मराठी

चित्रकथा

SURE PASS

CYBER PATRIOT

Indian Cyber Institute

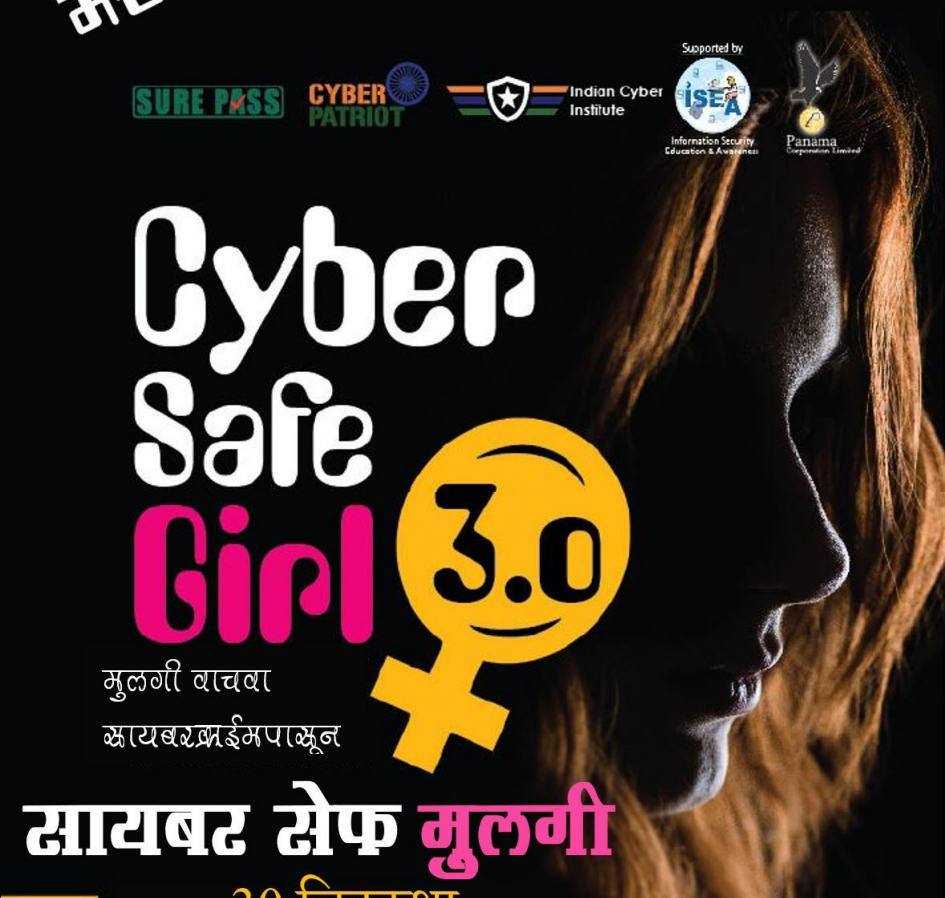
Supported by

ISEA Information Security Education & Awareness

Panama Corporation Limited

Cyber Safe Girl 3.0

मुलगी वाचवा
सायबरक्राईमपासून



सायबर सेफ मुलगी

30 चित्रकथा

मुलींच्या ऑनलाइन सुरक्षेसाठी

Ananth Prabhu G PhD, Post Doctoral Fellow

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

www.cybersafegirl.com

मोबाइल व कंप्युटर्स हे मित्र आहेत. उपयुक्त आहेत. पण त्यांचा घातक दुरुपयोग करणारे दुष्ट गुन्हेगार या जगात आहेत. विशेषतः मुलींना याचा धोका आहे. डॉ. अनंत प्रभू यांनी या धोक्यांची माहिती देणारी ही पुस्तिका पोलिसांच्या मदतीने तयार केली आहे. चित्रांच्या सहाय्याने धोक्यांची कल्पना देणारी ही पुस्तिका प्रत्येकाने वाचावी. एक तासाहूनही कमी वेळात आपले डोळे अंजन टाकणारी ही पुस्तिका मराठीकरण करून ई साहित्यतर्फे प्रकाशित करण्याची परवानगी डॉ. अनंत प्रभू यांनी दिली. त्याबद्दल आम्ही त्यांचे आभारी आहोत.

आपण स्वतः ही पुस्तिका वाचावी, समजून घ्यावी. शाळाकॉलेजातील व प्रत्येक घरात मुलामुलींपर्यंत ती पोहोचवावी म्हणून ही मुक्त आणि मोफत आहे.

आपल्या प्रतिक्रिया कळवा.

ई साहित्य प्रतिष्ठान
www.esahity.com
www.esahity.in
esahity@gmail.com

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 at Sahyadri College of Engineering and Management and Director of SurePass Academy Mangalore, 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.

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

Get a CYBER SAFE GIRL Certificate for FREE

Go through the online course comprising of videos and notes materials of 30 topics described in the Cyber Safe Girl v3.0 eBook. After going through all the study materials of the course, take an online exam. Upon successful completion, get an I AM A CYBER SAFE GIRL certificate with a unique reference number. If you manage to score top grades, get super cool #CyberSafeGirl merchandise for free.

Cyber Safe Girl 3.0

Beti Bachao,
Cyber Crime Se...

30 eye-opening sketches
to ensure online safety of girls

Title: Cyber Safe Girl

Version: Third

Publisher: Dr Ananth Prabhu G

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

First Published in India in 2018

Designed and printed by
Tarjani Communications Pvt. Ltd, Mangaluru

Credits


Sanjay Sahay, IPS


Ramachandra Rao, IPS


Arun Chakravarthy, IPS


Dr Murugan, IPS


Roopa D, IPS


Dr Vedamurthi, IPS


Reena Suvarna, KSPS


M C Kavitha, KSPS

Special Thanks to


Krishna J Palemar


Manjunath Bhandary


Vivek Shetty


Ch A S Murty
ISEA Team


Tapan J Mehta


Vaikunt Prabhu


Dhanesh Babu


Fazeel Ahmed


Dr Mustafa B
Tech Resource


Ganesh M Nayak
Convenor


Chaitra Mallikarjun
Outreach Head


Naveen Kumar


Anudeep Karkera
(Artist)

Index

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. This number is then misused to call or text you and exploit your ignorance or even emotionally manipulate you.

Sections Applicable

IPC Sections (to be applied to the Shop Keeper)

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

IPC Section 354C - Voyeurism

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

IPC Section 503 - Criminal Intimidation

IPC Section 506 - Punishment for Criminal Intimidation

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

IT Act:

IT Act Section 66E – Punishment for violation of privacy

Mobile Number Sale to Stalkers by Recharge Shop:

IPC Sections (to be applied to the Shop Keeper)

IPC Section 109 – Punishment for abetment

IPC Section 114 – Abettor present when offence is committed

IPC Section 120B – Punishment for Criminal Conspiracy

IPC Section 406 – Punishment for Criminal Breach of Trust

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


Bharath Recharge
मीना दुकानात ५० रुपयांचा मोबाईलचा रिचार्ज करायला गेली
Bharath Recharge
दुकानदार अखिल सर्व्हर डाऊन असल्याचे सांगून नंतर रिचार्ज करेन म्हणाला
अर्ध्या तासाने मीनाला ५०० रुपयांच्या रिचार्जचा मेसेज आला
Bharath Recharge
मीना पुन्हा जाऊन म्हणाली की तिच्याकडे ४५० नाहीत. तो म्हणाला नंतर दे.
Hi!
Hi
नंतर मीनाला अखिलचे छान छान मेसेज येत राहिले त्यांच्यात मैत्री झाली
एक दिवस अखिलने तिला जीवनसाथी व्हायचे वचन दिले.
मीना हवेत तरंगू लागली. ते फ़िरू लागले. तो तिला गिफ़्ट देऊ लागला.
LODGE
एके दिवशी त्याने तिला गोड बोलून लॉजवर नेले... नंतर सोडून दिले
आता तो ब्लॅकमेल करतो. व्हिडिओ शेअर करायची धमकी देतो. काळजी घ्या.

DEBIT CARD CLONING

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

Sections Applicable

IT Act for cloning

IT Act Section 66 – Computer related offences

IT Act Section 66C – Punishment for Identity Theft

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

Money Transaction followed by cloning:

IPC Section 419 – Punishment for cheating by personation

IPC Section 420 – Cheating

IT Act

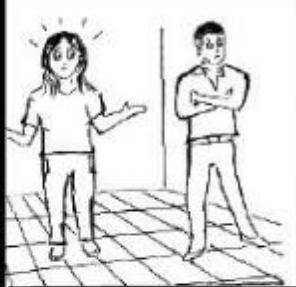
IT Act Section 66D – Punishment for cheating by personation by using computer resource

Cloning may blow up your Earning!

DEBIT CARD CLONING

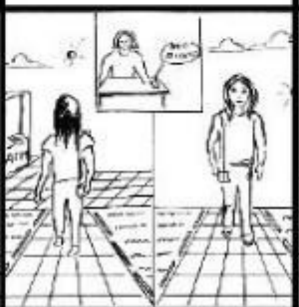
मीना आणि रीना एकाच कॉलेजातील खास मैत्रिणी होत्या

मीनाचा मित्र अर्जुनला ड्रग्सचे व्यसन आहे व तो तिच्याकडून कायम पैसे मागत असे



मीनाला तो सुधारेल ही आशा होती. पण तो कायम पैसे मागे व मैत्री तोडण्याची धमकी देई.

मीनाने रीनाकडे पैसे मागितले. रीनाने आपले ATM कार्ड व पिन नंबर दिला



थोड्याच वेळात मीना परत आली आणि रीनाला ५०० रुपये डेबिटचा मेसेज आला

आठवड्याने रीनाला पुन्हा ५०० रु डेबिटचा मेसेज आला. रीनाला तो धक्काच होता.

मीनाने जेव्हा कार्ड घेतले होते तेव्हा तिथे अर्जुन होता. त्याने ATM कार्ड घेतले होते.

स्किमिंग मशीन वापरून त्याने कार्डची कॉपी केली व पुन्हा पैसे काढले

आपले ATM कार्ड व पिन कोणालाही देऊ नये. भले ते कितीही जवळचे असोत.

KEYLOGGER

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

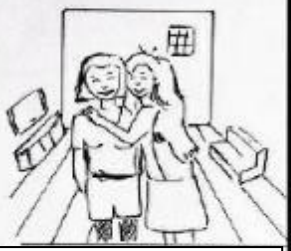
Sections Applicable

Key logger installation: IT Act Section 66
– Computer related offences
Stealing personal information: IT Act Section 66C
– Punishment for Identity Theft

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

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

Keylogger may empty your Coffer!



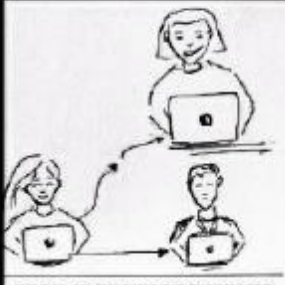
अनुषा आणि पूजा खास मैत्रिणी आणि PG च्या रूमपार्टनर. कंपनीही एकच

दोघींनाही त्यांचा तरूण बॉस विवेक अतिशय आवडत असे.

पूजाने वेळ न दवडता विवेककडे मन उघड केले व त्याने तिला होकारही दिला.

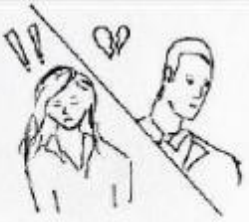
अनुषा मत्सराने जळू लागली आणि तिने पूजाला धडा शिकवण्याचे ठरवले

पूजाच्या लॅपटॉपमध्ये कीलॉगर स्पायवेअर इन्स्टॉल करून तिच्या गोष्टींवर लक्ष ठेवू लागली

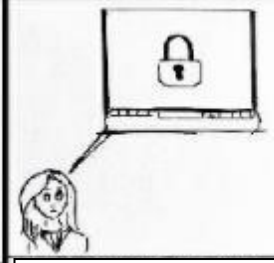


आपले पासवर्ड, फ़ोटो, चॅट, मेल व ब्रौझिंग सर्व अनुषा बघते हे पूजाला कळले नाही

अनुषाने त्या मेल्स पूजाच्या घरी पाठवल्या, खासगी फोटो सोशल मिडियावर निनावी टाकले.



विवेकला धक्काच बसला. त्यांचे संबंध तुटले. पूजा उद्ध्वस्तच झाली.



आता पूजाला लॅपटॉपला पासवर्ड न ठेवल्याचा आणि antivirus न वापरल्याचा पश्चात्ताप होतो.

SMS SPOOFING

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

Sections Applicable

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

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

SMS are Spoofed by Cyber Crooks!

ऐश्वर्याला खरेदीचे व्यसन आहे. ती अनेक ईकॉमर्स साइट्स ची मेंबर होती

कायम ऑफ़र्सच्या शोधात ती असे. खरेदी करी. फ्री कूपन्स वापरत असे.

एकदा तिला वॉलमार्टची मेल आली. तिला ५००० ची बॅग ५००त मिळण्याची खुशखबर

वॉलमार्टचा हा मेसेज आला. तिने online पे केले तर तिला ही ऑफ़र दोनदा मिळेल

ऐश्वर्याने बँकेत १००० भरले व ऑनलाइन ट्रान्स्फ़र केले.

महिना झाला तरी बॅग आली नाही. तिने हेल्पलाईनला फ़ोन लावला.

तिने क्लिक केलेली लिंक फ़ेक URL असल्याचे व त्यात Fishing व Spoofing झाल्याचे समजले

जेव्हा एखादी फ़ार मोठी सूट मिळत असेल तेव्हा सावध व्हावे हेही ती शिकली

अनेक नायजेरियन स्कॅम मेसेज नेटवर असतात व खुपजण या जाळ्यात फ़सतात.

CALL SPOOFING

Call spoofing happens through apps that enable a person with criminal intent to change one's number and voice to impersonate another to defraud the receiver.

Sections Applicable

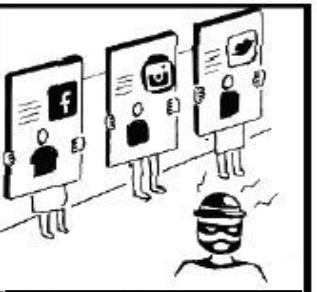
Act of hoax or trick or deceive a communication
IPC Section
IPC Section 465 – Making a false document(FORGERY)
IPC Section 419 – Punishment for cheating by personation

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

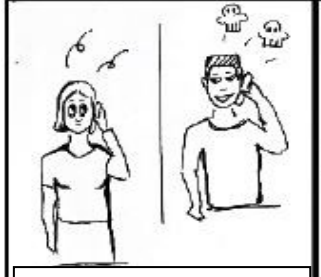
Call Spoofing, Caller is Confusing!

शबाना एक विधवा आहे. स्वतंत्र घरात ती एकटी रहाते

टाईमपाससाठी ती इंटरनेट व सोशल मिडियावर वावरत असे



कुणाचीही मैत्री विनंती ती मित्र बघून सहज स्विकारी. भोळेपणी.



तिच्या मुलाला एकदा १ लाखाची गरज पडली ते त्याने मित्राच्या अकाउंटवर ट्रान्स्फ़र करायला सांगितले.

मुलाचाच फ़ोन होता. तिने त्या अकाउंट ला १लाख ट्रान्स्फ़र केले

पैसे पाठवल्यावर तिने मुलाला फ़ोन करून पैसे मिळाले का ते विचारले

शफ़िक, तिच्या मुलाला आश्चर्य वाटले. त्याने फ़ोन केलाच नव्हता.

कॉल स्पूफ़िंगमुळे ती फ़सली हे तिच्या लक्षात आले व १ लाख गेले.

फ़सवणूक करण्याचे खुप ऍप उपलब्ध आहेत. सावध रहा

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 upon payment. Users are shown instructions as to how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable to cybercriminals in bitcoin.

Sections Applicable

Unauthorised access, Denial, Encryption :

IT Act Section 66 – Computer related offences

Demand without payment :

IPC Section 384 – Extortion

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

Demand & payment :

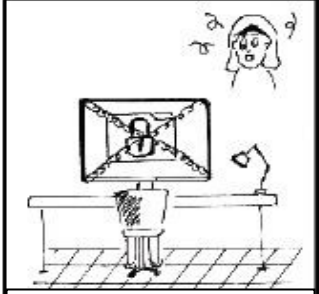
IPC Section 384 – Extortion.

Sensitize your Hardware and Software to avoid Ransomware!

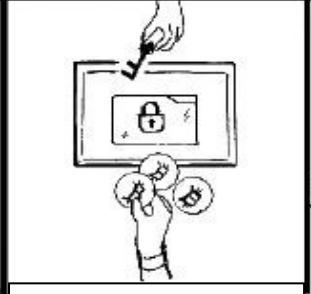
अलिशा मालक आहे. तिच्या कंपनीत ५०लोक व ६०सिस्टिम आहेत.

एकदा एका व्यापाऱ्या कडून तिला एक मेल आली. त्यात एक फ़ाईल होती.

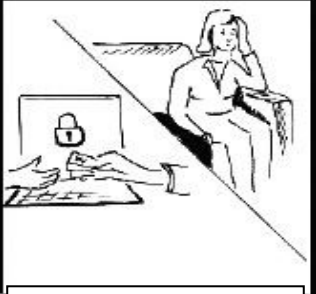
तिने ती फ़ाईल डाऊनलोड केली. Antivirus अपडेट नव्हता. त्यामुळे अलर्ट आला नाही.



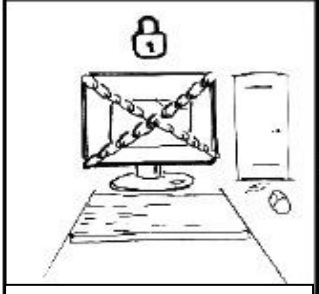
ती फ़ाईल उघडताच सर्व सिस्टिम लॉक झाली. सर्व फ़ाइल्स करप्ट झाल्या.



स्क्रीनवर मेसेज आला. १ लाख रुपये द्या. मगच अनलॉक होईल.



अलिशाने त्या बिटकॉइन पत्त्यावर १ लाख रुपये भरले.



पण हॅकरने की पाठवली नाही. फ़ाईल्स कायमच्या लॉक झाल्या.

मॅनेजरला समजले की तिला फ़िशिंगमेल व रॅन्समवेअर आली होती.

अलिशाला ती मेल उघड्ल्याचा व antivirus अपडेट न केल्याचा पश्चात्ताप झाला आहे.

CYBER STALKING

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

Sections Applicable

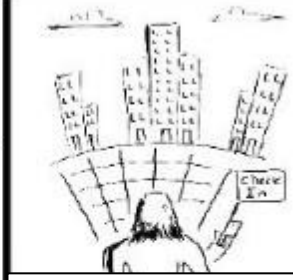
Offline :
IPC Section 354 D – Stalking

Online :
IPC Section 354 D – Stalking

Cyber Stalking Means Someone is Watching!

जुवेरिया NRI मुलगी. शिक्षण US व इंजिनियरिंग भारतात. मजेत जगण्याचा स्वभाव.

काहीही केलं की फ़ोटो सोशल मिडियात. १०००० फ़ॉलोअर्स होते तिचे.

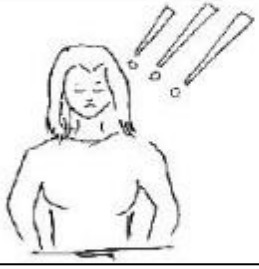


चेकइन फ़िचरमुळे तिचा ठिकाणा जगजाहिर असे. खासगी काहीच नाही.

एकदा गोव्याला जायचे सर्व प्लान, तारखा, जागा तिने वॉलवर टाकले.

किरण नावाच्या एक सराइत गुंड ते पाहून मागावर निघाला.

गोव्याला जाऊन त्याने तिला एकटे भेटण्यासाठी मेसेज केला.



त्याची प्रोफ़ाईल बघून जुवेरियाने त्याला ब्लॉक केले. पण तिला त्याचे प्लान माहित नव्हते

तिचे सर्व प्लान जगजाहिर होते. त्याने तिला एकटे गाठून विनयभंग केला.

जुवेरिया आता त्या अपलोड, अपडेट व पोस्टचा पश्चात्ताप करते

PICTURE MORPHING

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

Sections Applicable

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

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

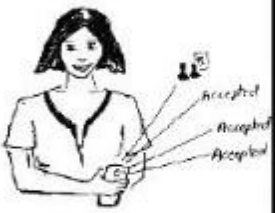
For publishing photos containing indecent representation of women:
Section 4 R/W Section 6 of Indecent Representation of Women's Act, 1986

Morphing is used for Defaming!

ऐश्वर्या ही मुंबईत रहाणारी १८ वर्षांची एक आनंदी मुलगी होती

ती नेहमीच आपले फ़ोटो इन्स्टा व टिकटॉकवर टाकत असे

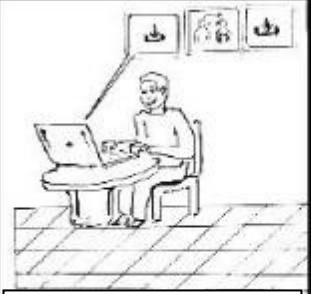
तिच्या प्रत्येक फ़ोटोला हजारो लाइक्स आणि शेकडो कॉमेंट्स मिळत



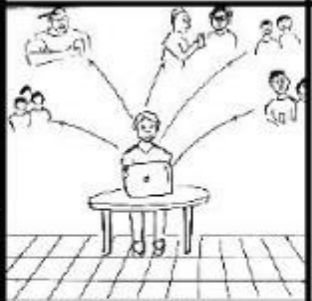
एकदा तिला आर्यन या मुलाची फ्रेंड रिक्वेस्ट आली. तिने ती स्विकारली

त्याने तिला कॉलेजच्या वाटेत गाठले व मागणी घातली

ऐश्वर्याने त्याला सरळ नकार दिला, त्याच्यावर ओरडली



आर्यन घरी गेला व तिचे फ़ोटो मॉर्फ़ करून एका नग्न मुलाबरोबर जोडले



ते त्याने मित्रांना पाठवले व अनेक साइट्सवर तिच्या फ़ोन नंबरसह टाकले.

ऐश्वर्या आपले फ़ोटो इन्स्टा व टिकटॉकवर टाकणे व फ्रेंड रिक्वेस्ट स्विकारण्याचा पश्चात्ताप करते. सावध व्हा.

PROFILE HACKING

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

Sections Applicable

IT Act

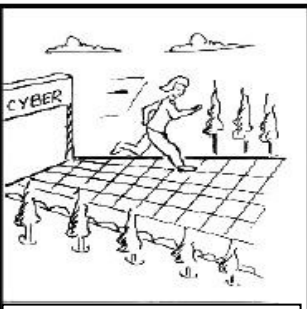
IT Act Section 66 – Computer related offences

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

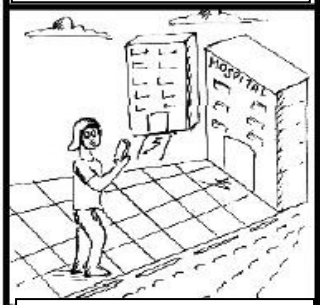
Profile Hacking means Security is Lacking!

तनुजाला सायबर कॅफ़ेमध्ये जाऊन वेब सर्फ़िंग करायला आवडे

एकदा सर्फ़िंग करत असता दुसऱ्या विंडोमध्ये Gmail उघडी राहिली



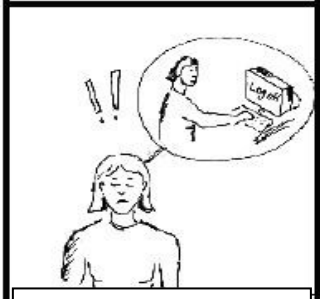
अचानक फ़ोन आला. तिचे आजोबा हॉस्पिटल मध्ये अत्यवस्थ आहेत.



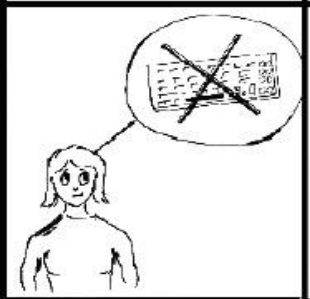
तनुजाचे आजोबांवर खुप प्रेम होते. ती सर्व तसेच टाकून हॉस्पिटलला गेली.

हॉस्पिटलमधे तिला gmail व FB पासवर्ड बदलल्याचे मेसेज आले.

तनुजाला आठवले. ती लॉगाउट झाली नव्हती. तिचे अकाउंट हॅक झाले.



दुसऱ्यांचा कंप्युटर वापरून झाल्यावर नेहमी लॉग आउट व्हावे



पासवर्ड टाकताना व्हर्च्युअल कीबोर्ड वापरावा

फ्री WIFI वापरणे टाळावे. VPN वापरावा.

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 like the notorious blue whale challenge even end in the victim ending her life. This is a personal as well as social challenge for the others around.

Sections Applicable

IPC Sections
The site

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

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

देविका एक ग्रामीण मुलगी. FY इंजिनियरिंग करत होती

तिच्या साधेपणामुळे वर्गमित्र तिला आपल्यात घेत नसत. online मित्रमैत्रिणीही नव्हते.

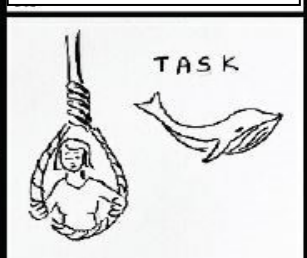
एकटेपणा घालवण्यासाठी ती मेलवर आलेलाब्लू व्हेल हा गेम खेळू लागली.

तिला खेळ आवडला. त्यात ५० लेव्हल्स होत्या. प्रत्येकीत एक टास्क होता.

लेव्हलवर पॉइंट मिळत. यातून निर्मित डोपामाइनचे तिला व्यसन लागले.

शरीरावर चाकूचे वार करणे, स्मशानयात्रा असे भयंकर टास्क असत

तिच्यामधे होणारे बदल दिसूनही कोणीच त्यांची दखल घेतली नाही



अंतिम टास्क गळफ़ासाने आत्महत्या. तिने आई वडलांना माफ़ीपत्र लिहीले व गळफ़ास घेतला

पत्रात होते- मला इतरांनी स्विकारावे वाटे. कोणीच आपल्यात घेतले नाही. मी जगून काय करू?

JOB CALL LETTER

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

Sections Applicable

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

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

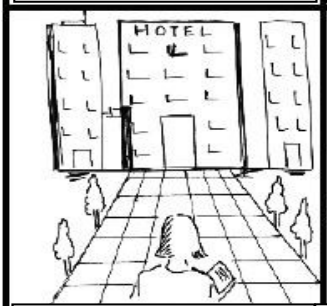
Abatement for offence
a. On the spot : IPC Section114 – Abettor present when offence is committed
b. Remotely: IPC Section109 – Punishment for abetment

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

निशिताला इंजिनियरिंगला फ़र्स्ट्क्लास मिळाला पण प्लेस्मेंट मिळाली नाही.

जॉबच्या आशेने ती तिचा रेझ्युमे नौकरी.कॉम व इतर साइटवर टाकत असे.

एक दिवस तिला मोठ्या कंपनीचे पत्र आले. सात आकडी पगार ऑफ़रसह.

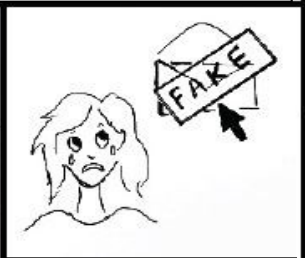


इंटरव्ह्यू शहरातील एका ५स्टार हॉटेलात होता. तिने रिक्षा करून हॉटेल गाठले.

ती एका मोठ्या रूममधे गेली. अनेकजण इंटरव्ह्यू ची तयारी करत होते.

तिला इंटरव्ह्यूपुर्वी प्यायला वेटरने ड्रिंक दिले. तिला चक्कर आली

नंतर घडले ते निशिताला कळले नाही.जाग आली तो ती बेडवर नग्नावस्थेत होती



तिला आलेली मेल फ़िशिंग होती. तिने अधिक चौकशी करायला हवी होती.

जॉब आशेवर असलेल्या लाखो मुलींना असे फ़सवण्यात येते. सावधान!

DEEPFAKES

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

Sections Applicable

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

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

जॅनेट MMBS ची विद्यार्थी होती व गेली तीन वर्षे जॉनच्या प्रेमात होती

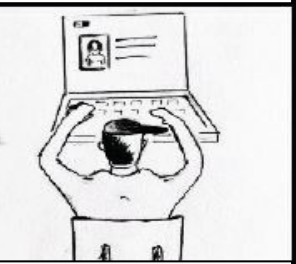
Tiktok व इंस्टाग्रामवर ती रोज दोन तरी पोस्ट अपलोड करत असे.

जॅनेटचे जॉनशी भांडण झाले ही बातमी सिनिअर अरूणला लागली

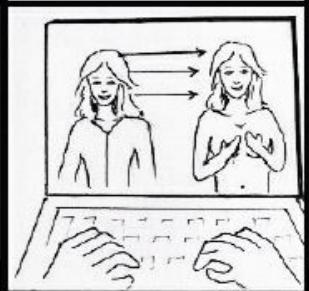
अरूणने संधीचा फ़ायदा घेत जॅनेटला मागणी घातली. तिने होकार दिला. पण मग तिला जॉनची आठवण आली

आठवड्यातच अरूणला नकार देऊन जॉनची माफ़ी मागून मैत्री केली.

भडकलेल्या अरूणने जॅनेटला धडा शिकवायचे ठरवले.



आर्टिफ़िशिअलइंटेलिजन्सचा वापर करून त्याने तिच्या व्हिडिओंचे डीपफ़ेक बनवले



या व्हिडिओंमध्ये जॅनेट अनेक मुलांबरोबर मौज करताना दिसत होती.

बघणारे ते खरेच समजले. जॅनेटला आपले व्हिडिओ टिकटॉकवर टाकण्याचा पश्चात्ताप होतो.

DATING WEBSITE

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

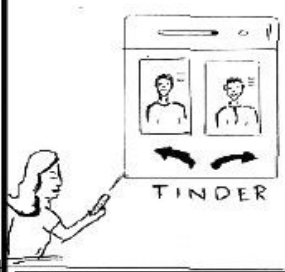
Sections Applicable

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

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

रश्मी MMBS ची विद्यार्थिनी होती. आताच तिला मिस फ्रेशर हा किताब मिळाला.

ऑनलाइन चॅट आवडे पण रोज त्याच त्या मुलांशी बोलून ती बोअर झाली



एकदा तिने टिंडर साइट पाहिली आणि जोरदार स्वाइपिंग सुरू केले.

तिला शक्स नावाचा एक रुबाबदार पैसेवाला गाड्या पार्टीवाला मुलगा भेटला.

शक्स गोड बोलायचा. रश्मी त्याच्या भूलथापांना भुलून फ़िरायला गेली.

ते दोघे मोठ्या हॉटेल मध्ये जेवले. रश्मी हवेत स्वप्ने पाहू लागली.

एकदा त्याने रश्मीकडे २लाख मागितले. त्याची अकाउंट सील झाली म्हणून. तिने चेन गहाण ठेवली व पैसे दिले.

नंतर त्याने तिला ब्लॉक केले. तिच्या मैत्रिणींनी तिला सांगितले की तो असेच मुलींना फ़सवतो.

डेटिंगसाइटमधून अनोळखी लोकांना भेटण्याचा व फ़ोटो देण्याचा तिला पश्चात्ताप झाला.

CAMERA HACKING

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

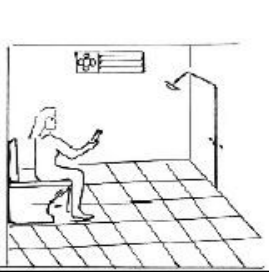
Sections Applicable

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

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

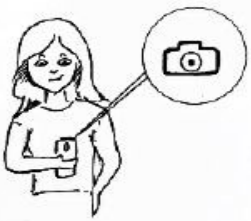
मनीषा कॉलेजातील सर्वात कूल मुलगी होती

मोबाईलने ती मेल, सोशल मिडिया व पैशाचे ऑनलाइन व्यवहार करी.



नेहमी बाथरूममधेही ती आपला फ़ोन नेई

नकळत एकदा तिने मेसेंजरवरून एक मालवेअरची ट्रोजनमेल डाऊनलोड केली



मालवेअरने तिच्या मोबाईलचे कॅमेरे चालू केले. तिला न कळता सर्व **व्हिडिओ बनले.**

मालवेअरबद्दल बेसावध होती. ती बाथरूममध्ये जे करते ते व्हिडिओ बनले.

एकदा जोएल या मित्राने तिला तिच्या आंघोळिचा व्हिडिओ पाहिल्याचे सांगितले.

मनिषा उद्ध्वस्तच झाली. तिच्या फोनमधे हे थांबव णारा antivirus नव्हता.

तिला मोबाइल फ़्लिपकव्हर व camera कव्हर न लावल्याचा पश्चात्ताप झाला.

SOCIAL TROLLING

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

Sections Applicable

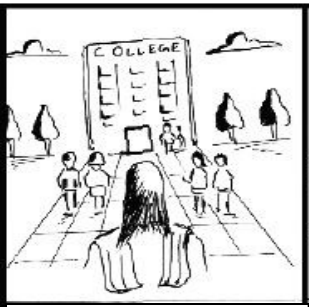
IPC Section 507 – Criminal Intimidation by an Anonymous communication

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

Stalking:
Offline: IPC Section 354 D – Stalking
Online : IPC Section 354 D – Stalking

Are you Trolling, the law may be soon following!

श्रुती साधी भोळी मध्यम वर्गीय मुलगी होती. देवभोळी आणि पापभिरू.

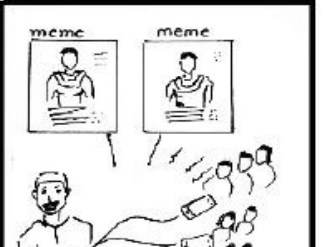


तिच्या कॉलेजातील मुले बिनधास्त फ़ॅशनेबल मौज मजा करणारी होती

ते श्रुतीची टर उडवत. तिला काहीबाही बोलत आणि तिला नकोनकोसे करत.

रोहन तर जास्तच आगावू होता. तो तिला बावळट आणि गांवढळ म्हणे.

तिची सहनशक्ती संपली. तिने त्याला गावरान हिसका दाखवून हाकलले



चिडलेल्या रोहनने घाणेरड्या जोक्समधे श्रुतीचे नाव घातले व मित्रांना पाठवले.

तिच्या नावाने ट्रोलपेज काढले. तिचे मीम्स व्हिडिओ त्यात घातले.

हे कॉलेजभर पसरलं. तिचं मन अभ्यासावरून उडालं. सर्व सोडावंसं वाटू लागलं

श्रुतीने या आधीच कॉलेज अधिकारी व पोलिसांना हे सर्व कळवायला हवं होतं.

PONZI SCHEME

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

Sections Applicable

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

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

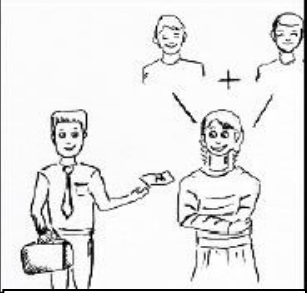
Investing in Ponzi schemes may make you run out of all other Schemes of life!

नेहा एक गरीब
मध्यमवर्गीय मुलगी होती

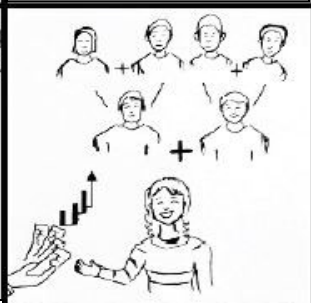
पण तिला जगातील सर्व
छानछोकी करावी वाटे.

एकदा ९९९९ रुपयांत
BMW कार विदेशयात्रेची
साइट तिला दिसली

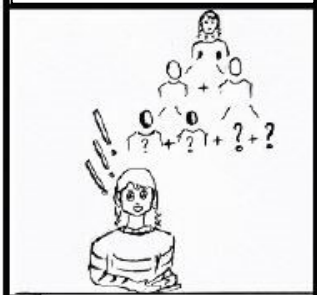
तिने त्यात नाव नोंदवले.
तिला एका **सिक्सस्टारहॉटेल**
मधे मीटिंगला बोलावले.



त्यांनी तिला दोन मेंबर आण
सांगितले. जसजशी डावी उजवी
ब्रांच वाढेल तिचे **कमीशन**ही



तिचे मेंबर्स जेव्हा अजून
मेंबर आणतील तेव्हा
कमीशन वाढेल



तिला आधी पैसे मिळाले.
नंतर मात्र थांबले. मग
मेंबर्सचे पैसे तिनेच गुंतवले.

एक दिवस ती वेबसाइट व
फ़ोन नंबर बंद झाले.
मालक गायब झाले.

मेंबर्स आता तिच्याकडे
पैसे मागतात. तिचा वेळही
फ़कट गेला. **सावधान**

FAKE MATRIMONIAL PROFILE

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

Sections Applicable

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

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

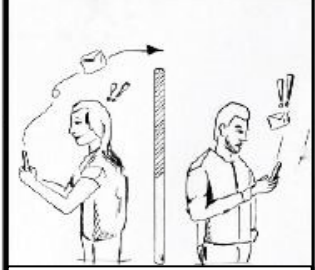
FAKE MATRIMONIAL PROFILE

फ़ातिमा अविवाहित इंजिनियर महिला. तिचे आईवडील तिच्यासाठी नवरा शोधत होते.

ती लग्नाच्या साइट्सची मेंबर होती. एखादा चांगला मुलगा मिळेल या आशेवर.

एका ३० वर्षाच्या मुलाचा तिला लग्नासाठी मेसेज आला.

तिने सर्च केल्यावर तो श्रीमंत घरचा आणि रेल्वेत ऑफ़िसर असल्याचे कळले



त्यांचे मेसेज सुरू झाले. तो मोहक होता. त्याने गोड बोलून तिला मोहित केले.

त्याच्या घरचे फ़ोटो, मित्र, त्याचे आयडी वगैरेंनी तिचा पूर्ण विश्वास बसला.

काही राजकीय मतभेदांत त्याची अचानक नोकरी गेल्याचे त्याने सांगितले व ती परत मिळवण्या साठी तिच्याकडे पैसे मागितले.

पासपोर्ट आयडी अशी कागदपत्रे त्याने तिला दिली व ५ लाख घेतले.

काही दिवसांत बातमी आली. अनेक मुलींना फ़सवल्याबद्दल त्याला पोलीसांनी अटक केली. तिचे पैसे गेले.

MOBILE REPAIR SHOP

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

Sections Applicable

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

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

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

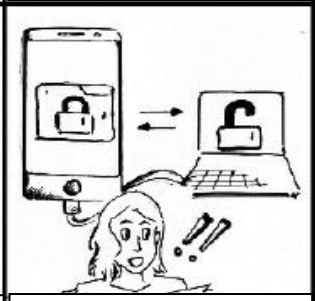
तन्वीला सेल्फ़ीचे व्यसन होते. तिचा मोबाइल कॅमेरा अद्ययावत स्पष्ट होता.

काही स्वतःचे Candid, बॉयफ्रेंड व रूममेट्सबरोबर फ़ोटो हे तिचे सर्वस्व होते.

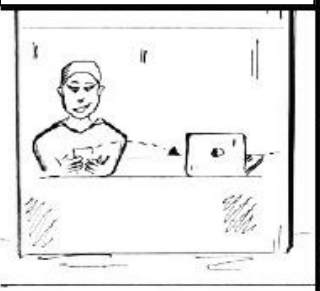
एकदा तिच्या हातून मोबाईल खाली पडला. काही केल्या तो पुन्हा सुरू होईना.

ती एका छोट्या दुकानात दुरुस्तीला गेली. *डेटा बघू नको* हे सांगायला विसरली नाही

मोबाइलला पॅटर्नलॉक होते त्यामुळे कोण पहाणार नाही याची तिला खात्री होती



पण पासवर्ड/पॅटर्न उघडण्याचे सॉफ़्टवेअर असतात हे तिला माहित नव्हते



दुकानदारने मोबाइल दुरुस्त केल्यावर त्यातले बरेच फ़ोटो कॉपी करून ठेवले.

तिचे फ़ोटो दुनियाभर व्हायरल झालेले तिच्या नातेवाइकांकडून कळले.

तन्वीला मोबाइल मधे फ़ोटो सेव्ह करून ठेवल्याचा पश्चात्ताप होतो

FAKE REVIEWS

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

Sections Applicable

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

Fake Reviews may give you wrong Overviews!

कॉलेजात शिकणारी निकिता मॉडेलिंग करत असे.

पेज ३ पार्ट्यांमध्ये ती नेहमी हजेरी लावी. कायम चर्चेत रहायचा प्रयत्न करी.

खुप काळ टिकणारे भारी परफ़्युम्स आणि मेक अप कॉस्मेटिक्स ती वापरे.

पण लवकरच ते परवडेना. ती ऑनलाइन स्वस्त मिळ-वायच्या प्रयत्नात लागली.

तेव्हा तीच प्रॉडक्ट अर्ध्या किंमतीत देणारी एक साइट तिला मिळाली.

तिला संशय आला. पण ४स्टार रेटिंगचे छान रिव्ह्यू पाहून तिने विश्वास ठेवला.

तिने पैसे भरले. पफ़्यूम कॉस्मेटिक्सची ऑर्डर कन्फ़र्म झाल्याचा sms आला.

वस्तू घरपोच आल्या. पण तिने वापरताच स्किनरॅश झाला. शेवटी ती हॉस्पिटल मधे ऍडमिट झाली

खोट्या रिव्ह्युंमुळे निकिता फ़सली. अनेक साइट्स फ़ेक रिव्ह्यु लिहून घेतात. सावधान

FAKE PROFILE WITH SEXTORTION

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

Sections Applicable

Capturing photograph/video:

IPC Section 354C – Voyeurism

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

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

IPC Section 419 – Punishment for cheating by personation

IPC Section 354A – Sexual Harassment and punishment for Sexual

IPC Section 507 – Criminal Intimidation by an Anonymous communication

Publishing online

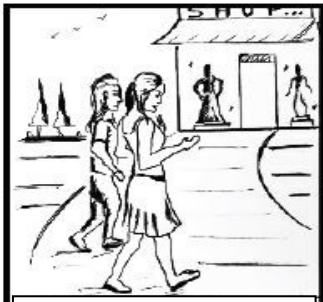
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form

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

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

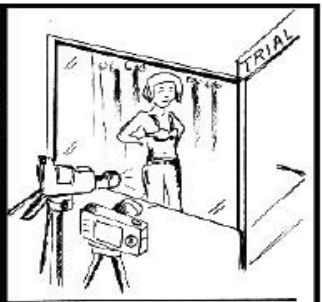
IPC Section 509 – Word, gesture or act intended to insult modesty of a woman

A Fake Ex may levy a unforgiving Tax!



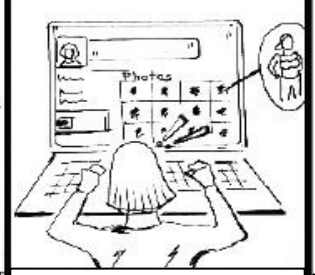
जान्हवी तिच्या मैत्रिणी बरोबर वाढदिवसाचे कपडे घ्यायला दुकानात गेली.

त्यातले काही घेऊन ती चेंजरूममधे ट्रायलसाठी गेली.



त्या रूमला टु वे आरसे होते. दुसऱ्या बाजूंना कॅमेरे लावलेले होते

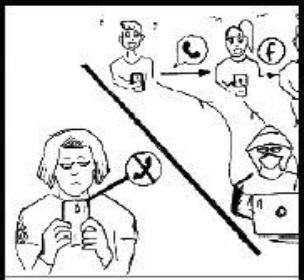
काही दिवसांनी तिच्या मैत्रिणींनी तिला नवीन फ़ेसबुक अकाउंट का केले असे विचारले



तिने ते अकाउंट पाहिले तर धक्काच बसला. त्यात तिचे खासगी फ़ोटो होते

तिने ते प्रोफ़ाइल रिपोर्ट केले. पण पोलिसांत गेली नाही. वाट पहात राहिली.

काही दिवसांनी एका परदेशी नंबरवरून तिला बाहेर भेट असा फ़ोन आला



तिने कॉलकडे दुर्लक्ष केले. तिच्या ओळखीतल्यांना तो तिचे फ़ोटो पाठवू लागला.

जान्हवीने नंतर पोलिसांना कळवले. पण तोवर बराच गाजावाजा झाला होता.

CYBER VULTURES

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

Sections Applicable

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

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

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

मिसेस लोबो एक मध्यम-वर्गीय महिला आणि दोन मुलींची आई होती

तिच्या बहिणीने तिला एका जास्त पैसे देणाऱ्या गुंतव-णूक स्कीमबद्दल सांगितले.

आपल्या पतीच्या इन्शुरंसचे सर्व पैसे तिने त्या स्कीममधे घातले.

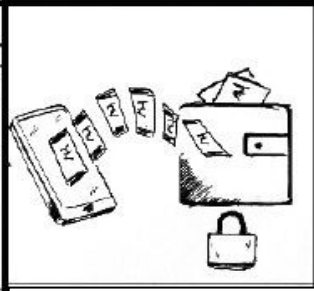
एके दिवशी स्कीमचे सर्व डायरेक्टर्स गायब झाले. तिने पैशांची आशा सोडली

पण एका हॅकरने साइट वरून या सर्व गुंतवणूक-दारांचा डेटा मिळवला.

प्रत्येकाला फ़ोन करून त्याने पैसे मिळवून देण्याची खात्री दिली. त्यातील ३०% त्याचे.

मिसेस लोबो तयार झाली. त्याला तिने हवे ते UPI कोड, ATM सर्व दिले.

ते मिळताच तिच्या अकाउंटमधील २ लाख त्याने गायब केले



ते पैसे फ़ेक अकाउंटच्या ई वॉलेट मधे गेले. त्यांचा पत्ता लागला नाही. सावधान

APP TRAPS

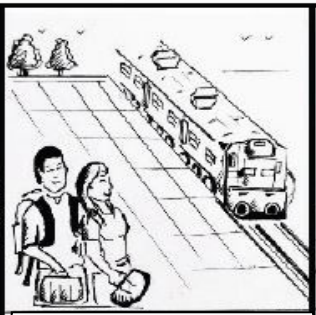
The internet could come with a hidden cost. One of these is preloaded apps that harvest users' data without their knowledge. These apps ask for permission to access files and once given, they may use videos, photos and storage media not only to be mined by marketers but also for other nefarious purposes.

Sections Applicable

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

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

विद्या व रौनक गेली पाच वर्षे एकमेकांच्या प्रेमात होते. नेहमी भेटत असत.

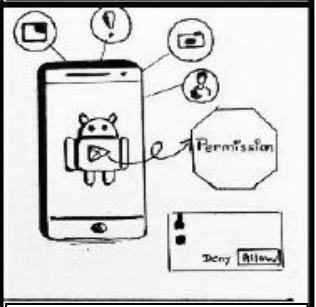


एका विकेंडला ते बाहेरगावी निघाले. बॅगा घेऊन ते स्टेशनवर आले.

तीन दिवस मौजमजा करून ते परतीला निघाले

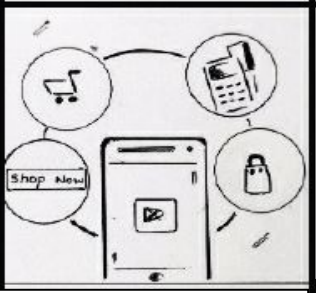
विद्या एक वैद्यकीय appचा नियमित वापर करत असे.

या महिन्यात तिचे पिरियड अनियमित झाल्याने तिने app वर प्रेग्नंसी तपासली

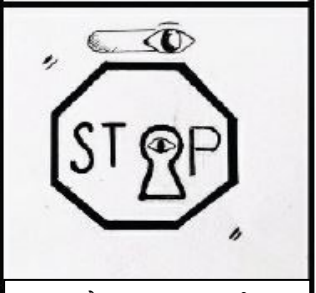


त्या app ने तिच्याकडून GPS, camera, contacts चा access मिळवला होता.

ते लोक तिची माहिती गर्भरोधक कंपनीला पुरवत. तिची प्रायव्हसी संपली.



त्या app ने तिला महाग किट्स घ्यायला लावले. तिच्या अवस्थेचा गैरफ़ायदा घेतला.



आपण जेव्हा app च्या अटी मान्य करतो तेव्हा कॅमेरा, स्टोरेज, मिडिया अशा सर्वांचा access देतो. सावधान

JUICE JACKING

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

Sections Applicable

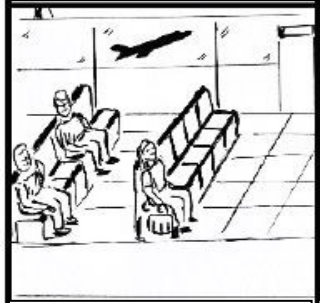
IT Act Section 66 – Computer Related Offences
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature/password/electronic signature)

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

निधी विवाह नियोजक होती तिला सतत विक्रेत्यां चे संयोजन करावे लागे

आयोजित केलेला प्रत्येक समारंभ व्यवस्थित पार पडेल अशी ती काळजी घेई

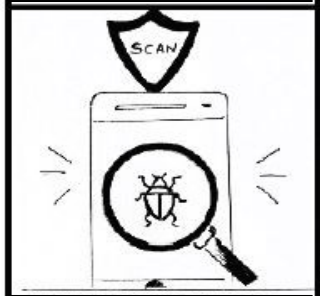
यासाठी विक्रेत्यांशी दोन दोन वेळा बोलून ती खात्री करून घेई.



तिला प्रवासही खुप करावा लागे. त्यामुळे एअरपोर्टवर तिचा बराच वेळ जाई.

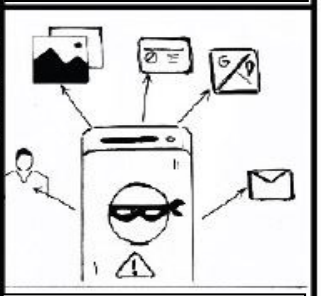
चार्जिंगसाठी ती एअरपोर्ट वर फ्री चार्जिंग स्टेशन वापरत असे.

एकदा तिला आपला फ़ोन स्लो व गरम झाल्याचे जाणवले.



तिने antivirus scan केले. तिच्या फ़ोनमधे एक भयंकर मालवेअर आलं होतं.

हे मालवेअर कोणीतरी चार्जिंग केबलमधून टाकलं होतं.



ज्युसजॅकिंग करून फ़ोनमधील फ़ोटो, माहिती चोरली होती. सावधान

WIFI HACKING

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

Sections Applicable

IT Act Section 66 – Computer Related Offences

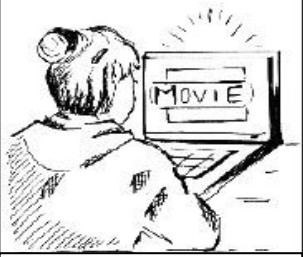
Wrongful gain, wrongful loss of internet data:
IPC Section 420 – Cheating

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

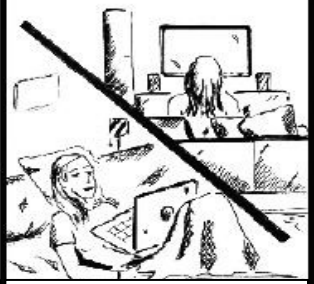
Publishing online
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form
IT Act Section 67A – Punishment for publishing or transmitting of material containing sexually explicit act etc., in electronic form
IT Act Section 67B – Punishment for publishing or transmitting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

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

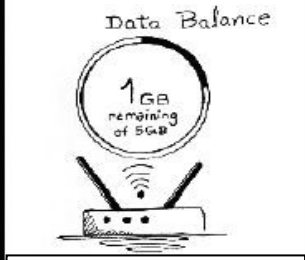
To live a highfy virtual life, better secure your Wi-Fi!



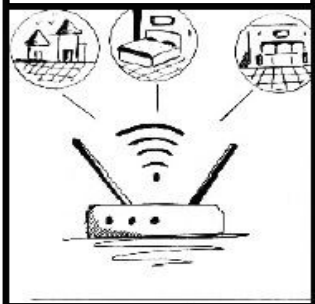
दिव्याला मुव्हीज आवडत. रोज दोन तरी सिनेमे ती नेटफ़्लिक्सवर पहात असे.



हॉलमधील स्मार्टटिव्ही किंवा बेडरूमच्या लॅपटॉप वर ती पहात असे.



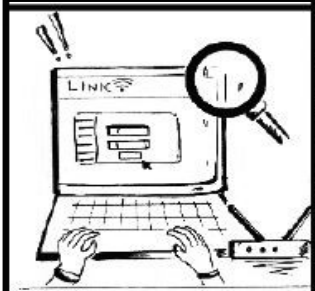
5GB चे तिचे डेली चार्ज होते व त्यातील 4GB ती वापरे. 1GB उरत असे.



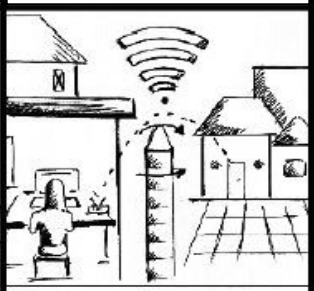
WIFI राउटर हॉलमधे होता. पूर्ण घरात त्याचा सिग्नल मिळे

एकदा तिला आपला नेट स्पीड कमी झाल्याचे जाणवले.

तिने बॅकग्राउंडला काही डाऊनलोड होत आहे का ते लॅपटॉपवर चेक केले.



राउटरच्या admin panel वर तिला तिसरा डिव्हाइस जोडलेला दिसला



तिचा पासवर्ड वापरून कोणी शेजारी तिचे wifi वापरत होते.

नंतर तिला कळले की तिचा wifi वापरून ते डार्क वेबवर ड्रग्ज विकत.

ONLINE RADICALIZATION

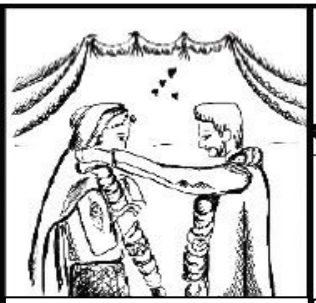
Young, vulnerable individuals can fall prey to terrorists' propaganda while spending time online and browsing the net. The targets of such extremists are individuals or groups of people who can be easily led towards terrorist ideologies because of their experiences, state of mind or sometimes their upbringing.

Sections Applicable

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

Don't get Radicalized, rather be Rationalized!

रेश्मा एक साधी मुलगी होती. तिने नुकतेच इंजिनियरिंग पूर्ण केले होते.



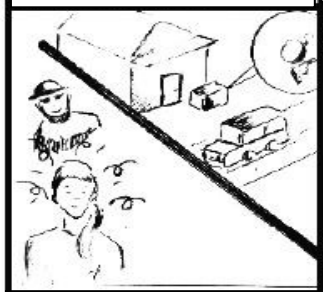
तिच्या वडलांनी तिचे लग्न आफ्रिकेतील एका इंजिनियरशी लावून दिले.

नवऱ्याबरोबर ती अफ्रिकेत गेली पण तिला नोकरी मिळाली नाही.

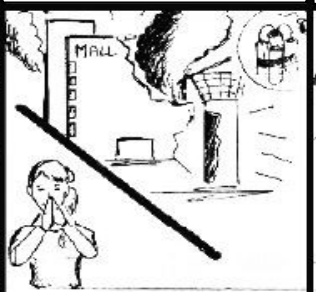
कामधाम नाही आणि बाहेरचं काही माहित नाही. त्यामुळे कायम ऑनलाइन

एकदा तिने एक एक लिंक क्लिक केली तर काहीबाही फ़ोटो आणि मेसेज आले

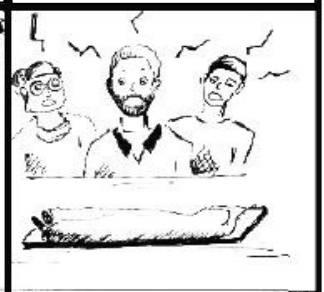
तिला तिकडून एक मेल आली व त्यांच्या नेत्याशी तिचा संवाद सुरू झाला



अतिरेकी विचार तिच्या मनाला पटू लागले. त्यांच्या शस्त्रांची नेआण करू



एक दिवस प्रार्थना करून एका मॉलमधे तिने स्वत:ला बॉबने उडवले.



ती अतिरेकी कशी बनली याचा तिच्या कुटुंबाला कधीच पत्ता लागला नाही.

HONEY TRAP

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

Sections Applicable

Capturing Picture/Video Over Online:

IPC Section 354C – Voyeurism

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

IT Act Section 66E – Punishment for violation of privacy

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

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

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

Demand for ransom (attempt):

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

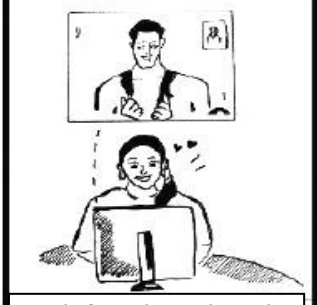
IPC Section 511 – Punishment for attempting to commit offence punishable with imprisonment for life or other imprisonment

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

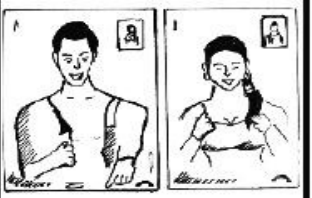
सुमाचे लग्न झाले पण तिला वैवाहिक सुख मिळत नव्हते.

रोज रात्री ती अनोळखी पुरूषांशी व्हिडिओ चॅट करून मग झोपत असे

एके रात्री तिला मोहन नावाचा एक भारी तरूण चॅटसाठी भेटला.



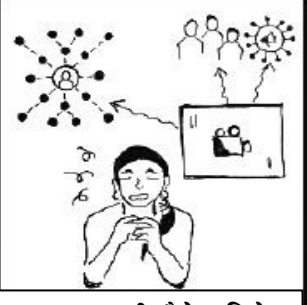
त्याने तिला नेहमी भेटायचे विचारले. तिने आनंदाने होकार दिला



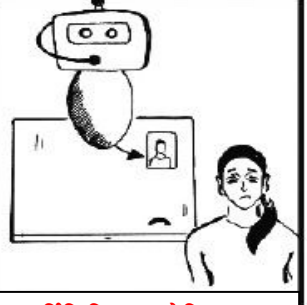
तो आपले एक एक कपडे उतरवू लागला तिलाही तसे करायला सांगितले.

तिने स्वखुशीने ते केले, सर्व कपडे काढल्यावर त्यांचा चॅट आनंदात संपला

पाच मिनिटांतच आला मेल तिचा कपडे उतरवतानाचा व्हिडिओ व पैशांची मागणी



सुमा घाबरली. पैसे न दिले तर सर्वत्र बदनामी आणि आयुष्य उद्ध्वस्त होणार



आर्टिफ़िशिअल इंटेलिजन्सचा वापर करून जुने व्हिडिओ वापरून तिला फ़सवले गेले.

QR CODE SCAM

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

Sections Applicable

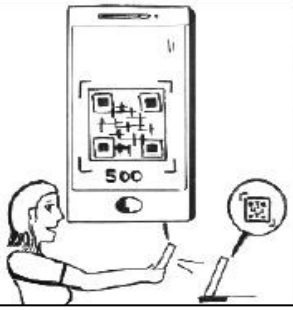
IPC Section 406 - Punishment for Criminal Breach of Trust
IPC Section 420 - Cheating

Unauthorised Access by Installing Malware in The Background:
IT Act Section 66 - Computer Related Offences

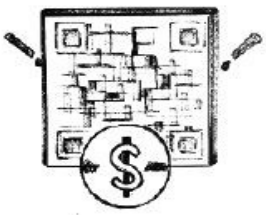
Your money is at Stake because of codes and apps that you may have downloaded are Fake.

कियारा एक टेक एक्स्पर्ट मुलगी आणि डिजिटल पेमेंटची उत्साही समर्थक

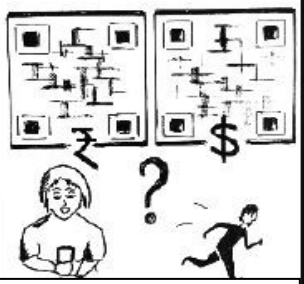
ई वॉलेट, क्रेडिट डेबिट कार्ड यांचा मोबाइलवरून ती प्रच्छन्न वापर करी



एकदा एक QR code स्कॅन करून तिने ५०० रु. ऑनलाइन पेमेंट केले.



QR code फ़सवा होता. त्यात ५०० रुपयांऐवजी ५०० डॉलर होते



कियाराने तो **आकडा** पाहिला **आणि चलनाकडे पाहिलेच नाही.**

पैसे परत मिळवण्याचे तिचे यत्न वाया गेले कारण तिने पैसे स्वखुशीने दिलेले होते

कियाराची मैत्रिण तान्याला अशाच QR Code मधून व्हायरस आला होता.

Drive by Download या टेक्निकने असे कोड बॅक्ग्राउंड ला जाऊन बसतात. **लुटतात**

QR स्कॅनिंगमुळे आपला app वरचा कंट्रोल निघून जाऊ शकतो. **सावधान**

RFID CLONING

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

Sections Applicable

IT Act Section 66 – Computer Related Offences

Stealing RFID data / RFID Cloning:

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

Retaining stolen data & Selling Credit Card Details:

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

IPC Section 420 – Cheating

Creating Replica of Digital ID & accessing server by impersonation:

IT Act Section 66 – Computer Related Offences

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

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

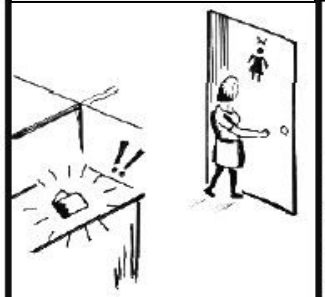
IPC Section 419 – Punishment for cheating by personation

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

आयेशा IT मधे काम करे.
कंपनीचे दरवाजे उघडण्यासाठी
ती RFID Tag वापरे

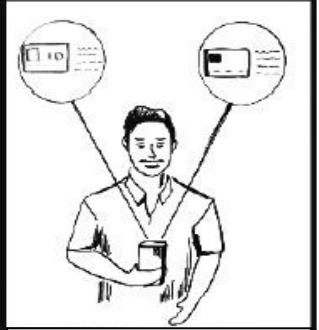
आपल्या पर्समधे ते कार्ड
ठेवी व दरवाजाजवळ
येताच ती ते काढ़न लावी

ती आपली पर्स टेबलवर
ठेवी. तिला सवयच होती



एकदा ती बाथरूमला, पर्स
टेबलवर तशीच ठेवून गेली.

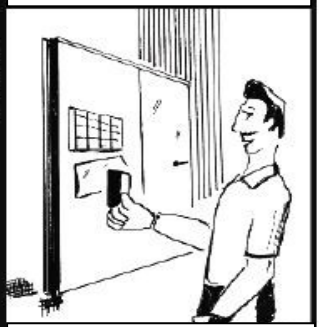
तिचा स्पर्धक जॉनने ते कार्ड
RFID रीडरवर scan केले



ऑफ़िसचे व क्रेडिट कार्ड
माहिती त्याला मिळाली.

डार्क वेबवर त्याने ती
माहिती विकली

तिची ऑफ़िशिअल
माहिती त्याने रेप्लिकेट
केली



ती घेऊन तो तिच्या नावाने सर्व्हर
रूम मधे गेला व सिस्टिम हॅक
केली. दोष आयेशावर आला.

DRONE SURVEILLANCE

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

Sections Applicable

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

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

IPC Section 354C – Voyeurism

IPC Section 354D – Stalking

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

IT Act Section 66E – Punishment for violation of privacy

Unauthorised access to WI FI by DRONE:

IT Act Section 66 – Computer Related Offences

Stealing personal information via WI FI Cracker:

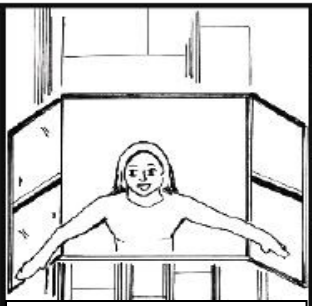
IT Act Section 66C – Punishment for Identity Theft (dishonestly or fraudulently using a unique identification feature)

Dropping hazardous materials to house via DRONE:

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

You are profiled day in and day out without doubt.Genes.

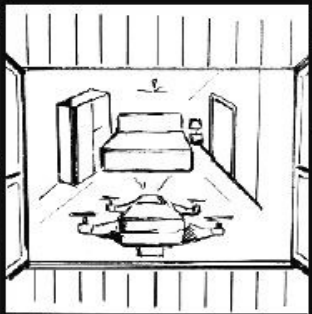
मेडिकल विद्यार्थिनी राधाचे घर ३३माळ्यावर होते.



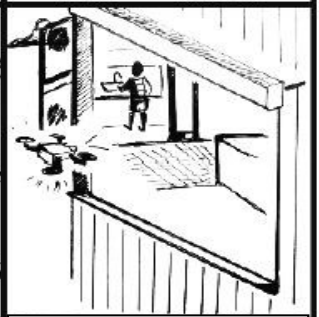
आसपास एवढी उंच बिल्डिंग नव्हती. त्यामुळे ती आपल्या सर्व खिडक्या उघड्या ठेवी

घरात एकटीच असल्याने ती कमी कपड्यात वावरे.

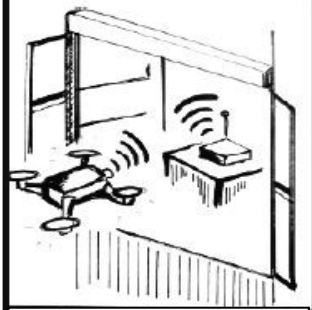
अक्षय तिचा एक्स बॉयफ्रेंड तिच्यावर पाळत ठेवण्या साठी ड्रोन कॅमेरा वापरे.



त्याने तिच्या बेड व हॉलचे व्हिडिओ रेकॉर्ड केले

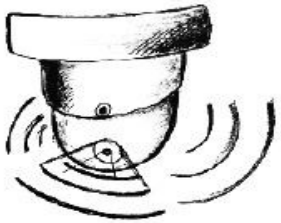


तिच्या येण्याजाण्याची वेळही त्याने रेकॉर्ड केली



त्यात WIFI Cracker तिची खास माहिती जमवी

ड्रोनने तो तिच्या घरात घातक स्फ़ोटक वस्तू टाकू शकत असे



तिने जर मोशन सेन्सर सह CCTV लावला असता तर तिला हे सर्व कळू शकले

SEARCH ENGINE RESULTS SCAM

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

Sections Applicable

IT Act Section 66 – Computer Related Offences

Replacing Original Contact Details by Fraudster Details:

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

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

IPC Section 419 – Punishment for cheating by personation

IPC Section 420 – Cheating

IPC Section 465 – Making a false document

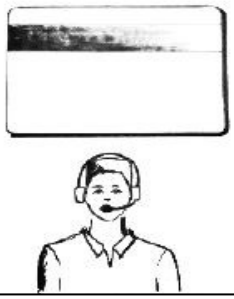
IPC Section 468 – Forgery for the purpose of cheating

Fake numbers of customer care may put you under intensive care

अक्षताने मेंगलोरसाठी प्लेन तिकिट बुक केले होते.

प्रवासाआधी दोन दिवस तिकिट कॅन्सल मेल आली

गुगलवरून नंबर शोधून तिने कंपनीला फ़ोन केला

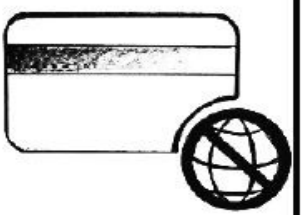


त्यांनी मागितल्याने तिने तिच्या क्रेडिट कार्डचे डिटेल व CVV दिला

थोड्यावेळात तिचे ५ वेळा १०००० रुपये गेले. ५००००

तिला आलेली मेल **spoof** होती. कंपनीकडून नव्हती

कॉलसेंटरनंबरही हॅकरने टाकलेला फ़ेक होता.



OTP दिला नाही. फॉरेन गेटवेना OTP लागत नाही

अक्षताने कार्डचा फॉरेन युज बंद करायला हवा होता.

INFOTOONS EXPLAINED!

TIPS TO STAY CYBER SAFE

Adv. Prashant Jhala

1. MOBILE RECHARGE:

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

2. DEBIT CARD CLONING:

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

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

3. KEYLOGGER:

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

from unknown source, do not download free songs, movies, videos, software's, applications, games etc for a keylogger could be embedded in them and you may end up downloading one for free. Make sure to enable Two Factor Authentication for an additional layer of security, use virtual keyboard to enter the username and password and install a good antivirus on your system to stay cyber safe.

4. SMS SPOOFING:

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

5. CALL SPOOFING:

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

This should help you in the quest to scam-proof your brain. Also, Never give credit card information to someone who calls you. You may also use Google reverse lookup or Truecaller for assistance.

6. RANSOMWARE:

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

7. CYBER STALKING:

Precaution: Cyberstalking is a serious crime, and no one wants to become a victim. One way to help protect yourself is to keep your personal information private on the internet. That's a start. Be careful about allowing physical access to your computer and other web-enabled devices like smartphones. Cyberstalkers can use software and hardware

devices (sometimes attached to the back of your PC without you even knowing it) to monitor their victims. Be sure you always log out of your computer programs when you step away from the computer and use a screensaver with a password. Delete or make private any online calendars or itineraries — even on your social network — where you list events you plan to attend. That information could allow a cyberstalker to know where and when you're planning to be somewhere. A lot of personal information is often displayed on social networks, such as your name, date of birth, where you work, and where you live. Use the privacy settings in all your online accounts to limit your online sharing with those outside your trusted circle. You can use these settings to opt out of having your profile appear when someone searches for your name. You can block people from seeing your posts and photos, too. If you post photos online via social networks or other methods, be sure to turn off the location services metadata in the photo. The metadata reveals a lot of information about the photo — where and when it was taken, what device it was taken on, and other private information. Most often, metadata comes from photos taken on a mobile phone. You can turn this off — it's usually a feature called geo-tagging — in your phone's settings.

8. PICTURE MORPHING:

Precautions: Morphing has become a child's plays with tools, apps, software's and technology made available by the internet for free. Various apps allow photo editing and high-end software's allows the act of morphing very easy. High end filters are available for free which can be used to enhance the quality of the pictures. With Drag and Drop and Cut, Copy and Paste options, super imposing or replacing the body and/or body parts of one individual with that of another can be done with considerable ease. Thus, porn and obscene contents are easily created to defame someone by using the victims face and other identification features that are similar to the victims and a lookalike picture of the

victims can be uploaded online thereby shaming them. Do not share your pictures with unknown people or strangers and while uploading on social networking sites like Fb, Instagram, Snapchat etc, one should have an appropriate privacy setting in place before sharing. Very recently a girl committed suicide when she learnt that a morphed vulgar picture of hers were circulated online by an accused. Care before you Share.

9. PROFILE HACKING:

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

10. ONLINE GAMES:

Precautions: Very recently it was reported that fake versions of online games (including Temple Run, Free Flow and Hill Climb Race) that are popular

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

11. JOB CALL LETTER:

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

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

12. DEEP FAKES:

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

13. DATING WEBSITES:

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

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

14. CAMERA HACKING:

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

and videos without your knowledge and there could be a huge privacy breach. Always use a masking tape on the webcam of your laptops to avoid breach of your privacy. As for mobile phones, put a piece of cloth on it when you are not using it. Remember that the mobile phones have cameras on both the side so precaution has to be adopted accordingly.

15. SOCIAL TROLLING:

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

16. PONZI SCHEMES:

Precautions: Schemes that offers to make you rich and wealth without much efforts are often dubious. Remember that Schemes that offers high returns on your investments most probably will never return the money that you originally may have invested. Unfortunately, both literate and illtreat people fall prey to such schemes. The greed to make money without efforts or to adopt a shortcut to become rich and wealthy may reduce your hard-earned income and make you poor and unhealthy thereby. There have been enough Ponzi schemes being reported and investigated by the law enforcement agencies but despite that new Ponzi schemes are floated and people fall prey to such schemes. Study the entire project and cross verify, make your own research before entrusting

your money to someone or investing it into any such schemes. Do not trust agents who promotes such schemes because they are appointed to paddle wrong information and paint a fake picture of the scheme that would attract your attention and make you not think rationally.

17. FAKE MATRIMONIAL SITES:

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

18. MOBILE REPAIR SHOP:

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

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

19. FAKE REVIEWS:

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

20. FAKE PROFILES WITH SEXTORTION:

Precautions: An upward trend in these crimes have been observed. Pictures and videos clicked with or without consent in the moments of privacy are used later to blackmail and or extort females for further gratification, to extort money or to get them indulged into commission of other crimes or getting them involved in criminal activities. Pictures and Videos clicked in your good times comes to haunt you when the relationship turns sour.

Never ever allow anyone to click a picture or a video that you may feel would go against you someday. Also called Revenge Porn.

21. CYBER VULTURES:

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

22. APP TRAPS:

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

23. JUICE JACKING:

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

24.WIFI HACKING:

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

25. ONLINE RADICALIZATION:

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

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

26. HONEY TRAP:

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

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

27. QR HACK:

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

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

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

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

For receiving money, no OTP is ever generated.

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

28. RFID CLONING

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

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

keyless entry ie. Card Key. CCTV cams helped to nail the culprit and he confessed that he had a device which could store 10 virtual keys and that copying the data of the keys was as easy as tapping on the actual key.

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

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

29. DRONE SURVEILLANCE

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

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

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

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

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

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

30. SEARCH ENGINE FRAUD

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

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

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

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

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

RBI has now provided and enabled an added feature as a Security

measure for Cards wherein you can now only make use of your cards at ATMs and on Point of Sale (POS) devices within the Country.

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

Profile: Advocate Prashant Jhala is a Cyber Lawyer from Mumbai.

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 and workshops/events/seminars organised by Information and Technology stake holders.

Mail: prashant@icladvocates.com

Call: +91 9869184691

Where to Report Cyber-Crimes

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

Disclaimer: The above-mentioned explanations herein are to the best of our knowledge and interpretations and are for information purpose only. They may be used as a guiding force. They should not be construed as legal opinion by any chance.

A NOTE FROM THE POLICE OFFICER

Yashavantha Kumar KN

Technology has driven our lives from the time we get up in the morning, with the chirping alarm from a mobile, a WhatsApp good morning, a digital calendar to remind us what to do the day, maps to navigate our roads, e-commerce and online banking to pay our bills, online games to keep us busy and apps to help us and feed our tech savviness.

Use of internet is an integral part of our lives and it has impacted us that it has become indispensable part of our lives. However, if technology has increased in a pace of 10, the cybercrimes have increased 100 folds. But most of us are unaware of such crimes or threats which we may be facing. Also, many a times, it happens without our knowledge.

It is also observed that the cybercrime has been affecting the women at large compared to the men. However, it can generally affect anyone, young or old, men or women, anyone could be susceptible to cybercrime. It is thus very important at this juncture, to create awareness to all, especially the worn, regarding the cybercrimes which is happening as a global phenomenon.

The preventive tips in the book can help keep us cybersafe to the maximum, if followed judiciously.

1. Sexual harassment is an act where a man provokes a woman in different ways, such as following her, make unwelcoming advances towards her, demand sexual favours, show obscene content against her will, etc. The man may try to assault her or use forces with an intention to disrobe her or force her to become naked

2. Voyeurism is an act of secretly watching or peeping into a woman

engaging in a private act. It can be an act where a man watches, captures, publishes or disseminates such images of a private act. The criminal tries to post obscene material in electronic form. The material could be lascivious, appealing to the prurient interest with the tendency to deprave or corrupt a person's mind. The material could be of the form which is readable, or a video to be watched, an audible content or embodied in electronic form.

The victim should understand any such acts mentioned above is an offence and must not keep quiet about it. The crime could include a person/ criminal who posts sexually explicit matter in electronic form by either publishing or helping others to publish.

3.Stalking: this act involves any man who follows, contacts or attempts to contact a woman for personal interaction offline or online intentionally. In online mode, the stalking is done by the man who monitors her over internet, emails, social media or any other electronic form. Stalking creates fear or a sense of harassment over the woman due to repeated unwanted act. Stalking intends to insult the modesty of any women by uttering unwanted words, making sounds, gestures or exhibits insulting objects. Any such act is an offence.

4. Identity thefts: An electronic identify includes electronic signature, password/ pin, biometric identifiers or any such unique identification features. Theft of such identify may occur in the form of downloading, copying, extracting personal information of anyone without permission, dishonestly. Such an act of fraudulence is an offence or crime.

5. Be aware of cheaters by personation: Personation act includes inducing a person to accept, agree, transact, deliver data or information to another person by force or for money. Such and act is an offence.

6. Smishing/ SMS phishing: This cyber offence includes the criminal suing fraudulent text message designed to trick you so that they can gather your personal, banking details, etc. Sometimes you receive a text message with phone number or links. These could be such fraudulent

texts to trap you and gather personal information from you. Hence it is important to be aware and not fall to such trap. Some of the advices to be followed are:

- Do not click such links
- Do not call back to such numbers
- Do not reply or text such numbers
- Report to authorities

7. Phishing: This act involves exploiting human nature by studying. In this case, the Fraudulent attempt to obtain Sensitive/personal information via online by disguising oneself as a trustworthy entity. this information could be usernames, passwords, banking details. Phishing can be identified by proper observations. Some of the observations include:

- poorly written texts
- an attempt to offer money
- asking financial assistance
- use of tactic messaging
- emails with strange email addresses
- texts or emails which arrives at an unexpected time or has out-of-character messaging from "known" senders

Phishing is an offence and becoming a victim can be avoided with following suggestions:

- Never click links/emails from unknown source
- Never open unsafe attachments
- Never share/type login credentials
- Never share banking credentials
- Never do money transaction

8. Vishing / Voice phishing: This is an act where criminals use phone calls (voice or VOIP) to gain access to victims' personal, financial information. However, it is possible to identify them by observing following tricks used by offender/ criminal:

- Uses Apps to pretend themselves as trusted organisation
- Impersonates themselves as bank official or trusted entity
- Communicates in language other than regional language
- Quotes some reasons which may feel like genuine

A visher may try some of the following tricks:

- Ask for personal /Banking /ATM card details
- Request for immediate/urgent actions
- Create panic
- Request him/her to connect remotely to your computer
- Request you to download some Apps
- Request you to Click link/ To share OTP/Code
- Abuses for non-co-operation and thus force you to some action.

It is possible to avoid visher by adhering to certain guidelines as follows:

- Be suspicious of unknown calls
- Ignore calls from unknown numbers
- Never call back to unknown numbers
- Never respond to strange voices messages
- Do not trust caller IDs as spoofing is very easy nowadays
- Never trust visher, nor cross question the visher
- Never get panicked by listening to their reasons
- Never act as per his/her instruction
- Never download any Apps like mysms, anydesk ,diskdigger, cashify etc.
- Never transfer money to any account for any offer/reasons
- Never click any suspicious link
- Never scan any QR code unless you are sure
- Never share/ send back any messages received on your mobile/system
- Never share sensitive information like user name, password, PIN, banking details
- Never share ATM card number, card expiry date, CVV, OTP
- Never relay upon search engine to gather contact details of bank, financial institution

9. OTP Scam: A person may request for OTP received in your mobile using reasons such as: telling that your card is blovked, requesting OTP to retrieve it, for card reneval, for card activation, or linking Aadhar or to update reward points etc. In case of OTP they may also request for information such as 16 digit card number, card expiry date, 3 digit CVV number and then OTP received on RMN. Be cautious of such fraudulents and report to authorities immediately. There are modules available using which a person retorts to OTP scam and thus your OTP being compromised.

- Direct Method: in this method, he/she may Instruct you to Read/ Forward SMS Received on RMN or instructs you to Click/Forward Link To The Specific Number
- Indirect method: This is done by Installing APPS Like MySMS or QR code scan in Victim's Mobile
- Remote Access: Instructs to Download App Like Any Desk, Disk digger
- Search Engine: Manipulating Bank /Service Provider Customer Care Number

10. Card Skimming: This is a case wherein the debit card is with you, you have not given card to anyone nor are you using the card, yet you may get message on your mobile about some transaction done by you. This situation arises in case called as card skimming. This is done using following traps:

- Key logger: The victim's Password/Pin is captured
- Pin- hole camera: The victim's finger movements on key pad is captured
- Black magnet card: The victim's card is clones or recreated

However, it is possible to prevent card from skimming by following certain precautions/ guidelines:

- Use Onsite ATM
- Use Secured ATM
- Use Daily Transaction Limit
- Use Switching ATM Card on/off By Mobile App

- Avoid usage of ATM Card in presence of other people
- Never take help from unknown in usage of ATM card
- Never write PIN on your card
- Destroy withdrawal slips carefully
- Inform immediately about unknown/sticky/cello/double side tape/ objects found
- Never allow to swipe your card to another machine for any technical reason
- Never allow unknown person to stand beside during ATM transaction

In case you become a victim of OTP or skimming fraud, then follow the guidelines below to avoid further damage:

- Block Your ATM Card
- Change PIN/Password/Security Questions
- Verify Fraudulent Transaction
- Capture Screenshots
- Report to Your Bank & Nearest CEN/CYBER /Police Station

11. Facebook/ Instagram/ social media related crimes: Many a times our social media accounts such as Facebook / Instagram accounts may be compromised. The criminal may create account or fake page using following tricks:

- Using Fake Credentials
- Using Credentials belonging to the victim
- Creates & Posts Victim Name, Pictures, Contact Details
- Take Control over Victims Original Account
- Hacking/Unauthorised Access of Victims Account

12. Matrimonial/ Gift fraud: This is the case where in the offender may try some of the following

- Creates Social Media Account using Fake Credentials
- Impersonates as professional at reputed overseas Organisation with Lavish Life Style
- Establishes Intimacy communication with the victim

- Informs that She/he is coming with or is sending valuable gifts
- Makes you feel that he/she is genuine by sending Invoice, Courier Bill, Tracking Id, Air Ticket Etc.
- Intimates that he is reached and that the gift he sent has reached to Indian international airport
- Victim gets calls from impersonated authorities
- Victim deposits amount to various bank accounts at different stages as directed by organised syndicate
- Blackmail/threaten/humiliates the victim

13. Online platform sale / purchase frauds: Many people become victim to such frauds wherein the criminal tries any of the following:

- Creates Fake Id on Olx /Quicker/ Facebook Platform
- Posts Advertisements with Attractive Offers, Contact Number
- Provokes Victim to Pay Partial Amount to Block
- Provokes Victim & Gets Deposits by Quoting Many Reasons

14. Sexual Harassment of Women At Work Place (Prevention, Prohibition And Redressal Act-2013: Sexual harassment includes un welcome sexually determined behavior such as follows:

- Physical contact and advances;
- A demand or request for sexual favors
- Sexually colored remarks
- Showing pornography

However, there are Guidelines and norms laid down by the honorable Supreme court in Vishaka and others v/s state of Rajasthan (JT 1997 (7 SC 384)

15. Juice Jacking: Do you often charge your phone from public port while travelling? Then be aware of trap known as juice jacking where attackers will make use of public charging ports to install malware, steel data or even to take complete control of your device.

To prevent being a victim of Juice jacking. One must follow certain guidelines:

- Carry a personal charger of your device
- Carry your personal power bank/backup

However, if the above is inevitable the do the following

- Disable data transfer mode
- Your phone shouldn't pair with other devices
- Switch off handset before recharging
- Avoid opening password pattern

16. SIM swapping or cloning fraud: There are chances that your SIM card may be cloned or swapped. This is an instance where in the criminal tries to do the following

- Identifies the target person & mobile number of that person used for online banking
- Creates fake documents in the name of target person
- Activates same number new sim card by impersonating target person
- Activates net banking with newly activated sim card in the name of target person

Therefore, in case your Sim gets suddenly deactivated, there are chances that your Sim is swapped. During such times, immediately inform your bank to stop all transaction and also inform your mobile service provider. Finally lodge a written complaint to cyber police station or nearest jurisdictional police station

Remember to be cautious when using internet as there are chances of being a victim of several vulnerabilities. However, with few precautions and guidelines, it is possible to stay away from such fraudulent. Awareness is the key to following the preventive tips. Be brave to report in case of such crimes incurred on you.

Stay cyber safe.

OFFENCES AND RELEVANT PENAL SECTIONS

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

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

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

23	Intermediaries not providing access to information stored on their computer to the relevant authorities	Section 69 of ITAA 2008 imprisonment up to 7 years and fine	
24	Failure to Block Web sites, when ordered	Section 69A of ITAA 2008 imprisonment up to 7 years and fine	
25	Sending threatening messages by e-mail		Section 506 IPC 2 years or fine or both
25	Word, gesture or act intended to insult the modesty of a woman		Section 509 IPC 1 years or fine or both — IPC as applicable
26	Sending defamatory messages by e-mail		Section 500 IPC 2 years or fine or both
27	Bogus Web sites, cyber frauds	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC 3 years imprisonment or fine Section 420 IPC 7 years imprisonment and fine
28	E-mail Spoofing	Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC 2 years or fine or both Section 468 IPC 7 years imprisonment and fine
29	Making a false document	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC 2 years or fine or both
30	Forgery for purpose of cheating	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC 7 years imprisonment and fine
31	Forgery for purpose of harming reputation	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section. 469 IPC 3 years and fine
32	E-mail Abuse		Sec. 500 IPC 2 years or fine or both
33	Punishment for criminal intimidation		Sec. 506 IPC 2 years or fine or both — if threat be to cause death or grievous hurt, etc. — 7 years or fine or both
34	Criminal intimidation by an anonymous communication		Sec. 507 IPC 2 years along with punishment under section 506 IPC
35	Copyright infringement	Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both	Sec. 63, 63B Copyrights Act 1957
36	Theft of Computer Hardware		Sec. 379 IPC 3 years imprisonment or fine or both
37	Online Sale of Drugs		NDPS Act
38	Online Sale of Arms		Arms Act

Do you want to invite

Dr Ananth Prabhu G

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

contact

+91 89515 11111

info@ananthprabhu.com

to follow his regular updates like the page

www.facebook.com/educatorananth

Beti Bachao
Cyber Crime Se...

Don't be a victim
of cyber crime.

Be a #CyberSafeGirl

www.cybersafegirl.com