SURE PASS

CYBER PATRIOT

Indian Cyber Institute

CYBER JAGRITHI

Supported by

ISEA Information Security Education & Awareness

CYBER SAFE GIRL 7.0

Beti Bachao Cyber Crime Se

70 EYE-OPENING INFOTOONS TO ENSURE ONLINE SAFETY OF NETIZENS

Ananth Prabhu G PhD, Post Doctoral Fellow

Co-Authors : **Adv Prashant Jhala**

Art by : Artist **Anudeep Karkera**

Blueline Group
Since 1968

Blueline Foods (India) Pvt Ltd

FISHERIES • AGRI • CONSTRUCTION • REAL ESTATE

AN ISO 9001:2015, ISO 14001:2015, ISO 22000:2018, ISO 45001:2018, HALAL, GMP+, HACCP& EU CERTIFIED COMPANY

Manufacturers & Exporters Of

FISH MEAL, FISH OIL, FISH SOLUBLE PASTE & OTHER MARINE PRODUCTS

★★★ THREE STAR EXPORT HOUSE ★★★

4th Floor, Suite No 406, Crystal Arc, Balmatta Road, Mangalore - 575 001, Karnataka, India
Ph: +91-824-2427744 / 2441466
Email: info@bluelinefoods.in

Corporate Video

E-Brochure

www.bluelinefoods.in

CYBER SAFE GIRL 7.0

Beti Bachao Cyber Crime Se

70 EYE-OPENING INFOTOONS TO ENSURE ONLINE SAFETY OF NETIZENS

Title: Cyber Safe Girl

Version: 7.0

Publisher: Dr Ananth Prabhu G

Co-Authors: Adv Prashant Jhala

First Published in India in 2018

Copyright (C) Campus Interview Training Solutions 2025

All rights reserved. Without limiting the rights under copyright reserved above, no part of this publication may be reproduced, stored or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording or otherwise), without the prior written permission of the copyright owner.

Requests for permission should be directed to
educatorananth@gmail.com

Designed and printed by
Tarjani Communications Pvt. Ltd, Mangaluru

This is a work of fiction, names, characters, businesses, places, events, locales and incidents are either the products of the author's imagination or used in a fictitious manner. Any resemblance to actual persons, living or dead, or actual events is purely coincidental. The authors and publishers disclaim any liability in connection with the use of the information provided in this book.

9 789334 000849

Credits

Sanjay Sahay
IPS (Rtd)

Roopa D
IPS

Raghavendra Suhas
IPS

Rajshekara N
IPS

Dr Vedamurthi
IPS

Hanumantharaya
IPS

Avinash Pandey
IPS

Chennabasavanna SL
IPS

Hariram S
IPS

Narasimha V T
KSPS

M C Kavitha
KSPS

Ravishankar
KSP

Seema VS
KSP

Gopalkrishna K
KSP

C Naresh Babu
APP

Special Thanks to

Dr Manjunath Bhandary, MLC

Ch A S Murty
ISEA Team

Dr Varadraj G

Sheikh Salim
Director- Overseas

Vivek Raj
Sponsor

Ashwin Bekal

Dhanyashree Bhat

Shonal D

Naveen Kumar

Vaikunt Prabhu

Dr Mustafa B
Tech Resource

Rohan Don
Web Architect

Shashank Kamath

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-Author

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

FOREWORD

The Cyber Safe Girl project was initiated in 2016, inspired by Prime Minister Narendra Modi's vision of Beti Bachao, Beti Padhao. In an increasingly digital world, this initiative extends that mission—Beti Bachao Cyber Crime Se. Women and young girls are often targeted in online frauds, scams, and exploitation, making cyber awareness a crucial part of their safety. Cyber Safe Girl 7.0 is a continuation of this mission, evolving with new threats such as fake influencers, digital arrests, and AI-driven scams. By shedding light on these dangers, this book empowers readers with the knowledge and tools to protect themselves in the digital landscape.

Over the years, Cyber Safe Girl has become a trusted guide for students, professionals, and parents alike. Each new edition addresses the latest cyber crimes, backed by legal provisions and real-world cases, ensuring that readers stay informed and vigilant. As technology advances, so do cyber threats—but with awareness and the right precautions, we can outsmart cyber criminals. This book is not just a resource; it is a movement toward a safer digital future for every girl and woman.

The seventh edition of Cyber Safe Girl incorporates the latest cyber crime tactics and their corresponding legal implications under the IPC, BNSS, BSA, IT Act, and other relevant laws. It serves as a handbook for law enforcement, educators, and digital users, equipping them with the necessary insights to recognize, prevent, and respond to online dangers. Cyber security is not just about technology—it is about people, awareness, and collective responsibility. With this book, we take another step toward making cyberspace safer for all. Jai Hind!

With respectful regards,

K. Annamalai

Former IPS Officer

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

MESSAGE
with good wishes

It gives me immense pleasure to see Cyber Safe Girl 7.0 continue its journey of empowering young minds with digital awareness and cyber resilience. In today's hyper-connected world, every click holds power-either to build or to destroy. This book simplifies complex cyber crimes through engaging infotoons, real-life-inspired stories, and clear legal guidance. It acts as both a mirror and a shield—showing us the reality of online threats while also equipping us with the knowledge to stay safe.

I congratulate the entire team behind this mission for their relentless efforts since 2016. Your commitment to Beti Bachao Cyber Crime Se is both visionary and timely. May this edition educate millions more and inspire them to become digital warriors of safety and responsibility. My heartfelt wishes to every reader-may you browse safely, think critically, and become ambassadors of cyber awareness.

With respectful regards,

Prithesh Shetty

The Mysore Cafe

Topics

The offences and their modus operandi are not gender specific but are gender neutral.

MOBILE RECHARGE SHOP 01
DEBIT CARD CLONING 03
KEYLOGGER 05
SMS SPOOFING 07
CALL SPOOFING 09
RANSOMWARE 11
CYBER STALKING 13
PICTURE MORPHING 15
PROFILE HACKING 17
ONLINE GAMES 19
JOB CALL LETTER 21
DEEPFAKES 23
DATING WEBSITE 25
CAMERA HACKING 27
SOCIAL TROLLING 29
PONZI SCHEME 31
FAKE MATRIMONIAL PROFILE 33
MOBILE REPAIR SHOP 35
FAKE REVIEWS 37
FAKE PROFILE WITH SEXTORTION 39
CYBER VULTURES 41
APP TRAPS 43
JUICE JACKING 45
WIFI HACKING 47
ONLINE RADICALIZATION 49
HONEY TRAP 51
QR CODE SCAM 53
RFID CLONING 55
DRONE SURVEILLANCE 57
SEARCH ENGINE RESULTS SCAM 59
IDN HOMOGRAPH ATTACK 61
SCRATCH CARD SCAM 63
SIM SWAP 65
CRYPTOJACKING 67
VIDEO CONFERENCE SCAM 69
KIDS MOBILE PHONE 71
SMART HOMES 73
MICRO LOANS 75
BLUE SNARFING 77
STOLEN PHONE 79
EXAM MALPRACTICE 81
CONNECTED CAR 83
DRUG TRAFFICKING 85
DOXING 87
CYBER GROOMING 89
CRYPTO FRAUDS 91

Topics

CYBER SEX TRAFFICKING 93

CYBERWARFARE 95

HACKTIVISM 97

METAVERSE 99

SESSION HIJACKING ATTACK 101

PROMPT ENGINEERING 103

FILELESS ATTACKS 105

DELIVERY SCAM 107

VIRTUAL KIDNAPPING 109

FORMJACKING 111

CYBERSQUATTING 113

DNS HIJACKING 115

SMS BOMBING 117

INSIDER THREATS 119

FAKE INFLUENCER SCAM 121

DIGITAL ARREST 123

JUMPED DEPOSIT 125

CALL MERGE SCAM 127

MALVERTISING 129

WATERING HOLE ATTACK 131

LLM JAILBREAK 133

FAKE NEWS 135

FAKE PRODUCTIVITY APPS 137

STEGANOGRAPHY 139

DO'S AND DON'TS OF CYBER SAFETY 141
by Yashavantha Kumar KN

WHERE TO REPORT THE CYBER-CRIMES 144

GOOGLE ANDROID HARDENING CHECKLIST 145
by Manjunath R G

APPLE IOS HARDENING CHECKLIST 147

DO'S AND DON'TS 149
by Sheik Salim

CYBER SAFETY CHECKLIST FOR STUDENTS 159

CYBER SAFETY CHECKLIST FOR PARENTS 160

CYBER SAFETY CHECKLIST FOR TEACHERS 161

15 DIGITAL WELLBEING & HEALTH TIPS 162

OFFENCES AND RELEVANT PENAL SECTIONS 163

ONLINE COMPLAINT & HELPLINE NUMBERS 166

WE'D LOVE YOUR FEEDBACK! 167

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.

IT Sections Applicable

IPC Sections (to be applied to the Shop Keeper)

IPC Section 354A/BNS 75 - Sexual Harassment and punishment for Sexual Harassment

IPC Section 354C/ BNS 77 - Voyeurism

IPC Section 383/384/ BNS 308 - Extortion (IF ANY DEMAND)

IPC Section 503/BNS 351 - Criminal Intimidation

IPC Section 506/BN 351 - Punishment for Criminal Intimidation

IPC Section 509/BNS 79 - 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/BNS 49 - Punishment for abetment

IPC Section 114/BNS 54 - Abettor present when offence is committed

IPC Section 120B/BNS 61 - Punishment for Criminal Conspiracy

IPC Section 406/BNS 316 - 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. 500/-.
Bharath Recharge
SHOPKEEPER AKHIL MENTIONS THAT NETWORK IS DOWN, HE WILL RECHARGE AFTER SOME TIME.
MEENA RECEIVES A MESSAGE: RS 1500/- CREDITED AFTER HALF AN HOUR.
Bharath Recharge
SHE REVISITS SHOP, SHOPKEEPER AGREES TO COLLECT RS 1000/- LATER.
Hi!
Hi!
AKHIL and MEENA BECOME FRIENDS, TEXT & CALL EACH OTHER.
AKHIL PROPOSES MENA, PROMISING LIFELONG COMPANIONSHIP
MEENA STARTS TRUSTING AKHIL, SPENDS TIME WITH HIM.
LODGE
IN FEW DAYS, AKHIL PERSUADES MEENA TO SPEND TIME IN A HOTEL.
HE SECRETLY RECORDS THE INTIMATE MOMENTS, LATER BLACKMAILS & THREATENS TO PUBLISH. STAY 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.

IT Sections Applicable

IT Act for cloning

Section 43: This section deals with unauthorized access to computer systems, data breaches, and other computer-related offenses.

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/BNS 319 – Punishment for cheating by personation

IPC Section 420/BNS 318 – Cheating

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

IT Act Section 72A – This section deals with the punishment for disclosing personal information obtained in the course of providing services under the terms of lawful contract.

IT Act Section 84A – This section empowers the Central Government to prescribe modes or methods for encryption.

Cloning may blow up your Earnings!

MEENA AND REENA WERE COLLEGE CLASSMATES AND STUDIED TOGETHER.
MEENA'S BOYFRIEND ARJUN, A DRUG ADDICT, FREQUENTLY SEEKS MONEY FROM HER.
ARJUN ALWAYS THREATENED & BLACKMAILED MEENA FOR MONEY.
MEENA ASKS REENA FOR ₹7,500, AND REENA TRUSTINGLY SHARES HER ATM CARD AND PIN.
MEENA WITHDRAWS RS. 7500/- AND RETURNS THE CARD.
NEXT DAY, SURPRISINGLY SHE RECEIVES A RS. 10,000/- DEBIT ALERT.
REENA LEARNED FROM MEENA THAT ARJUN TOOK THE CARD TO WITHDRAW MONEY WHILE MEENA STAYED HOME.
ARJUN USED A SKIMMING DEVICE AND COPIED THE CARD, WITHDREW WITH PIN.
SO, NEVER SHARE YOUR CARD AND Its CREDENTIALS WITH ANYONE. STAY AWARE!

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.

IT Sections Applicable

Key logger installation: IT Act
IT Act Section 43 – Deals with unauthorized access, damage to computer systems, and data.
IT Act Section 66 – Computer Related Offences
Stealing personal information: IT Act
IT Act Section 66C – Punishment for Identity Theft
Creating fake profile & posting private conversation :
IT Act Section 66C – Punishment for Identity Theft
IT Act Section 66D – Punishment for cheating by personation by using computer resources
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO
IT Act Section 72 – Breach of Confidentiality and Privacy
IT Act Section 79 – Intermediary Liability Protection
IPC Sections:
IPC Section 354A/BNS 75 – Sexual Harassment and punishment for Sexual Harassment
If in hard copy, IPC Sections 292/BNS 294, 293/BNS 295 294/BNS 296

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 A KEYLOGGER ON POOJA'S LAPTOP.
ANUSHA SECRETLY ACCESSES POOJA'S PASSWORDS, PHOTOS, CHATS, EMAILS, AND BROWSING HISTORY.
ANUSHA CREATES A FAKE PROFILE AND SHARES ALL THE DETAILS ON SOCIAL MEDIA PLATFORMS.
VIVEK WAS SURPRISED WITH THE INVASION OF HIS PERSONAL LIFE AND BROKE UP WITH POOJA.
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.

IT Sections Applicable

Act of hoax or trick or deceive a communication
IPC Section
IPC Section 465/BNS 336 – Making a false document (FORGERY)
IPC Section 419/BNS 319 – Punishment for cheating by personation
IT Act Section 43 – While not directly related to SMS spoofing, this section deals with unauthorized access to computer systems, which could apply if someone gains unauthorized access to systems for the purpose of carrying out SMS spoofing.
IT Act Section 43A and Section 72A: These sections deal with the compensation for failure to protect data and confidentiality of information. If SMS spoofing leads to a breach of sensitive information, these sections might come into play.
IT Act Section 66C – This section deals with identity theft. If SMS spoofing issued to impersonate someone else and commit fraud or deceive others, it could be covered under this section.
IT Act Section 66D – Punishment for cheating by personation by using computer resource
IT Act Section 66E – This section addresses violations of privacy and the capturing, publishing, or transmitting of images of a private area of any person without their consent. If SMS spoofing is used to invade someone's privacy in this manner, this section could apply.

SMS are Spoofed by Cyber Crooks!

KHUSHI, 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.
SHE RECEIVES A TEXT ABOUT A ₹5000 WALMART HANDBAG OFFERED FOR ₹500.
EXCITED, KHUSHI CLICKS THE LINK AND MAKES MULTIPLE ONLINE PURCHASES.
BANK
KHUSHI FAILS TO CONNECT TO THE HELPLINE AND VISITS HER BANK TO VERIFY TRANSACTIONS.
PANICKING, SHE CALLS THE CYBER HELPLINE, WHO MENTIONS THAT SHE MIGHT BE A VICTIM OF CYBER FRAUD.
NOW, SHE REALIZES THE LINK WAS FAKE—A CLEAR CASE OF PHISHING AND MESSAGE SPOOFING.
DISCOUNT 90%
KHUSHI VOWS TO AVOID UNKNOWN LINKS AND STAY VIGILANT.
DANGER NIGERIAN -SCAM-
BEWARE OF NIGERIAN SCAMS—STAY CAUTIOUS AND PROTECTED.

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.

IT Sections Applicable

Act of hoax or trick or deceive a communication
IPC Section
IPC Section 465/BNS 336 – Making a false document(FORGERY)
IPC Section 419/BNS 319 – 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 or fraudulently making use of the electronic signature, password or any other unique identification feature of any other person. Call spoofing can fall under the ambit of this section if it involves stealing someone's unique identification feature for wrongful gain.

Additionally, IT Act 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 WHILE HER SON STUDIES IN ANOTHER CITY.
TO KEEP HERSELF OCCUPIED, SHABANA SURFS THE INTERNET AND IS HIGHLY ACTIVE ON SOCIAL MEDIA.
SHABANA ACCEPTED REQUESTS FROM ANYONE WITH MUTUAL FRIENDS, UNAWARE OF SOCIAL ENGINEERING.
ONE DAY, SHE GETS A CALL FROM AN UNKNOWN NUMBER, IMPERSONATING SHAFIQ AND URGENTLY DEMANDING ₹1 LAKH.
SHABANA PANICS AND TRANSFERS THE AMOUNT IMMEDIATELY IN THE ACCOUNT PROVIDED.
9876xxxxx
AFTER TRANSFERRING, SHE CALLS SHAFIQ TO CONFIRM RECEIPT.
SHAFIQ IS SURPRISED AND MENTIONS THAT HE NEVER CALLED HIS MOTHER FOR MONEY.
SHABANA REALISES THAT SHE HAS FALLEN VICTIM TO CALL SPOOFING AND TRANSFERRED MONEY TO A SCAMSTER.
BEWARE OF SCAMMERS WHO USE SOCIAL ENGINEERING TECHNIQUES TO CARRY OUT CYBER FRAUDS.

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 cyber criminals in bitcoin.

IT Sections Applicable

Unauthorised access, Denial, Encryption :

IT Act Section 43 – This section deals with unauthorized access, damage to computer 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 using a computer resource.

Demand without payment :

IPC Section 384/BNS 308 – Extortion

IT Act Section 386/BNS 308 – This section deals with extortion by a putting person in fear of death or grievous hurt.

IPC Section 511/BNS 62 – Punishment for attempting to commit offence punishable with imprisonment for life or other imprisonment

Demand & payment :

IPC Section 384/BNS 308 – Extortion

Sensitize your Hardware and Software to avoid Ransomware!

ALISHA MANAGES A STARTUP WITH 50 STAFF AND 60 COMPUTER DEVICES.
ONE DAY, SHE RECEIVES AN EMAIL WITH AN ATTACHMENT FROM AN UNKNOWN SENDER.
ALISHA'S OUTDATED ANTIVIRUS ALLOWED THE ATTACHMENT TO DOWNLOAD.
UPON OPENING THE FILE, HER INTERNAL FILES GET ENCRYPTED AND THE SYSTEM GETS LOCKED.
A MESSAGE ON THE SCREEN DEMANDS BITCOIN PAYMENT TO UNLOCK THE DEVICE.
ALISHA FINDS NO OTHER WAY BUT TO MAKE THE PAYMENT.
EVEN AFTER PAYMENT THE HACKER WITHHOLDS THE KEY AND THE SYSTEM REMAINS LOCKED.
ALISHA TRIES TO RESTORE DATA AND DECRYPT THE FILES BUT SHE IS UNSUCCESSFUL.
ALISHA REGRETS IGNORING UPDATES AND OPENING UNKNOWN ATTACHMENTS.

CYBER STALKING

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

IT Sections Applicable

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

Offline:
IPC Section 354 D/BNS 78 – Stalking

Online :
IPC Section 354 D/BNS 78 – This section was introduced through the Information Technology (Amendment) Act, 2013, and specifically deals with the offense of cyber stalking. It states that any person who monitors these by a woman of the internet, email, or any other form of electronic communication, commits the offense of cyber stalking. It also criminalizes actions that cause the woman to fear for her safety or the safety of her relatives. Conviction under this section can result in imprisonment for a term which may extend to three years and a fine.

Cyber stalking means
someone is keeping an eye on you remotely!

MONIKA, A SOLO TRAVELLER, LOVES BACKPACKING AND EXPLORING NEW PLACES.
fb
Insta
Snapchat
SHE IS ALSO AN INFLUENCER WHO OPENLY DISCUSSES HER LIFE ON SOCIAL MEDIA WITH HER 10K FOLLOWERS.
Check in!
SHE CONSTANTLY LIVE UPDATES HER WHEREABOUTS ON HER SOCIAL MEDIA STORIES AND POSTS.
Check in
SHE DECIDED TO EMBARK ON A SOLO TRIP TO GOA AND POST HER PLANS ON SOCIAL MEDIA.
YUSUF, RECENTLY RELEASED ON BAIL, TRACKED HER WHEREABOUTS ON SOCIAL MEDIA.
HE BOARDS A BUS AND REACHES THE PLACE THAT MONIKA HAD MENTIONED IN HER POSTS AND TEXTS HER
MONIKA GETS ALARMED AND BLOCKS THE NUMBER UNMINDFUL OF THE DANGER
YUSUF, AWARE OF MONIKA'S MOVEMENTS FOLLOWS HER WAITS AND MOLESTS HER IN A REMOTE LOCATION
MONIKA IS DEVASTATED AND REGRETS SHARING HER PRIVATE DETAILS ON SOCIAL MEDIA.

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.

IT Sections Applicable

IPC Sections

IPC Section 292/BNS 294 – Sale etc of Obscene books etc (if in hardcopy)

IPC Section 465/BNS 336 – Morphing photographs and creating a false electronic record

IPC Section 469/BNS 336 – Making false electronic document for causing defamation

IPC Section 507/BNS 351 – Criminal Intimidation by an Anonymous communication

IPC Section 509/BNS 79 – Word, gesture 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
RIA IS AN 18-YEAR-OLD RESIDENT OF MUMBAI.
SHE IS A JOYFUL GIRL WHO LOVES PHOTOGRAPHY AND INSTAGRAM.
HER INSTAGRAM POSTS ATTRACT THOUSANDS OF LIKES AND COMMENTS
5
ONE DAY SHE RECEIVES A FRIEND REQUEST FROM ARYAN, AND SHE PROMPTLY ACCEPTS
ARYAN INVITES RIA FOR AN AD CAMPAIGN BUT INSTEAD CONFESSES HIS OBSESSION.
RIA, FURIOUS, REJECTS ARYAN AND SHOWS HER DISPLEASURE.
ARYAN, SEEKING REVENGE, MORPHS RIA'S PICTURES INTO EXPLICIT CONTENT.
ARYAN THEN PUBLISHES THE CONTENT ON SOCIAL MEDIA.
RIA REGRETS TRUSTING UNKNOWN PEOPLE ON THE INTERNET. STAY CAUTIOUS!

PROFILE HACKING

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

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/BNS 303 & 380/BNS 305 :
Theft of data or credentials.

IPC Section. 463/BNS 336, 464/BNS 335, 468/BNS 336 :
Forgery of electronic records for fraud.

IPC Section. 507/BNS 351 :
Criminal intimidation through hacking.

Profile Hacking means Security is Lacking!

CYBER
TANYA 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 GRANDPA'S ILL HEALTH
TANYA RUSHES TO THE HOSPITAL SINCE SHE ADORES HER GRANDFATHER.
WHEN SHE IS IN HOSPITAL, SHE RECEIVES PASSWORD RESET NOTIFICATIONS FOR GMAIL AND FACEBOOK.
CYBER
TANYA REALISES SHE DIDN'T LOG OUT PROPERLY, RESULTING IN ACCOUNT COMPROMISE.
LOG OFF
TANYA RECALLS HER PROFESSOR WARNING STUDENTS TO LOG OUT AFTER USING PUBLIC COMPUTERS.
SHE RECALLS THAT USING A VIRTUAL KEYBOARD ENHANCES SECURITY ON PUBLIC COMPUTERS.
FREE
FURTHER, VPN ALSO IMPROVES THE SECURITY ON A PUBLIC WIFI NETWORK.

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.

IT Sections Applicable

Information Technology Act, 2000:
Section 43 – This section deals with unauthorized access to computer systems, computer networks, or data. It covers actions such as hacking, introducing viruses, and damaging computer systems.
Section 66 – This section deals with computer-related offenses, including hacking, identity theft, and other forms of cyber crime
Section 67A – This section deals with the punishment for publishing or transmitting sexually explicit content in electronic form.
Section 67B – This section deals with the punishment for publishing or transmitting material depicting children in sexually explicit acts.
Section 79 – This section provides safe harbor to intermediaries,including online platforms and game hosting services, from liability for third-party content. However, they are required to adhere to certain conditions, including taking down illegal content upon receiving notice.

IPC Sections
IPC Section 299/BNS 100 – Culpable homicide
IPC Section 305/BNS 107 – Abetment of suicide of Child or Insane Person
IPC Section 306/BNS 108 – Abetment of suicide
IPC Section 321/BNS 115 – Voluntarily causing hurt
IPC Section 335/BNS 122 – Voluntarily causing grievous hurt on provocation
IPC Section 336/BNS 125 – 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 AN INTROVERT AND STAYED ISOLATED FROM HER COLLEGE CLASSMATES.
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 WHEN UNNOTICED BY EVERYONE.
TASK
SHE HUNG HERSELF AND APOLOGISED TO HER PARENTS BEFORE THE ACT.
HER LAST 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.

IT Sections Applicable

Fake account / ID: IT Act

Section 43A – Compensation for failure to protect data: This section deals with the liability of a body corporate in case of a breach of sensitive personal data due to negligence in implementing and maintaining 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 deals with 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 revealing information in breach of a lawful contract.

IPC Section 419/BNS 319 – Punishment for cheating by personation
IPC Section 420/BNS 318 – Cheating
IPC Section 465/BNS 336 – Making a false document (DEFINITION SECTION)
IPC Section 468/BNS 336 – Forgery for cheating
IPC Section 471/ BNS 340 – Using forged document as genuine
IPC Section 474/BNS 339 – Procession of forged document
IPC Section 120B/BNS 61 – Punishment for Criminal Conspiracy
IPC Section 34/BNS 3(5) – Acts done by several persons in furtherance of Common Intention

Abatement for offence

a. On the spot : IPC Section 114/BNS 54 – Abettor present when offence is committed

b. Remotely: IPC Section 109/BNS 49 – Punishment for abetment

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

NISHITA COMPLETED HER ENGINEERING WITH FIRST CLASS, BUT SHE WAS NOT ABLE TO SECURE CAMPUS PLACEMENT.
SHE USED TO ALWAYS UPLOAD HER RESUME ON JOB PORTALS, HOPING TO GET A GOOD JOB.
SHE GETS AN EMAIL FOR A WALK-IN INTERVIEW WITH A 7-FIGURE SALARY OFFER.
HOTEL
NISHITA TOOK AN AUTO TO THE 5-STAR HOTEL FOR THE INTERVIEW.
INTERVIEW
SHE ENTERED A SUITE ROOM, SEEING JOB ASPIRANTS EXIT POST-INTERVIEW.
BEFORE NISHITA'S INTERVIEW, A WAITER OFFERED HER A DRINK. SOON, SHE FELT DIZZY.
NISHITA WOKE UP IN A COMPROMISING POSITION, HORRIFIED TO REALIZE SHE HAD BEEN EXPLOITED.
FAKE
SHE CONTACTS THE COMPANY AND REALIZES THE EMAIL WAS A PHISHING SCAM.
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.

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 sections deal with the compensation payable to an individual whose personal data and information have been negligently disclosed, which could be applicable in cases where deepfakes lead to privacy breaches.
IPC Section 419/BNS 319 - Punishment for cheating by personation
IPC Section 420/BNS 318 - 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/BNS 75 - Sexual Harassment and punishment for Sexual Harassment
Section 465/BNS 336 - Making a false document
Section 499/BNS 356 - Defamation
Section 500/BNS 356 - Punishment for Defamation
Section 507/BNS 351 - Criminal Intimidation by an Anonymous communication
SEC 509/BNS 79 – Insulting modesty of women
Stalking: IPC Section 354 D/BNS 78 - Stalking Offline
: IPC Section 354 D/BNS 78 - Stalking Online
IPC Section 120-B/BNS 61 - Punishment for Criminal Conspiracy
IPC Section 34/BNS 3(5) - Acts done by several persons in furtherance of Common Intention
Abatement for offence:
a. On the spot: IPC Section114/BNS 54 – Abettor present when offence is committed
b. Remotely: IPC Section109/BNS 49 – 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 WAS A SOCIAL PERSON WHO HAD MANY FOLLOWERS
JANET WAS IN A RELATIONSHIP WITH JOHN, BROKE UP WITH HIM AND ARJUN GOT TO KNOW.
ARJUN PROPOSED TO JANET, WHO ACCEPTED BUT LATER REALIZED HE WASN'T A SUITABLE MATCH.
JANET ENDED HER RELATIONSHIP WITH ARJUN AND RECONCILED WITH JOHN.
ARJUN BECAME VENGEFUL AND PLANNED TO TEACH JANET A LESSON.
HE CREATED AI DEEPFAKE VIDEOS OF JANET.
A DEEPFAKE VIDEO OF JANET IN A COMPROMISING POSITION WENT VIRAL ON SOCIAL MEDIA.
MOST WHO RECEIVED THE VIDEO BELIEVED IT. DEVASTATED, JANET FILED A CYBER COMPLAINT.

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.

IT Sections Applicable

ITA Section 43A – This section deals with the compensation for failure to protect 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 personal information without consent.
IPC Section 419/BNS 319 – Punishment for cheating by personation
IPC Section 420/BNS 318 – Cheating
IPC Section 354A/BNS 75 – Sexual Harassment and punishment for Sexual Harassment
IPC Section 354C/BNS 77 – Voyeurism
IPC Section 354D/BNS 78 – Deals with stalking.
Stalking : Offline – IPC Section 354 D/BNS 78 – Stalking
Online – IPC Section 354 D/BNS 78 – 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/BNS 351 – Criminal Intimidation by an Anonymous communication
IPC Section 509/BNS 79 – Word, gesture or act intended to insult modesty of a woman
IPC Section 465/BNS 336 – Making a false document

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

RASHMI IS A SOFTWARE ENGINEER.
SHE CHATTED WITH INTERNET BUDDIES BUT QUICKLY GOT BORED.
TINDER
SHE DOWNLOADS A DATING APP TO KILL HER BOREDOM AND BEGINS SWIPING THROUGH PROFILES.
SHE MEETS ALEX, AN ATTRACTIVE MAN LIVING A LIFE OF OPULENCE.
RASHMI AFTER TEXTING AND CALLING ALEX DEVELOPED A LIKING FOR HIM.
ALEX CHARMS RASMI OVER A CANDLELIGHT DINNER, ACTING GENTLEMANLY AND GIFTING HER LAVISHLY.
RASHMI STARTS TRUSTING ALEX AND ONE DAY ALEX SCHEMES AN EMERGENCY AND BORROWS 5 LAKHS FROM HER.
ALEX ABSCONDS AFTER TAKING THE MONEY AND BLOCKS RASHMI ON ALL PLATFORMS.
LATER, RASHMI REALISES THAT ALEX WAS A HABITUAL OFFENDER AND HAS CONNED MANY WOMEN ON DATING APPS.

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.

IT Sections Applicable

Hacking-
IT Act Section 43 - Penalty for unauthorized access to computer systems,data disruption, and theft.
IT Act Section 66 - Computer related offences
Section 66B - Punishment for dishonestly receiving stolen computer resources or communication devices.
Capturing photograph/video:
IPC Section 354C/BNS 77 - 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/BNS 319 - Punishment for cheating by personation
Online Sexual harassment to a woman
IPC Section 354A/BNS 75 - Sexual Harassment and punishment for Sexual Harassment.
IPC Section 354C/BNS 77 - Voyeurism (capturing or transmitting images of private parts without consent).
Stalking : Offline : IPC Section 354D/BNS 78 - Stalking
Online : IPC Section 354D/BNS 78 - Stalking
Publishing online
IT Act 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.
IT Act Section 72 - Breach of Confidentiality and Privacy under the IT Act
IPC Section 507/BNS 351(4) - Criminal Intimidation by an Anonymous communication
IPC Section 509/BNS 79 - Word, gesture or act intended to insult modesty of a woman

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

AMISHA IS A CHEERFUL AND A BEAUTIFUL GIRL.
SHE EXTENSIVELY USES HER PHONE TO CHECK MAILS, SOCIAL MEDIA AND TRANSFER MONEY.
SHE OBSESSIVELY BROWSES UNKNOWN WEBSITES WITHOUT PRECAUTIONS.
SHE UNKNOWINGLY DOWNLOADS A FILE, WHICH WAS A TROJAN WITH MALWARE.
THE MALWARE ACTIVATED HER CAMERAS, SECRETLY RECORDING HER.
REC
MALWARE SECRETLY RECORDS HER IN WASHROOMS THROUGH HER PHONE.
KARTHIK, AMISHA'S FRIEND, INFORMS THAT HE FOUND HER SHOWER VIDEOS ONLINE.
AMISHA WAS DEVASTATED WITH THE NEWS!
SHE REGRETTED NOT USING ANTIVIRUS, A FLIP COVER, OR A CAMERA GUARD.

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.

IT Sections Applicable

IPC Section 507/BNS 351 – Criminal Intimidation by an Anonymous communication
IPC Section 509/BNS 79 – Word, gesture or act intended to insult modesty of a woman

Stalking:
Offline: IPC Section 354D/BNS 78 – Stalking
Online : IPC Section 354D/BNS 78 – Stalking

IT Act Section 66A – Punishment for sending offensive messages through communication service, etc.
IT Act Section 66C – Punishment for identity theft.
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.

Are you Trolling, the law may be soon following!

VEDA, FROM A MIDDLE-CLASS FAMILY, DRESSES MODESTLY FOR COLLEGE AND OUTINGS.
COLLEGE
HOWEVER, MANY OF HER FRIENDS WERE FASHION OBSESSED AND USED TO BE SKIMPILY DRESSED.
COLLEGE
THOSE FRIENDS USED TO MOCK HER AND CALL HER UNFASHIONABLE AND OUTDATED.
GEORGE, A BULLY IN HER COLLEGE, CALLED HER INAPPROPRIATE NAMES LIKE AUNTY JI, BHABHI JI ETC.
VEDA KEPT SILENT WITHOUT ESCALATING THE ISSUE DESPITE FREQUENT ALTERCATIONS WITH GEORGE
meme
meme
GEORGE CONTINUED BULLYING HER AND WENT ON TO CREATE A MEME PAGE ABOUT VEDA & HER LOOKS.
TROLL PAGE
fb
MANY TROLL PAGES GOT CREATED MAKING VEDA A BIG VIRAL JOKE.
VEDA FACED SEVERE HUMILIATION AND WENT INTO DEPRESSION.
VEDA RECOVERED FROM THE TRAUMA WITH DIFFICULTY, REGRETTED NOT LODGING A 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.

IT 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 counter fraudulent practices in securities trading, including Ponzi schemes.

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

IPC Section 120B/BNS 61 – Punishment for Criminal Conspiracy

IPC Section 406/BNS 316 – Punishment for Criminal Breach of Trust

IPC Section 420/BNS 318 – Cheating

IPC Section 34/BNS 3(5) – 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 DREAMS BIG AND HOPES TO GET RICH ONE DAY.
SHE CRAVES ALL THE LUXURIES OF LIFE
ONE DAY SHE COMES ACROSS A WEBSITE PROMISING HIGH RETURNS ON INVESTMENT.
SHE INVESTED $10,000/- AND PROMISED $ 1,000/- INCOME IN ONE MONTH.
SHE RECEIVES $1,000 /- AND IS PROMISED 2X RETURNS FOR ENROLLING TWO MORE.
NEHA BECAME GREEDY & MADE MORE PEOPLE JOIN THE SCHEME TO RECEIVE HIGHER RETURNS.
NEHA EVENTUALLY RAN OUT OF NEW INVESTORS REQUIRED TO SUSTAIN THE RETURNS.
AS THE SCHEME COLLAPSED AND THE ORGANIZER ABSCONDED WITH THE REMAINING FUNDS.
THE LATE STAGE INVESTORS SUFFERED HUGE LOSSES AND PULLED NEHA INTO VARIOUS LITIGATIONS.

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.

IT 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/BNS 318 – Punishment for cheating.
IPC Section 419/BNS 319 – Punishment for cheating by personation
IPC Section 420/BNS 318 – Cheating
IPC Section 464/BNS 335 – Making a false document.
IPC Section 465/BNS 336(2) – punishment for forgery
IPC Section 468/BNS 336(3) – Forgery for purpose of cheating.
IPC Section 471/BNS 340 – Using as genuine a forged document.
IPC Section 507/BNS 351 – 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 WEBSITES
30-YEAR-OLD INDIAN MAN MESSAGES HER, EXPRESSING INTEREST IN HER.
THE PROFILE MENTIONS THAT THE MAN IS A SERVING OFFICER IN CBI.
THEY INSTANTLY CLICK AND EXCHANGE CALLS AND TEXTS.
HE PROPOSES HER, AND FATHIMA BEING BLIND IN LOVE ACCEPTS.
ONE DAY HE TELLS HER THAT HE IS UNDERGOING DEPT ENQUIRY
HE REVEALS THAT HIS ACCOUNT WAS FROZEN AND ASKS 5 LAKHS FROM FATHIMA AND ABSCONDS.
AFTER MONTHS, FATHIMA FINDS OUT THAT HE WAS A CONMAN WHO WAS ARRESTED FOR SCAMMING MANY WOMEN.

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.

IT Sections Applicable

IT Act Section 43A – This section deals with compensation for failure to protect sensitive personal data.

IT Act Section 66 – Computer Related Offences

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

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

IT Act Section 72A – It criminalizes the disclosure of personal information without consent, intending to cause wrongful loss or gain

IPC Section 406/BNS 316 – 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/BNS 351 – Punishment for Criminal Intimidation

IPC Section 507/BNS 351 – Criminal Intimidation by an Anonymous communication

IPC Section 509/BNS 79 – 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 WAS OBSESSED WITH CLICKING PHOTOGRAPHS
SHE STORED HER PRIVATE PHOTOS, INCLUDING INTIMATE PICTURES WITH HER PARTNER.
ONE DAY, SHE DROPPED HER PHONE AND IT STOPPED WORKING.
Mobile shop
SHE GIVES HER PHONE TO A REPAIR SHOP AND WARNS HIM TO NOT ACCESS HER DATA.
TANVI THOUGHT HER LOCKED PHOTOS AND CHATS WERE SAFE.
SHE WAS UNAWARE THAT PATTERNS/PASSCODES COULD BE CRACKED.
WHILE FIXING THE PHONE, THE SHOPKEEPER ILLICITLY DOWNLOADED HER PRIVATE PHOTOS.
DAYS LATER, TANVI WAS SHOCKED TO FIND HER PRIVATE PHOTOS GOING VIRAL ON SOCIAL MEDIA.
TANVI'S PHOTO MISHAP BECOMES A 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.

IT Sections Applicable

IPC Section 406/BNS 316 - Punishment for Criminal Breach of Trust

IPC Section 420/BMS 318 - Cheating

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

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

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

Fake Reviews may give you wrong Overviews!

COLLEGE
NIKKI IS A FIRST YEAR STUDENT AND ASPIRING MODEL.
SHE FREQUENTED PARTIES TO ENSURE THAT SHE SLAYED THE SPOTLIGHT
SHE WORE EXPENSIVE COSMETICS AND LONG-LASTING PERFUME.
SHE SOUGHT AFFORDABLE ONLINE ALTERNATIVES FOR BUYING THOSE ITEMS.
LESS 50%
WHILE SEARCHING, SHE FOUND A WEBSITE WITH 50% DISCOUNT FOR THE SAME PRODUCTS.
REVIEWS
SHE REVIEWED THAT VERIFIED RATINGS: 4 STAR AVERAGE.
TRUSTING THE REVIEWS, SHE BOUGHT FEW COSMETICS.
AFTER USING THE PRODUCTS SHE GOT SEVERE RASHES AND HAD TO BE HOSPITALISED.
REAL
FAKE
NIKKI'S ERROR HIGHLIGHTS THE IMPORTANCE OF NOT TO BLINDLY TRUST RANDOM 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.

IT 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/BNS 318 – Cheating.
IPC Section 416/BNS 319 – Cheating by personation.
IPC Section 419/BNS 319 – Punishment for cheating by personation
IPC Section 354A/BNS 75 – Sexual Harassment and punishment for Sexual
IPC Section 354C/BNS 77 – Voyeurism
IPC Section 354D/BNS 78 – Stalking.
IPC Section 503/BNS 351 – Criminal intimidation.
IPC Section 507/BNS 351 – 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/BNS 79 – 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 OF WHICH DRESS TO CHOOSE; SHE TOOK THREE DRESSES AND WENT TO THE TRIAL ROOM.
UNAWARE THAT THE MIRROR WAS A SPY MIRROR WITH A CAMERA RECORDING HER THROUGHOUT
A DAY LATER SHE GOT A PHONE CALL FROM A FRIEND ASKING HER WHY SHE OPENED ANOTHER FACEBOOK ACCOUNT.
THE FAKE PROFILE DISPLAYED HER PUBLIC INFO AND A PRIVATE PHOTO.
SHE REPORTS THE PROFILE ONLINE AND DOESN'T APPROACH THE POLICE.
+1(234)
SHE GETS CALLS FROM UNKNOWN NUMBERS DEMANDING MONEY IN LIEU OF THE PRIVATE PHOTOS
MEANWHILE, SHE REALISES THAT HER PHOTOS WERE ALREADY IN CIRCULATION
SHE REGRETS NOT APPROACHING THE POLICE AT THE CORRECT TIME.

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.

IT 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)
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.

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/BMS 318 – 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 INVESTS MAJORITY OF HER MONEY INTO THE SAME SCHEME.
Fraud
SCAM
ONE DAY, DIRECTORS ABSCONDED WITH ALL THE MONEY
THE FIRM'S SERVER WITH INVESTOR DATA WAS COMPROMISED DUE TO WEAK SECURITY.
MRS. LOBO GETS A CALL FROM A SCAMMER POSING AS AN INVESTOR, PROMISING A REFUND.
THE CALLER ASKS MRS LOBO TO SHARE HER CARD CREDENTIALS AND SHE OBLIGES.
Debited
TO HER HORROR, MRS LOBO RECEIVES MULTIPLE SMS OF DEBIT FROM HER ACCOUNT.
THE FRAUDSTER USED SYMPATHY AS A TOOL TO FOOL MRS LOBO OF HER HARD-EARNED MONEY.

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.

IT Sections Applicable

IPC Section 406/BNS 316 – Punishment for Criminal Breach of Trust

IPC Section 420/BMS 318 – Cheating

Information Technology Act, 2000 (IT Act):

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

b. IT Act 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 ARE HAPPILY MARRIED.
VIDYA AND RONAL PLAN A WEEKEND GETAWAY TO MANALI.
THEY CAME BACK WITH TREASURED MEMORIES FROM MANALI.
Health
VIDYA DOWNLOADED A HEALTH APP TO MONITOR HER REAL-TIME PARAMETERS.
SHE EVEN CONSUMED THE APP FOR GETTING ADVICES DURING HER PREGNANCY
Permission
THE APP REQUIRED ACCESS TO HER LOCATION, CAMERA, STORAGE & CONTACTS.
SHE CARELESSLY HAD CONSENTED. THE APP BENEFITTED BY SELLING HER PRIVATE DATA
Shop Now
THE APP ALSO SENT NOTIFICATIONS TO PURCHASE EXPENSIVE MEDICAL KITS FREQUENTLY
STOP
BE CAREFUL, GRANTING PERMISSION ENABLES APP TO COVERTLY ACCESS MEDIA, RECORDS 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.

IT Sections Applicable

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

IT Act Section 66 – Computer Related Offences

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

IT Act Section 66D – This section pertains to cheating by personation using a computer resource.

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

IT Act Section 72 – This section deals with the breach of confidentiality and privacy of information.

Data Theft – **IPC Section 379/BNS 303**

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 WITH VENDORS FOR EVENTS.
SHE GUARANTEES FLAWLESS UNFORGETTABLE WEDDINGS IN HER PLANS
NIDHI VERIFIED ORDERS BY CALLING VENDORS TWICE.
DUE TO EXPENSIVE TRAVEL FOR HER JOB SHE SPENT SIGNIFICANT TIME AT AIRPORTS.
SHE CHARGED HER PHONE AT AIRPORTS 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 STATIONS, COMPROMISING HER PHONE.
SENSITIVE MEDIA GETS 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.

IT Sections Applicable

IT Act Section 66 – Computer Related Offences
IT Act Section 66B – Punishment for dishonestly receiving stolen computer resource or communication device
IT Act Section 66C – Identity Theft
IT Act Section 72 – Breach of Confidentiality and Privacy
Wrongful gain, wrongful loss of internet data:
IPC Section 420/BNS 318 – Cheating
Mischief by internet utility:
IPC Section 425/BNS 324/426/BNS 324 – Mischief
Publishing online
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO
Other provisions of Narcotic Drugs and Psychotropic Substances Act, 1985.

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

Movie
Data Balance
1GB remaining of 5GB
DIVYA, 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.

IT Sections Applicable

IT Act Section 66F – Punishment for Cyber Terrorism

IPC Section 120-B/BNS 61 – Punishment of Criminal Conspiracy

IPC Section 121/BNS 147 – Waging or attempting to wage war, or abetting waging of war, against the Government of India

IPC Section 121A/BNS 148 – Conspiracy to commit offences punishable under Section 121A

IPC Section 122/BNS 149 – Collecting arms, etc., with intention of waging war against the Government of India

Don't get Radicalized, rather be Rationalized!

ANKITA FELL FOR SAIF ONLINE, WHO PROMISED HER LOVE, FREEDOM & A BEAUTIFUL LIFE.
SHE FOUGHT WITH HER FAMILY TO MARRY SAIF DESPITE STRONG RESERVATIONS
RIGHT AFTER MARRIAGE, SAIF TOOK ANKITA TO THE MIDDLE EAST FOR THEIR HONEYMOON.
UPON ARRIVAL, ANKITA WAS FORCED TO FOLLOW SAIF'S RELIGION.
SHE READ AND PRACTICED THE LITERATURE, BLINDFOLDED BY LOVE.
CUT OFF FROM FAMILY AND BRAINWASHED, SHE WAS ASSIGNED TASKS.
MALL
HER TASK INVOLVED DELIVERING A CONSIGNMENT OF ARMS & AMMUNITIONS
BRAINWASHED BY IDEOLOGY, SHE PRAYS AND LATER DETONATES HERSELF IN A MALL, SEEKING HEAVEN.
HER ENTIRE 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.

IT Sections Applicable

Capturing Picture/Video Over Online:

IPC Section 354C/BNS 77 – Voyeurism

IPC Section 509/BNS 79 – 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/BNS 308 – Putting person in fear of injury in order to commit extortion

IPC Section 511/BNS 62 – 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 OFTEN VIDEO CHATTED WITH RANDOM MEN 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.
SUMA ENGAGES IN AN PLAYFUL ACT ONLINE UPON PERSISTENCE BY MOHAN
SHE FORGETS TO DRAW A LINE EXPOSING HERSELF ON THE WEBCAM
AFTER SOME TIME, HER JOY TURNS TO HORROR AFTER RECEIVING A RANSOM WEBCAM EMAIL
SHE WAS THREATENED TO PAY RANSOM OR HAVE HER EXPLICIT VIDEOS LEAKED.
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.

IT Sections Applicable

IPC Section 406/BNS 316 – Punishment for Criminal Breach of Trust
IPC Section 420/BMS 318 – Cheating

Unauthorised Access by installing malware in the background:

IT Act Section 43 – Unauthorized Access
IT Act Section 66 – Computer related offences
IT Act Section 66C – Identity Theft
IT Act Section 66D – Cheating by Personation
IT Act 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.
VISA
SHE MAKES TRANSACTIONS VIA 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 PROVIDER DENIED A REFUND, CLAIMING SHE MADE THE TRANSACTION VOLUNTARILY.
TANYA SCANNED A QR CODE AND INFECTED HER DEVICE.
THE CODE INSTALLS INVISIBLY VIA DRIVE-BY DOWNLOAD.
CAUTION: SCANNING UNKNOWN CODES MAY 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!

IT 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/BNS 318 – 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/BNS 319 – 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.
RFID
SHE KEPT THE RFID CARD INTO HER WALLET AND USED TO PRESS IT FOR SCANNING.
BEING A CARELESS SHE USED TO LEAVE HER WALLET ON THE DESK.
ONE DAY, SHE LEFT HER WALLET AT HER DESK WHILE GOING TO THE WASHROOM
RFID READER
HER COLLEAGUE JOHN EXAMINES HER WALLET THROUGH RFID READER.
JOHN COLLECTS HER OFFICE ID AND HER CREDIT CARD INFORMATION.
SOLD
JOHN SELLS THE CREDIT CARD DETAILS ON DARK WEB FOR MONEY.
REAL
REPLICA
USING THE COLLECTED DETAILS, JOHN CREATES A REPLICA OF AYESHA'S OFFICE ID.
JOHN INFILTRATES THE SERVER ROOM, HACKS SYSTEMS, AND FALSELY IMPLICATED 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.

IT Sections Applicable

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

IPC Section 354A/BNS 75 – Sexual Harassment and punishment for Sexual Harassment

IPC Section 354C/BNS 77 – Voyeurism

IPC Section 354D/BNS 78 – Stalking

IPC Section 509/BNS 79 – 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/BNS 326 – 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.
SHE LEFT HER WINDOWS OPEN, ASSUMING NO ONE COULD OVERLOOK HER PLACE.
LIVING ALONE, SHE MOVED AROUND IN MINIMAL CLOTHING.
AKSHAY, HER EX-BOYFRIEND, 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 HAS 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.

IT 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/BNS 319 – Punishment for cheating by personation

IPC Section 420/BNS 318 – Cheating

IPC Section 465/BNS 336 – Making a false document

IPC Section 468/BNS 336 – Forgery for the purpose of cheating

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

AKSHATA HAD RESERVED A FLIGHT 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 ASKED FOR HER CARD INFO AND CVV FOR VERIFICATION
SHE LOSES RS. 10,000/- FIVE TIMES, TOTALLING RS. 50,000/-.
THE EMAIL SHE RECEIVED WAS A SPOOF, NOT FROM THE AIRLINE.
HACKERS INJECTED A FAKE CALL CENTRE NUMBER IN THE SEARCH RESULTS TO DECEIVE.
ALTHOUGH SHE DIDN'T SHARE THE OTP, SOME FOREIGN GATEWAYS BYPASS IT.
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 typo squatting. 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.

IT 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/BNS 319 – Punishment for cheating by personation

IPC Section 420/BNS 318 – Cheating

Crackers replacing Letters & Characters to commit frauds.

SUCHETA INTENDS TO SEND MONEY TO HER MOTHER, RESIDING IN A DIFFERENT CITY.
GIFT VOUCHER ₹ 500/-
SHE RECEIVES A MESSAGE FROM HER BANK.
EXCLUSIVE OFFER! TRANSACT USING NEFT TODAY AND GET A FREE
WWW.EDFCBANK.COM
UPON OPENING, THE MESSAGE READS AS FOLLOWS
EXCITEDLY, SHE CLICKS THE LINK AND ENTERS HER LOGIN DETAILS.
FAILED LOGIN
AFTER CLICKING SUBMIT, THE WEBPAGE FAILED TO LOAD, RETURNING HER TO LOGIN PAGE.
SHE MAKES ANOTHER ATTEMPT AND SUCCESSFULLY CARRIES OUT THE TRANSACTION.
DEBITED
₹18000
TO HER SURPRISE, SHE FINDS RS 10,000/- DEBITED FROM HER ACCOUNT INSTEAD OF A GIFT VOUCHER.
WWW. ..... .Com
WWW. ..... .Com
IDN HOMOGRAPH ATTACKS, INVOLVING DECEPTIVE DOMAINS RESEMBLING GENUINE ONES.
UPDATE
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.

IT 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/BNS 319 – Punishment for cheating by personation

IPC Section 420/BNS 318 – Cheating

Sharing sensitive Credentials will bring about losses that would be Substantial

AMRIN IS IN A FINANCIAL CRISIS AND EXTREMELY CONCERNED.
SHE HOPED FOR A MIRACLE TO RECEIVE INR 2 LAKHS.
SHE GETS A WHATSAPP SCRATCH CARD PROMISING UP TO 5 LAKHS.
AMRIN CLICKS THE LINK, THE SCRATCH CARD LOADS, AND SHE EAGERLY SCRATCHES IT.
WINNING 3 LAKHS, SHE EXPRESSES GRATITUDE TO GOD FOR ANSWERING HER PRAYERS.
THE WALLER 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 sim jacking, 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.

IT 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/BNS 319 – Punishment for cheating by personation

IPC Section 420/BNS 318 – Cheating

Swapping of Sim could lead you to a situation thats Dim

ARPITHA HAD LINKED HER PHONE NUMBER TO NUMEREOUS 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 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.

CRYPTO JACKING

It is a type of cyber attack in which a hacker co-opts a target's computing power to illicitly mine crypto currency on the hacker's behalf. Crypto jacking 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.

IT 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/BNS 319	- Punishment for cheating by personation
IPC Section 420/BNS 318	- Cheating

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

Crypto jacking 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 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 HAS CLICKED ON AN UNFAMILIAR LINK, WHICH LED TO THE INSTALLATION OF THIS APP.
RAM
PROCESSOR
CYBERCRIMINALS EXPLOIT HER RAM AND PROCESSOR FOR PROFITABLE MINING.
A PAID ANTIVIRUS AND BROWSER EXTENSION COULD HAVE SECURED HER SYSTEM.

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.

IT 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/BNS 319	- Punishment for cheating by personation
IPC Section 420/BNS 318	- 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 A 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 EMBARRESSMENT.
Meeting ID
SHE HAD SHARED THE MEETING ID AND PASSWORD IN THE SAME MESSAGE ON A DISCUSSION FORUM.
A 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 CAREFUL.

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.

IT Sections Applicable

If Gambling is involved:
The acts may attract Provisions of **IT Act Section 69A** 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
AT TIMES, HE BUYS IN-GAME COINS TO ADVANCE FASTER.
HE ERASES THE SMS TRANSACTION MESSAGES TO KEEP HIM MOTHER UNAWARE.
BILL
₹xxxx
SUMAN WAS SURPRISED TO FIND A 14,000/- CHARGE FROM THE PLAY STORE ON HER MONTHLY CREDIT CARD BILL.
PARENTAL CONTROLS ON IOS/ANDROID WOULD HAVE LIMITED ARNAAV'S PHONE USAGE TO STUDIES.

SMART HOMES

Smart-home devices hold a treasure trove of personal information, from your birth date to credit card details, that cyber criminals 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.

IT Sections Applicable

Digital outreach may lead to Privacy Breach

IPC Section 354/BNS 74 – Sexual harassment

IPC Section 354C/BNS 77 – Voyeurism

IPC Section 509/BNS 79 – 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 SALES ON INTERNET OF THINGS (IOT) DEVICES.
60%
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 WIFI CONNECTED ALSO CONTAINED A HIDDEN NANO CAMERA.
THE CAMERA RECORDED BEDROOM ACTIVITIES AND UPLOADED THEM TO THEIR SERVER.
IOTSAFE
SHE HARDLY REALISED THAT IOT DEVICES SHOULD BE BOUGHT FROM REPUTABLE VENDORS AND SECURED PROPERLY.
ANY INTERNET - ENABLED DEVICE CAN BE EXPLOITED FOR SURVELLANCE, TECHNOLOGY IS A TWO-SIDED BLADE. BE CAREFUL.

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.

IT Sections Applicable

IPC Section 420/BNS 318 - Cheating

IPC Section 503/BNS 351/ 506/BNS 351 - Criminal Intimidation

IPC Section 383/BNS 308 - Extortion

IPC Section 306/BNS 108 - Abetment of Suicide

IPC Section 499/BNS 356 / 500/BNS 356 - Defamation

IPC Section 120B/BNS 61 - Criminal Conspiracy

IPC Section 34/BMS 3(5) - 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.
DURING PLACEMENT INTERVIEWS, SAMANTHA REALIZED SHE NEEDED MORE CERTIFICATIONS.
₹ 10,000
WANTING TO ENROLL IN AN ONLINE COURSE, SAMANTHA NEEDED RS. 10,000/- BUT HESITATED TO ASK HER PARENTS.
Ad
SHE DOWNLOADED AN APP THAT PROVIDES EASY LOANS WITHOUT DOCUMENTATION.
LOAN!!
SHE MISSED OUT ON HER FIRST EMI AND SHE GOT A NOTIFICATION TO REPAY THE SAME WITH HEFTY INTEREST.
SHE BARELY REALIZED THE APP ACCESSED HER FRIEND LIST, CONTACTS AND OTHER DATA FROM HER PHONE.
SHE RECEIVED ABUSIVE CALLS, AND HER CONTACTS WERE THREATENED TOO.
%
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. Blue snarfing 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.

IT 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/BNS 319	- Punishment for cheating by personation
IPC Section 420/BNS 318	- 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 E - LEARNING COURSES, SHE PURCHASED A TAB FROM GREY MARKET.
SHE KEPT BLUETOOTH ON SINCE HER EARPODS WERE CONTINUOUSLY CONNECTED TO THE TABLET.
HER NEIGHBOR, ANUSH, HAD DEVELOPED HACKING SKILLS BY STUDYING ONLINE COURSES ON THE DARK WEB.
HE DOWNLOADS A TOOLKIT THAT CAN PAIR WITH VULNERABLE DIGITAL DEVICES.
KNOWING BLUETOOTH'S 10-METER RANGE, HE HIDES IN HER GARDEN AND CONNECTS TO THE TABLET.
AFTER SUCCESSFULLY 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 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.

IT Sections Applicable

IPC Section 378/BNS 303/ 379/BNS 303 – Theft
This section deals with theft and covers the unlawful taking of movable property, including stolen phones.

IPC Section 406/BNS 316
This section pertains to criminal breach of trust.

IPC Section 411/BNS 317
This section deals with dishonestly receiving stolen property.

IT Act Section 66 – Computer related offences

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

IT Act Section 66D – This section pertains to cheating by personation using computer resources.

Lost cell phone, it may affect your cells and hormone

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

AN UNKNOWN PERSON HUNG UP THE PHONE AND SWITCHED IT OFF.

ANAMIKA REALIZED HER PHONE WAS STOLEN. ENABLING "FIND MY DEVICE" COULD HAVE HELPED TRACK IT.

SHE ALSO REALISED SHE COULD HAVE 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.

IT Sections Applicable

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

Information Technology Act, 2000 – IPC Section 43: This section covers penalties for unauthorized access, damages to computer systems, and data breaches.

Indian Penal Code, 1860 – IT Act Section 420: This section deals with cheating and dishonestly inducing delivery of property.

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

UGC Regulations / University Rules: Universities and educational institutions often 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 CONCERENED ABOUT HER UPCOMING EXAMS.
NITYA, HER BEST FRIEND ADVICES HER TO CHEAT IN EXAMS.
SHE GIVES HER AN EAR BLUETOOTH SPY GADGET.
NITARA COMMUNICATED 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 TO TAKE EXAMS 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!

IT Sections Applicable

IPC Section 354D/BNS 78 – 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 :

IT Act Section 43 – Unauthorized access to computer systems and data.

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

IT Act 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 liability in case of accidents involving connected vehicles.

Privacy Laws :

Personal Data Protection Bill (proposed) or any relevant amendments to existing 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 in connected car systems.

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

SHOWROOM
DISHA GOES TO A CAR DEALERSHIP TO PURCHASE HER FIRST CAR.
SHE IS IMPRESSED BY THE CONNECTED VEHICLE.
MAJORITY OF THE CAR FUNCTIONALITIES CAN BE OPERATED REMOTELY BY 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.
UPDATE
DISHA HAD NOT KEPT HER CAR'S FIRMWARE AND SOFTWARE UPDATED.
DATA SECURE
HER LAZINESS LED TO VEHICLE THEFT, SAFETY EQUIPMENT MANIPULATION, AND PERSONAL DATA BREACH.
HER LAZINESS LED TO VEHICLE THEFT, SAFETY EQUIPMENT MANIPULATION, AND PERSONAL DATA BREACH.

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.

IT 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 BREAKS UP WITH HER BOYFRIEND ANUDEEP FOR A TRIVIAL REASON.
ISHYA FALLS INTO DEPRESSION, UNABLE 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 HER FAMILY MEMBERS ARE AWARE OF THIS.
THE DRUG CARTEL AND ALL OF ITS CUSTOMERS ARE APPREHENDED BY THE NARCOTICS 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.

IT Sections Applicable

IT Act Section 66C - Identity Theft (Information Technology Act, 2000): This section deals with the punishment for identity theft.

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

IT Act Section 72 - Breach of Confidentiality and Privacy (Information Technology Act, 2000): This section deals with the punishment for unauthorized access to computer material, including personal data, and the breach of confidentiality and privacy.

IPC Section 354D/BNS 78 - Stalking (Indian Penal Code, 1860): While not specific to cyber crime, this section criminalizes stalking

IPC Section 509/BNS 79 - Word, Gesture or Act Intended to Insult the Modesty of a Woman (Indian Penal Code, 1860): Again, not specific to cyber crime, this section could be relevant if the doxxing includes the sharing of explicit or private 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 WERE IN A LIVE-IN RELATIONSHIP.
SHE RECEIVED 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.
xx99xxxxx
HE PUBLISHES HER PERSONAL PHONE NUMBER.
HE SENDS SCREENSHOTS OF PRIVATE CHATS, PERSONAL DETAILS, AND BANK INFO.
RABYA BEGINS TO RECEIVE UNWANTED PHONE CALLS FROM UNKNOWN NUMBERS.
STALKERS ALSO FOLLOW HER AROUND HER HOUSE.
RABYA IS SUBJECTED TO DOXING 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.

IT Sections Applicable

Sections of POCSO,

IPC Section 292/BNS 294

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

IT Act Section 67B - Publishing or Transmitting Obscene Material: This section addresses the publishing or transmitting of sexually explicit material, including messages, images, or videos, which can be used a stools for grooming activities.

IT Act Section 67C - Preservation and Retention of Information by Intermediaries

IT Act Section 67A - Punishment for Publishing or Transmitting of Material Containing Sexually Explicit Act

IT 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 SPENDS HER TIME ONLINE AFTER SHE RETURNS FROM SCHOOL.
SHE RECEIVES A FRIEND REQUEST FROM A MAN NAMED ASEEM ONE DAY.
INITIALLY HESITENT, SHE ACCEPTS THE REQUEST LATER.
ASEEM COOKS UP A STORY PRETENDING TO BE THEIR FAMILY FRIEND, WHO IS NOT IN GOOD TERMS WITH HER FAMILY ANYMORE.
HE PERSUADES HER TO HELP HIM, TO REUNITE BOTH THE FAMILIES. SHE BELIEVES HIM.
HE LURES HER INTO HIS CAR, SEXUALLY ABUSES HER, AND RECORDS IT.
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 crypto currency 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.

IT Sections Applicable

IT Act Section 43(a) – This section deals with unauthorized access to computer systems and data breaches

IT Act Section 66C – This section pertains to identity theft and could be applied to cases where individuals' identities are stolen for fraudulent purposes related to crypto currencies.

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

IPC Section 420/BNS 318 – Although not part of the IT Act, Section 420 of the IPC covers cheating and dishonestly inducing delivery 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 5X RETURNS ON CRYPTO TRADING.
ENTICED BY AN AD, SHE OPENS A CRYPTO ACCOUNT AND INVESTS HER SAVINGS.
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 HER FRIENDS AND INVESTS IT IN HER CRYPTOCURRENCY ACCOUNT.
?
SHE LOGS INTO THE WEBSITE THE NEXT DAY; SHE IS ASTONISHED TO FIND IT DISAPPEARED.
AFTER SHE GAVE HER WALLET INFORMATION, THE FAKE SITE STOLE HER CRYPTOCURRENCY.

CYBER SEX TRAFFICKING

Cyber sex trafficking, or online sexual exploitation, is a cyber crime and a form of modern slavery. Cyber sex 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.

IT Sections Applicable

IPC Section 499/BNS 356, IPC Section 506/BNS 351, IPC Section 509/BNS 79, IPC Section 354A/BNS 75, IPC Section 370/BNS 143, 347 IPC Section 347/BNS 127, 357 IPC Section 357/BNS 135
IPC Section 370A – Trafficking of persons for exploitation, which includes trafficking 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 (Prevention of Immoral Trafficking Act).

67 & 67A IT Act:
IT Act Section 67B – Prohibition of publishing or transmitting sexually explicit material in electronic form, which includes content that promotes 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 PLACED ON CAMPUS.
SHE APPEARED FOR OFF-CAMPUS INTERVIEWS AT SEVERAL COMPANIES EVERYDAY.
SALIL, A NEARBY ROWDY, WAS AWARE THAT AMARA NEEDED MONEY.
HE GETS CONNECTED TO AMARA THROUGH A DATING APP USING A SOCK PUPPET ACCOUNT.
HE LAVISHES HER WITH GIFTS SUCH AS PERFUMES, COSMETICS, HANDBAGS AND MANY MORE THINGS.
HE INVITED AMARA TO HIS HOUSE AND INDULGES IN PHYSICAL INTIMACY WITH HER.
AFTER SOME TIME AMARA REALISES THAT THE ACT HAS BEEN LIVESTREAMED ON VARIOUS APPS.
AMARA IS THREATENED TO REPEAT THE SAME ACT WITH HIS FRIENDS.
FEARING SOCIAL STIGMA AMIRA OBLIGES AND HER VIDEOS UNDERGOE EXPLOITATION BY SALIL AND HIS FRIENDS.

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.

IT Sections Applicable

IT Act Section 43 – Deals with unauthorized access to computer systems and data breaches.
IT Act Section 66 – Addresses computer-related offenses, including hacking.
IT Act Section 66F – Focuses on cyber terrorism, which can be relevant to cyber warfare activities.
IT Act Section 70 A – This section was introduced through an amendment in 2008 to provide the government with powers to issue directions for ensuring the security of cyberspace. It empowers the government to take measures for identification, analysis, and prevention of cyber threats.
IT Act Section 69 – This section grants the Indian government the power to intercept, monitor, and decrypt any information generated,transmitted, received, or stored in any computer resource if it is necessary for national security or for maintaining public order.

IPC Section 121/BNS 147. 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 WAS 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.

IT Sections Applicable

Information Technology Act, 2000 - Section 43: This section deals with unauthorized access to computer systems, data, or networks.

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

Information Technology Act, 2000 - Section 66F: This section specifically targets cyber terrorism and related activities.

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

IPC Section 120A/BNS 61, IPC Section 121/BNS 147
IPC Section 122/BNS 149, IPC Section 153/BNS 192
IPC Section 153A/BNS 196, IPC Section 107/BNS 45

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 LEADERS 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.

IT Sections Applicable

IPC Section 354/BNS 74, IPC Section 506/BNS 351
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 interactions within 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, and patents 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 against harassment, hate speech, and cyber bullying could apply to interactions in the metaverse.

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

Cyber security Laws : Laws related to cyber security and hacking could apply to unauthorized access, data breaches, and other security incidents within the metaverse.

Be well versed that Metaverse is not the real Universe.

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

SESSION HIJACKING ATTACK

In a session hijacking attack, cyber criminals 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.

IT Sections Applicable

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

IT Act Section 66C – This section specifically addresses identity theft. If a session hijacking attack is carried out with

the intention of impersonating an individual or causing financial or reputational harm to them, this section could be invoked.

IT Act Section 66D – This section covers cheating by impersonation using a computer resource.

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

IT Act Section 72 – This section protects the confidentiality and privacy of information 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 WAS SHORT OF MONEY FOR HER ONLINE SHOPPING BINGE.
BROWSER Extension.
HER FRIEND SUGGESTED A DISCOUNT BROWSER EXTENSION TO HELP HER SAVE MONEY.
SHE ENTHUSIASTICALLY INSTALLED THE EXTENSION AND GRANTED ALL PERMISSIONS.
2FA
SHE WAS SMART IN ENABLING 2FA ON ALL OF HER ACCOUNTS.
60%
Coupon 15%
70% OFF
THE EXTENSION SUCCESSFULLY APPLIES DISCOUNTS VIA COUPONS.
SHE WOKE UP TO FIND HACKED SOCIAL PROFILES AND SUSPICIOUS TRANSACTIONS.
DESPITE HAVING 2FA ENABLED, THE ADD-ON GRABBED COOKIES AND HIJACKED ALL ACCOUNTS.
Authenticator
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 cyber criminals trick individuals into disclosing passwords, personal data, or financial details.

IT Sections Applicable

IT Act Section 43 – Unauthorized access to computer systems.

IT Act Section 66 – Computer-related offenses, including hacking.

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

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

IT Act Section 72 – Breach of confidentiality and privacy.

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

IT Act 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 or methods for encryption.

IT Act 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 LOVES EXPERIMENTING WITH TECHNOLOGY AND DEVELOPING APPS FOR FUN.
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 RELATIONSHIP STATUS.
A CHATBOT ON THE DARK WEB CREATES PROGRAMMES DEPENDING ON ANY PROMPT.
SPY WARE
HE INTENDS TO CREATE A 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 cyber criminals with remote access to systems for data theft, surveillance, or launching further attacks.

IT Sections Applicable

IT Act Section 43 (Unauthorized Access) – This section deals with unauthorized access to computer systems, data, or networks.
IT Act Section 43A (Compensation for Data Breach) – This section deals with the compensation for improper disclosure of personal information.
IT Act Section 66 (Computer-Related Offenses) – This section covers various computer-related offenses, including hacking.
IT Act Section 66B (Punishment for Receiving Stolen Computer Resources or Communication Devices) – If fileless attacks involve receiving stolen computer resources or communication devices, this section might be invoked.
IT Act Section 66C (Identity Theft) – If a fileless attack leads to identity theft, this section might apply.
IT Act Section 66E (Violation of Privacy) – In cases where privacy is violated through fileless attacks, this section might be invoked.
IT Act 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 FAKE BANK EMAIL ASKED FOR HER DETAILS– ALWAYS VERIFY BEFORE REPLYING.
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.
UNAUTHORIZED TRANSACTIONS ON SAKSHI'S ACCOUNT WENT UNNOTICED FOR DAYS.
SHE FELT VIOLATED, AS IF HER STUFF HAD BEEN TAKEN FROM HER HOME.
SAKSHI REALISED THAT FILELESS ASSAULTS ENDANGER EVERYONE, EVEN HERSELF.

DELIVERY SCAM

A delivery scam involves cyber criminals 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.

IT Sections Applicable

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

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

IPC Section 419/BNS 319 – Punishment for cheating by personation.

IPC Section 420/BNS 318 – 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 GOT AN OTP TEXT FROM AN UNKNOWN NUMBER.
SANJANA QUICKLY SENT THE OTP WITHOUT HESITATION.
UNAUTHORIZED TRANSACTIONS DRAINED HER ACCOUNT, SHOCKING HER.
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.

IT Sections Applicable

Information Technology Act, 2000

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

IT Act 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)

IPC Section 503/BNS 351

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

IPC Section 506/BNS 351

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 FOR EMPLOYEE COMMUNICATION.
SHE COMMUNICATES WITH EMPLOYEES VIA WHATSAPP, INSTAGRAM, AND OTHER PLATFORMS.
THE CLIENT STATED THE LOAN WAS PAID AND OFFERED PROOF VIA EMAIL.
RITHU CHECKED 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 cyber criminals to engage in payment fraud or identity theft.

IT Sections Applicable

Information Technology Act, 2000:

IT Act Section 43 – This section deals with unauthorized access to computer systems and data breaches.

IT Act Section 43A – This section deals with the compensation for failure to protect sensitive personal data.

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

IT Act Section 66C – This section deals with identity theft.

Indian Penal Code, 1860:

IPC Section 420/BNS 318 – This section deals with cheating and dishonestly inducing delivery of property.

IPC Section 463/BNS 336 – This section deals with forgery.

IPC Section 464/BNS 335 – This section deals with making a false document.

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

SASHA HAS OVERJOYED AT THE IDEA OF GETTING A NEW LAPTOP ONLINE.
E-COMMERCE
SHE MADE HER PURCHASE IT ON AN UNPOPULAR E-COMMERCE WEBSITE.
DETAILS
CHECKOUT WAS COMPLETED—DOUBLE-CHECK DETAILS 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 HAS BEEN A VICTIM OF FOAMJACKING.
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.

IT Sections Applicable

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

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

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

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

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

IT Act 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 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.

IT Sections Applicable

IT Act Section 43 – This section deals with unauthorized access to computer systems and data.

IT Act Section 66 – This section deals with computer-related offenses like hacking, which could cover unauthorized access, interference, or damage to computer systems.

IT Act Section 66C– This section deals with identity theft. If someone uses another person's identity to commit an offense related to DNS hijacking, this section could be invoked.

IT Act Section 66D – This section covers cheating by personation using computer resources.

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

IT Act Section 72 – This section protects the privacy and confidentiality of information 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 RECEIVED A CALL FROM THE HELPLINE STATING TO HER THAT THE 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 ATTACKERS 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.

IT Sections Applicable

IT Act Section 66C - Identity theft : This section deals with punishment for identity theft, which includes dishonestly using another person's electronic signature, password, or any other unique identification feature.

IT Act Section 66D - Cheating by personation using computer resource :

This section addresses the act of cheating by personation using a computer resource, and it prescribes penalties for such actions.

IT Act Section 43 - Penalty and compensation for damage to computer, computer system, etc. : This section deals with penalties for unauthorized access to computer systems, data breaches, and causing damage to computer resources.

IT Act Section 66 - Computer-related offenses : This section covers various offenses related to computer systems, including hacking, unauthorized access, 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 HER PHONES 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.

IT Sections Applicable

IT Act Section 43A	– Compensation for Data Breach
IT Act Section 66C	– Identity Theft
IT Act Section 66D	– Cheating by Personation by using Computer Resource
IT Act Section 72	– Breach of Confidentiality and Privacy
IT Act Section 72A	– Punishment for Disclosure of Information in Breach of Law
IPC Section 408/BNS 316	– Criminal Breach of Trust by Clerk or Servant

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

RAJ, A RELIABLE EMPLOYEE, HANDLES SENSITIVE DATA IN A LARGE FIRM.
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
RAJ MANAGED TO GET AROUND THE COMPANYS SECURITY MEASURES AND 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.

FAKE INFLUENCER SCAM

A fake social media influencer lures followers with giveaways and luxury brand deals. Victims pay registration fees but never receive prizes. The influencer vanishes after collecting money.

IT Sections Applicable

IT Act, 2000:

Section 66D - Cheating by personation using a computer resource

Section 79 - Liability of intermediaries for hosting fraudulent content

IPC / BNS:

Section 419 / BNS 319(2) - Punishment for cheating by personation

Section 420 / BNS 318(4) - Cheating and dishonestly inducing delivery of property

Section 468/ BNS 336(3) - Forgery for purpose of cheating

Consumer Protection Act, 2019:

Section 2(47) - Misleading advertisements

Section 21 - Penalties for false endorsements

Following fake fame can lead to real fraud!

GIVEAWAY
Wow!
RIYA FOLLOWS A POPULAR INFLUENCER PROMOTING LUXURY BRANDS AND GIVEAWAYS.
ONE DAY, THE INFLUENCER ANNOUNCES A LIMITED-TIME GIVEAWAY OF EXPENSIVE GADGETS.
TO ENTER, RIYA MUST PAY A SMALL "REGISTRATION FEE" AND SHARE HER PERSONAL DETAILS.
ZALI
REGISTRATION
PAY EEE
Wow!
EXCITED, SHE QUICKLY MAKES THE PAYMENT AND SUBMITS HER DETAILS.
DAYS PASS, BUT SHE HEARS NOTHING BACK. MEANWHILE, THE INFLUENCER DELETES THE GIVEAWAY POST.
SHE CHECKS THE PROFILE AGAIN—IT'S FILLED WITH FAKE COMMENTS AND STOLEN IMAGES FROM REAL CELEBRITIES.
WHEN SHE TRIES TO MESSAGE, THE ACCOUNT IS DELETED, AND HER MONEY IS GONE.
SHE REALIZES SHE FELL FOR A SCAM—THOUSANDS OF OTHERS HAVE LOST MONEY THE SAME WAY.
SHE SHOULD HAVE VERIFIED THE INFLUENCER'S AUTHENTICITY BEFORE MAKING ANY PAYMENT.

DIGITAL ARREST

A scammer posing as a police officer threatens victims with fake criminal charges. They demand immediate payment to "settle" the case. Victims panic and transfer money, only to realize there's no such legal provision.

IT Sections Applicable

IT Act, 2000 :

Section 66C - Identity theft

Section 66D - Impersonation using a computer resource

IPC / BNS:

Section 170 / BNS 204 - Personating a public servant

Section 171 / BNS 205 - Wearing garb or carrying a token used by a public servant

Section 383/ BNS 308 - Extortion

Indian Evidence Act, 1872:

Section 65B - Admissibility of electronic records as evidence in fraud cases

BSA, 2023:

Section 63 - Admissibility of electronic records as evidence in fraud cases

If WhatsApp says you're under arrest,
reply with a lawyer emoji and block!

PRIYA GETS A WHATSAPP CALL FROM A MAN CLAIMING TO BE A POLICE OFFICER.
HE SAYS HER NAME IS LINKED TO A FINANCIAL CRIME AND THREATENS ARREST.
HE SOUNDS AUTHORITATIVE AND PROVIDES A FAKE CASE ID.
HE DEMANDS AN IMMEDIATE FINE TO AVOID LEGAL TROUBLE.
BANK
TRANSFER
PANICKED, PRIYA TRANSFERS THE MONEY TO THE GIVEN ACCOUNT.
HE ASKS FOR MORE PAYMENTS TO "SETTLE" THE CASE
LATER, SHE SPEAKS TO A FRIEND AND REALIZES SHE WAS SCAMMED
THERE IS NO LEGAL PROVISION FOR DIGITAL ARREST UNDER ANY INDIAN LAW.
SHE SHOULD HAVE VERIFIED WITH THE REAL POLICE AND NEVER PAID MONEY UNDER PRESSURE.

JUMPED DEPOSIT

A scammer claims to have sent extra money to a seller and fakes a bank notification. The seller, believing the transaction is real, refunds the excess amount. Later, they discover no deposit was made.

IT Sections Applicable

IT Act, 2000 :

Section 66D – Cheating by personation using a computer resource

Section 43 – Unauthorized access and fraud

IPC / BNS:

Section 406 / BNS 316(2) – Criminal breach of trust

Section 417/ BNS 318/(2) – Cheating

Section 420/ BNS 318(4) – Cheating and dishonestly inducing delivery of property

Consumer Protection Act, 2019:

Section 74 – Unfair trade practices

If it's too jumpy to track,
it's too risky to pay!

MEERA LISTS A SOFA ONLINE AND QUICKLY GETS A BUYER OFFERING ₹10,000.
₹10,000
MEERA RECEIVES AN SMS CLAIMING ₹15,000 WAS CREDITED TO HER ACCOUNT.
NOW!
₹5,000
SHE REFUNDS THE "EXTRA PAYMENT" WITHOUT VERIFYING HER BALANCE.
REFUND?
THE BUYER INSISTS SHE SEND THE EXTRA AMOUNT BACK IMMEDIATELY TO AVOID ISSUES.
NOW!
But...
WITHOUT CHECKING HER BANK ACCOUNT, MEERA REFUNDS ₹5,000 AS REQUESTED.
₹5000 DEBITED
AFTER THE CALL ENDS, SHE OPENS HER BANK APP —NO MONEY WAS EVER DEPOSITED!
After the call ends...
NO DEPOSIT
SMS
AFTER THE CALL ENDS, SHE OPENS HER BANK APP —NO MONEY WAS EVER DEPOSITED!
THE SMS WAS FAKE, AND THE BUYER WAS A SCAMMER WHO TRICKED HER INTO SENDING REAL MONEY.
SHE SHOULD HAVE VERIFIED THE ACTUAL BANK BALANCE BEFORE MAKING ANY REFUND.

CALL MERGE SCAM

A fraudster calls a victim, pretending to be from the bank. They ask the victim to merge another call, where an accomplice requests an OTP. The scammer secretly listens, steals the OTP, and empties the victim's account.

IT Sections Applicable

IT Act, 2000:

Section 66C – Identity theft

Section 66D - Cheating by personation

IPC / BNS:

Section 420 / BNS 318(4) – Cheating

Section 468 / BNS 336(3) – Forgery for purpose of cheating

Section 511/ BNS 62 – Attempt to commit offenses punishable with life imprisonment

Telegraph Act, 1885:

Section 25 – Unauthorized interception of messages

Three's not company
when the third one's a fraudster!

SNEHA GETS A CALL FROM SOMEONE CLAIMING TO BE HER BANK'S FRAUD DEPARTMENT.
THE CALLER SAYS HER ACCOUNT IS UNDER ATTACK AND ASKS HER TO STAY ON THE CALL.
HE TELLS HER TO MERGE A SECOND CALL FROM THE "BANK'S VERIFICATION TEAM"
THE SECOND CALLER SAYS AN UNAUTHORIZED TRANSACTION IS IN PROGRESS.
OTP
SPM
796815
HE REQUESTS AN OTP TO BLOCK IT, WHICH IS SENT VIA CALL INSTEAD OF SMS
THE CYBERCRIMINAL, SECRETLY LISTENING ON THE MERGED CALL, NOTES THE OTP.
MOMENTS LATER, SNEHA GETS MESSAGES ABOUT LARGE WITHDRAWALS FROM HER ACCOUNT.
BANK
SHE CONTACTS THE REAL BANK, ONLY TO REALIZE SHE HAS BEEN SCAMMED
!
SHE SHOULD HAVE DISCONNECTED THE CALL AND CONTACTED THE BANK DIRECTLY.

MALVERTISING

Clicking on an online ad for discounts or free products can install malware. The malicious ad redirects users to fake sites that steal login details. Victims lose money or have their data compromised.

IT Sections Applicable

IT Act, 2000:

Section 43 – Unauthorized access and damage to computer systems

Section 66 – Hacking and fraudulent use of computer resources

Section 69A – Blocking of harmful content

IPC / BNS:

Section 425/ BNS 324 – Mischief

Section 426/ BNS 324(2) – Punishment for mischief

Consumer Protection Act, 2019:

Section 89 – Deceptive online advertising penalties

Those flashy ads could flash your data too!

AD
SALE
KAVYA SEES AN ONLINE AD FOR A LUXURY BRAND AT A HUGE DISCOUNT.
Luxury Brand
SALE
SHE CLICKS THE AD, WHICH TAKES HER TO A FLASHY WEBSITE
SPECIAL OFFER
SUBMIT
THE SITE ASKS HER TO ENTER HER DETAILS FOR A "SPECIAL OFFER."
AS SOON AS SHE ENTERS HER DATA, HER PHONE SLOWS DOWN.
UNKNOWN APPS APPEAR ON HER HOME SCREEN.
BANK
HER BANK SENDS A MESSAGE ABOUT AN ATTEMPTED LOGIN.
SHE REALIZES HER SAVED PASSWORDS HAVE BEEN STOLEN.
A CYBERSECURITY EXPERT TELLS HER THE AD CONTAINED MALWARE.
SHE SHOULD HAVE AVOIDED CLICKING ON SUSPICIOUS ADS AND CHECKED THE WEBSITE'S AUTHENTICITY.

WATERING HOLE ATTACK

Hackers infect a trusted website frequently visited by a specific group. When users access the site, their devices get compromised. Cyber criminals steal credentials or install spyware without the victim's knowledge.

IT Sections Applicable

IT Act, 2000:

Section 43 – Unauthorized access
Section 66 – Hacking with intent to cause harm
Section 72 – Breach of confidentiality and privacy

IPC / BNS:

Section 426 / BNS 324(2) – Mischief
Section 471 / BNS 340(2) – Using forged document as genuine
Section 120B / BNS 61(2) – Criminal conspiracy

Even safe-looking sites might be poison puddles – tread carefully

DIVYA REGULARLY VISITS A POPULAR TECH BLOG FOR STUDY MATERIALS.
TECH BLOG
ONE DAY, AS USUAL SHE BROWSES THE WEBSITE
HER LAPTOP SUDDENLY LAGS AND RESTARTS
UNKNOWN POP-UPS BEGIN APPEARING.
HER PASSWORDS STOP WORKING, AND SHE'S LOCKED OUT OF ACCOUNTS.
THE WEBSITE WAS HACKED
SHE LEARNS THAT THE WEBSITE WAS HACKED.
HACKERS TARGETED USERS OF THAT SITE TO STEAL CREDENTIALS USING DRIVE BY DOWNLOADS.
MANY OTHERS REPORT BEING AFFECTED.
SHE SHOULD HAVE USED A STRONG ANTIVIRUS AND CHECKED FOR WEBSITE SECURITY ALERTS.

LLM JAILBREAK

A user manipulates an AI chatbot to bypass safety rules. The AI shares restricted information like hacking techniques. Authorities track misuse, and the user unknowingly becomes part of a cyber crime investigation.

IT Sections Applicable

IT Act, 2000:

Section 66 – Hacking and system manipulation
Section 67B – Publishing harmful content
Section 69 – Government access and control over AI misuse

IPC / BNS :

Section 505 / BNS 353 – Statements conducing to public mischief
Section 120B / BNS 61(2) – Criminal conspiracy

Copyright Act, 1957:

Section 51 – Infringement of copyright through AI-generated content

Don't teach the bot to be bad
– it might graduate with honors in hacking!

RIYA EXPERIMENTS WITH AN AI CHATBOT AND TRIES "JAILBREAK" PROMPTS.
HACKING TRICKS
THE CHATBOT STARTS GIVING HER SECRET HACKING TRICKS.
SHE FEELS EXCITED AND KEEPS TESTING ITS LIMITS.
SHE COPIES THE INSTRUCTIONS TO TRY THEM LATER.
WARNING
DAYS LATER, SHE GETS A WARNING FROM THE AUTHORITIES.
THE AI COMPANY HAD FLAGGED HER ACCOUNT FOR MISUSE.
SHE REALIZES HER ACTIONS WERE BEING MONITORED.
SHE UNKNOWINGLY BECAME PART OF A CYBERCRIME INVESTIGATION.
SHE SHOULD HAVE UNDERSTOOD THE ETHICAL LIMITS OF AI AND AVOIDED MISUSE.

FAKE NEWS

A communal rumor about a violent incident spreads rapidly online. People react emotionally and forward false information. Chaos ensues before authorities confirm the news was fake.

IT Sections Applicable

IT Act, 2000:

Section 69A – Blocking of information in public interest

Section 66F – Cyber terrorism if fake news incites violence

IPC / BNS:

Section 153A / BNS 196 – Promoting enmity between groups

Section 505 / BNS 353 – Statements conducing to public mischief

Section 124A – Sedition, if applicable (This section is deleted in BNS 2023)

Press Council Act, 1978:

Section 14 – Powers of the Press Council to address fake news

Not every forwarded message is the gospel – sometimes it's gossip!

ADITI SEES A SHOCKING NEWS ALERT: "ATTACK ON RELIGIOUS SITE!"

THE MESSAGE CLAIMS A VIOLENT INCIDENT IN HER CITY, SHOWING INJURED PEOPLE.

ANGERED AND ALARMED, SHE QUICKLY FORWARDS IT TO HER FAMILY AND FRIENDS.

WITHIN MINUTES, THE MESSAGE SPREADS ACROSS MULTIPLE WHATSAPP GROUPS.

PEOPLE REACT WITH OUTRAGE—SOME EVEN PLAN PROTESTS AND RETALIATION.

LOCAL NEWS CHANNELS BEGIN REPORTING TENSIONS IN THE AREA.

POLICE CONFIRM THE INCIDENT NEVER HAPPENED; IMAGES WERE OLD AND FROM ANOTHER COUNTRY.

REALIZING HER MISTAKE, ADITI IS FILLED WITH REGRET—SHE HELPED SPREAD FAKE NEWS.

SHE SHOULD HAVE VERIFIED THE NEWS FROM OFFICIAL SOURCES BEFORE FORWARDING IT.

FAKE PRODUCTIVITY APPS

An app claiming to improve focus or time management secretly collects user data. Once installed, it asks for excessive permissions and starts spying on calls and messages. Victims lose privacy and sensitive information.

IT Sections Applicable

IT Act, 2000:

Section 43 – Unauthorized data collection and misuse
Section 66 – Computer-related offenses
Section 72 – Breach of privacy

IPC / BNS:

Section 420 / BNS 318(4) – Cheating
Section 468 / BNS 336(3) – Forgery for fraud
Section 120B / BNS 61(2) – Criminal conspiracy

Consumer Protection Act, 2019:

Section 10 – Product liability for defective digital services

If the app promises too much,
it's probably taking more than your time!

I NEED A GOOD STUDY PLANNER APP FOR MY EXAMS!
TANVI NEEDS A GOOD STUDY PLANNER AND FINDS A "FREE" APP.
THE APP LOOKS PROFESSIONAL BUT SHE DID NOT CHECK RATINGS AND REVIEWS
STUDY PLANNER
INSTALL
SHE INSTALLS IT AND GRANTS ALL PERMISSIONS.
SOON, HER PHONE STARTS ACTING STRANGELY.
ADS
MEGASTORE
ADS
MEGASTORE
ADS
MEGASTORE
INSTALLING
Storage
Contacts
Location
ADS APPEAR EVEN WHEN SHE'S NOT USING THE APP.
!
Unauthorized Login
Gmail
SHE NOTICES UNAUTHORIZED LOGINS TO HER EMAIL.
CYBERSECURITY EXPERTS SAY THE APP WAS STEALING DATA
MANY OTHERS REPORT SIMILAR ISSUES.
SHE SHOULD HAVE DOWNLOADED APPS ONLY FROM TRUSTED SOURCES AND CHECKED REVIEWS.

STEGANOGRAPHY

A seemingly harmless image file hides malicious code. When downloaded or opened, malware gets installed on the device. Cyber criminals use this technique to spread spyware and steal information.

IT Sections Applicable

IT Act, 2000:

Section 66F – Cyberterrorism if used for extremist purposes
Section 69 – Government's power to decrypt and monitor
Section 72 – Breach of confidentiality and privacy

IPC / BNS:

Section 201 / BNS 238 – Causing disappearance of evidence
Section 120B / BNS 61(2) – Criminal conspiracy
Section 124A – Sedition, if applicable (This section is deleted in BNS 2023)

Official Secrets Act, 1923:

Section 3 – Espionage using steganography

If a file looks innocent but acts guilty,
it's steganography in disguise!

NISHA RECEIVES AN IMAGE FILE FROM A FRIEND ON WHATSAPP.
IT LOOKS LIKE A NORMAL MEME, SO SHE OPENS IT.
HER PHONE SUDDENLY STARTS RUNNING SLOWER.
SHE IGNORES IT, THINKING IT'S A MINOR ISSUE.
THE NEXT DAY, HER EMAIL PASSWORD DOESN'T WORK.
HER FRIEND CALLS AND SAYS HIS ACCOUNT WAS HACKED TOO.
SHE CONSULTS A CYBER EXPERT, WHO FINDS MALWARE HIDDEN IN THE IMAGE.
VIRUS
HACKERS USED STEGANOGRAPHY TO SPREAD A VIRUS.
SHE SHOULD HAVE AVOIDED OPENING UNKNOWN FILES AND USED AN UPDATED ANTIVIRUS.

TIPS TO STAY CYBER SAFE

by **Yashavantha Kumar KN, DySP**

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 cyber security 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 **Manjunath R G, DySP**

Basic Security

1. Enable Device Encryption – Ensure full-disk encryption is enabled for data protection.
2. Use Strong Screen Lock – Set a strong PIN, password, or biometric authentication.
3. Disable Smart Lock Features – Avoid unlocking in trusted places to prevent unauthorized access.
4. Turn Off Developer Options – Disable USB debugging and OEM unlocking.
5. Enable Google Play Protect – Keep Play Protect active to scan apps for threats.
6. Install Apps Only from Google Play Store – Avoid side loading APKs from untrusted sources.
7. Use a VPN – Encrypt internet traffic, especially on public Wi-Fi.
8. Enable Automatic Updates – Keep the OS and apps updated for security patches.
9. Review App Permissions – Revoke unnecessary permissions from apps.
10. Disable Unused Connectivity Features – Turn off Bluetooth, Wi-Fi, and NFC when not in use.
11. Use Secure Messaging Apps – Prefer encrypted apps like Signal or WhatsApp.
12. Turn Off Nearby Device Scanning – Prevent unauthorized tracking and data exchange.
13. Restrict Background Data for Apps – Control app internet access when inactive.

14. Disable Clipboard Access for Apps – Avoid clipboard snooping by malicious apps.
15. Set Up Two-Factor Authentication (2FA) – Use Google Authenticator for extra security.
16. Enable Find My Device – Locate or wipe lost devices remotely.
17. Use a Secure DNS – Configure encrypted DNS (e.g., Cloudflare, Google).
18. Disable Google Assistant on Lock Screen – Prevent unauthorized voice access.
19. Turn Off USB File Transfers – Prevent data theft via USB connections.
20. Disable Auto-Connect to Wi-Fi – Avoid automatic connection to open networks.
21. Block Unknown Callers & Messages – Reduce phishing and spam attacks.
22. Monitor Background Running Apps – Stop unused apps from running in the background.
23. Remove Unused Google Accounts – Reduce attack surfaces by limiting linked accounts.
24. Disable Auto-Save Passwords – Use a password manager instead.
25. Turn Off Ad Personalization – Minimize data tracking by disabling personalized ads.
26. Use Secure Folder (Samsung Devices) – Store sensitive files in an encrypted space.
27. Regularly Clear Cache and App Data – Remove stored sensitive information.
28. Avoid Using Public Charging Stations – Use a USB data blocker or charge-only cable.
29. Factory Reset Before Selling – Wipe all data before handing over your device.
30. Monitor Device Logs for Suspicious Activity – Use tools like ADB to check logs for security threats.

APPLE IOS HARDENING CHECKLIST

by **Akshaya Kumar Nayak, OPS**

Basic Security

1. Enable Strong Device Passcode – Use a 6-digit PIN or alphanumeric password.
2. Turn On Automatic Updates – Ensure iOS and app updates are installed automatically.
3. Enable Face ID or Touch ID – Use biometric authentication for secure access.
4. Disable USB Accessories When Locked – Prevent unauthorized access via Lightning port.
5. Turn Off Lock Screen Access – Restrict notifications, Siri, and Control Center on the lock screen.
6. Enable Two-Factor Authentication (2FA) – Secure Apple ID with 2FA.
7. Use Private Wi-Fi Address – Avoid Wi-Fi tracking by enabling randomized MAC addresses.
8. Disable Airdrop for Strangers – Set AirDrop to "Contacts Only" or turn it off.
9. Turn Off Unused Location Services – Manage location access for apps.
10. Use iCloud Keychain for Passwords – Store credentials securely with end-to-end encryption.
11. Limit App Tracking Requests – Prevent apps from tracking your activity.
12. Block Unwanted Messages & Calls – Reduce spam and phishing attempts.
13. Disable Safari Autofill for Passwords – Use a dedicated password manager.

14. Use a VPN for Secure Browsing – Encrypt internet activity on public Wi-Fi.
15. Enable Find My iPhone – Track and remotely wipe lost devices.
16. Disable Bluetooth When Not in Use – Reduce exposure to hacking attacks.
17. Restrict Siri on Lock Screen – Prevent voice access without authentication.
18. Enable Mail Privacy Protection – Block email trackers from gathering data.
19. Limit Camera and Microphone Access – Prevent apps from unnecessary access.
20. Use Sign in with Apple – Protect your identity when signing into apps.
21. Enable Encrypted iCloud Backup – Securely store device backups.
22. Turn Off Shared Wi-Fi Networks – Avoid automatically joining untrusted networks.
23. Disable Analytics & Personalized Ads – Reduce Apple's data collection.
24. Monitor App Permissions Regularly – Revoke access when unnecessary.
25. Enable Private Relay (iCloud+) – Hide IP addresses for better privacy.
26. Clear Safari Browsing Data Regularly – Prevent tracking and improve security.
27. Avoid Using Public Charging Stations – Use charge-only cables to prevent juice-jacking.
28. Limit Exposure on Apple AirTags – Disable AirTag tracking if unnecessary.
29. Use Lockdown Mode for High-Risk Users – Activate for extreme security needs.
30. Perform Factory Reset Before Selling – Ensure complete data erasure before transfer.

DO'S & DONT'S

by **Sheik Salim,** Partner - TorSecure Cyber LLP

1. KYC SCAM

Do's

- Always verify the identity of the caller before sharing any personal details.
- Contact customer care numbers only from official websites or apps.
- Install caller identification apps to detect fraud calls.
- Report any suspicious calls or messages to the authorities.

Dont's

- Do not click on unknown or suspicious links received via SMS or WhatsApp.
- Never share OTPs, PINs, passwords or account details over the phone.
- Do not trust random callers claiming to be from banks or KYC teams.
- Avoid calling customer care numbers obtained from search engines.

2. ONLINE JOB SCAM

Do's

- Verify the legitimacy of job offers via official company websites.
- Be cautious if the job offers high pay for minimal work or asks for payment upfront.
- Keep records of your communication and job offer details.
- Research company reviews and complaints online.

Dont's

- Do not pay for job registration, training or offer letters.
- Never share your personal or financial documents unless you're sure of the company's authenticity.
- Avoid clicking on suspicious job links received via SMS or emails.
- Do not entertain jobs that promise earnings without clear job roles.

3. ONLINE SHOPPING FRAUD

Do's ✓

- Shop only from trusted and verified e-commerce websites or apps.
- Check seller ratings and product reviews before purchasing.
- Use secure payment methods like credit/debit cards or trusted wallets.
- Maintain transaction records for future reference.

Dont's ✗

- Don't fall for deals that look too good to be true.
- Avoid making payments outside the official platform.
- Never share card PINs, OTPs or CVV numbers with anyone.
- Do not shop from links shared over unknown social media profiles or groups.

---

4. LOAN SCAM

Do's ✓

- Confirm whether the lending company is registered with RBI.
- Read all documents carefully before accepting a loan.
- Take loans only from banks or NBFCs that are regulated.
- Cross-check interest rates and repayment terms.

Dont's ✗

- Do not pay any advance fee for processing or approval.
- Don't fall for schemes offering instant loans without documentation.
- Avoid loan apps not listed on official app stores.
- Never share PAN, Aadhaar, or bank details without verification.

---

5. INVESTMENT FRAUD

Do's ✓

- Do thorough research before investing in any scheme.
- Verify the credentials of brokers or advisors.
- Seek advice from certified financial planners if unsure.
- Use SEBI-registered platforms and agents.

Dont's

- Don't trust guarantees of high returns with no risk.
- Never invest based on WhatsApp or Telegram forwards.
- Avoid links that promise doubling of money quickly.
- Don't share bank or trading credentials online.

6. SEXTORTION

Do's

- Be cautious when making video calls to unknown people.
- Report and block individuals asking for explicit content.
- Maintain privacy settings on social media.
- Preserve evidence and immediately report to cybercrime cell.

Dont's

- Do not share intimate photos or videos online.
- Never give in to threats or blackmail demands.
- Don't engage with suspicious online profiles.
- Avoid accepting random friend or chat requests.

7. ONLINE GAMING FRAUD

Do's

- Use parental controls if children are involved.
- Set spending limits and track in-app purchases.
- Report suspicious behavior or cheating.
- Download games only from official app stores.

Dont's

- Don't reveal personal details while gaming online.
- Avoid linking debit/credit cards to game accounts.
- Don't fall for fake in-game currency offers.
- Never respond to messages from unknown gamers asking for payments.

8. ONLINE MATRIMONIAL FRAUD

Do's ✓

- Verify identity of the person through video calls or background checks.
- Involve family in decision-making.
- Cross-check information provided in the profile.
- Report any suspicious or pressuring behavior.

Dont's ✗

- Don't share personal or financial information quickly.
- Avoid transferring money for emergencies or visas.
- Don't trust individuals who avoid meeting in person.
- Do not ignore red flags like emotional manipulation.

---

9. OTP FRAUD

Do's ✓

- Be cautious before entering OTPs anywhere online.
- Understand why you're receiving an OTP.
- Register for SMS alerts for transactions.
- Inform the bank if an unknown OTP is received.

Dont's ✗

- Never share OTPs with anyone.
- Don't enter OTPs from random calls or messages.
- Avoid saving OTPs or passwords in unsecured apps.
- Don't assume OTP requests are always harmless.

---

10. QR CODE FRAUD

Do's ✓

- Scan QR codes only from trusted sources.
- Use a scanner app that shows the URL before opening.
- Double-check if you're paying or receiving money.
- Keep transaction receipts.

Dont's

- Don't scan QR codes sent by unknown persons.
- Avoid scanning codes from messages, emails or untrusted shops.
- Never scan to receive payments.
- Don't believe calls asking you to scan for refunds.

11. LOAN APP SCAM

Do's

- Download only RBI-approved apps from trusted app stores.
- Read reviews and permissions before installing apps.
- Check for privacy policies and terms.
- Use apps only with two-factor authentication.

Dont's

- Do not allow unnecessary permissions like access to contacts or photos.
- Avoid apps that promise instant loans with no verification.
- Don't click on links received from unknown numbers.
- Never pay advance money to loan agents.

12. CYBER BULLYING

Do's

- Keep evidence of bullying (screenshots, chats).
- Block and report the bully on the platform.
- Inform parents, teachers or cyber cells.
- Use platform privacy settings.

Dont's

- Don't retaliate or engage with bullies.
- Avoid posting sensitive personal content.
- Don't ignore persistent threats or abuse.
- Never meet online bullies offline.

13. CYBER STALKING

Do's ✓

- Keep a record of stalking incidents with time and dates.
- Block the stalker and adjust your privacy settings.
- Inform police or cyber cell and provide evidence.
- Let someone close know you are being stalked.

Dont's ✗

- Do not ignore persistent messages or calls.
- Never share location or schedule online.
- Avoid responding to the stalker's messages.
- Don't meet the stalker to 'resolve' issues.

---

14. CYBER GROOMING

Do's ✓

- Teach children about online safety and red flags.
- Keep communication open with children.
- Use parental controls and monitor online activity.
- Encourage kids to report any inappropriate contact.

Dont's ✗

- Don't leave children unsupervised online.
- Never dismiss a child's fear or suspicion.
- Avoid letting kids engage with strangers online.
- Don't share children's photos publicly.

---

15. IMPERSONATION

Do's ✓

- Set social media profiles to private.
- Report fake accounts impersonating you.
- Inform friends about impersonation attempts.
- Save screenshots for proof.

Dont's

- Don't ignore when someone pretends to be you.
- Avoid sharing too much personal information online.
- Don't click on suspicious friend requests or messages.
- Never share login credentials.

16. FAKE PROFILES

Do's

- Verify before accepting friend/follow requests.
- Reverse search profile photos using Google or TinEye.
- Block and report suspicious profiles.
- Alert others if you see a fake profile using someone's identity.

Dont's

- Don't accept requests from unknown persons.
- Avoid chatting with or meeting someone based on limited info.
- Never send personal images or videos.
- Don't believe everything in a profile.

17. VISHING

Do's

- Hang up and verify the number via official sources.
- Report suspicious calls to your bank or telecom provider.
- Use call-blocking apps.
- Be aware of common phishing call patterns.

Dont's

- Never share banking or personal info on calls.
- Don't trust caller IDs; they can be spoofed.
- Avoid urgent-sounding calls demanding immediate action.
- Don't panic; scammers thrive on pressure.

18. PHISHING

Do's

- Check for spelling errors in emails and URLs.
- Hover over links to see actual URLs before clicking.
- Enable spam filters.
- Use two-factor authentication for accounts.

Dont's

- Don't click on links in unsolicited emails or messages.
- Avoid downloading attachments from unknown sources.
- Never enter credentials on suspicious websites.
- Don't reply to phishing emails.

---

19. SMISHING

Do's

- Treat unexpected SMS messages with caution.
- Verify links or numbers via official sources.
- Report smishing messages to your telecom provider.
- Keep your device OS and antivirus updated.

Dont's

- Don't respond to suspicious SMS messages.
- Never click on unknown links.
- Avoid entering OTPs or personal info on unknown websites.
- Don't believe all messages that seem to be from banks or services.

---

20. SIM SWAP FRAUD

Do's

- Contact your mobile service provider if your SIM stops working.
- Monitor bank messages and transaction alerts.
- Enable mobile security PINs.
- Use alternate number for banking OTPs.

Dont's

- Don't ignore loss of mobile signal for long.
- Avoid sharing SIM or phone details online.
- Don't discard personal documents carelessly.
- Don't rely solely on SMS-based authentication.

21. IDENTITY THEFT

Do's

- Shred documents with personal details before disposing.
- Use strong passwords and change them regularly.
- Review bank and credit card statements frequently.
- Monitor your digital footprint.

Dont's

- Never share sensitive documents or IDs online.
- Don't store confidential data on shared devices.
- Avoid using public Wi-Fi for banking.
- Don't disclose identity proofs without purpose.

22. ATM SKIMMING

Do's

- Inspect ATM card slots before using.
- Cover keypad while entering PIN.
- Use ATMs in well-lit, secure locations.
- Check bank statements for unauthorized transactions.

Dont's

- Don't use ATMs that look tampered or suspicious.
- Avoid taking help from strangers at ATMs.
- Don't leave receipts behind.
- Never share ATM PIN.

23. DATA THEFT

Do's

- Secure all devices with passwords and encryption.
- Regularly backup data to secure locations.
- Restrict access to confidential files.
- Use updated antivirus and firewalls.

Dont's

- Don't leave devices unattended in public.
- Avoid sharing passwords or data over email.
- Don't store sensitive data without encryption.
- Don't ignore unauthorized data access.

---

24. RANSOMWARE

Do's

- Backup important data frequently.
- Use licensed antivirus software.
- Train staff or family about phishing attacks.
- Disconnect infected systems immediately.

Dont's

- Never pay ransom; it encourages further crimes.
- Don't open unknown attachments or email links.
- Avoid downloading pirated software.
- Don't delay reporting ransomware to authorities.

CYBER SAFETY CHECKLIST
FOR STUDENTS

- ☐ I use complex, unique passwords for every online account.
- ☐ I never share my passwords with anyone except trusted guardians.
- ☐ I activate two-factor authentication on all accounts where available.
- ☐ I don't click on unknown links or download attachments from strangers.
- ☐ I avoid chatting with unknown people online, even if they seem friendly.
- ☐ I never post personal information (like my school name, address, or phone number) on public platforms.
- ☐ I regularly update my operating system, apps, and antivirus software.
- ☐ I know how to block and report users who behave inappropriately.
- ☐ I think before I share — not everything needs to be posted online.
- ☐ I understand the meaning of cyberbullying and avoid engaging in it.
- ☐ I keep my webcam covered when not in use.
- ☐ I avoid using pirated software and games.
- ☐ I have basic awareness of cybercrime laws in India (IT Act, 2000).
- ☐ I report anything suspicious online to a trusted adult or authority.
- ☐ I log out of accounts after using public or shared devices.

CYBER SAFETY CHECKLIST
FOR PARENTS

- ☐ I talk to my child regularly about their online activity and friends.
- ☐ I encourage open communication without judgment if something goes wrong online.
- ☐ I have installed parental control tools on devices used by my child.
- ☐ I monitor screen time and set appropriate usage boundaries.
- ☐ I follow or supervise my child's social media presence.
- ☐ I have taught my child about privacy settings and safe sharing.
- ☐ I know how to report and file complaints in case of cyberbullying or online abuse (cybercrime.gov.in).
- ☐ I stay updated about the apps and games my child is using.
- ☐ I teach my child to never meet online strangers in real life.
- ☐ I encourage critical thinking about online content, memes, and forwards.
- ☐ I use secure Wi-Fi and avoid sharing passwords with guests or neighbors.
- ☐ I ensure digital wellbeing is part of our household discussions.
- ☐ I lead by example — practicing responsible digital behavior myself.
- ☐ I attend workshops/webinars on online safety whenever possible.
- ☐ I store emergency cyber helpline numbers for quick access.

CYBER SAFETY CHECKLIST
FOR TEACHERS

- ☐ I include digital safety as part of my classroom discussions.
- ☐ I teach students about strong passwords and personal privacy online.
- ☐ I help students identify fake news, misinformation, and deepfakes.
- ☐ I understand how cyberbullying manifests and how to respond.
- ☐ I encourage respectful online communication and digital citizenship.
- ☐ I collaborate with parents to ensure a unified approach to cyber wellness.
- ☐ I stay updated with emerging digital trends (e.g., chat apps, gaming, AI tools).
- ☐ I use only licensed educational software and platforms.
- ☐ I maintain a clear boundary between professional and personal social media.
- ☐ I know how to escalate and report a cyber incident involving a student.
- ☐ I conduct digital literacy sessions with the help of IT faculty or experts.
- ☐ I verify the authenticity of digital resources before sharing them.
- ☐ I create a safe space where students can share online concerns.
- ☐ I attend certified cyber awareness and safety programs.
- ☐ I maintain confidentiality and sensitivity when dealing with digital issues.

15 DIGITAL WELLBEING & HEALTH TIPS

by **Rushikesh Upadhyay,** IPS

1. **FOLLOW THE 20-20-20 RULE:** Every 20 minutes of screen time, look at something 20 feet away for 20 seconds to reduce eye strain.
2. **USE BLUE-LIGHT BLOCKING GLASSES:** Wear blue-cut lenses while using devices to reduce digital eye strain, especially in the evening.
3. **ENABLE NIGHT MODE OR EYE COMFORT MODE:** Most devices offer warm light filters — activate them after sunset.
4. **AVOID SCREENS IN THE DARK:** Do not look at screens in complete darkness — it strains your eyes and disturbs melatonin production.
5. **KEEP A STRAIGHT POSTURE:** Sit upright with your back supported and screen at eye level to avoid neck and back issues.
6. **BLINK FREQUENTLY:** Consciously blink often to avoid dry eyes while staring at screens.
7. **TAKE TECH-FREE BREAKS:** Designate at least 30–60 minutes a day without any digital devices.
8. **AVOID SCREENS 1 HOUR BEFORE SLEEP:** Exposure to screens before bedtime can affect your sleep quality.
9. **KEEP DEVICES OUT OF THE BEDROOM:** Make your sleeping area a gadget-free zone to ensure deeper sleep.
10. **USE "DO NOT DISTURB" OR FOCUS MODES:** These help in staying mindful and avoiding constant interruptions.
11. **LIMIT SOCIAL MEDIA TIME:** Use apps that track your usage and gently remind you to take breaks.
12. **HYDRATE WELL:** Drink water regularly — screen time often makes people forget to stay hydrated.
13. **ADJUST SCREEN BRIGHTNESS TO MATCH ROOM LIGHTING:** Avoid using very bright or dim screens in contrast with your environment - it reduces eye strain and helps maintain focus.
14. **PRACTICE EYE EXERCISES:** Simple activities like eye rolling or palm cupping can relieve tension.
15. **STRETCH & MOVE:** Get up every hour and do basic stretches or walk around to improve blood circulation.

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/BNS 303 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.)	IT Act Section 66 B of ITAA 2008 3 years imprisonment or Rupees one lakh fine or both	Section 411 IPC/BNS 317 3 years imprisonment or fine or both
3	Data owned by you or your company in any form is stolen	IT Act Section 66 of ITAA 2008 3 years imprisonment or fine up to rupees five lakh or both	Section 379 IPC/BNS 303 3 years imprisonment or fine or both
4	A password is stolen and used by someone else for fraudulent purpose.	IT Act Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh IT Act Section 66D ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC/BNS 319 3 years imprisonment or fine Section 420 IPC/BNS 318 7 years imprisonment and fine
6	An e-mail is read by someone else by fraudulently making use of password	IT Act Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both IT Act Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	
7	A biometric thumb impression is misused	IT Act Section 66C of ITAA 2008 3 years imprisonment and fine up to IT Act 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	IT Act Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC/BNS 319 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	IT Act Section 66E of ITAA 2008 3 years imprisonment or fine not exceeding Rupees two lakh or both	Section 292 IPC/BNS 294 2 years imprisonment and fine Rupees 2000 and 5 years and rupees 5000 for second and subsequent conviction
12	Tampering with computer source Documents	IT Act Section 65 of ITAA 2008 3 years imprisonment or fine up to Rupees two lakh or both IT Act Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both	
13	Data Modification	IT Act 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/BNS 356 2 years or fine or both Section 504 IPC/BNS 351 2 years or fine or both Section 506 IPC/BNS 351 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/BNS 351 2 years along with punishment under IT Act Section 506 IPC/BNS 351 Section 508 IPC/BNS 351 1 year or fine or both Section 509 IPC/BNS 79 1 years or fine or both of IPC as applicable
15	Publishing or transmitting obscene material in electronic form	IT Act 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/BNS 294 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	IT Act 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/BNS 294 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	IT Act 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/BNS 294 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	IT Act Section 66 3 years imprisonment or fine up to Rupees five lakh or both IT Act Section 66F life imprisonment of ITAA 2008	
19	Planting a computer virus that acts against the state	IT Act 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	IT Act 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.	IT Act 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	IT Act Section 69 of ITAA 2008 imprisonment up to 7 years and fine	

24	Failure to Block Web sites, when ordered	IT Act Section 69A of ITAA 2008 imprisonment up to 7 years and fine	
25	Sending threatening messages by e-mail		Section 506 IPC/BNS 351 2 years or fine or both
25	Word, gesture or act intended to insult the modesty of a woman		Section 509 IPC/BNS 79 1 years or fine or both - IPC as applicable
26	Sending defamatory messages by e-mail		Section 500 IPC/BNS 356 2 years or fine or both
27	Bogus Web sites, cyber frauds	IT Act Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC/BNS 319 3 years imprisonment or fine Section 420 IPC/BNS 318 7 years imprisonment and fine
28	E-mail Spoofing	IT Act Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC/BNS 336 2 years or fine or both Section 468 IPC/BNS 336 7 years imprisonment and fine
29	Making a false document	IT Act Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC/BNS 336 2 years or fine or both
30	Forgery for purpose of cheating	IT Act Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC/BNS 336 7 years imprisonment and fine
31	Forgery for purpose of harming reputation	IT Act Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 469 IPC/BNS 336 3 years and fine
32	E-mail Abuse		Section 500 IPC/BNS 356 2 years or fine or both
33	Punishment for criminal intimidation		Section 506 IPC/BNS 351 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		Section 507 IPC/BNS 351 2 years along with punishment under Section 506 IPC/BNS 351
35	Copyright infringement	IT Act Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both	Section 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.

ONLINE COMPLAINT

1. National Cyber crime Reporting Portal
   www.cybercrime.gov.in
2. National Commission for Women
   www.ncw.gov.in
   ncwapps.nic.in

HELPLINE NUMBERS

Cyber Crime Helpline	: **1930**
National Emergency Number	: **112**
Police	: **100**
Women Helpline	: **1091**
Women Helpline Domestic Abuse	: **181**
Student / Child Helpline	: **1098**
Mental Health Helpline	: **1800-599-0019**
iCall Suicide Helpline	: **9152987821**
Fire	: **101**
Ambulance	: **102**
Disaster Management Service	: **108**

National Commission For Women
Domestic Violence, Sexual Violence & Harassment:
78271 70170, 011-26942369, 26944754

We'd Love Your Feedback!

Help us improve the next edition of Cyber Safe Girl.

If you've read the book and would like to suggest improvements, new topics, or share your own experiences, please drop an email to

educatorananth@gmail.com

Your suggestions make this mission stronger and more effective!

Are you Certified ?

www.cybersafegirl.com

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

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

SURE PASS

CYBER PATRIOT

Indian Cyber Institute

CYBER JAGRITHI

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