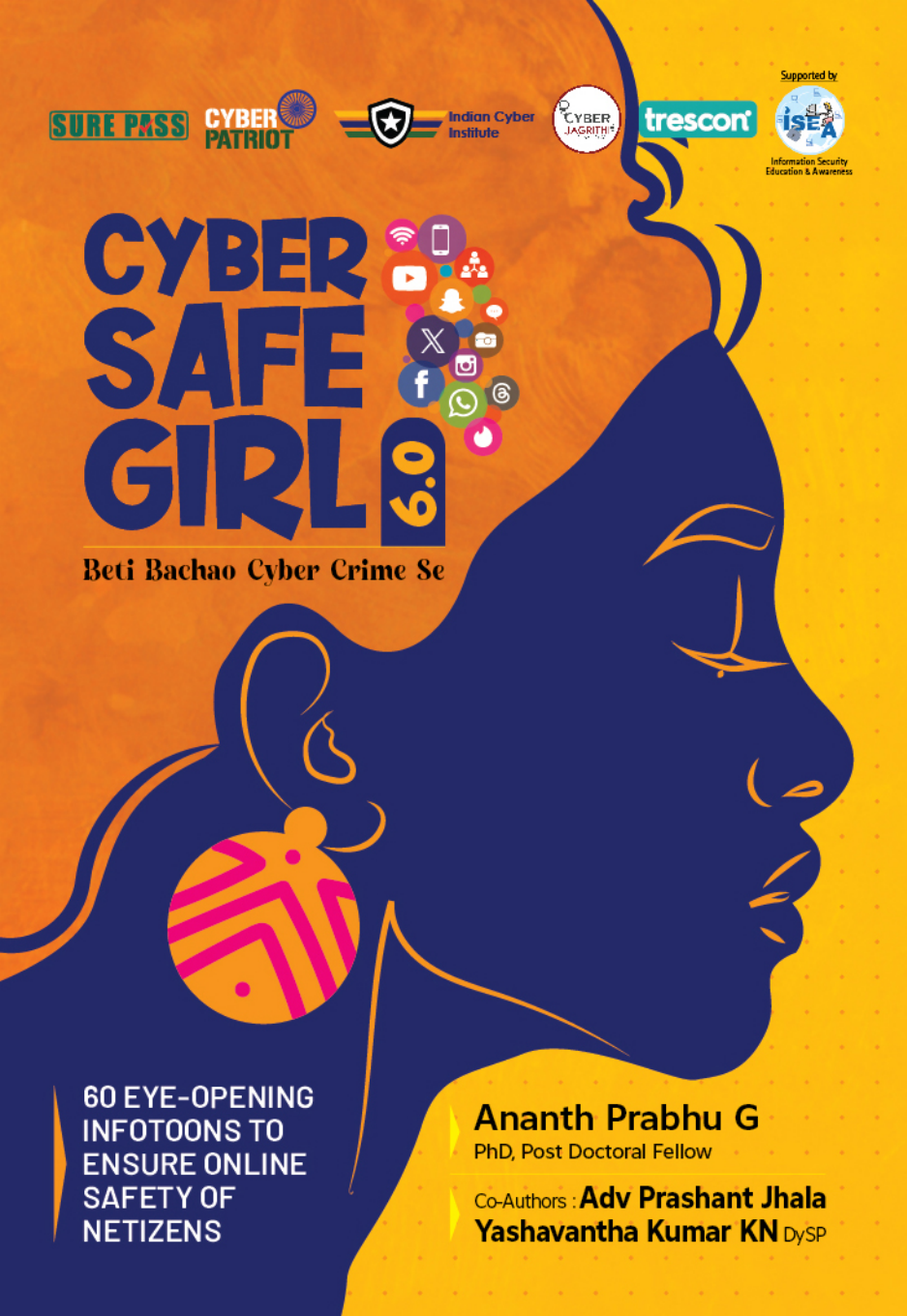
Supported by

ISEA

Information Security Education & Awareness

CYBER SAFE GIRL 6.0

Beti Bachao Cyber Crime Se



60 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

trescon

Connecting Businesses With Opportunities

- Facilitating Investments
- Driving Innovation
- Promoting Sustainability
- Propagating Technologies
- Fostering Communities
- Creating Business Opportunities
- Delivering Social Impact
- Stimulating Economic Growth

Futuristic Events	Managed B2B Events
Bespoke Events	Education & Training

UAE | INDIA | SINGAPORE | SAUDI ARABIA | INDONESIA
MAURITIUS | QATAR | THAILAND

tresconglobal.com

SMART 1,000

An Initiative by

YUVA UNSTOPPABLE

Aiming to transform over 1,000 Anganwadis across rural areas of India into hygienic & smart classrooms.

yuvaunstoppable.org

In partnership with

trescon foundation

Bridging the digital divide between students in rural and urban areas and enabling access for a level playing field

trescon foundation.com

CLEAN & SMART CLASSROOMS FOR A BETTER INDIA

trescon foundation.com

CYBER SAFE GIRL 6.0

Beti Bachao Cyber Crime Se

60 EYE-OPENING INFOTOONS
TO ENSURE ONLINE SAFETY
OF NETIZENS

Title: Cyber Safe Girl

Version: Sixth

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

Avinash Pandey
IPS

Amit Vasava
IPS

Narasimha V T
KSPS

M C Kavitha
KSPS

Ravishankar
KSP

Gopalkrishna K
KSP

Special Thanks to

Dr Manjunath Bhandary, MLC

Ch A S Murty
ISEA Team

Dr Varadraj G

Sheikh Salim
Director- Overseas

Nisheeth Dixit

Vivek Shetty

CA Mohan Vishwa

Jagadish R Chandra

Naveen Kumar

Vaikunt Prabhu

Dr Mustafa B
Tech Resource

Rohan Don
Web Architect

Yashwanth A S

Chaithra K M

Anudeep Karkera
Artist

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

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

1. MOBILE RECHARGE SHOP
2. DEBIT CARD CLONING
3. KEYLOGGER
4. SMS SPOOFING
5. CALL SPOOFING
6. RANSOMWARE
7. CYBER STALKING
8. PICTURE MORPHING
9. PROFILE HACKING
10. ONLINE GAMES
11. JOB CALL LETTER
12. DEEPFAKES
13. DATING WEBSITE
14. CAMERA HACKING
15. SOCIAL TROLLING
16. PONZI SCHEME
17. FAKE MATRIMONIAL PROFILE
18. MOBILE REPAIR SHOP
19. FAKE REVIEWS
20. FAKE PROFILE WITH SEXTORTION
21. CYBER VULTURES
22. APP TRAPS
23. JUICE JACKING
24. WIFI HACKING
25. ONLINE RADICALIZATION
26. HONEY TRAP
27. QR CODE SCAM
28. RFID CLONING
29. DRONE SURVEILLANCE
30. SEARCH ENGINE RESULTS SCAM

Topics

31. IDN HOMOGRAPH ATTACK
32. SCRATCH CARD SCAM
33. SIM SWAP
34. CRYPTOJACKING
35. VIDEO CONFERENCE SCAM
36. KIDS MOBILE PHONE
37. SMART HOMES
38. MICRO LOANS
39. BLUE SNARFING
40. STOLEN PHONE
41. EXAM MALPRACTICE

42. CONNECTED CAR
43. DRUG TRAFFICKING
44. DOXING
45. CYBER GROOMING
46. CRYPTO FRAUDS
47. CYBER SEX TRAFFICKING
48. CYBERWARFARE
49. HACKTIVISM
50. METAVERSE
51. SESSION HIJACKING ATTACK
52. PROMPT ENGINEERING
53. FILELESS ATTACKS
54. DELIVERY SCAM
55. VIRTUAL KIDNAPPING
56. FORMJACKING
57. CYBERSQUATTING
58. DNS HIJACKING
59. SMS BOMBING
60. INSIDER THREATS

FOREWORD

Cyberspace has become the real world in today's society, where cyber identities hold a greater fascination than real identities. With the growing trend of people connecting, expressing emotions, and conducting transactions online, it is crucial to be aware of the vulnerabilities present in cyberspace.

Throughout my extensive tenure as 4 time MLA and Minister of various departments, I have witnessed numerous instances of girls falling victim to various cyber offenses. As human relationships increasingly involve online connections, the impact of cyber offenses extends far beyond monetary or property loss, often leaving lasting effects on lives.

I am pleased to see that the Cyber Safe Girl 6.0 resource simplifies the understanding of girls' vulnerability in cyberspace. The engaging illustrations and informative cartoons ensure the content remains relevant and dynamic. I am confident that this book will serve as a comprehensive guide for the majority of girls in the new millennial generation, empowering them to become savvy users of technology. Let us hope that this book aids girls in developing their digital intelligence.

Warm Regards,

U T Khader
Honorable Speaker
Karnataka Legislative Assembly

BEST WISHES

In a world where everything can be connected, from intelligent fridges to driverless cars, technology plays a prominent role in all our personal and professional lives. However, this offers multiple platforms for cyber attackers.

Given the rapidly growing number of devices with internet and communication protocol addresses, cybersecurity has never been more challenging and crucial.

Instead of solely discussing the increasing and evolving types of threats and attacks, we should focus on solutions, beginning with education and awareness.

This book aims to create awareness among women and children on proactively identifying and avoiding potential cybercrimes.

Cyber safety is a collective responsibility. Let's own it.

Warm Regards,

Mohammed Saleem
Founder & Chairman, Trescon

Naveen Bharadwaj
CEO, Trescon

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 6.0 has come out very well and it would definitely help millions of girls and netizens. The 60 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)

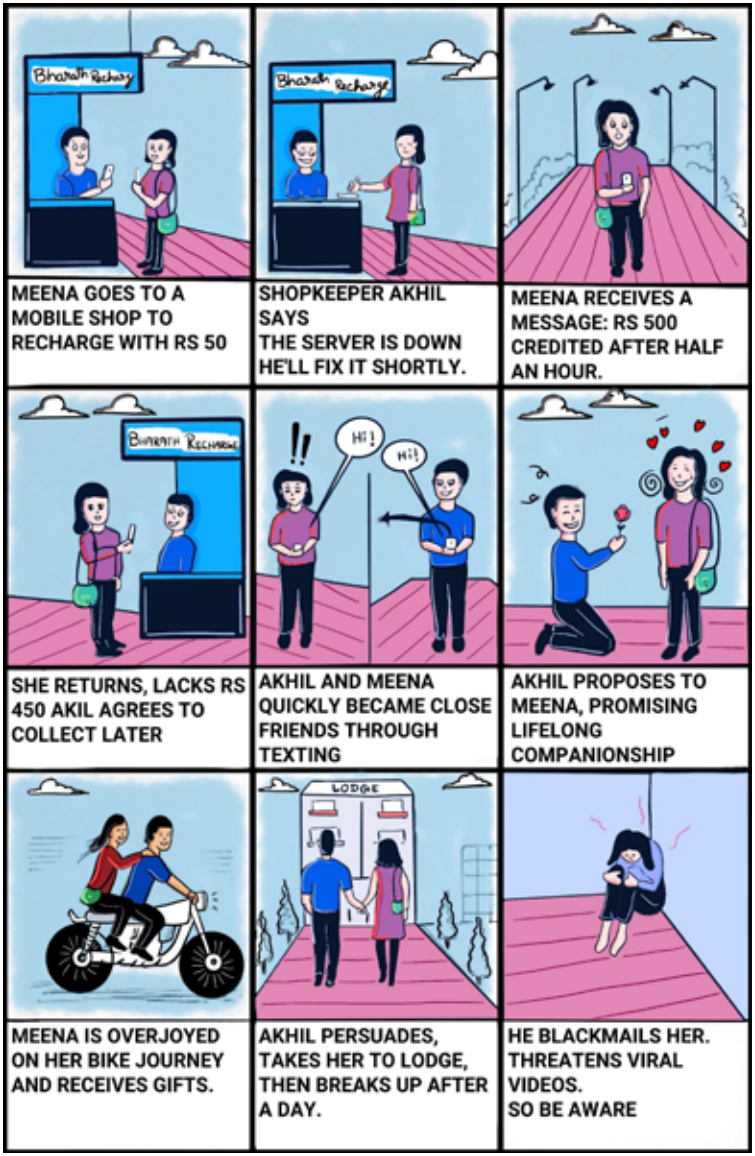
IPC Section 109 - Punishment for abetment

IPCSection 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 WITH RS 50
Bharath Recharge
SHOPKEEPER AKHIL SAYS
THE SERVER IS DOWN
HE'LL FIX IT SHORTLY.
MEENA RECEIVES A MESSAGE: RS 500 CREDITED AFTER HALF AN HOUR.
Bharath Recharge
SHE RETURNS, LACKS RS 450 AKIL AGREES TO COLLECT LATER
Hi!
Hi!
AKHIL AND MEENA QUICKLY BECAME CLOSE FRIENDS THROUGH TEXTING
AKHIL PROPOSES TO MEENA, PROMISING LIFELONG COMPANIONSHIP
MEENA IS OVERJOYED ON HER BIKE JOURNEY AND RECEIVES GIFTS.
LODGE
AKHIL PERSUADES, TAKES HER TO LODGE, THEN BREAKS UP AFTER A DAY.
HE BLACKMAILS HER. THREATENS VIRAL VIDEOS.
SO BE AWARE

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

Section 43: This section deals with unauthorized access tocomputer systems, data breaches, and other computer-relatedoffenses.

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.

Section 72A – This section deals with the punishment for disclosingpersonal information obtained in the course of providing servicesunder the terms of lawful contract.

Section 84A – This section empowers the Central Government toprescribe modes or methods for encryption.

Cloning may blow up your Earnings!


MEENA AND REENA WERE COLLEGE CLASSMATES WHO STUDIED TOGETHER.
MEENA'S BOYFRIEND ARJUN, A DRUG ADDICT, FREQUENTLY SEEKS MONEY FROM HER.
MEENA HOPED ARJUN WOULD CHANGE, BUT HE KEPT USING THREATS TO BORROW MONEY.
MEENA ASKS REENA FOR 7500; REENA TRUSTS AND SHARES ATM CARD & PIN.
MEENA RETURNS, AND REENA RECEIVES A RS. 500 DEBIT ALERT 15 MINUTES LATER.
A WEEK LATER, REENA RECEIVES AN UNEXPECTED RS. 500 DEBIT, LEAVING HER SHOCKED.
MEENA BORROWED AN ATM CARD, WHICH ARJUN ACCEPTED WHILE WAITING OUTSIDE.
HE USED A SKIMMING DEVICE, COPIED THE CARD, WITHDREW WITH PIN AFTER A WEEK.
SO, KEEP ATM CARD AND PIN PRIVATE AND PROTECT YOUR PERSONAL INFORMATION.

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 43 – Deals with unauthorized access, damage to computer systems, and data.

Section 66 – Computer Related Offences

Stealing personal information: IT Act

Section 66C – Punishment for Identity Theft

Creating fake profile & posting private conversation : IT Act

Section 66C – Punishment for Identity Theft

Section 66D – Punishment for cheating by personation by using computer resources

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

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

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

Section 72 – Breach of Confidentiality and Privacy

Section 79 – Intermediary Liability Protection

IPC Sections:

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, CLOSE FRIENDS, SHARE A PG ROOM AND WORK AT THE SAME MNC.
BOTH DEVELOP STRONG FEELINGS FOR BOSS VIVEK: A COINCIDENTAL WORKPLACE CRUSH.
FIRST POOJA PROPOSED AND VIVEK ACCEPTS. THEY COMMENCE A STRONG ROMANTIC RELATIONSHIP.
ANUSHA, WHO IS HEARTBROKEN, WISHES TO OFFER POOJA A MEMORABLE LIFE LESSON.
ANUSHA SECRETLY INSTALLS KEYLOGGER ON POOJA'S LAPTOP.
NOW ANUSHA HAS ACCESS TO POOJA'S PASSWORDS, PHOTOS, CHATS, EMAILS, AND BROWSING HISTORY UNKNOWINGLY.
ANUSHA SHARES PRIVATE CONVERSATION, PHOTOS ON SOCIAL MEDIA USING FAKE PROFILE, UPSETTING POOJA'S PARENTS.
VIVEK WAS STUNNED AND BROKE UP WITH POOJA, NOW SHE WAS TOTALLY HEART BROKEN
POOJA REGRETS NOT SECURING HER PC WITH A PASSWORD AND ANTIVIRUS.

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
Section 465 – Making a false document(FORGERY)
Section 419 – Punishment for cheating by personation
IT Act
Section 43 – While not directly related to SMS spoofing, this sectiondeals with unauthorized access to computer systems, which couldapply if someone gains unauthorized access to systems for the purposeof carrying out SMS spoofing.
Section 43A and Section 72A: These sections deal with thecompensation for failure to protect data and confidentiality ofinformation. If SMS spoofing leads to a breach of sensitive information, these sections might come into play.
Section 66C – This section deals with identity theft. If SMS spoofing isused to impersonate someone else and commit fraud or deceiveothers, it could be covered under this section.
Section 66D – Punishment for cheating by personation by using computer resource
Section 66E – This section addresses violations of privacy and thecapturing, publishing, or transmitting of images of a private area of anyperson without their consent. If SMS spoofing is used to invadesomeone's privacy in this manner, this section could apply.

SMS are Spoofed by Cyber Crooks!


AISHWARIYA, AN ACTIVE SHOPPER, WAS A PREMIUM MEMBER OF SEVERAL E-COMMERCE WEBSITES.
SHE PATIENTLY WAITED FOR THE RIGHT OFFERS, MAKING PURCHASES AND REDEEMING COUPON CODES.
ONE DAY AISHWARIYA GETS A RS 5000 HANDBAG FROM WALMART FOR RS 500.
WALMART TEXT AISHWARIYA, ALLOWING HER TO USE THE OFFER TWICE FOR ONLINE PAYMENTS ONLY, NOT CASH ON DELIVERY.
BANK
BEFORE COMPLETING THE ONLINE TRANSACTION, AISHWARYA RUSHES TO THE BANK AND DEPOSITS RS1000.
AFTER A MONTH, AS THE PRODUCTS ARE STILL NOT DELIVERED, SHE CALLS THE HELPLINE FOR INQUIRY.
THEN SHE REALIZES THE CLICKED LINK WAS A FAKE URL, ITS A CLEAR CASE OF PHISHING AND MESSAGE SPOOFING.
DISCOUNT 90%
SHE LEARNS TO STAY VIGILANT AND VERIFY UNBELIEVABLE OFFERS WITH MASSIVE DISCOUNTS.
DANGER NIGERIAN -SCAM-
BEWARE OF NIGERIAN SCAM MESSAGES FLOODING THE INTERNET; STAY CAUTIOUS AND PROTECT YOURSELF.

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
Section 66C – Identity Theft : This section of the Information Technology Act deals with identity theft, which includes dishonestly orfraudulently making use of the electronic signature, password or anyother unique identification feature of any other person. Call spoofingcan fall under the ambit of this section if it involves stealing someone'sunique identification feature for wrongful gain.

Additionally, Section 66D – Cheating by Personation using Computer Resource can also be applied. This section addresses cheating by personation through the use of a computer resource. If call spoofing is done with the intention to cheat or deceive someone, it could potentially fall under this section.

Call Spoofing is always with criminal intent!


SHABANA, A WIDOW, LIVES ALONE IN HER INDEPENDENT HOUSE.
TO KEEP HERSELF OCCUPIED, SHABANA SURFS THE INTERNET AND IS HIGHLY ACTIVE ON SOCIAL MEDIA.
UNAWARE OF SOCIAL ENGINEERING, SHABANA USED TO ACCEPT FRIEND REQUESTS FROM ANYONE WITH MUTUAL FRIENDS ON SOCIAL MEDIA.
SHABANA'S SON MAKES AN EMERGENCY CALL, REQUESTING 1 LAKH TO BE TRANSFERRED TO HIS FRIEND'S ACCOUNT.
AFTER VERIFYING HER SON'S VALID NUMBER. SHABANA ADDS THE BENEFICIARY AND THE TRANSFERS THE AMOUNT.
9876xxxxx
AFTER THE TRANSFER, SHABANA CALLS HER SON TO CONFIRM IF AMOUNT REFLECTS IN HIS ACCOUNT OR NOT?
SHAFIQ IS SURPRISED AS HE HAD NOT CALLED HIS MOTHER AT ALL.
SHABANA REALIZES SHE FELL VICTIM TO CALL SPOOFING AND TRANSFERRED MONEY TO A SCAMSTER.
BEWARE OF SCAMMERS USING FAKE PHONE NUMBERS.

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 43 – This section deals with unauthorized access, damage tocomputer systems, and data breaches.

IT Act Section 66 – Computer related offences

Section 66C – This section deals with identity theft.

Section 66D – This section deals with cheating by impersonation usinga computer resource.

Demand without payment :

IPC Section 384 – Extortion

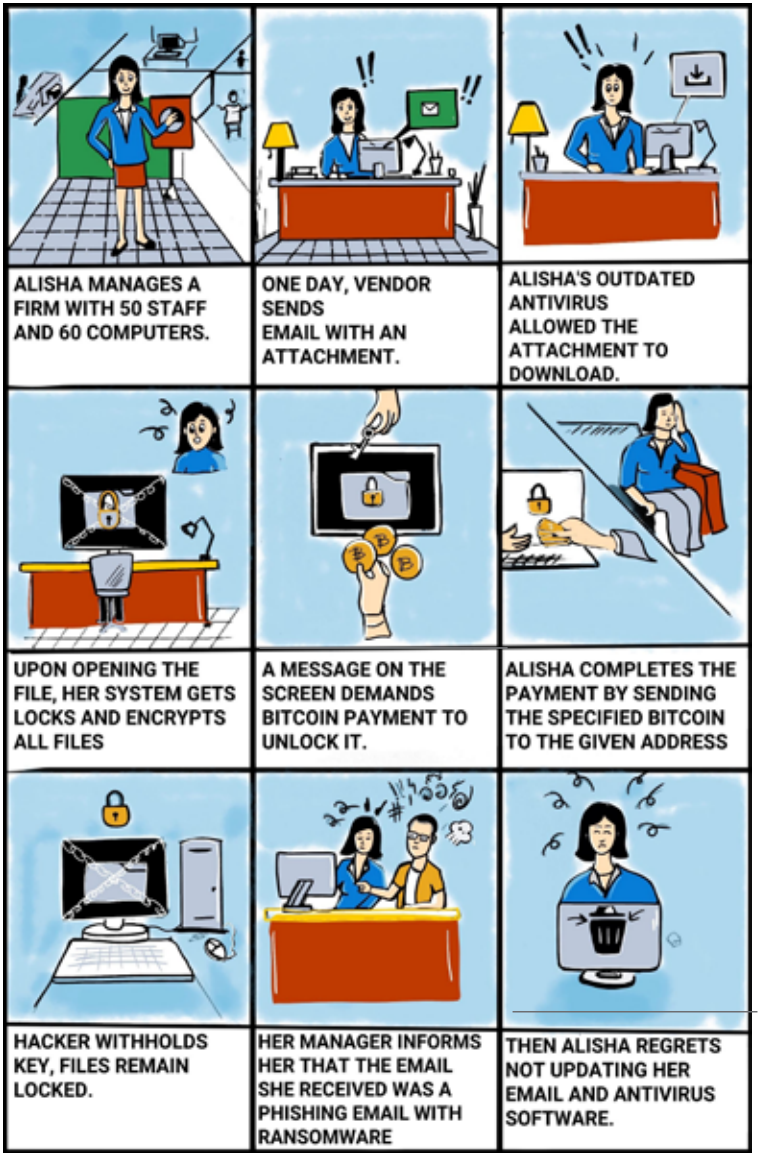
Section 386 – This section deals with extortion by putting a person infear of death or grievous hurt.

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 MANAGES A FIRM WITH 50 STAFF AND 60 COMPUTERS.
ONE DAY, VENDOR SENDS EMAIL WITH AN ATTACHMENT.
ALISHA'S OUTDATED ANTIVIRUS ALLOWED THE ATTACHMENT TO DOWNLOAD.
UPON OPENING THE FILE, HER SYSTEM GETS LOCKS AND ENCRYPTS ALL FILES
A MESSAGE ON THE SCREEN DEMANDS BITCOIN PAYMENT TO UNLOCK IT.
ALISHA COMPLETES THE PAYMENT BY SENDING THE SPECIFIED BITCOIN TO THE GIVEN ADDRESS
HACKER WITHHOLDS KEY, FILES REMAIN LOCKED.
HER MANAGER INFORMS HER THAT THE EMAIL SHE RECEIVED WAS A PHISHING EMAIL WITH RANSOMWARE
THEN ALISHA REGRETS NOT UPDATING HER EMAIL AND ANTIVIRUS SOFTWARE.

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

Section 66A – This section previously dealt with the offense of sendingoffensive messages through communication services. However, it wasstruck down by the Supreme Court of India in 2015 on grounds ofbeing vague and overbroad, and violating the right to free speech.

Offline:
IPC Section 354 D – Stalking

Online :
IPC Section 354 D – This section was introduced through the InformationTechnology (Amendment) Act, 2013, and specifically deals with theoffense of cyberstalking. It states that any person who monitors theuse by a woman of the internet, email, or any other form of electroniccommunication, commits the offense of cyberstalking. It alsocriminalizes actions that cause the woman to fear for her safety or thesafety of her relatives. Conviction under this section can result inimprisonment for a term which may extend to three years and a fine.

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


fb
Insta
Snapchat
#Check in
Check in
JUVERIYA, AN NRI, ENJOYS LIFE WHILE STUDYING ENGINEERING IN INDIA.
SHE DISCUSSES HER LIFE WITH HER 10K+ FOLLOWERS WITH JOY
SHE SKIPS PRIVACY BY FREQUENTLY CHECKING IN AT HUMEROUS AREAS.
SHE DECIDES TO EMBARK ON A SOLO TRIP TO GOA ONE DAY AND POSTS HER PLANS AND SCHEDULE ON HER FACEBOOK.
KIRAN, A HABITUAL STALKER, KEPT TRACK OF ALL HER DETAILS AND WAS RECENTLY RELEASED ON BAIL
HE TAKES A BUS TO GOA AND TEXTS JUVERIYA FROM HIS HOTEL ROOM, EXPRESSING HIS DESIRE TO MEET HER.
AFTER CHECKING OUT HIS PROFILE, JUVERIYA BLOCKS HIM, UNAWARE OF WHAT FATE HAD PLANNED FOR HER SHORTLY
ACCORDING TO HER PLANNING, HE FINDS HER IN A REMOTE LOCATION AND MOLESTS HER
JUVERIYA DEEPLY REGRETS OVERSHARING ON SOCIAL MEDIA, CAUSING DISTRESS

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 modesty of a woman

IT Act

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

Section 66E – Punishment for Violation of Privacy

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

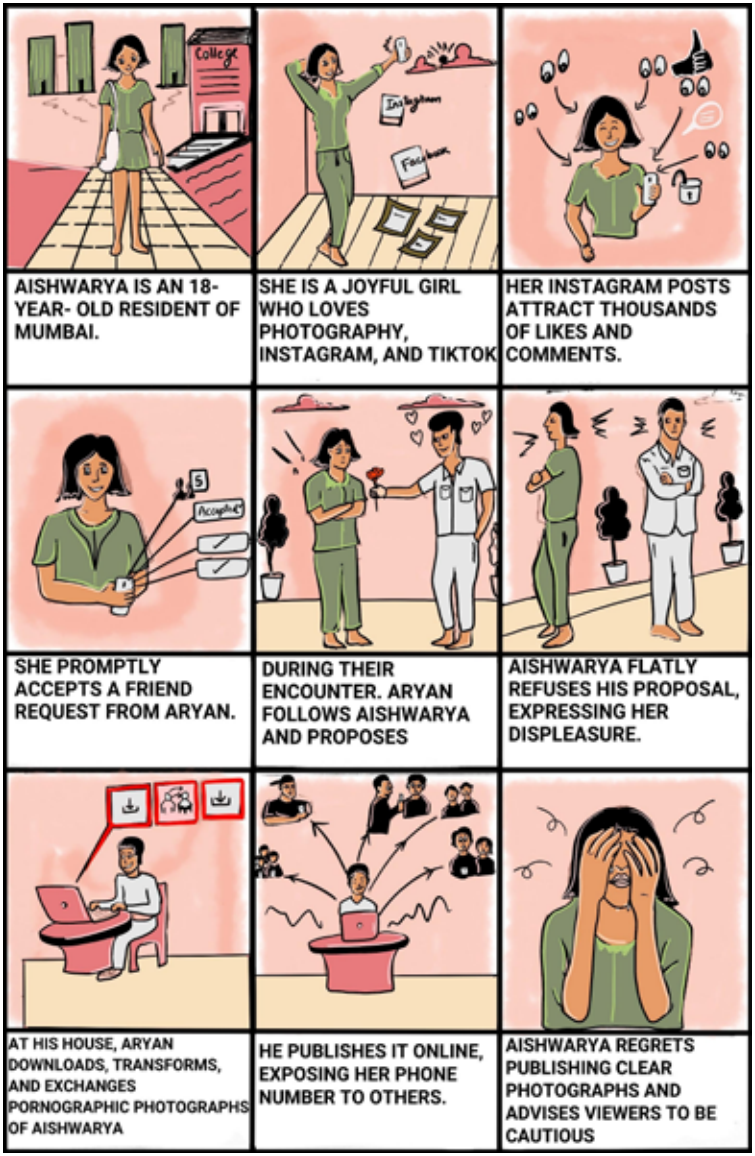
Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form

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

Section 72 – Penalty for Breach of Confidentiality and Privacy

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
Instagram
Facebook
5
Accept
AISHWARYA IS AN 18-YEAR- OLD RESIDENT OF MUMBAI.
SHE IS A JOYFUL GIRL WHO LOVES PHOTOGRAPHY, INSTAGRAM, AND TIKTOK
HER INSTAGRAM POSTS ATTRACT THOUSANDS OF LIKES AND COMMENTS.
SHE PROMPTLY ACCEPTS A FRIEND REQUEST FROM ARYAN.
DURING THEIR ENCOUNTER. ARYAN FOLLOWS AISHWARYA AND PROPOSES
AISHWARYA FLATLY REFUSES HIS PROPOSAL, EXPRESSING HER DISPLEASURE.
AT HIS HOUSE, ARYAN DOWNLOADS, TRANSFORMS, AND EXCHANGES PORNOGRAPHIC PHOTOGRAPHS OF AISHWARYA
HE PUBLISHES IT ONLINE, EXPOSING HER PHONE NUMBER TO OTHERS.
AISHWARYA REGRETS PUBLISHING CLEAR PHOTOGRAPHS AND ADVISES VIEWERS TO BE CAUTIOUS

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

Section. 43 – Unauthorized access to computer systems, networks,data.

Section 66 – Computer related offences

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

Section. 66D – Impersonation cheating through computer resources.

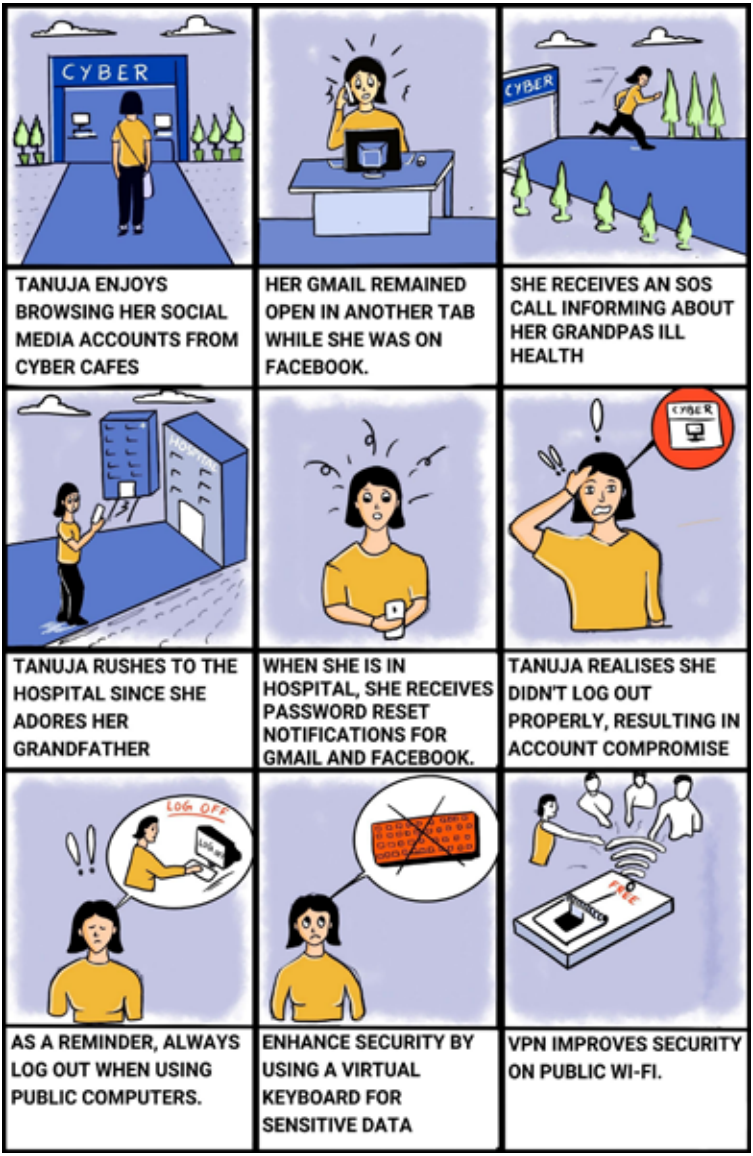
IPC

Section. 379 & 380 IPC : Theft of data or credentials.

Section. 463, 464, 468 IPC : Forgery of electronic records for fraud.

Section. 507 IPC : Criminal intimidation through hacking.

Profile Hacking means Security is Lacking!


CYBER
TANUJA ENJOYS BROWSING HER SOCIAL MEDIA ACCOUNTS FROM CYBER CAFES
HER GMAIL REMAINED OPEN IN ANOTHER TAB WHILE SHE WAS ON FACEBOOK.
CYBER
SHE RECEIVES AN SOS CALL INFORMING ABOUT HER GRANDPAS ILL HEALTH
HOSPITAL
TANUJA RUSHES TO THE HOSPITAL SINCE SHE ADORES HER GRANDFATHER
WHEN SHE IS IN HOSPITAL, SHE RECEIVES PASSWORD RESET NOTIFICATIONS FOR GMAIL AND FACEBOOK.
CYBER
TANUJA REALISES SHE DIDN'T LOG OUT PROPERLY, RESULTING IN ACCOUNT COMPROMISE
LOG OFF
AS A REMINDER, ALWAYS LOG OUT WHEN USING PUBLIC COMPUTERS.
ENHANCE SECURITY BY USING A VIRTUAL KEYBOARD FOR SENSITIVE DATA
FREE
VPN IMPROVES SECURITY ON PUBLIC WI-FI.

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

Information Technology Act, 2000:
Section 43 – This section deals with unauthorized access tocomputer systems, computer networks, or data. It covers actionssuch as hacking, introducing viruses, and damaging computersystems.
Section 66 – This section deals with computer-related offenses,including hacking, identity theft, and other forms of cybercrime
Section 67A – This section deals with the punishment forpublishing or transmitting sexually explicit content in electronicform.
Section 67B – This section deals with the punishment forpublishing or transmitting material depicting children in sexuallyexplicit acts.
Section 79 – This section provides safe harbor to intermediaries,including online platforms and game hosting services, from liability forthird-party content. However, they are required to adhere to certainconditions, including taking down illegal content upon receiving notice.

IPC Sections
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, A FIRST-YEAR ENGINEERING STUDENT FROM A REMOTE VILLAGE IN KARNATAKA
FRIENDS
SHE WAS TOO SIMPLE FOR CLASSMATES AND LACKED ONLINE FRIENDS
!!
GAME
OUT OF LONELINESS, SHE CLICKED "THE BLUE WHALE" GAME LINK
DEVIKA WAS LOOKING FORWARD TO THE 50-LEVEL GAME'S CHALLENGES
SHE EARNED BROWNIE POINTS FOR TASK ACCOMPLISHMENT, AND THE DOPAMINE RUSH CAPTIVATED HER.
ASSIGNED DANGEROUS TASKS: KNIFE TATTOOING AND GRAVEYARD WALKS
HER NOTICEABLE CHANGES WENT UNNOTICED BY EVERYONE
TASK
SHE HUNG HERSELF, APOLOGIZING TO PARENTS BEFORE THE ACT.
THE LETTER SAID, "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 43A – Compensation for failure to protect data: This sectiondeals with the liability of a body corporate in case of a breach ofsensitive personal data due to negligence in implementing andmaintaining reasonable security practices and procedures.

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

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

Section 72 – Breach of confidentiality and privacy: This section dealswith the punishment for breach of confidentiality and privacy.

Section 72A – Punishment for disclosure of information in breach of lawful contract: This section pertains to the punishment for revealinginformation in breach of a lawful contract.

IPC

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 – P unishment for Criminal Conspiracy

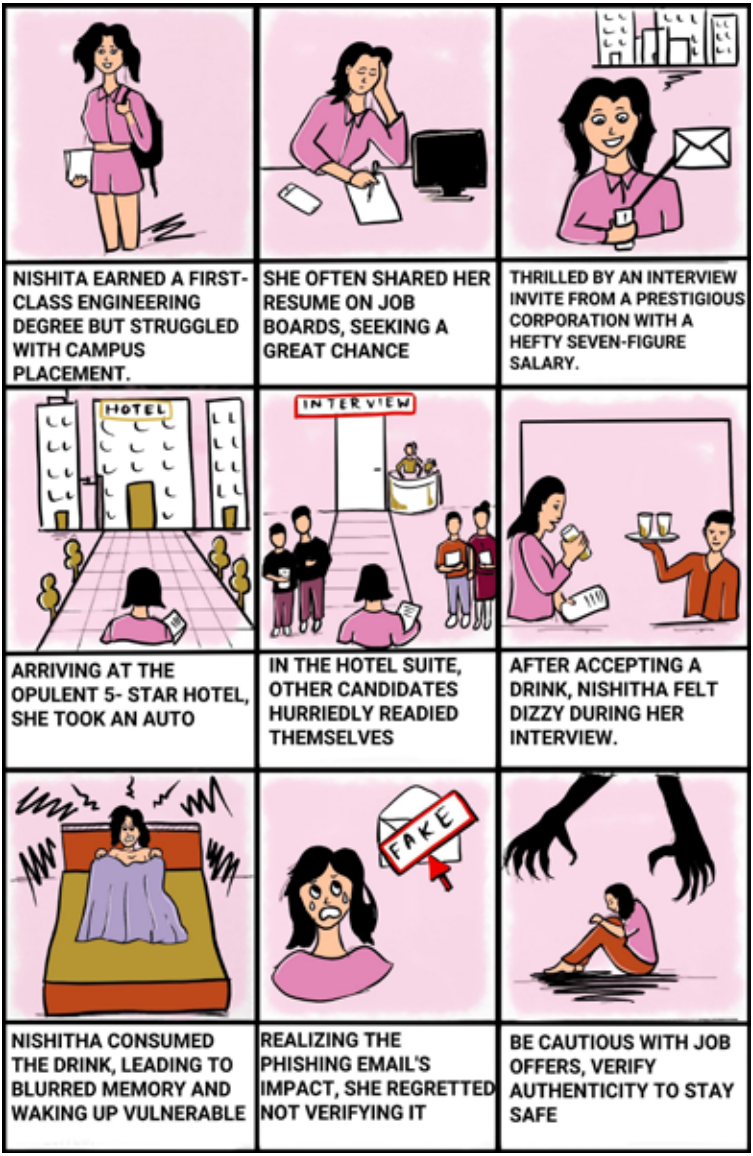
IPC Section 34 – Acts done by several persons in furtherance of Common Intention

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 EARNED A FIRST-CLASS ENGINEERING DEGREE BUT STRUGGLED WITH CAMPUS PLACEMENT.
SHE OFTEN SHARED HER RESUME ON JOB BOARDS, SEEKING A GREAT CHANCE
THRILLED BY AN INTERVIEW INVITE FROM A PRESTIGIOUS CORPORATION WITH A HEFTY SEVEN-FIGURE SALARY.
HOTEL
ARRIVING AT THE OPULENT 5- STAR HOTEL, SHE TOOK AN AUTO
INTERVIEW
IN THE HOTEL SUITE, OTHER CANDIDATES HURRIEDLY READIED THEMSELVES
AFTER ACCEPTING A DRINK, NISHITHA FELT DIZZY DURING HER INTERVIEW.
NISHITHA CONSUMED THE DRINK, LEADING TO BLURRED MEMORY AND WAKING UP VULNERABLE
FAKE
REALIZING THE PHISHING EMAIL'S IMPACT, SHE REGRETTED NOT VERIFYING IT
BE CAUTIOUS WITH JOB OFFERS, VERIFY AUTHENTICITY TO STAY SAFE

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.
ITA Section 43A and Section 72A of the Information Technology Act, 2000 - Compensation for Failure to Protect Data and Privacy: These sectionsdeal with the compensation payable to an individual whose personal dataand information have been negligently disclosed, which could beapplicable in cases where deepfakes lead to privacy breaches.
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
Section 465 - Making a false document
Section 499 - Defamation:
Section 500 - Punishment for Defamation:
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!


FINAL-YEAR MBBS STUDENT, JANET, HAD A 3-YEAR RELATIONSHIP WITH JOHN.
SHE USED TO BE A FREQUENT TIKTOK AND INSTAGRAM CREATOR, PUBLISHING TWICE A DAY.
JANET ENDED HER RELATIONSHIP WITH JOHN AFTER A FIGHT, AND ARJUN FOUND OUT ABOUT IT
!!!
JANET ACCEPTED ARJUN'S PROPOSAL BUT AFTERWARDS REGRETTED HER DECISION TO LEAVE JOHN
JANET STOPPED HER RELATIONSHIP WITH ARJUN BUT RECONCILED WITH JOHN
ARJUN PLANNED TO TEACH JANET A LESSON FOR HER ACTIONS.
PRODUCED AL DEEPFAKE VIDEOS OF HER
JANET WAS PRESENTED IN ADULTEROUS CIRCUMSTANCES IN VIRAL DEEPFAKE VIDEOS
JANET WAS AFRAID OF SHARING MEDIA SINCE SHE BELIEVED IN VIDEOS.

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

ITA Section 43A – This section deals with the compensation for failure toprotect data and is relevant for data breaches.
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.
Section 72A: This section penalizes the disclosure of personalinformation without consent.
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
IPC Section 354D – Deals with stalking.
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, A FIRST-YEAR MEDICAL STUDENT, WAS CROWNED MISS FRESHER
SHE CHATTED WITH INTERNET BUDDIES BUT QUICKLY BECAME BORED.
SHE DOWNLOADS TINDER AND BEGINS SWIPING THROUGH MATCHES
SHE MEETS SHAKS, AN ATTRACTIVE MAN LIVING A LIFE OF OPULENCE.
SHAKS ATTRACTED RASHMI AND LANDED A DATE
RASHMI BELIEVES HE'S THE ONE AFTER THE CANDLELIT MEAL.
SHAKS COOKS UP A STORY AND BORROWS 2 LAKHS EMERGENCY MONEY FROM RASHMI. MAKES HER SELL HER GOLD CHAIN
SHAKS BLOCKS HER. LATER, SHE LEARNS HE WAS A MARRIED CONMAN THROUGH A FRIEND.
SHE REPENTS FOR SHARING HER PRIVATE PHOTOS WITH HIM.

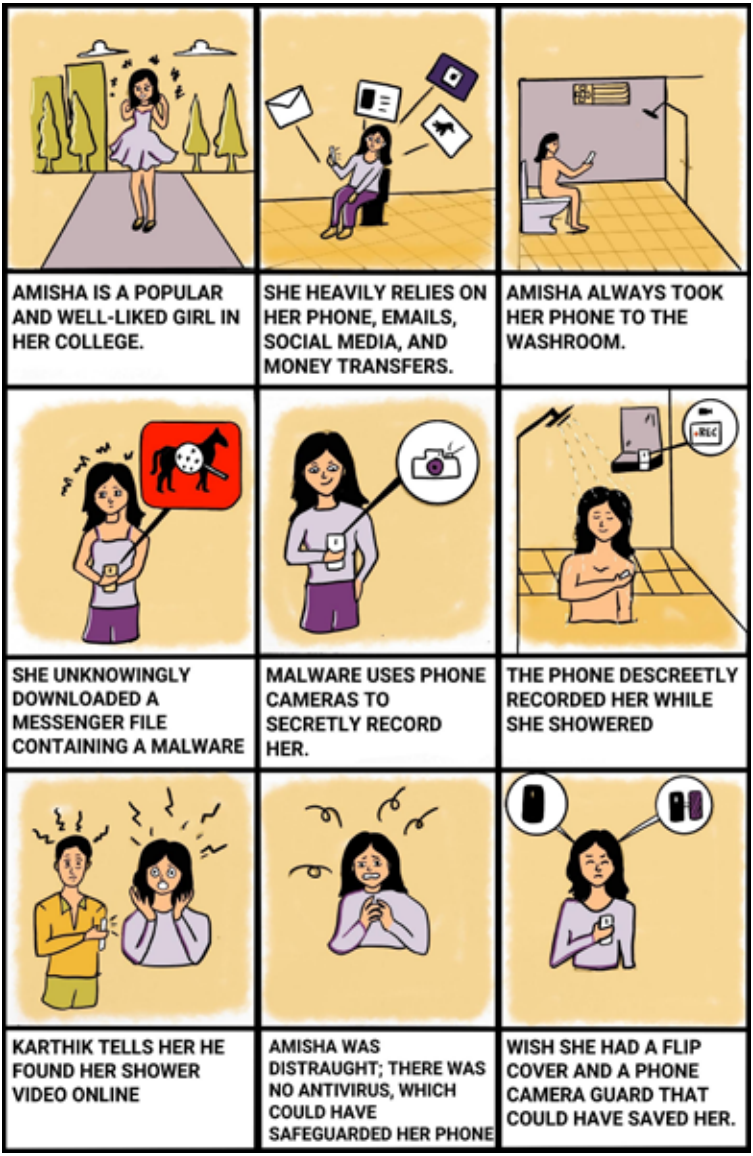
CAMERA HACKING

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-
ITA Section 43 - Penalty for unauthorized access to computer systems,data disruption, and theft.
ITA Section 66 - Computer related offences
Section 66B - Punishment for dishonestly receiving stolen computerresources or communication devices.
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.
Section 354C - Voyeurism (capturing or transmitting images ofprivate parts without consent).
Stalking : Offline : IPC Section 354 D - Stalking
Online : IPC Section 354 D - Stalking
Publishing online
Section 66F - Cyber Terrorism under the 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.
Section 72 - Breach of Confidentiality and Privacy under the IT Act

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


AMISHA IS A POPULAR AND WELL-LIKED GIRL IN HER COLLEGE.
SHE HEAVILY RELIES ON HER PHONE, EMAILS, SOCIAL MEDIA, AND MONEY TRANSFERS.
AMISHA ALWAYS TOOK HER PHONE TO THE WASHROOM.
SHE UNKNOWINGLY DOWNLOADED A MESSENGER FILE CONTAINING A MALWARE
MALWARE USES PHONE CAMERAS TO SECRETLY RECORD HER.
REC
THE PHONE DESCREETLY RECORDED HER WHILE SHE SHOWERED
KARTHIK TELLS HER HE FOUND HER SHOWER VIDEO ONLINE
AMISHA WAS DISTRAUGHT; THERE WAS NO ANTIVIRUS, WHICH COULD HAVE SAFEGUARDED HER PHONE
WISH SHE HAD A FLIP COVER AND A PHONE CAMERA GUARD THAT COULD HAVE SAVED HER.

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

ITACT
Section 66A – Punishment for sending offensive messages through communication service, etc.
Section 66C – Punishment for identity theft.
Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act, etc., in electronic form.
Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc., in electronic form.

Are you Trolling, the law may be soon following!

VIADHEI, FROM A MIDDLE- CLASS FAMILY, UPHOLDS STRONG MORALS AND ETHICS

MANY COLLEGE STUDENTS WERE CAREFREE AND FASHION-OBSESSED.

MANY STUDENTS WOULD MAKE FUN OF HER AND CALL HER NAMES

KULDEEP, A BULLY OF THE COLLEGE INSULTED HER, CALLED HER GAWAR

VAIDEHI BRAVELY TELLS HIM TO MIND HIS OWN BUSINESS, ENDING THE MENACE

ANNOYED KULDEEP EDITS JOKES WITH VAIDEHI'S NAME AND SHARES.

CREATES TROLL PAGE, MEMES & FUNNY VIDEOS OF VAIDHEI.

VAIDEHI'S HUMILIATED AND CONSIDERING QUITTING SCHOOL

VAIDEHI REGRETS NOT REPORTING TO COLLEGE AUTHORITIES OR FILING POLICE COMPLAINT.

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.

SEBI Act, 1992 – Section 11B: This empowers SEBI to counterfraudulent practices in securities trading, including Ponzi schemes.

Companies Act, 2013 – Section 447: It penalizes fraud, encompassingPonzi schemes, with imprisonment and fines.

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 FROM A LOWER- MIDDLE-CLASS FAMILY
SHE CRAVED LIFE'S LUXURIES
SHE FINDS A WEBSITE WITH BMW CARS AND FOREIGN TOURS AT RS. 9999/-!
ENROLLING FOR COUNSELING, SHE GETS A 5-STAR HOTEL INVITE.
THE SCHEME IS TO ENROLL 2 PEOPLE UNDER YOU. FOR EVERY PAIR, YOU EARN RS 500
THE COMMISSION INCREASES AS SHE ENROLLS AND INDUCTS NEW PEOPLE
SHE GOT COMMISSION BUT INVESTED MORE FOR SELF- ENROLLMENTS DUE TO LOW SIGN UPS
THE WEBSITE IS OFFLINE. THE HOTLINE IS IDLE, AND THE PROMOTERS ARE AWOL
ENROLLED MEMBERS EXTORT MONEY FROM HER, INCURRING HER SIGNIFICANT LOSSES. DON'T BE A VICTIM; STAY ALERT

FAKE MATRIMONIAL PROFILE

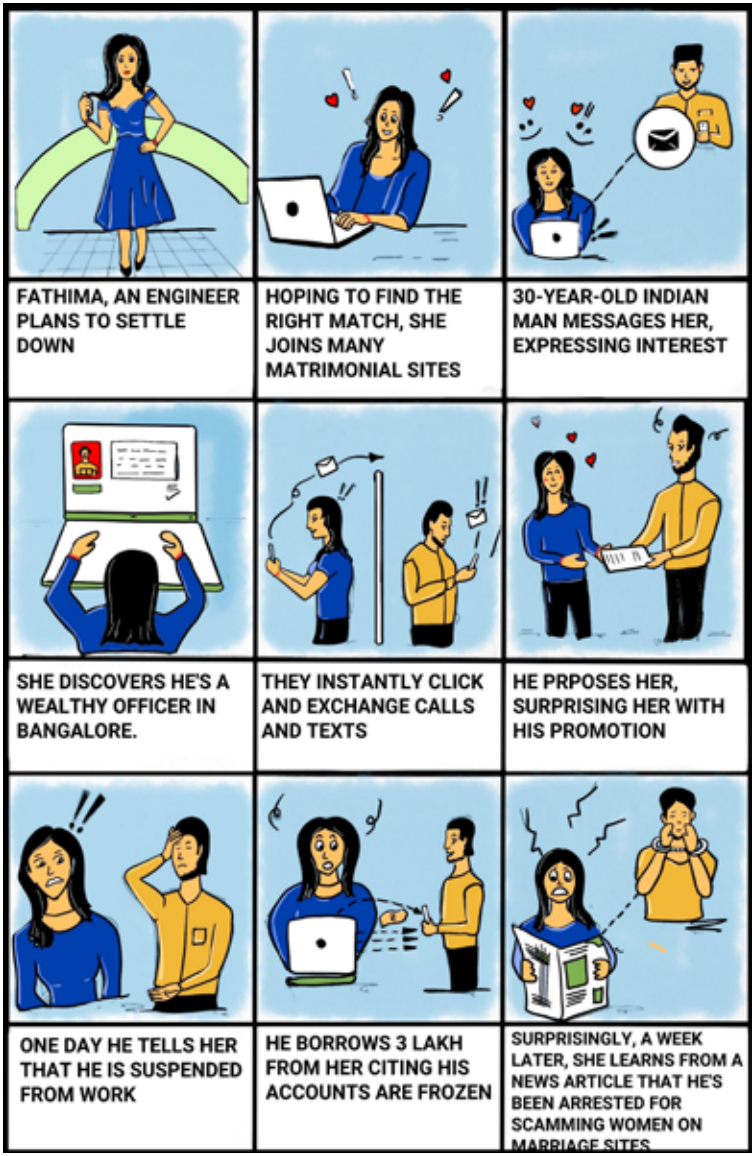
A fraudster may have registered on a matrimonial site with a fake profile. The details and profile pic may not be his. He can dupe a naive girl who falls for his practised charm and believes in the authenticity of supportive material that he provides to back up his identity.

Sections Applicable

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
IT Act Section 66E – Punishment for violation of privacy.

IPC Section 415 – Punishment for cheating.
IPC Section 419 – Punishment for cheating by personation
IPC Section 420 – Cheating
IPC Section 464 – Making a false document.
IPC Section 465 – punishment for forgery
IPC Section 468 – Forgery for purpose of cheating.
IPC Section 471 – Using as genuine a forged document.
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, AN ENGINEER PLANS TO SETTLE DOWN
HOPING TO FIND THE RIGHT MATCH, SHE JOINS MANY MATRIMONIAL SITES
30-YEAR-OLD INDIAN MAN MESSAGES HER, EXPRESSING INTEREST
SHE DISCOVERS HE'S A WEALTHY OFFICER IN BANGALORE.
THEY INSTANTLY CLICK AND EXCHANGE CALLS AND TEXTS
HE PRPOSES HER, SURPRISING HER WITH HIS PROMOTION
ONE DAY HE TELLS HER THAT HE IS SUSPENDED FROM WORK
HE BORROWS 3 LAKH FROM HER CITING HIS ACCOUNTS ARE FROZEN
SURPRISINGLY, A WEEK LATER, SHE LEARNS FROM A NEWS ARTICLE THAT HE'S BEEN ARRESTED FOR SCAMMING WOMEN ON MARRIAGE SITES

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

ITAct Section 43A – This section deals with compensation for failure to protectsensitive personal data.

IT Act Section 66 – Computer Related Offences

IT Act Section 66C – Prohibits identity theft, which includes impersonatingsomeone with the intent to cause wrongful loss.

IT Act Section 66D – Deals with cheating by impersonation using computerresources.

ITA Section 72A – It criminalizes the disclosure of personal information withoutconsent, intending to cause wrongful loss or gain

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

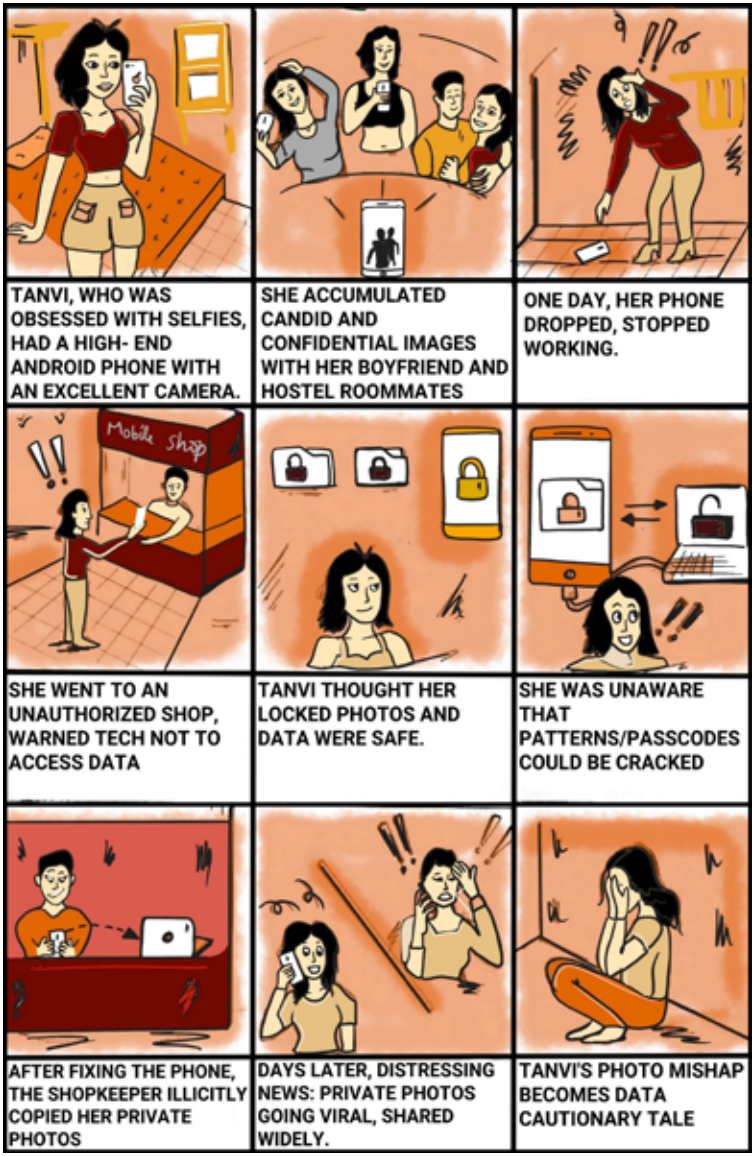
IPC Section 507 – Criminal Intimidation by an Anonymous communication

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

Indian Copyright Act, 1957 – Section 63B: Online Copyright Infringement

Section 63B deals with the offense of knowingly circumventing technological measures to infringe copyright.

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


TANVI, WHO WAS OBSESSED WITH SELFIES, HAD A HIGH- END ANDROID PHONE WITH AN EXCELLENT CAMERA.
SHE ACCUMULATED CANDID AND CONFIDENTIAL IMAGES WITH HER BOYFRIEND AND HOSTEL ROOMMATES
ONE DAY, HER PHONE DROPPED, STOPPED WORKING.
Mobile Shop
SHE WENT TO AN UNAUTHORIZED SHOP, WARNED TECH NOT TO ACCESS DATA
TANVI THOUGHT HER LOCKED PHOTOS AND DATA WERE SAFE.
SHE WAS UNAWARE THAT PATTERNS/PASSCODES COULD BE CRACKED
AFTER FIXING THE PHONE, THE SHOPKEEPER ILLICITLY COPIED HER PRIVATE PHOTOS
DAYS LATER, DISTRESSING NEWS: PRIVATE PHOTOS GOING VIRAL, SHARED WIDELY.
TANVI'S PHOTO MISHAP BECOMES DATA CAUTIONARY TALE

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

IT Act:

Section 43(a) – Compensation for Damage to Computer, ComputerSystem, etc. (IT Section 66C - Punishment for Identity Theft (IT Act, 2000)

Section 66D – Punishment for Cheating by Personation (IT Act, 2000)

Section 66F – Punishment for Cyber Terrorism (IT Act, 2000)

Fake Reviews may give you wrong Overviews!


COLLEGE
NIKITA IS A FIRST-YEAR STUDENT AND ASPIRING MODEL
SHE FREQUENTED PAGE 3 PARTIES TO ENSURE THE SHE STAYED IN THE SPOTLIGHT
SHE WORE PRICEY COSMETICS AND PERFUME THAT LASTED THROUGHOUT THE PARTY
SHE SOUGHT AFFORDABLE ONLINE ALTERNATIVES FOR BUYING THOSE ITEMS.
LESS 50%
WHILE SEARCHING, SHE FOUND A WEBSITE WITH 50% DISCOUNT ON SAME PRODUCTS, SEEMED SUSPICIOUS
Reviews
CURIOUS, SHE REVIEWED VERIFIED RATINGS: 4-STAR AVERAGE
TRUSTING REVIEWS, SHE BOUGHT PERFUME ONLINE. GOT SMS CONFIRMATION.
AFTER USING THE PRODUCTS, SHE GOT SEVERE RASHES AND HAD TO BE HOSPITALIZED.
REAL
FAKE
NIKITA'S ERROR HIGHLIGHTED IMPORTANCE OF CHECKING REVIEWS ON WEBSITES.

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:
IT Act Section 43 – Unauthorized access to computer systems, data, orinformation.
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
Section 66E – Violation of privacy.
IPC Section 415 – Cheating.
IPC Section 416 – Cheating by personation.
IPC Section 419 – Punishment for cheating by personation
IPC Section 354A – Sexual Harassment and punishment for Sexual
IPC Section 354C – Voyeurism
IPC Section 354D – Stalking.
IPC Section 503 – Criminal intimidation.
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
VAISHNAVI WANTS TO BUY OUTFITS FOR HER BIRTHDAY. SHE WENT SHOPPING WITH HER FRIEND.
SHE WAS UNSURE WHICH DRESS TO CHOSE, SO SHE TOOK THREE DRESSES AND WENT TO THE TRIAL ROOM
UNWARE, THE MIRROR WAS TWO SIDED WITH THE CAMERA RECORDING HER THROUGHOUT
A DAY LATER, SHE RECEIVES A PHONE CALL FROM A BUDDY ASKING WHY SHE OPENED ANOTHER FACEBOOK ACCOUNT
Photos
HER PROFILE, IRONICALLY, DISPLAYS PUBLIC INFORMATION BUT HER PRIVATE PHOTOGRAPHS STAY VISIBLE
SHE REPORTS THE PROFILE ONLINE BUT DOES NOT CONTACT THE POLICE. DESPITE HER EFFORTS, SHE RECEIVES NO RESULTS
+1(234)
AFTER SOME DAYS, SHE RECEIVES A PHONE CALL FROM AN INTERNATIONAL NUMBER REQUESTING MONEY.
DISREGARDING THE CALLER. HE PROCEEDS TO SHARE IMAGES WITH HER CONTACTS USING A FABRICATED ACCOUNT
VAISHNAVI DECIDES TO INVOLVE THE POLICE, BUT THE HARM HAS ALREADY OCCURRED. BE CAUTIOUS.

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)
Section 67 – Punishment for publishing or transmitting obscene material inelectronic form.
Section 67A – Punishment for publishing or transmitting of material containingsexually explicit act, etc., in electronic form.

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, A WIDOW FROM A MIDDLE CLASS FAMILY HAS 2 DAUGHTERS.
A RELATIVE CONVINCED HER TO INVEST SAVINGS IN A PONZI SCHEME FOR HIGHER RETURNS.
SHE EVEN INVESTS HER HUSBANDS SAVING INTO THE NEW SCHEME.
Fraud
SCAM
ONE DAY, DIRECTORS DISAPPEAR WITH INVESTOR MONEY AND MRS. LOBO GOT SCAMMED.
A HACKER ILLICITLY INFILTRATES INVESTMENT FIRM'S SERVER, AND COMPROMISING INVESTOR DATA.
HACKER CALL AND PROMISES 70% OF INVESTED AMOUNT TO THE INVESTORS.
MRS. LOBO SHARES UPI, ATM, AND ACCOUNT INFO WITH HACKER.
2***** Debited
SWIFTLY, THE HACKER DEDUCTS RS 2 LAKHS FROM HER ACCOUNT.
THE HACKER WAS SUCCESSFUL IN STEALING MONEY FROM THE CYBER CRIME VICTIM.

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

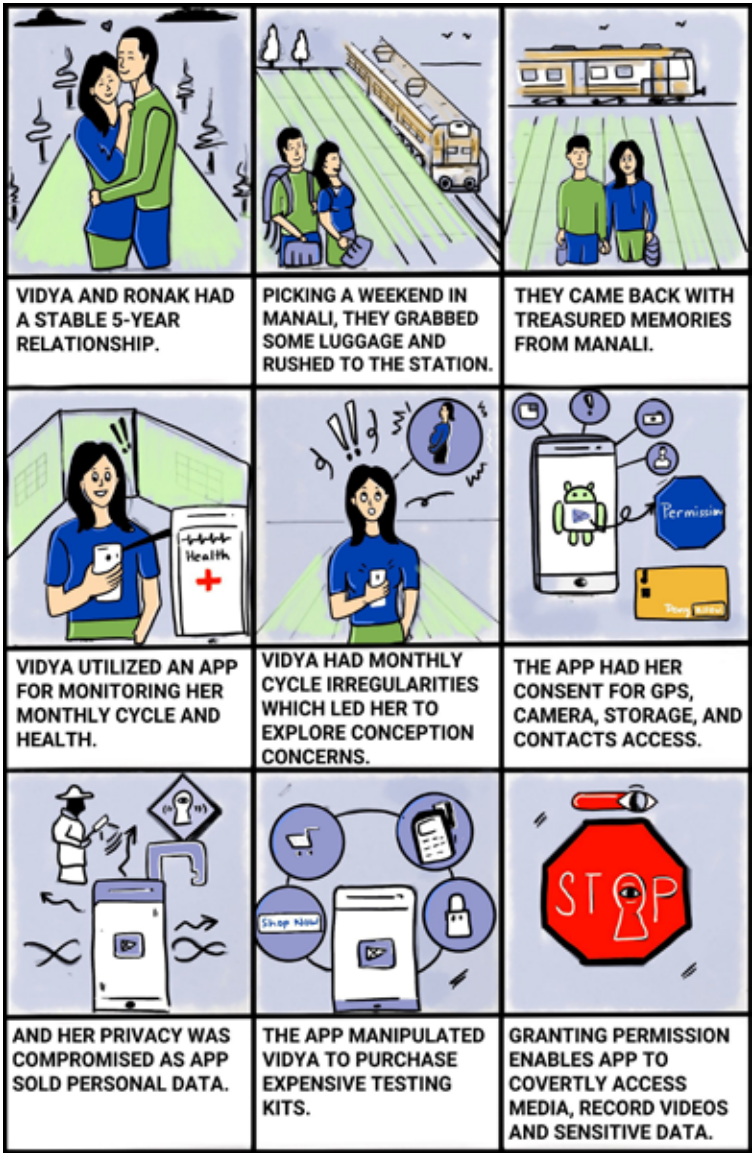
IPC Section 420 – Cheating

Information Technology Act, 2000 (IT Act):

a. Section 43A – This section deals with the compensation for failure toprotect data. Organizations handling sensitive personal data are required toimplement reasonable security practices to protect such data. If they fail todo so and a person suffers harm as a result, the organization could be liableto pay compensation.

b. Section 66 – This section deals with computer-related offenses, including unauthorized access, data theft, and damage to computer systems.

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


VIDYA AND RONAK HAD A STABLE 5-YEAR RELATIONSHIP.
PICKING A WEEKEND IN MANALI, THEY GRABBED SOME LUGGAGE AND RUSHED TO THE STATION.
THEY CAME BACK WITH TREASURED MEMORIES FROM MANALI.
Health
VIDYA UTILIZED AN APP FOR MONITORING HER MONTHLY CYCLE AND HEALTH.
VIDYA HAD MONTHLY CYCLE IRREGULARITIES WHICH LED HER TO EXPLORE CONCEPTION CONCERNS.
Permission
THE APP HAD HER CONSENT FOR GPS, CAMERA, STORAGE, AND CONTACTS ACCESS.
AND HER PRIVACY WAS COMPROMISED AS APP SOLD PERSONAL DATA.
Shop Now
THE APP MANIPULATED VIDYA TO PURCHASE EXPENSIVE TESTING KITS.
STOP
GRANTING PERMISSION ENABLES APP TO COVERTLY ACCESS MEDIA, RECORD VIDEOS AND SENSITIVE DATA.

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

Section 43 – This section deals with unauthorized access to computersystems, computer networks, or resources.

Section 66 – Computer Related Offences

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

Section 66D – This section pertains to cheating by personation using acomputer resource.

Section 66E – This section deals with violation of privacy.

Section 72 – This section deals with the breach of confidentiality andprivacy of information.

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


NIDHI, A WEDDING PLANNER, COORDINATES VENDORS FOR EVENTS.
SHE GUARANTEES FLAWLESS, UNFORGETTABLE WEDDINGS IN HER PLANS.
NIDHI VERIFIED ORDERS BY CALLING VENDORS TWICE.
DUE TO EXTENSIVE TRAVEL FOR HER JOB, SHE SPENT SIGNIFICANT TIME AT AIRPORTS.
SHE CHARGED HER PHONE AT AIRPORT`S FREE STATIONS WHEN LOW ON BATTERY.
SHE NOTICED HER PHONE SLOWING DOWN AND HEATING UP.
SCAN
AN ANTIVIRUS SCAN REVEALED HARMFUL MALWARE CAUSING PERFORMANCE DECLINE.
MALWARE INFILTRATED THROUGH CHARGING CABLES AT STATIONS, COMPROMISING HER PHONE.
SENSITIVE MEDIA STOLEN VIA JUICE JACKING. STAY VIGILANT AND CAUTIOUS.

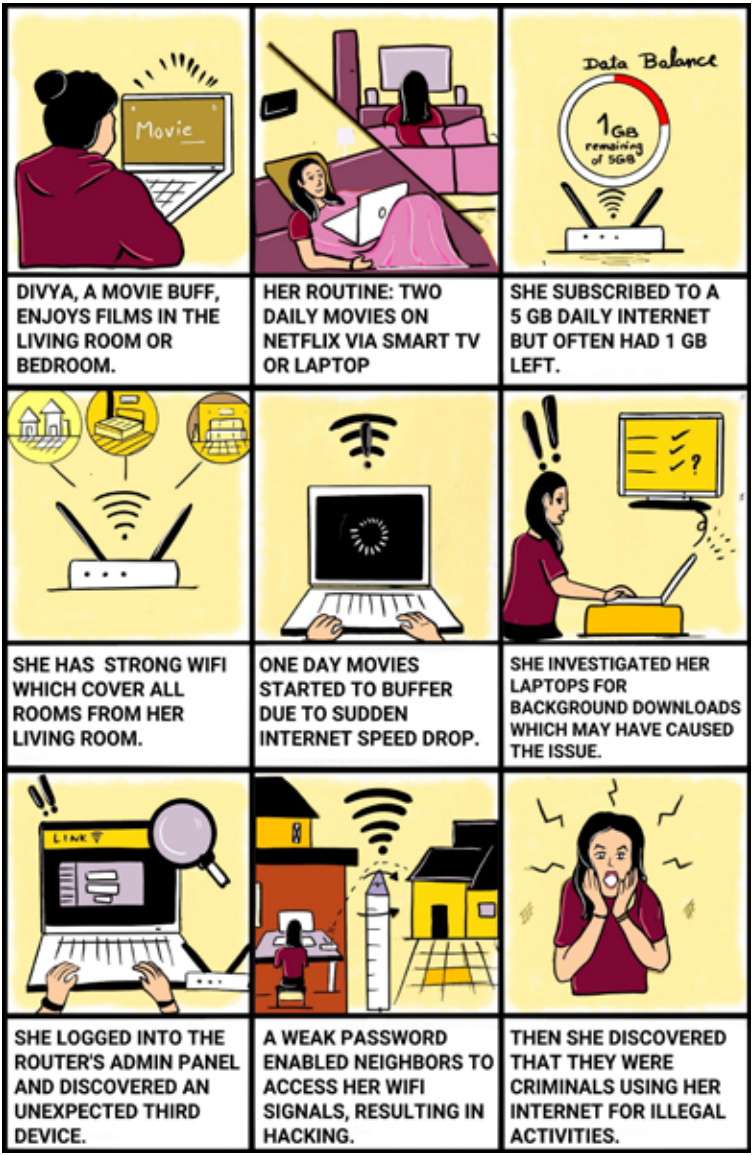
WIFI HACKING

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
Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device
Section 66C – Identity Theft
Section 72 – Breach of Confidentiality and Privacy
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!



DIVYA, A MOVIE BUFF, ENJOYS FILMS IN THE LIVING ROOM OR BEDROOM.

HER ROUTINE: TWO DAILY MOVIES ON NETFLIX VIA SMART TV OR LAPTOP

SHE SUBSCRIBED TO A 5 GB DAILY INTERNET BUT OFTEN HAD 1 GB LEFT.

SHE HAS STRONG WIFI WHICH COVER ALL ROOMS FROM HER LIVING ROOM.

ONE DAY MOVIES STARTED TO BUFFER DUE TO SUDDEN INTERNET SPEED DROP.

SHE INVESTIGATED HER LAPTOPS FOR BACKGROUND DOWNLOADS WHICH MAY HAVE CAUSED THE ISSUE.

SHE LOGGED INTO THE ROUTER'S ADMIN PANEL AND DISCOVERED AN UNEXPECTED THIRD DEVICE.

A WEAK PASSWORD ENABLED NEIGHBORS TO ACCESS HER WIFI SIGNALS, RESULTING IN HACKING.

THEN SHE DISCOVERED THAT THEY WERE CRIMINALS USING HER INTERNET FOR ILLEGAL ACTIVITIES.

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, A MODEST GIRL, FINISHED HER ENGINEERING STUDIES.
HER PARENTS ARRANGED HER MARRIAGE TO AN AFRICAN ENGINEER, DESPITE HER OBJECTIONS.
HER HUSBAND TOOK HER TO AFRICA, BUT SHE COULD NOT GET A JOB THERE.
DUE TO BEING STUCK AT HOME ALL THE TIME, SHE SPENDS MOST OF HER TIME ON THE INTERNET.
ONE DAY, SHE CLICKED ON A POST THAT LED TO A WEBSITE CONTAINING STRANGE IMAGES AND POSTS.
SHE RECEIVED EMAILS FROM THAT WEBSITE AND BEGAN REGULAR CONVERSATIONS WITH ITS LEADER.
HE INSTILLED THEIR IDEOLOGY IN HER INNOCENT MIND AND SUPPLIED WEAPONS TO HER HOME.
MALL
AFTER RECITING PRAYERS, SHE DETONATES HERSELF IN A MALL, SEEKING HEAVEN.
HER HUSBAND AND FAMILY WERE STUNNED, UNAWARE OF THIS HIDDEN ONLINE RADICALIZATION.

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

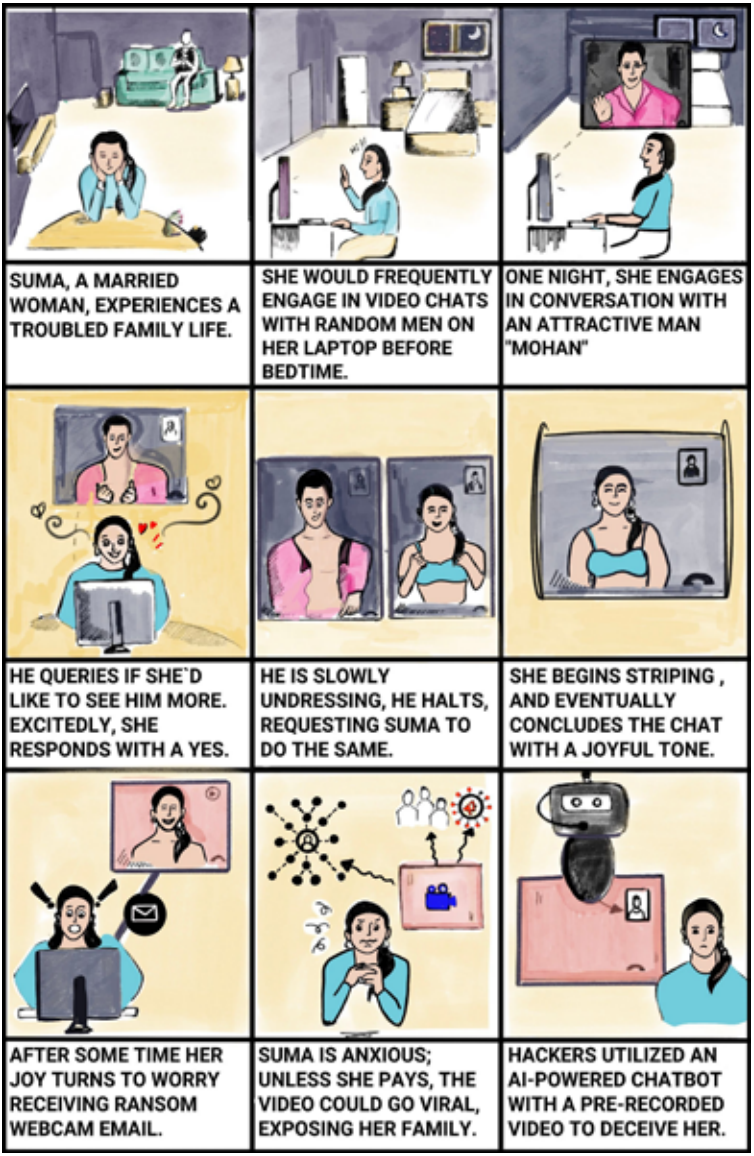
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

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, A MARRIED WOMAN, EXPERIENCES A TROUBLED FAMILY LIFE.
SHE WOULD FREQUENTLY ENGAGE IN VIDEO CHATS WITH RANDOM MEN ON HER LAPTOP BEFORE BEDTIME.
ONE NIGHT, SHE ENGAGES IN CONVERSATION WITH AN ATTRACTIVE MAN "MOHAN"
HE QUERIES IF SHE'D LIKE TO SEE HIM MORE. EXCITEDLY, SHE RESPONDS WITH A YES.
HE IS SLOWLY UNDRESSING, HE HALTS, REQUESTING SUMA TO DO THE SAME.
SHE BEGINS STRIPING , AND EVENTUALLY CONCLUDES THE CHAT WITH A JOYFUL TONE.
AFTER SOME TIME HER JOY TURNS TO WORRY RECEIVING RANSOM WEBCAM EMAIL.
SUMA IS ANXIOUS; UNLESS SHE PAYS, THE VIDEO COULD GO VIRAL, EXPOSING HER FAMILY.
HACKERS UTILIZED AN AI-POWERED CHATBOT WITH A PRE-RECORDED VIDEO TO DECEIVE HER.

QR CODE SCAM

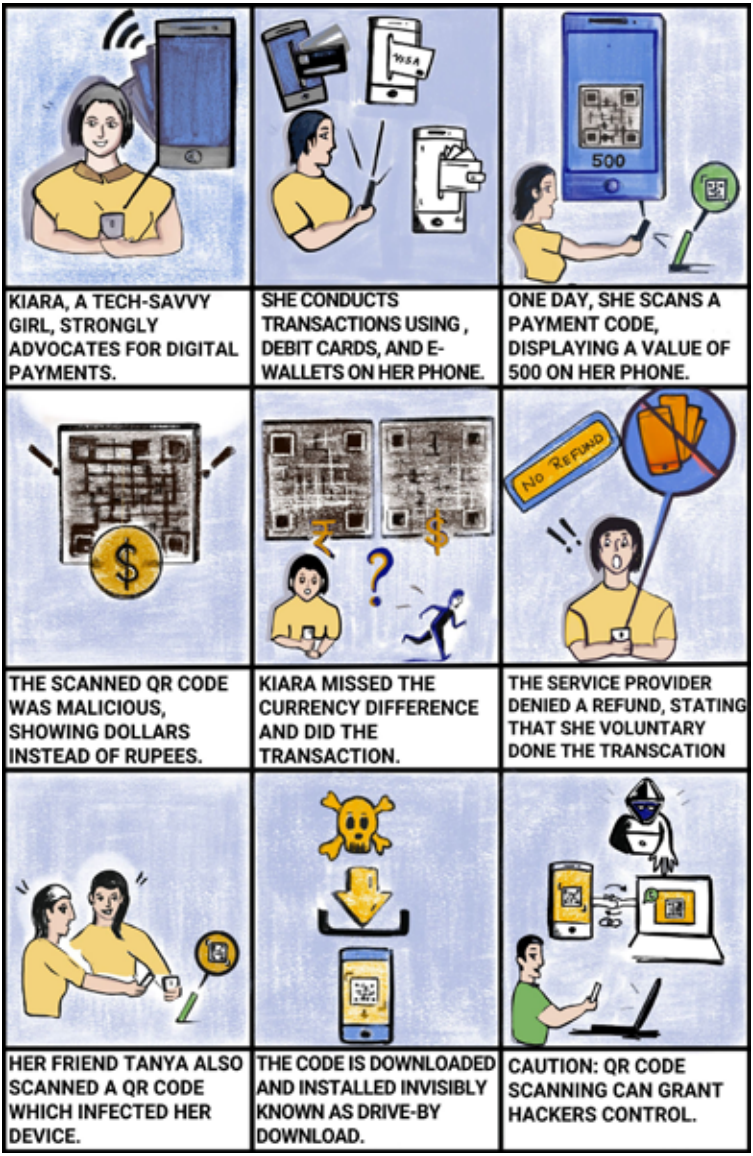
A QR (Quick Response) code is nothing more than a two-dimensional barcode. This type of code was designed to be read by robots that keep track of produced items in a factory. As a QR code takes up a lot less space than a legacy barcode, its usage soon spread and Hackers took it to their advantage! QR 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 43 – Unauthorized Access
Section 66 – Computer related offences
Section 66C – Identity Theft
Section 66D – Cheating by Personation
Section 66E – Privacy Violation

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


KIARA, A TECH-SAVVY GIRL, STRONGLY ADVOCATES FOR DIGITAL PAYMENTS.
SHE CONDUCTS TRANSACTIONS USING , DEBIT CARDS, AND E-WALLETS ON HER PHONE.
500
ONE DAY, SHE SCANS A PAYMENT CODE, DISPLAYING A VALUE OF 500 ON HER PHONE.
THE SCANNED QR CODE WAS MALICIOUS, SHOWING DOLLARS INSTEAD OF RUPEES.
KIARA MISSED THE CURRENCY DIFFERENCE AND DID THE TRANSACTION.
NO REFUND
THE SERVICE PROVIDER DENIED A REFUND, STATING THAT SHE VOLUNTARY DONE THE TRANSCATION
HER FRIEND TANYA ALSO SCANNED A QR CODE WHICH INFECTED HER DEVICE.
THE CODE IS DOWNLOADED AND INSTALLED INVISIBLY KNOWN AS DRIVE-BY DOWNLOAD.
CAUTION: QR CODE SCANNING CAN GRANT HACKERS CONTROL.

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, AN IT EMPLOYEE, UTILISED HER RFID TAG FOR DOOR ACCESS.

SHE INSERTED THE RFID CARD INTO HER WALLET AND PRESSED IT ON THE SCANNER.

HER BAD HABIT WAS TO LEAVE HER WALLET ON THE DESK.

ONE DAY, SHE LEFT HER WALLET AT HER DESK WHILE GOING TO THE WASHROOM.

AYESHAS COLLEAGUE JOHN EXAMINES HER WALLET WITH AN RFID READER DUE TO JEALOUSY.

JOHN COLLECTS HER OFFICE ID AS WELL AS HER CONTACTLESS CREDIT CARD INFORMATION.

JOHN SELLS THE CREDIT CARD DETAILS ON THE DARK WEB FOR MONEY.

USING THE COLLECTED DETAILS, JOHN CREATES A REPLICA OF AYESHA'S OFFICE ID.

JOHN INFILTRATES THE SERVER ROOM, HACKS SYSTEMS, AND FALSELY IMPLICATES AYESHA.

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 ON THE 33RD FLOOR WITH OPEN WINDOWS IN HER APARTMENT.
SHE KEPT ALL HER WINDOWS OPEN SINCE THERE WERE NO TALLER NEARBY BUILDINGS TO OVERLOOK HER PLACE.
SHE MOVED INSIDE WITH MINIMAL CLOTHES AS SHE LIVED ON HER OWN AND WASN'T SHARING HER HOME.
AKSHAY, HER EX-BOYFRIEND, HE USED A DRONE TO SECRETLY MONITOR HER.
HE COVERTLY FLEW THE DRONE AND RECORDED HER MOVEMENTS.
THE DRONE MONITORED HER ARRIVALS AND DEPARTURES AT HOME.
AKSHAY EVEN ADDED A WIFI CRACKER TO THE DRONE AND BREACHING PRIVACY.
HE COULD ALSO USE THE DRONE TO DELIVER DANGEROUS MATERIALS OR WEAPONS TO HER HOUSE.
IF SHE HAD INSTALLED A MOTION SENSOR CCTV CAMERA INITIALLY, SHE COULD HAVE DETECTED THE DRONE.

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 RESERVED A FLIGHT TICKET TO MANGALORE.
BEFORE HER TRIP, SHE RECEIVES AN EMAIL STATING HER TICKETS HAVE BEEN CANCELLED.
SHE LOOKS FOR A HELPLINE NUMBER AND CONTACTS THE NUMBER IN THE SEARCH RESULTS.
THE REPRESENTATIVE ASKS FOR HER CARD INFO AND CVV FOR VERIFICATION.
SHE LOSES RS 10,000 FIVE TIMES, TOTALING RS 50,000.
THE EMAIL SHE RECEIVED WAS A SPOOF, NOT FROM THE AIRLINE.
HACKERS INJECTED A FAKE CALL CENTER NUMBER IN THE SEARCH RESULTS TO DECEIVE.
WHILE SHE HADN'T SHARED THE OTP, FOREIGN GATEWAYS OFTEN DON'T REQUIRE IT FOR TRANSACTIONS.
AKSHATA HADN'T DISABLED HER INTERNATIONAL USAGE ON 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.

SUCHETA INTENDS TO SEND MONEY TO HER MOTHER, RESIDING IN A DIFFERENT CITY.

SHE RECEIVES A MESSAGE FROM HER BANK

UPON OPENING, THE MESSAGE READS AS FOLLOWS:

EXCITEDLY, SHE CLICKS THE LINK AND ENTERS HER LOGIN DETAILS.

AFTER CLICKING SUBMIT, THE WEBPAGE FAILED TO LOAD, RETURNING HER TO THE LOGIN PAGE.

SHE MAKES ANOTHER ATTEMPT AND SUCCESSFULLY CARRIES OUT THE TRANSACTION.

TO HER SURPRISE, SHE FINDS RS 10,000 DEBITED FROM HER ACCOUNT INSTEAD OF A GIFT VOUCHER.

IDN HOMOGRAPH ATTACKS, INVOLVING DECEPTIVE DOMAINS RESEMBLING GENUINE ONES,

UPDATING HER BROWSER COULD HAVE ALERTED HER TO THE FAKE CYRILLIC DOMAIN MIMICKING 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 A FINANCIAL CRISIS AND EXTREMELY CONCERNED.
SHE HOPES FOR A MIRACLE TO RECEIVE INR 2 LAKHS.
SHE RECEIVES A SCRATCH CARD IN A WHATSAPP GROUP, OFFERING A CHANCE TO WIN UP TO 5 LAKHS.
AMRIN CLICKS THE LINK, THE SCRATCH CARD LOADS, AND SHE EAGERLY SCRATCHES IT.
You won REWARD
Youve won
WINNING INR 3 LAKHS, SHE EXPRESSES GRATITUDE TO GOD FOR ANSWERING HER PRAYERS.
ENTER PIN
THE WALLET APPLICATION LAUNCHES, REQUESTING THE PIN CODE.
₹ 30,000
Pay from your bank
Pay ₹ 30,000
AMRIN HADN'T NOTICED THAT THE TRANSACTION WAS FOR PAYMENT INSTEAD OF RECEIVING.
Debited
ENTERING THE PIN, AMRIN LOSES HER PAINSTAKINGLY EARNED INR 30,000.
ENTER PIN
UNAWARE THAT WALLETS DON'T REQUIRE A 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 PHONE NUMBER TO NUMEROUS APPS ON HER PHONE FOR AUTHENTICATION.
SOME INCLUDED MOBILE WALLETS, 2FA FOR EMAIL, BANK ACCOUNTS, AND SOCIAL MEDIA.
ONE NIGHT, ARPITHA RECEIVES A CALL FROM A CYBERCRIMINAL POSING AS HER CELL PHONE COMPANY.
SWITCH OFF
5G
HE CONVINCES HER TO POWER OFF HER PHONE FOR 2 HOURS, PROMISING AN 5G ACTIVATION FOR A FEW CUSTOMERS.
ARPITHA POWERS OFF HER PHONE AND SLEEPS. UPON WAKING, SHE DISCOVERS NO NETWORK.
THE HACKER SUBMITTED HER DOCUMENTS FOR A NEW SIM, RENDERING THE OLD ONE USELESS UPON ACTIVATION.
USING "FORGOT PASSWORD" AND OTP VERIFICATION, THE HACKER GAINS CONTROL OF HER ACCOUNTS.
Gallery
HE ALSO GAINS CONTROL OF HER WHATSAPP, ACCESSING PRIVATE CHATS/PHOTOS FOR BLACKMAIL.
OTP
HACKERS USE VISHING TO REQUEST OTPS AND HACK 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

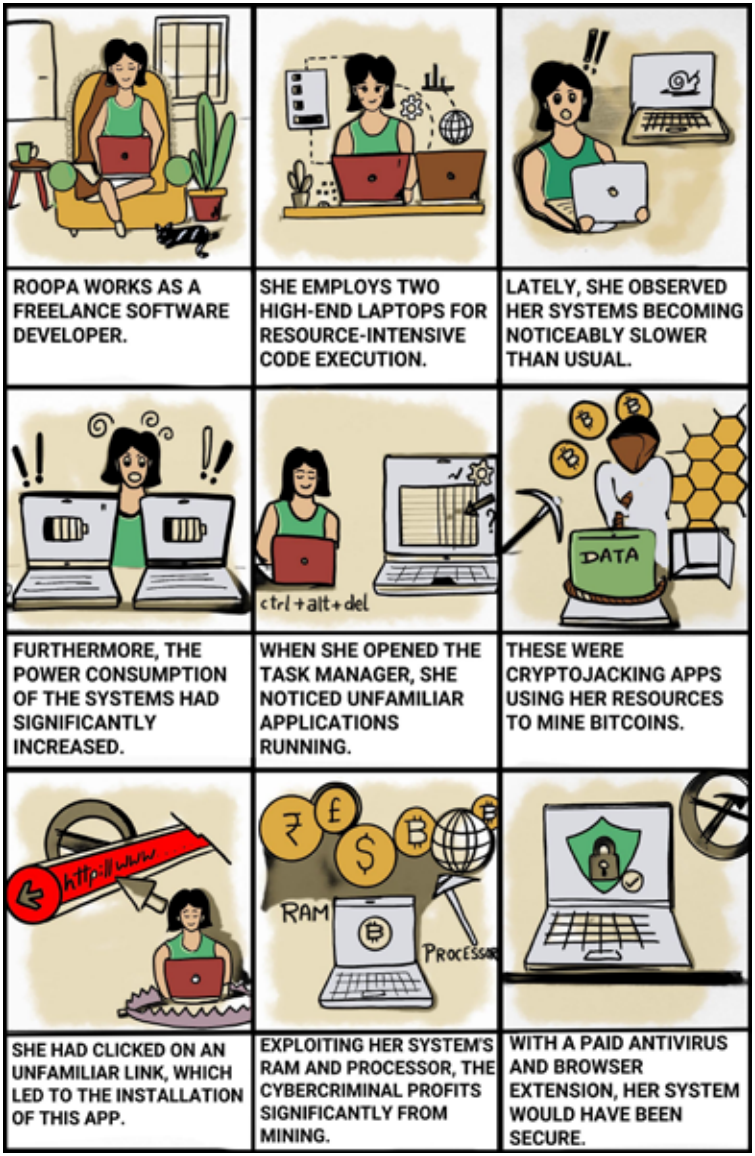
IT Act Section 66D – Punishment for cheating by personation using a computer resource

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 WORKS AS A FREELANCE SOFTWARE DEVELOPER.
SHE EMPLOYS TWO HIGH-END LAPTOPS FOR RESOURCE-INTENSIVE CODE EXECUTION.
LATELY, SHE OBSERVED HER SYSTEMS BECOMING NOTICEABLY SLOWER THAN USUAL.
FURTHERMORE, THE POWER CONSUMPTION OF THE SYSTEMS HAD SIGNIFICANTLY INCREASED.
ctrl+alt+del
WHEN SHE OPENED THE TASK MANAGER, SHE NOTICED UNFAMILIAR APPLICATIONS RUNNING.
DATA
THESE WERE CRYPTOJACKING APPS USING HER RESOURCES TO MINE BITCOINS.
http://www
SHE HAD CLICKED ON AN UNFAMILIAR LINK, WHICH LED TO THE INSTALLATION OF THIS APP.
RAM
PROCESSOR
EXPLOITING HER SYSTEM'S RAM AND PROCESSOR, THE CYBERCRIMINAL PROFITS SIGNIFICANTLY FROM MINING.
WITH A PAID ANTIVIRUS AND BROWSER EXTENSION, HER SYSTEM WOULD HAVE BEEN SECURE.

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 IS A TEAM LEADER AT AN MNC AND HAS RECENTLY CHOSEN TO WORK FROM HOME.
SHE FREQUENTLY HOSTS ONLINE MEETINGS TO COORDINATE WITH HER TEAM.
CLIENTS ALSO OCCASIONALLY ENGAGE IN VIDEO CONFERENCES TO REVIEW PROGRESS AND PROPOSE MODIFICATIONS.
DURING A CLIENT MEETING ONE MORNING, AN UNKNOWN USER LOGS IN AND SHARES EXPLICIT CONTENT.
AMRITA CHOSE TO EXIT THE MEETING DUE TO EMBARRASSMENT.
Meeting ID
SHE HAD SHARED THE MEETING ID AND PASSWORD IN THE SAME MESSAGE ON A DISCUSSION FORUM.
AN DISGRUNTLED EMPLOYEE FROM THE CLIENT'S SIDE LOGGED IN UNDER A PROXY NAME.
WAITING ROOM
ADMIT
THE PARTICIPANTS WEREN'T FILTERED THROUGH AN ENABLED WAITING ROOM.
Share Screen
File Share
SCREEN AND FILE SHARING PERMISSIONS WERE NOT DISABLED FOR ALL PARTICIPANTS. BE CAREFULL

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, A SINGLE MOTHER, RESIDES WITH HER 9-YEAR-OLD SON, ARNAAV.
SHE WORKS AS A BEAUTICIAN AT A SALON NEAR HER RESIDENCE.
DUE TO THE PANDEMIC, ALL CLASSES ARE ONLINE; ARNAAV ATTENDS THEM USING HIS MOTHER'S MOBILE PHONE.
GAME
RATHER THAN ATTENDING CLASSES, ARNAAV ENGAGES IN PLAYING VIDEO GAMES.
DOWNLOAD
HE ALSO DOWNLOADS PAID APPS FROM THE PLAY STORE USING THE STORED CREDIT CARD.
GAME
₹ XXXX
OCCASIONALLY, HE EVEN PURCHASES IN-GAME COINS TO PROGRESS THROUGH LEVELS MORE QUICKLY.
HE ERASES THE SMS TRANSACTION MESSAGES TO KEEP HIS MOTHER UNAWARE.
BILL
-----₹XXXX
SUMAN WAS SURPRISED TO FIND A RS 14000 CHARGE FROM THE PLAY STORE ON HER MONTHLY CREDIT CARD BILL.
ENABLING PARENTAL CONTROLS ON IOS/ANDROID WOULD HAVE RESTRICTED ARNAAV'S PHONE USAGE TO ACADEMIC PURPOSES ONLY.

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

Digital outreach may lead to Privacy Breach

IPC Section 354 – Sexual harassment

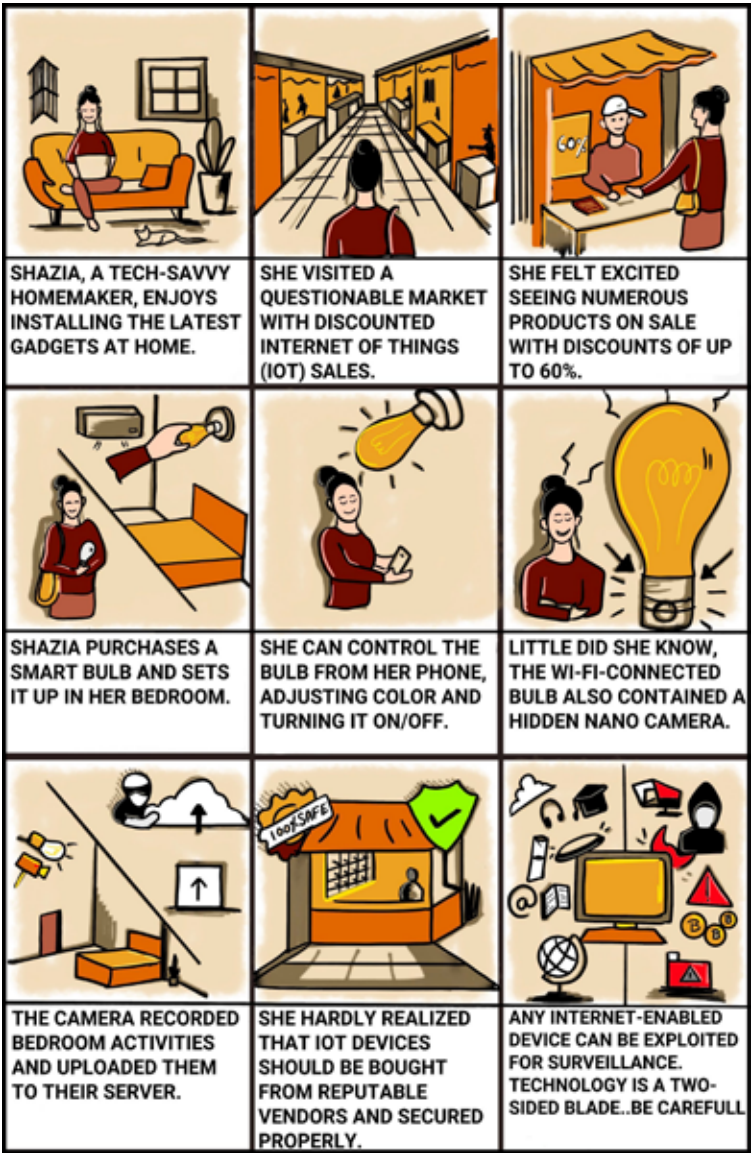
IPC Section 354C – Voyeurism

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, A TECH-SAVVY HOMEMAKER, ENJOYS INSTALLING THE LATEST GADGETS AT HOME.
SHE VISITED A QUESTIONABLE MARKET WITH DISCOUNTED INTERNET OF THINGS (IOT) SALES.
SHE FELT EXCITED SEEING NUMEROUS PRODUCTS ON SALE WITH DISCOUNTS OF UP TO 60%.
SHAZIA PURCHASES A SMART BULB AND SETS IT UP IN HER BEDROOM.
SHE CAN CONTROL THE BULB FROM HER PHONE, ADJUSTING COLOR AND TURNING IT ON/OFF.
LITTLE DID SHE KNOW, THE WI-FI-CONNECTED BULB ALSO CONTAINED A HIDDEN NANO CAMERA.
THE CAMERA RECORDED BEDROOM ACTIVITIES AND UPLOADED THEM TO THEIR SERVER.
IOT SAFE
SHE HARDLY REALIZED THAT IOT DEVICES SHOULD BE BOUGHT FROM REPUTABLE VENDORS AND SECURED PROPERLY.
ANY INTERNET-ENABLED DEVICE CAN BE EXPLOITED FOR SURVEILLANCE. TECHNOLOGY IS A TWO-SIDED BLADE..BE CAREFULL

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

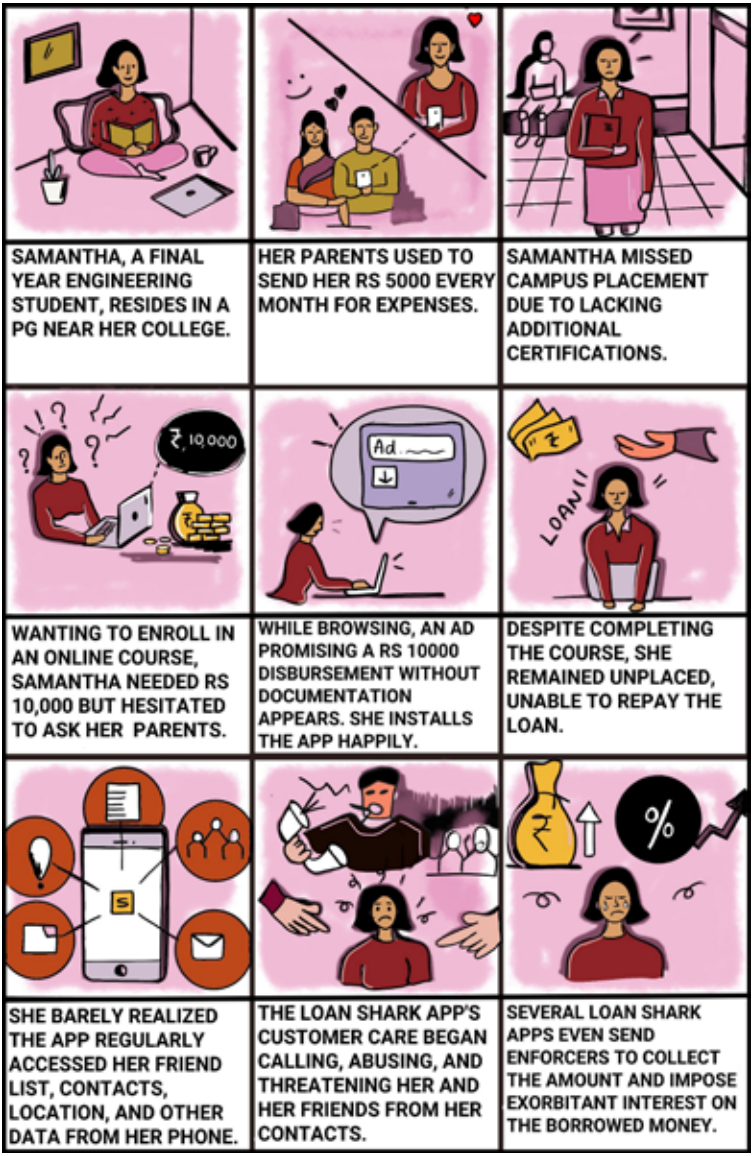
IPC Section 120B – Criminal Conspiracy

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, A FINAL YEAR ENGINEERING STUDENT, RESIDES IN A PG NEAR HER COLLEGE.
HER PARENTS USED TO SEND HER RS 5000 EVERY MONTH FOR EXPENSES.
SAMANTHA MISSED CAMPUS PLACEMENT DUE TO LACKING ADDITIONAL CERTIFICATIONS.
₹ 10,000
WANTING TO ENROLL IN AN ONLINE COURSE, SAMANTHA NEEDED RS 10,000 BUT HESITATED TO ASK HER PARENTS.
Ad
WHILE BROWSING, AN AD PROMISING A RS 10000 DISBURSEMENT WITHOUT DOCUMENTATION APPEARS. SHE INSTALLS THE APP HAPPILY.
LOAN!!
DESPITE COMPLETING THE COURSE, SHE REMAINED UNPLACED, UNABLE TO REPAY THE LOAN.
SHE BARELY REALIZED THE APP REGULARLY ACCESSED HER FRIEND LIST, CONTACTS, LOCATION, AND OTHER DATA FROM HER PHONE.
THE LOAN SHARK APP'S CUSTOMER CARE BEGAN CALLING, ABUSING, AND THREATENING HER AND HER FRIENDS FROM HER CONTACTS.
%
SEVERAL LOAN SHARK APPS EVEN SEND ENFORCERS TO COLLECT THE AMOUNT AND IMPOSE EXORBITANT INTEREST ON THE BORROWED MONEY.

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

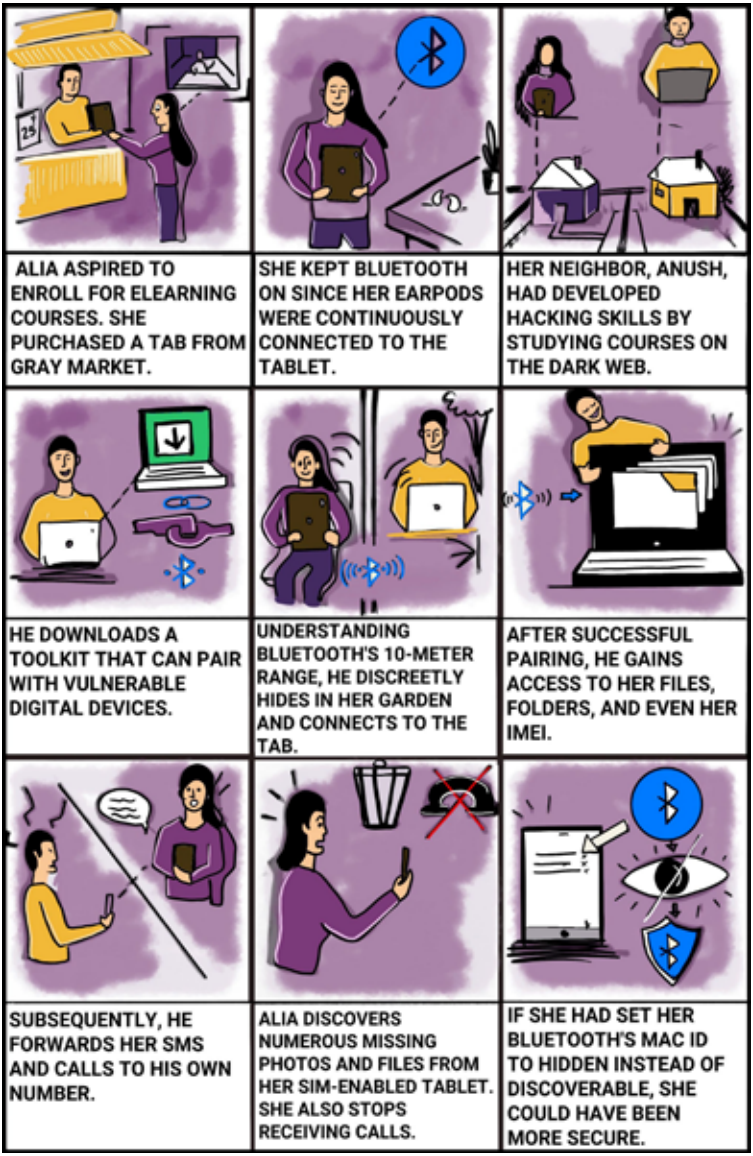
IT Act Section 66C – Punishment for Identity Theft

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 ASPIRED TO ENROLL FOR ELEARNING COURSES. SHE PURCHASED A TAB FROM GRAY MARKET.
SHE KEPT BLUETOOTH ON SINCE HER EARPODS WERE CONTINUOUSLY CONNECTED TO THE TABLET.
HER NEIGHBOR, ANUSH, HAD DEVELOPED HACKING SKILLS BY STUDYING COURSES ON THE DARK WEB.
HE DOWNLOADS A TOOLKIT THAT CAN PAIR WITH VULNERABLE DIGITAL DEVICES.
UNDERSTANDING BLUETOOTH'S 10-METER RANGE, HE DISCREETLY HIDES IN HER GARDEN AND CONNECTS TO THE TAB.
AFTER SUCCESSFUL PAIRING, HE GAINS ACCESS TO HER FILES, FOLDERS, AND EVEN HER IMEI.
SUBSEQUENTLY, HE FORWARDS HER SMS AND CALLS TO HIS OWN NUMBER.
ALIA DISCOVERS NUMEROUS MISSING PHOTOS AND FILES FROM HER SIM-ENABLED TABLET. SHE ALSO STOPS RECEIVING CALLS.
IF SHE HAD SET HER BLUETOOTH'S MAC ID TO HIDDEN INSTEAD OF DISCOVERABLE, SHE COULD HAVE BEEN MORE SECURE.

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
This section deals with theft andcovers the unlawful taking of movable property, including stolen phones.

Section 406 of the IPC
This section pertains to criminal breach of trust.

Section 411 of the IPC
This section deals with dishonestly receiving stolen property.

IT Act

Section 66 – Computer related offences

Section 66 – This sectionaddresses identity theft and unauthorized use of electronic signatures, passwords, or any other unique identification feature.

Section 66D – This section pertainsto cheating by personation using computer resources.

Lost cell phone, it may affect your cells and hormone


CARNIVAL
ANAMIKA HAD A CELL PHONE ADDICTION, FREQUENTLY USING SOCIAL MEDIA APPS
SHE AND HER FRIEND DIVYA VISITED A CARNIVAL TOGETHER.
EXCITEDLY, THEY BOTH BOUGHT TICKETS AND GOT ON THE FERRIS WHEEL.
ANAMIKA DROPPED HER PHONE WITHOUT REALIZING.
AT THE FERRIS WHEEL'S PEAK, SHE DISCOVERED HER MISSING PHONE WHILE ATTEMPTING A SELFIE.
DISTRESSED, SHE CALLED HER NUMBER FROM DIVYA'S PHONE
THE PERSON WHO HAD STOLEN HER PHONE HUNG UP AND LATER SWITCHED IT OFF.
ANAMIKA COULD HAVE ACCESSED THE FIND MY DEVICE PORTAL TO TRACK HER PHONE.
SHE ALSO HAD THE OPTION TO REMOTELY FORMAT HER PHONE TO SAFEGUARD 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

Information Technology Act, 2000 – Section 66: This section deals withcomputer-related offenses, including unauthorized access to computersystems.

Information Technology Act, 2000 – Section 43: This section coverspenalties for unauthorized access, damages to computer systems, and databreaches.

Indian Penal Code, 1860 – Section 420: This section deals with cheating anddishonestly inducing delivery of property.

Prevention of Unfair Means Act (PUMA): While not a cyber law, this act isrelevant as it addresses unfair practices during exams.

UGC Regulations / University Rules: Universities and educational institutionsoften have their own rules and regulations to prevent exam malpractice.

Short cuts may cut short your career.


NITARA IS A HIGHLY QUALIFIED STUDENT
SHE BECOMES INFECTED WITH COVID AND IS UNABLE TO ATTEND CLASSES
EXAMS
NITARA IS CONCERNED ABOUT HER UPCOMING EXAM
NITYA, HER BEST FRIEND ADVICES HER TO CHEAT IN THE EXAMS
SHE GIVES HER AN EAR BLUETOOTH SPY GADGET
NITARA COMMUNICATES WITH NITYA, WHO IS SEATED OUTSIDE THE EXAM HALL
SHE ALSO WEARS SMART GLASSES WITH A CAMERA, MICROPHONE, AND INTERNET ACCESS
THE INVIGILATOR SEES NITARA'S UNUSUAL CONDUCT AND FRISKS HER.
NITARA IS PROHIBITED FOR THREE YEARS, AND HER ACADEMIC CAREER IS SHATTERED.

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).

Information Technology Act, 2000 :

Section 43 – Unauthorized access to computer systems and data.

Section 66 – Computer-related offenses, including hacking and datatheft.

Section 66B – Punishment for dishonestly receiving stolen computer resources or communication devices.

Motor Vehicles Act, 1988 :

Various sections related to road safety, licensing, registration, and liabilityin case of accidents involving connected vehicles.

Privacy Laws :

Personal Data Protection Bill (proposed) or any relevant amendments toexisting laws. These laws would govern the collection, storage, processing, and sharing of personal data by connected vehicles.

Consumer Protection Laws :

Consumer Protection Act, 2019: Pertinent sections related to productliability and consumer rights in case of defects or malfunctions inconnected car systems.

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

DISHA GOES TO A CAR DEALERSHIP TO PURCHASE HER FIRST CAR

SHE IS IMPRESSED BY THE CONNECTED VEHICLE.

MAJORITY OF THE CARS FUNCTIONALITIES CAN BE OPERATED REMOTELY VIA CELL PHONE APP

HER EX-BOYFRIEND ARUSH WAS OFTEN SPYING AND SNOOPING ON HER.

HE DISCOVERS SECURITY FLAWS IN HER LINKED AUTOMOBILE AND HACKS IT.

ARUSH GAINS ACCESS TO HER CURRENT LOCATION AS WELL AS OTHER FACTS ABOUT HER VOYAGE.

DISHA HAD NOT KEPT HER CARS FIRMWARE AND SOFTWARE UPDATED!

THE RESULTS OF HER LAZINESS INCLUDE VEHICLE THEFT, MANIPULATION OF SAFETY- CRITICAL EQUIPMENT, AND TESTING OF PERSONAL DATA.

SOME OF THE SECURITY THREATS ASSOCIATED WITH CONNECTED CARS INCLUDE MISCONFIGURATION AND DENIAL OF SERVICE.

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)

NDPS Act:

Section 8(c) – Prohibition of Certain Operations

Section 18 – Punishment for contravention in relation to manufactured drugsand preparations

Section 21 – Punishment for contravention in relation to poppy straw

Section 27A – Punishment for financing illicit traffic and harbouring offenders

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 WHO DOES WELL IN SCHOOL.
SHE BREAKUP WITH HER BOYFRIEND ANUDEEP OVER A TRIVIAL REASON.
ISHYA FALLS INTO DEPRESSION AS A RESULT OF HER INABILITY TO MOVE ON FROM THE SEPARATION.
ISHYA LOOKS FOR WAYS TO COMBAT DESPAIR, MEDICATIONS TO KEEP HER JOYFUL, AND SO ON.
DRUGS
DRUGS ADV
SHE RECEIVES ADVERTISING AND EMAILS FOR RECREATIONAL DRUGS BASED ON HER SEARCH RESULTS.
ORDER SUCCESS
SHE ORDERS THEM QUIETLY VIA THE DARK WEB, AND THEY ARE DELIVERED TO HER HOUSE
INITIALLY, NEITHER HER FRIENDS NOR FAMILY MEMBERS ARE AWARE OF THIS.
THE DRUG CARTEL AND ALL OF ITS CUSTOMERS ARE APPREHENDED BY THE INTELLIGENCE DEPARTMENT.
ISHYA IS ARRESTED FOR HAVING AND USING A PSYCHOTROPIC MEDICATION.

DOXING

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. Doxing 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

Section 66C – Identity Theft (Information Technology Act, 2000): Thissection deals with the punishment for identity theft.

Section 66D – Cheating by Personation (Information Technology Act,2000): This section addresses the offense of cheating by personation using acomputer resource

Section 72 – Breach of Confidentiality and Privacy (Information TechnologyAct, 2000): This section deals with the punishment for unauthorized access tocomputer material, including personal data, and the breach of confidentialityand privacy.

Section 354D – Stalking (Indian Penal Code, 1860): While not specific tocybercrime, this section criminalizes stalking

Section 509 – Word, Gesture or Act Intended to Insult the Modesty of aWoman (Indian Penal Code, 1860): Again, not specific to cybercrime, thissection could be relevant if the doxxing includes the sharing of explicit orprivate material with the intent to insult or harm the victim.

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


KARTHIK AND RABYA ARE IN A LIVE-IN RELATIONSHIP.
SHE RECEIVES A VERY GOOD JOB OFFER FROM THE UNITED KINGDOM, SOMETHING SHE HAD ALWAYS DESIRED.
RABYA DECIDES TO BREAK HER FOUR-YEAR RELATIONSHIP WITH KARTHIK AND EMBARK ON A NEW ADVENTURE
KARTHIK IS HEARTBROKEN. HE INTENDS TO TEACH HER A LIFE LESSON.
xxx99xxxx
HE PUBLISHES HER PERSONAL PHONE NUMBER.
HE SENDS SCREENSHOTS OF PRIVATE COMMUNICATION, PERSONAL INFORMATION AND BANK ACCOUNT INFORMATION.
RABYA BEGINS TO RECEIVE UNWANTED PHONE CALLS FROM UNKNOWN NUMBERS
STALKERS ALSO FOLLOW HER AROUND HER HOUSE.
RABYA IS SUBJECTED TO 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,

Section 292 IPC.

IT Act

Section 66E – Violation of Privacy: This section deals with capturing,transmitting, or publishing private images of a person without theirconsent, leading to the violation of their privacy

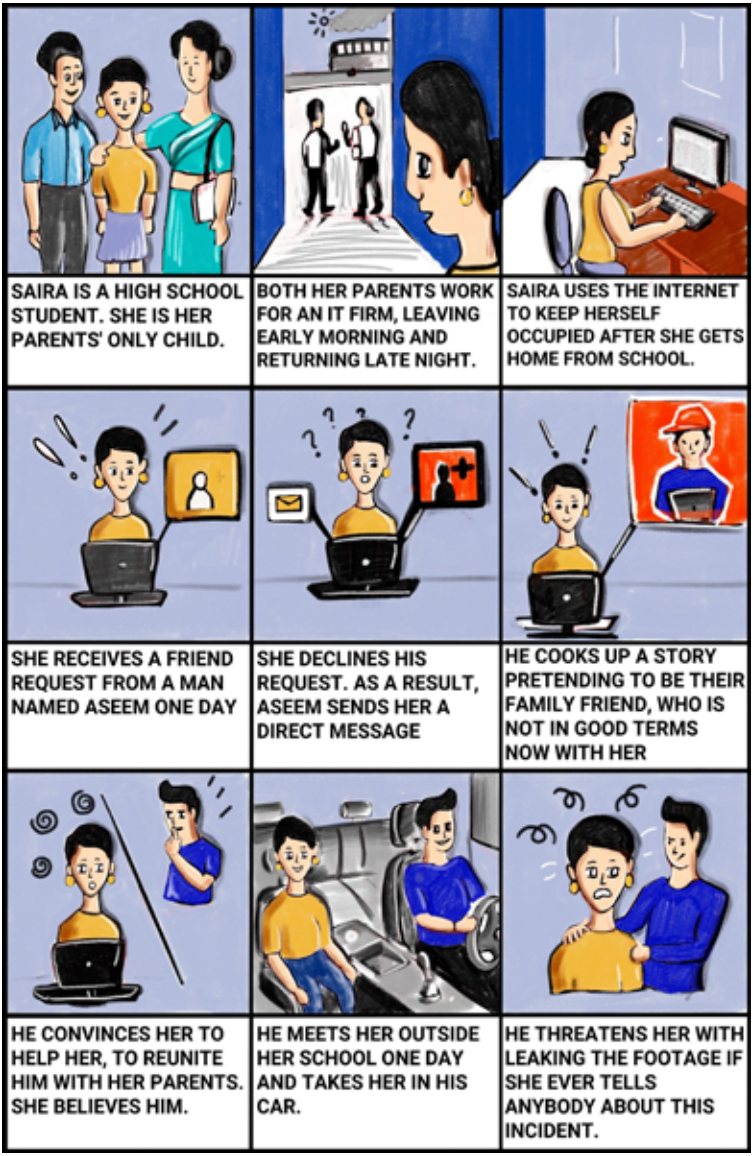
Section 67B – Publishing or Transmitting Obscene Material: Thissection addresses the publishing or transmitting of sexually explicit material, including messages, images, or videos, which can be used astools for grooming activities.

Section 67C – Preservation and Retention of Information by Intermediaries

Section 67D – Punishment for Publishing or Transmitting of Material Containing Sexually Explicit Act

Section 67 – Publishing or Transmitting of Material Containing sexually explicit act, etc. in electronic form

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 STUDENT. SHE IS HER PARENTS' ONLY CHILD.
BOTH HER PARENTS WORK FOR AN IT FIRM, LEAVING EARLY MORNING AND RETURNING LATE NIGHT.
SAIRA USES THE INTERNET TO KEEP HERSELF OCCUPIED AFTER SHE GETS HOME FROM SCHOOL.
SHE RECEIVES A FRIEND REQUEST FROM A MAN NAMED ASEEM ONE DAY
SHE DECLINES HIS REQUEST. AS A RESULT, ASEEM SENDS HER A DIRECT MESSAGE
HE COOKS UP A STORY PRETENDING TO BE THEIR FAMILY FRIEND, WHO IS NOT IN GOOD TERMS NOW WITH HER
HE CONVINCES HER TO HELP HER, TO REUNITE HIM WITH HER PARENTS. SHE BELIEVES HIM.
HE MEETS HER OUTSIDE HER SCHOOL ONE DAY AND TAKES HER IN HIS CAR.
HE THREATENS HER WITH LEAKING THE FOOTAGE IF SHE EVER TELLS ANYBODY ABOUT THIS INCIDENT.

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

Section 43(a) of the IT Act – This section deals with unauthorized accessto computer systems and data breaches

Section 66C of the IT Act – This section pertains to identity theft andcould be applied to cases where individuals' identities are stolen forfraudulent purposes related to cryptocurrencies.

Section 66D of the IT Act – This section addresses cheating bypersonation by using computer resources and communication devices.

Section 420 of the Indian Penal Code (IPC) – Although not part of the ITAct, Section 420 of the IPC covers cheating and dishonestly inducingdelivery of property.

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


RAMYA WORKS IN A CALL CENTER. SHE MOSTLY HAS NIGHT AND WEEKEND SHIFTS.
SHE USED TO PERFORM CRYPTO TRADING DURING THE DAY AFTER HOME TASKS
SHE COMES ACROSS AN AD THAT PROMISES SX RETURNS ON CRYPTO TRADING.
AS RESULT OF ADVERTISEMENT, SHE REGISTERS A CRYPTO TRADING ACCOUNT AND INVESTS HER HARD-EARNED MONEY.
SHE IS OVERJOYED TO SEE THE CRYPTOCURRENCY IN WHICH SHE INVESTED PERFORM WELL.
BONUS
THE TRADING PLATFORM ALSO OFFERS HER A BONUS TO ENTICE HER TO INVEST ADDITIONAL MONEY.
RAMYA BORROWS MONEY FROM FRIENDS AND INVESTS IT IN HER CRYPTOCURRENCY ACCOUNT.
?
WHEN SHE LOGS INTO THE WEBSITE THE NEXT DAY, SHE IS ASTOUNDED TO FIND IT DISAPPEARED.
AFTER SHE GAVE HER WALLET INFORMATION, THE FAKE SITE STOLE HER CRYPTOCURRENCY.

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

IPC Section 370A – Trafficking of persons for exploitation, which includestrafficking for sexual exploitation through electronic means. Disclosing sexually explicit or filthy content Section 292 of IPC.

Sections of Immoral Traffic (Prevention) Act 1956 also known as PITA (Preventionof Immoral Trafficking Act).

67 & 67A IT Act:

IT Act Section 67B – Prohibition of publishing or transmitting sexuallyexplicit material in electronic form, which includes content thatpromotes or facilitates cyber sex trafficking.

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, AN UNDERGRADUATE WITH POOR GRADES, WAS NOT CAMPUS PLACED.
SHE APPEARED FOR OFF-CAMPUS INTERVIEWS AT SERVERAL COMPANIES EVERYDAY.
SALIL, A NEARBY ROWDY, WAS AWARE THAT AMARA NEEDED MONEY.
HE JOINS AMARA'S DATING SERVICE USING A SOCK PUPPET ACCOUNT
HE LAVISHES HER WITH GIFTS SUCH AS PERFUMES, COSMETICS, HANDBAGS AND MANY MORE.
AMARA UNKNOWINGLY VISITS HIS HOUSE AND DISCOVERS A CYBERSEX DEN INVITATION
HE UNDRESSES HER AND LIVE STREAMS IT ON VARIOUS APPS.
ORDEALS REPEATED WITH FRIENDS, HIDDEN BY SOCIAL JUDGEMENT AND FEAR
THE ORDEAL IS REPEATED BY HIS FRIENDS ON HER

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

IT Act

Section 43 – Deals with unauthorized access to computersystems and data breaches.

Section 66 – Addresses computer-related offenses, includinghacking.

Section 66F – Focuses on cyber terrorism, which can berelevant to cyber warfare activities.

Section 70 A – This section was introduced through an amendment in 2008 toprovide the government with powers to issue directions forensuring the security of cyberspace. It empowers thegovernment to take measures for identification, analysis, andprevention of cyber threats.

Section 69 – This section grants the Indian government the power tointercept, monitor, and decrypt any information generated,transmitted, received, or stored in any computer resource if itis necessary for national security or for maintaining publicorder.

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, AN INTROVERTED ENGINEERING STUDENT, IS A TECH GENIUS.
SHE GOES HOME AFTER COLLEGE AND CODES MADLY IN FRONT OF HER LAPTOP.
AN ACTIVE FORUM USER KNOWN FOR HER DEBUGGING AND COMMENTING ABILITIES.
ONE DAY, SHE RECEIVES A MESSAGE SAYING, "ATTACK RUSSIA, LARGE REWARD PROMISED."
TASK
THE PERSON PROMISES THAT SHE WOULD NEVER HAVE TO WORK EVER AGAIN AS SHE WOULD RETIRE WEALTHY.
RUHI USES PROXIES AND STEALTH TACTICS TO LAUNCH DDOS ATTACKS ON RUSSIAN SERVERS
BANK
SHE TARGETS THE POWER GRID AND FINANCIAL SYSTEMS.
RUHI IS IDENTIFIED AS A PREPARATOR BY RUSSIA'S INTELLIGENCE SQUAD.
SHE'S BEEN ARRESTED AND FACES LIFE IN PRISON

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

Information Technology Act, 2000 – Section 43: This section deals withunauthorized access to computer systems, data, or networks.

Information Technology Act, 2000 – Section 66: This section addressescomputer-related offenses, including hacking and unauthorized access.

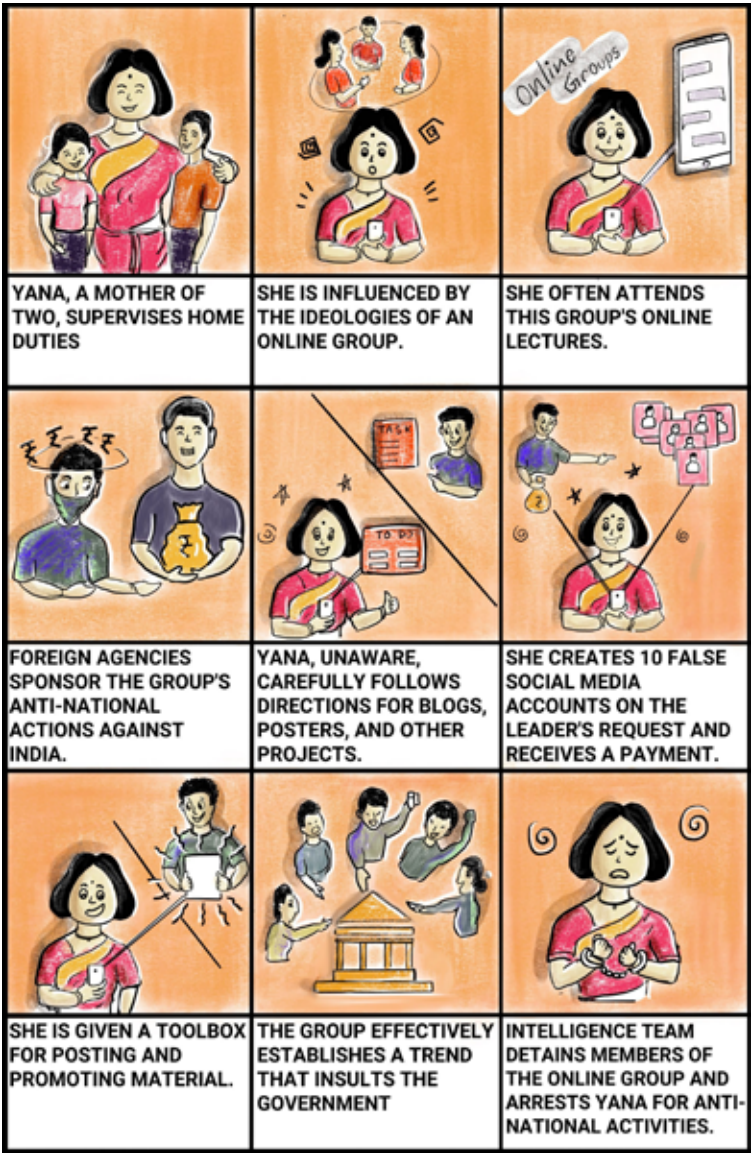
Information Technology Act, 2000 – Section 66F: This section specificallytargets cyber terrorism and related activities.

Information Technology Act, 2000 – Section 70: This section empowers thegovernment to secure cyberspace by issuing directions for the interception,monitoring, or decryption of any information through any computer resource.

Indian Penal Code – Section 124A: While not exclusively related tohacktivism, this section criminalizes sedition.

120A, 121, 122, 153, 153A, 107 IPC

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


YANA, A MOTHER OF TWO, SUPERVISES HOME DUTIES
SHE IS INFLUENCED BY THE IDEOLOGIES OF AN ONLINE GROUP.
Online Groups
SHE OFTEN ATTENDS THIS GROUP'S ONLINE LECTURES.
FOREIGN AGENCIES SPONSOR THE GROUP'S ANTI-NATIONAL ACTIONS AGAINST INDIA.
TASK
TO DO
YANA, UNAWARE, CAREFULLY FOLLOWS DIRECTIONS FOR BLOGS, POSTERS, AND OTHER PROJECTS.
SHE CREATES 10 FALSE SOCIAL MEDIA ACCOUNTS ON THE LEADER'S REQUEST AND RECEIVES A PAYMENT.
SHE IS GIVEN A TOOLBOX FOR POSTING AND PROMOTING MATERIAL.
THE GROUP EFFECTIVELY ESTABLISHES A TREND THAT INSULTS THE GOVERNMENT
INTELLIGENCE TEAM DETAINS MEMBERS OF THE ONLINE GROUP AND ARRESTS YANA FOR ANTI-NATIONAL ACTIVITIES.

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.

Data Protection and Privacy Laws: Laws regulating the collection, storage,processing, and sharing of personal data could apply to user interactionswithin the metaverse. In India, this might include compliance with the Personal Data Protection Bill, once enacted into law.

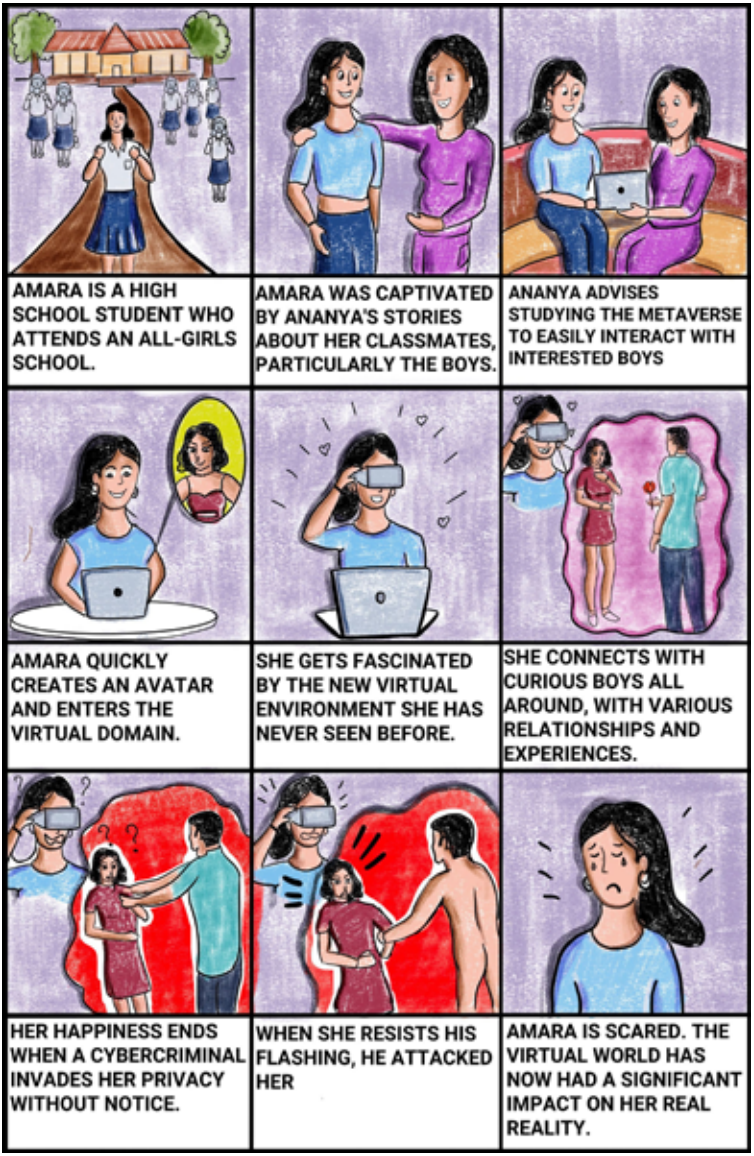
Intellectual Property Laws: Laws governing copyrights, trademarks, andpatents could extend to creations within the metaverse, such as virtual goods,artwork, and designs.

Online Conduct and Harassment Laws: Just as in the real world, laws againstharassment, hate speech, and cyberbullying could apply to interactions in the metaverse.

Digital Transactions and Consumer Protection Laws: If virtual goods andservices are bought and sold within the metaverse, laws related to digital transactions and consumer rights might be relevant.

Cybersecurity Laws : Laws related to cybersecurity and hacking could apply tounauthorized access, data breaches, and other security incidents within themetaverse.

Be well versed that Metaverse is not the real Universe.


AMARA IS A HIGH SCHOOL STUDENT WHO ATTENDS AN ALL-GIRLS SCHOOL.
AMARA WAS CAPTIVATED BY ANANYA'S STORIES ABOUT HER CLASSMATES, PARTICULARLY THE BOYS.
ANANYA ADVISES STUDYING THE METAVERSE TO EASILY INTERACT WITH INTERESTED BOYS
AMARA QUICKLY CREATES AN AVATAR AND ENTERS THE VIRTUAL DOMAIN.
SHE GETS FASCINATED BY THE NEW VIRTUAL ENVIRONMENT SHE HAS NEVER SEEN BEFORE.
SHE CONNECTS WITH CURIOUS BOYS ALL AROUND, WITH VARIOUS RELATIONSHIPS AND EXPERIENCES.
HER HAPPINESS ENDS WHEN A CYBERCRIMINAL INVADES HER PRIVACY WITHOUT NOTICE.
WHEN SHE RESISTS HIS FLASHING, HE ATTACKED HER
AMARA IS SCARED. THE VIRTUAL WORLD HAS NOW HAD A SIGNIFICANT IMPACT ON HER REAL REALITY.

SESSION HIJACKING ATTACK

In a session hijacking attack, cybercriminals gain unauthorized access to an active user session by exploiting vulnerabilities in web applications or networks. By taking control of the session, they can impersonate the user, access sensitive information, or conduct unauthorized actions, compromising the user's privacy and security.

Sections Applicable

Section 43 – This section deals with unauthorized access to computersystems, data theft, and other computer-related offenses.

Section 66C – This section specifically addresses identity theft. If asession hijacking attack is carried out with

the intention ofimpersonating an individual or causing financial or reputational harmto them, this section could be invoked.

Section 66D – This section covers cheating by impersonation using acomputer resource.

Section 66E – This section deals with violation of privacy.

Section 72 – This section protects the confidentiality and privacy ofinformation handled by service providers.

Don't let cyber intruders hijack your online ride;
secure your sessions and protect your stride.

SONAM, AN ENERGETIC CLASS XII STUDENT, IS QUITE ACTIVE ON SOCIAL MEDIA PLATFORMS.

SHE HAS TO PUNISH HERSELF FOR HER ONLINE SHOPPING BINGE!

HER FRIEND SUGGESTED A DISCOUNT BROWSER EXTENSION TO HELP HER SAVE MONEY

SHE ENTHUSIASTICALLY INSTALLED THE EXTENSION AND GRANTED ALL PERMISSIONS.

SHE WAS SMART IN ENABLING 2FA ON ALL OF HER ACCOUNTS

THE EXTENSION SUCCESSFULLY APPLIES DISCOUNTS VIA COUPONS

SHE WOKE UP TO FIND HACKED SOCIAL PROFILES AND SUSPICIOUS TRANSACTIONS.

DESPITE HAVING 2FA ENABLED, THE ADDON GRABBED COOKIES AND HIJACKED ALL ACCOUNTS

REGRETS LACKING AN AUTHENTICATOR APP AND INSTALLING POSSIBLY HARMFUL PLUG-INS.

PROMPT ENGINEERING

Prompt engineering refers to the manipulation of users through carefully crafted messages or prompts to deceive them into revealing sensitive information or performing unintended actions. This social engineering technique is commonly used in phishing attacks, where cybercriminals trick individuals into disclosing passwords, personal data, or financial details.

Sections Applicable

Section 43 – Unauthorized access to computer systems.

Section 66 – Computer-related offenses, including hacking.

Section 67 – Punishment for publishing or transmitting obscene materialin electronic form.

Section 69 – Power to issue directions for interception or monitoring ordecryption of any information through any computer resource.

Section 72 – Breach of confidentiality and privacy.

Section 79 – Intermediaries not to be liable in certain cases.

Section 84A – Modes or methods for encryption. The Central Government may, for secure use of the electronic medium and for promotion of e-governance and e-commerce, prescribe the modes ormethods for encryption.

Section 85 – Offenses by companies.

Stay cautious and alert, so prompt engineering won't make you divert.


ANAND, A 10TH GRADER, IS A COMPUTER GENIUS
App
HE ENJOYS EXPERIMENTING WITH TECHNOLOGY, DEVELOPING APPS, AND HAVING FUN WITH IT.
HE LIKED HIS CLASSMATE ANJALI AND TEXTED HER FREQUENTLY.
HE WAS INCREDIBLY SHY AND RARELY INTERACTED WITH GIRLS.
HE WAS ALWAYS CURIOUS ABOUT ANJALI'S MARITAL STATUS
A CHATBOT ON THE DARK WEB CREATES PROGRAMMES DEPENDING ON ANY PROMPT.
SPY WARE
HE INTENDS TO CREATE SPYWARE USING THIS CHATBOT FOR MALICIOUS PURPOSES.
WITHOUT HER KNOWLEDGE, HE STEALTHILY PUT SPYWARE ON HER PHONE.
HE STARTED WATCHING HER EVERY MOVE.

FILELESS ATTACKS

This attack evades traditional antivirus and detection systems by executing malicious code directly in computer memory, without leaving traces on the file system. These stealthy attacks exploit vulnerabilities in software, making them harder to detect and providing cybercriminals with remote access to systems for data theft, surveillance, or launching further attacks.

Sections Applicable

Section 43 (Unauthorized Access) – This section deals with unauthorized access to computer systems, data, or networks.
Section 43A (Compensation for Data Breach) – This section deals with the compensation for improper disclosure of personal information.
Section 66 (Computer-Related Offenses) – This section covers various computer-related offenses, including hacking.
Section 66B (Punishment for Receiving Stolen Computer Resourcesor Communication Devices) – If fileless attacks involve receiving stolen computer resources or communication devices, this section might be invoked.
Section 66C (Identity Theft) – If a fileless attack leads to identity theft, this section might apply.
Section 66E (Violation of Privacy) – In cases where privacy is violated through fileless attacks, this section might be invoked.
Section 66F (Cyber Terrorism) – If the fileless attack is carried out with the intent of causing terror or destabilizing critical infrastructure, this section could apply.

Silent and sneaky, fileless foes;
fortify your defenses and block their throes.


SAKSHI, A TECH LOVER, SHARED PERSONAL DETAILS VIA DECEPTIVE BANK EMAIL
A LEGITIMATE-LOOKING BANK EMAIL DEMANDED HER INFORMATION. CHECK VALIDITY BEFORE ANSWERING
LINK
SAKSHI CLICKED ON THE LINK WITHOUT HESITATION.
MALICIOUS CODE WAS INJECTED; THE ATTACKER GAINED ACCESS UNNOTICED AND LEFT NO TRACE.
SAKSHI WAS NOT AWARE OF THE RECENT FILELESS ATTACK.
LINK?
THE INTRUDER STOLE HER PERSONAL AND FINANCIAL INFORMATION, INCLUDING CREDIT CARD INFORMATION.
UNAUTHORISED TRANSACTIONS OCCURRED ON SAKSHI'S BANK ACCOUNT. IT WAS DISCOVERED AFTER A FEW DAYS
SHE FELT VIOLATED, AS IF HER STUFF HAD BEEN TAKEN FROM HER HOME.
SAKSHI, A TECH ENTHUSIAST,REALISED THAT FILELESS ASSAULTS ENDANGER EVERYONE, EVEN HERSELF

DELIVERY SCAM

A delivery scam involves cybercriminals sending fake notifications or tracking information to deceive recipients into believing they have a package or delivery pending. The scam aims to trick victims into revealing personal information, clicking on malicious links, or paying fake shipping fees, leading to financial loss or data compromise.

Sections Applicable

Section 43 – Penalty for unauthorized access, damage to computer systems, etc.

Section 66 – Computer-related offenses, including cheating by personation using a computer resource.

Section 419 – Punishment for cheating by personation.

Section 420 – Cheating and dishonestly inducing delivery of property.

Don't fall for the scammer's snare;
verify before you click 'Accept' or 'Share'.


OTP
BANK BALANCE
₹.0/-
SCAM
SANJANA ORDERED PIZZA AND RECEIVED AN OTP CONFIRMATION TEXT FROM AN UNKNOWN NUMBER.
SANJANA QUICKLY SENT THE OTP WITHOUT HESITATION
UNAUTHORISED TRANSACTIONS DEPLETED HER BANK ACCOUNT, MUCH TO HER AMAZEMENT.
SANJANA WAS DUPED BY A DELIVERY OTP FRAUD
SHE REPORTED THE SCAM TO HER BANK AND THE POLICE.
TOO LATE; THE SCAMMER VANISHED WITHOUT A TRACE
SANJANA LEARNED AND RESOLVED TO BE CAUTIOUS IN THE FUTURE.
WHEN SHE SHARED THE STORY, A FRIEND DESCRIBED A SIMILAR PAYMENT AT DELIVERY EXPERIENCE
THE DELIVERY BOY TOOK THE OTP, DID ILLEGAL ACTIONS, AND DELIVERED A WRONG ITEM.

VIRTUAL KIDNAPPING

This is a psychological extortion scheme where perpetrators manipulate victims into believing a loved one has been kidnapped, demanding ransom to ensure their release. Though no actual abduction occurs, the emotional distress and fear generated can lead victims to comply with the demands.

Sections Applicable

Information Technology Act, 2000

Section 66C – This section deals with identity theft, which could be relevant if someone's identity is misused in a virtual kidnapping scenario.

Section 66D – This section covers cheating by impersonation using a computer resource, which could apply if the perpetrator impersonates the victim.

Indian Penal Code (IPC)

Section 503 – This section deals with criminal intimidation, which could be relevant if threats are made in a virtual kidnapping scenario.

Section 506 – This section deals with criminal intimidation by threat of injury to a person's reputation, etc.

Guard your virtual realm with might;
virtual kidnappers shall lose the fight.


BANK
RITHU, A BANK MANAGER, USED SOCIAL MEDIA WELL FOR EMPLOYEE COMMUNICATION
SHE CONNECTS WITH HER EMPLOYEES USING WHATSAPP, INSTAGRAM, AND OTHER ONLINE PLATFORMS.
CLIENT STATED LOAN WAS PAID AND OFFERED PROOF VIA EMAIL
RITHU CLICKED ON THE FILE WITHOUT HESITATION.
UNAWARE, A SINGLE CLICK RESULTED IN HIJACKED SESSIONS AS A RESULT OF MACROS MALWARE.
HER ATTEMPTS TO ACCESS SOCIAL MEDIA ACCOUNTS THE NEXT DAY WERE UNSUCCESSFUL
SHE BECAME A VICTIM OF CYBER KIDNAPPING AND LOST HER ENTIRE ONLINE IDENTITY.
THE HACKER SENT A MESSAGE TO EMPLOYEES DEMANDING MONEY TRANSFER
SCAN
THIS INCIDENT HIGHLIGHTS THE DANGERS OF IMPULSIVE ONLINE ACTIONS.

FORMJACKING

It is an attack that involves injecting malicious code into e-commerce websites' payment forms. The code steals payment card details or personal information entered by customers during online transactions, allowing cybercriminals to engage in payment fraud or identity theft.

Sections Applicable

Information Technology Act, 2000:

Section 43 – This section deals with unauthorized access to computersystems and data breaches.

Section 43A – This section deals with the compensation for failure toprotect sensitive personal data.

Section 66 – This section deals with computer-related offenses,including hacking.

Section 66C – This section deals with identity theft.

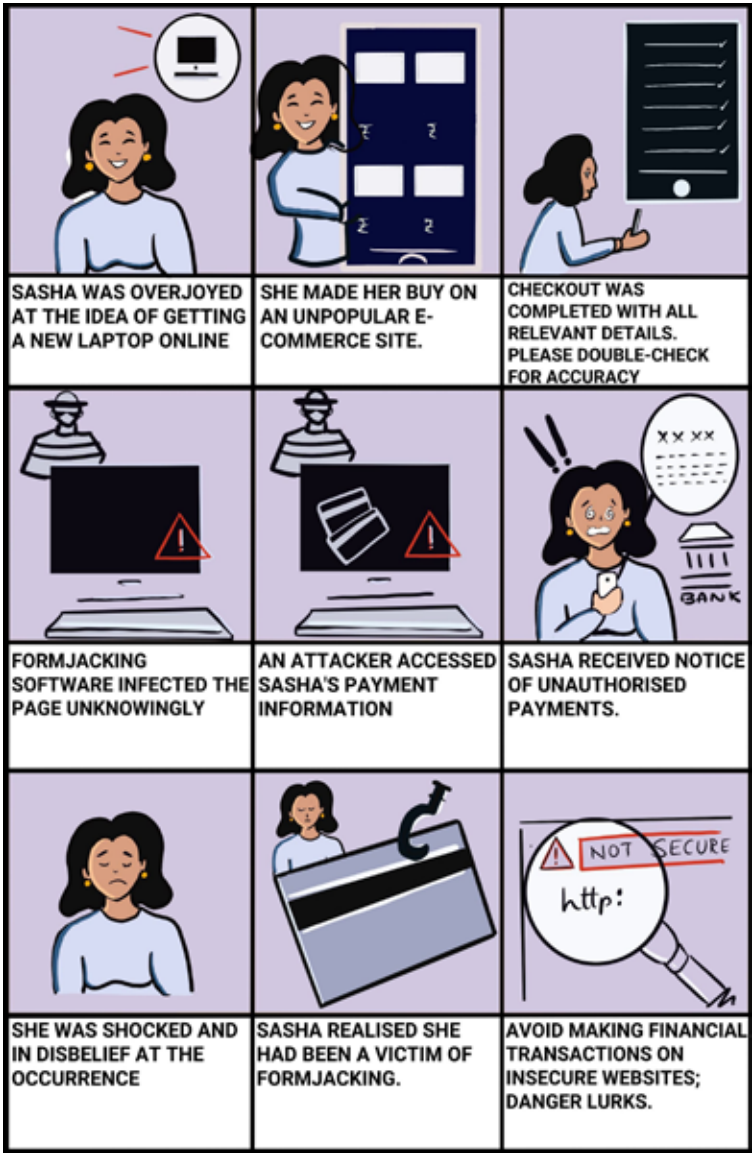
Indian Penal Code, 1860:

Section 420 – This section deals with cheating and dishonestly inducingdelivery of property.

Section 463 – This section deals with forgery.

Section 464 – This section deals with making a false document.

Protect your forms with utmost care;
formjackers won't find their share.


SASHA WAS OVERJOYED AT THE IDEA OF GETTING A NEW LAPTOP ONLINE
SHE MADE HER BUY ON AN UNPOPULAR E-COMMERCE SITE.
CHECKOUT WAS COMPLETED WITH ALL RELEVANT DETAILS. PLEASE DOUBLE-CHECK FOR ACCURACY
FORMJACKING SOFTWARE INFECTED THE PAGE UNKNOWINGLY
AN ATTACKER ACCESSED SASHA'S PAYMENT INFORMATION
XX XX
BANK
SASHA RECEIVED NOTICE OF UNAUTHORISED PAYMENTS.
SHE WAS SHOCKED AND IN DISBELIEF AT THE OCCURRENCE
SASHA REALISED SHE HAD BEEN A VICTIM OF FORMJACKING.
NOT SECURE
http:
AVOID MAKING FINANCIAL TRANSACTIONS ON INSECURE WEBSITES; DANGER LURKS.

CYBERSQUATTING

It refers to the practice of registering domain names similar to established brands or trademarks with the intent to profit from the brand's reputation or sell the domain back to the rightful owner at an inflated price. This can lead to brand dilution, reputation damage, and confusion among consumers.

Sections Applicable

Section 2(1)(r) – Defines "domain name," which is crucial in understanding the context of cybersquatting.

Section 43 – This section deals with penalties and compensation for damage to computer systems

Section 66-D – This section covers the offense of cheating by impersonation using a computer resource

Section 66-A – Although this section was struck down by the Supreme Court of India in 2015 for being unconstitutional,

Section 79 – While not directly focused on cybersquatting, this section deals with intermediary liability.

Section 81 – This section ensures that the provisions of the IT Act have an overriding effect, not with standing anything inconsistent in any other law for the time being in force.

Stake your claim in the digital space;
cybersquatters will find no place.


KIRAN, A SUCCESSFUL IT PROFESSIONAL, HAS GAINED JOB STABILITY
HE IS AN EXPERT IN WEB SERVER ADMINISTRATION.
HIS FIRM UNEXPECTEDLY SETTLED ON MASS LAYOFFS.
KIRAN, UNFORTUNATELY, WAS AFFECTED BY THE LAYOFFS
HE SET OUT ON A HOSTILE VOYAGE AGAINST HIS FIRM, CONSUMED BY RESENTMENT.
KIRAN PURCHASES DOMAINS THAT WERE SIMILAR TO THAT OF HIS COMPANIES.
Real !
?
FAKE !
HE BUILT THE SAME WEBSITE AND ADVERTISED IT WIDELY AS PLANNED
HE MADE MATTERS WORSE BY EMAILING ALL CLIENTS, ADDING TO THE CONFUSION
FRAUD!
Company
THE INCIDENT SEVERELY HARMED THE COMPANY'S REPUTATION.

DNS HIJACKING

This attack involves altering the Domain Name System (DNS) settings of a computer or network, redirecting legitimate traffic to malicious websites. By intercepting and manipulating DNS queries, attackers can lead users to phishing pages, distribute malware, or engage in other malicious activities.

Sections Applicable

Section 43 – This section deals with unauthorized access tocomputer systems and data.

Section 66 – This section deals with computer-related offenses likehacking, which could cover unauthorized access, interference, ordamage to computer systems.

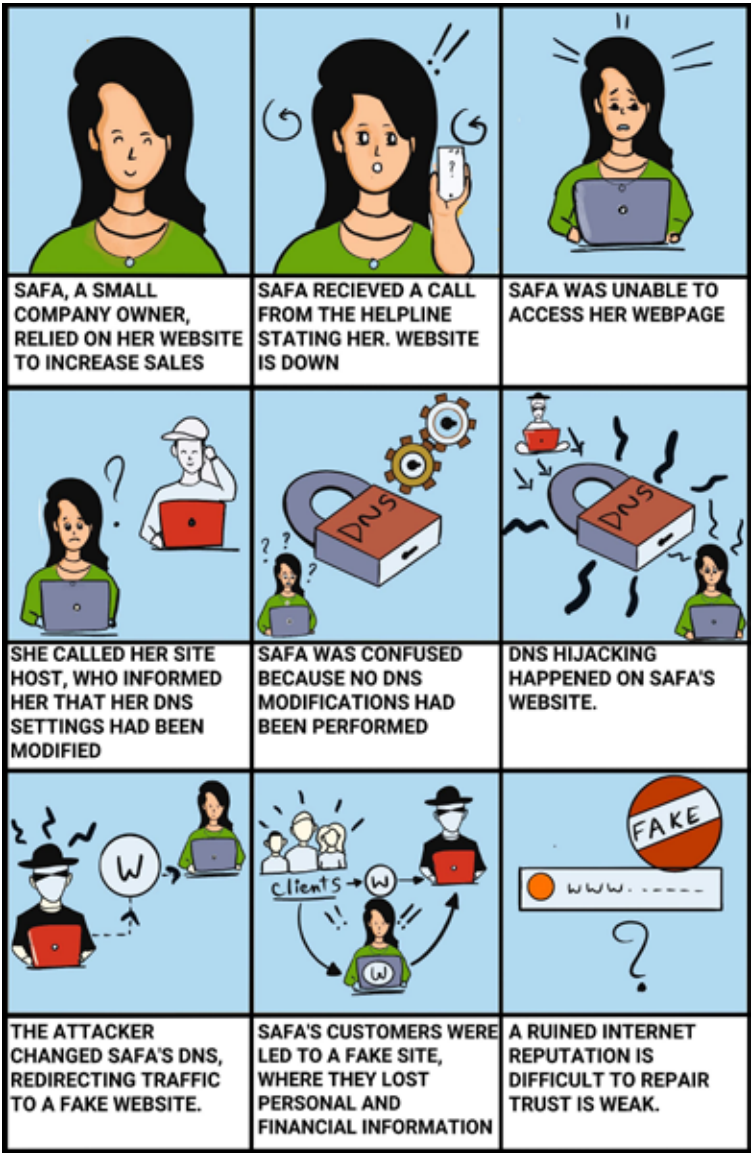
Section 66C – This section deals with identity theft. If someoneuses another person's identity to commit an offense related toDNS hijacking, this section could be invoked.

Section 66D – This section covers cheating by personation usingcomputer resources.

Section 66E – This section deals with violation of privacy.

Section 72 – This section protects the privacy and confidentiality ofinformation stored in a computer resource.

Don't let your online path divert; secure your DNS, stay alert.


SAFA, A SMALL COMPANY OWNER, RELIED ON HER WEBSITE TO INCREASE SALES
SAFA RECIEVED A CALL FROM THE HELPLINE STATING HER. WEBSITE IS DOWN
SAFA WAS UNABLE TO ACCESS HER WEBPAGE
SHE CALLED HER SITE HOST, WHO INFORMED HER THAT HER DNS SETTINGS HAD BEEN MODIFIED
DNS
SAFA WAS CONFUSED BECAUSE NO DNS MODIFICATIONS HAD BEEN PERFORMED
DNS
DNS HIJACKING HAPPENED ON SAFA'S WEBSITE.
W
THE ATTACKER CHANGED SAFA'S DNS, REDIRECTING TRAFFIC TO A FAKE WEBSITE.
Clients
W
W
SAFA'S CUSTOMERS WERE LED TO A FAKE SITE, WHERE THEY LOST PERSONAL AND FINANCIAL INFORMATION
FAKE
www.
A RUINED INTERNET REPUTATION IS DIFFICULT TO REPAIR TRUST IS WEAK.

SMS BOMBING

It is a form of harassment where attackers overwhelm a victim's mobile device with a large number of unwanted text messages, disrupting normal communication and potentially causing psychological distress. This attack aims to disrupt the victim's peace of mind or sabotage their ability to use their phone.

Sections Applicable

Section 66C – Identity theft : This section deals with punishment foridentity theft, which includes dishonestly using another person'selectronic signature, password, or any other unique identificationfeature.

Section 66D – Cheating by personation using computer resource : This section addresses the act of cheating by personation using acomputer resource, and it prescribes penalties for such actions.

Section 43 – Penalty and compensation for damage to computer, computer system, etc. : This section deals with penalties forunauthorized access to computer systems, data breaches, and causingdamage to computer resources.

Section 66 – Computer-related offenses : This section covers variousoffenses related to computer systems, including hacking, unauthorizedaccess, and introduction of viruses.

Bombarded by texts, it's no fun;
safeguard your phone, block the SMS gun.


SRUTHI, A CHEERFUL TEEN, LOVES TEXTING HER FRIENDS.
HER PHONE CONSTANTLY BUZZES WITH NOTIFICATIONS
TEXT MESSAGES CONTINUE TO FLOOD HER PHONE!
Storage
TEXT MESSAGES CONTINUE TO FLOOD MY PHONE'S MEMORY.
BLOCK
DESPITE TRYING TO BLOCK THE NUMBER, IT KEEPS CONTINUING.
AS A RESULT, SRUTHI'S PHONE FREEZES, PROHIBITING CALLS AND TEXTS.
SRUTHI STRUGGLES WITH DESPAIR AND WONDERS WHAT THE POINT OF HER ORDEAL IS.
SHE REALISES SHE'S BEEN SMS BOMBED, A TERRIBLE TRICK PLAYED ON HER BY SOMEONE.
Phone Number
Sharing
THIS EXPERIENCE HAS MADE SRUTHI WARY OF DISCLOSING HER PHONE NUMBER ONLINE

INSIDER THREATS

Refers to security risks posed by individuals with legitimate access to an organization's systems, networks, or sensitive information. These threats may arise from employees, contractors, or business partners who intentionally or unintentionally misuse their privileges to steal data, commit fraud, or compromise the organization's security.

Sections Applicable

Section 43A – Compensation for Data Breach

Section 66C – Identity Theft

Section 66D – Cheating by Personation by using Computer Resource

Section 72 – Breach of Confidentiality and Privacy

Section 72A – Punishment for Disclosure of Information in Breach of Law

Section 408 – Criminal Breach of Trust by Clerk or Servant

Be cautious of those who reside within;
trust but verify, and potential harm will thin.


RAJ IS A RELIABLE EMPLOYEE IN A LARGE FIRM WHO IS IN CHARGE OF HANDLING SENSITIVE DATA.
HE WAS AUTHORIZED TO ACCESS THE COMPANY'S VITAL DOCUMENTS.
RAJ WASN'T HAPPY WITH HIS JOB, SO HE WANTED TO LEAVE.
AT A TURNING POINT, HE DECIDED TO SELL THE COMPANY'S PRIVATE DATA TO A COMPETITOR.
DATA
RAJ GOT THROUGH SECURITY AND STOLE DATA UNNOTICED.
MONEY
MONEY
RAJ MANAGED TO GET AROUND THE COMPANY'S SECURITY MEASURES AND STOLE THE DATA WITHOUT BEING CAUGHT.
MONEY
RAJ FELT VICTORIOUS AND LEFT THE COMPANY WITHOUT FEELING GUILTY.
INVESTIGATION
BUT EVENTUALLY, THE COMPANY DISCOVERED THE THEFT AND STARTED AN INVESTIGATION.
FRAUD
RAJ WAS ARRESTED, FACED SERIOUS LEGAL CONSEQUENCES AND HIS REPUTATION WAS SEVERELY HARMED

DO'S AND DON'TS OF CYBER SAFETY

By Adv. Prashanth Jhala

TIPS TO STAY CYBER SAFE

1. KEEP SOFTWARE UPDATED:

Regularly update your operating system, applications, and devices to ensure you have the latest security patches and bug fixes.

2. BEWARE OF PHISHING:

Be cautious of suspicious emails, links, and attachments. Avoid sharing personal information or clicking on unfamiliar links.

3. SECURE YOUR WI-FI NETWORK:

Set a strong password for your Wi-Fi network, enable WPA3 encryption, and change the default router login credentials.

4. USE A VIRTUAL PRIVATE NETWORK (VPN):

When using public Wi-Fi or accessing sensitive information, use a reputable VPN to encrypt your internet connection and protect your data.

5. SECURE SOCIAL MEDIA PROFILES:

Review your privacy settings on social media platforms to control who can see your posts, and be mindful of the information you share publicly.

6. REGULARLY REVIEW ACCOUNT ACTIVITY:

Check your online accounts for any suspicious activity and log out from devices you no longer use.

7. SECURE PHYSICAL DEVICES: Lock your devices with a PIN, password, or biometric authentication. Consider enabling features like "Find My Device" to help locate and remotely wipe your device if lost.

8. USE SECURE NETWORKS:

Avoid conducting sensitive transactions or accessing confidential information over public Wi-Fi networks, as they may be less secure.

9. EDUCATE YOURSELF:

Stay informed about the latest cybersecurity threats and best practices to ensure you're adapting to new security challenges.

10. REGULARLY MONITOR FINANCIAL STATEMENTS:

Keep an eye on your bank and credit card statements for any unauthorized transactions, and report any discrepancies immediately.

11. USE SECURE PASSWORDS:

Create strong, unique passwords for each of your accounts. Avoid using easily guessable information like birthdays or names, and consider using a combination of letters, numbers, and symbols.

12. IMPLEMENT FIREWALL PROTECTION:

Enable a firewall on your devices to control incoming and outgoing network traffic, adding an extra layer of defense against unauthorized access.

13. DISABLE UNNECESSARY SERVICES:

Turn off any unnecessary services or features on your devices to reduce potential vulnerabilities and attack vectors.

14. REGULARLY AUDIT APP PERMISSIONS:

Review the permissions granted to apps on your devices and revoke any that don't seem necessary for the app's function.

15. SECURE CLOUD STORAGE:

If you use cloud storage services, enable strong encryption and utilize two-factor authentication to safeguard your data.

16. BE CAUTIOUS WITH DOWNLOADS:

Only download files and software from reputable sources. Avoid downloading files from unknown websites or clicking on suspicious links.

17. SECURE PHYSICAL DOCUMENTS:

Keep physical documents containing sensitive information in a secure location, and shred any documents you no longer need.

18. USE BIOMETRIC AUTHENTICATION:

Whenever possible, enable biometric authentication methods like fingerprint or facial recognition for an additional layer of security.

19. SECURE IOT DEVICES:

If you have smart home devices, change their default passwords, update their firmware regularly, and isolate them on a separate network if possible.

20. CREATE A DIGITAL ESTATE PLAN:

Prepare a plan for your online accounts and digital assets in case of incapacity or death, including instructions for how to handle them.

WHERE TO REPORT THE CYBER-CRIMES

- 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.
- 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).
- Online portals are also available in mega cities to register cyber-crimes complaints. At the national level, we have https://cybercrime.gov.in/
- 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.
- 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.
- 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.
- You may also call the National Cyber Crime Helpline number 1930 and lodge a complaint.

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

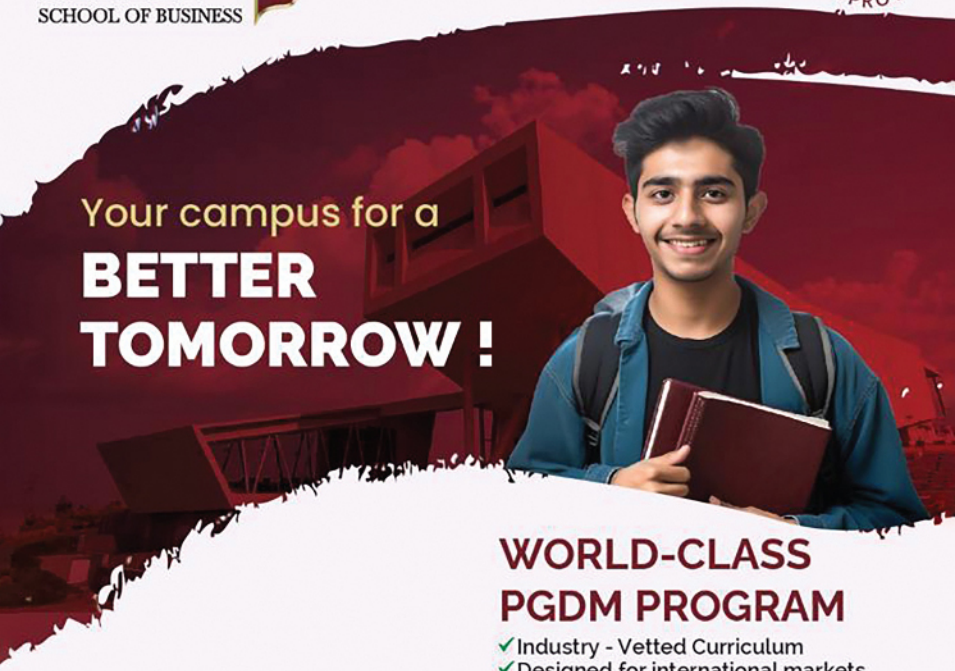
Disclaimer: The above-mentioned explanations made herein are to the best of our knowledge and interpretations and are purely for academic and information purpose only. They may be used as a guiding force. They should not be construed as legal opinion by any stretch of imagination. We are thankful to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

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

MYRA
SCHOOL OF BUSINESS

APPROVED AICTE APPROVED



Your campus for a
BETTER TOMORROW !

WORLD-CLASS PGDM PROGRAM

- ✓ Industry - Vetted Curriculum
- ✓ Designed for international markets

Top international faculty with corporate experience from Harvard, NYU Stern, Texas A&M, top IIMs and IITs

Great Alumni Network

Products and Strategy Specialist at BOSCH | Business Analyst at TECH mahindra | Deputy Manager at HDFC BANK

...and many more

Enhance your learning journey at our **acclaimed campus**

Step into a promising future

- ✓ Center for Excellence in Entrepreneurship and Family Business
- ✓ Unique Digital Mastery Program
- ✓ Unique Career Success Program
- ✓ International Immersion Program
- ✓ Award Winning Campus
- ✓ Merit-based Scholarship available

Academic Partner of CYBERVERSE FOUNDATION
SECURING THE DIGITAL UNIVERSE

State-of-the-art Cybersecurity phygital lab on MSB's campus offers awareness and courses about Cybersecurity.

Call For More Info
+91 99015 83333
+91 99018 53333

Near Infosys, opposite Power Grid, Yelawala, Karnataka

admissions@myra.ac.in
www.myra.ac.in

SURE PASS CYBER PATRIOT Indian Cyber Institute CYBER JAGRITHI trescon

Supported by ISEA Information Security Education & Awareness

Beti Bachao Cyber Crime Se

Don't be a victim of cyber crime.

9 789334 000849

www.cybersafegirl.com

Be a #CyberSafeGirl