CYBER PATRIOT

Indian Cyber Institute

Supported by

ISEA

Information Security Education & Awareness

Cyber Safe GIRL

Beti Bachao, Cyber Crime Se...

2.0

25 eye-opening sketches
to ensure online safety of girls

ANANTH PRABHU G PhD

FOREWORD BY **VIVEK SHETTY**

www.cybersafegirl.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 in Sahyadri College of Engineering and Management. He is also the Cyber Law Guest Faculty at the Karnataka Judicial Academy and Cyber Security Guest Faculty at the Karnataka Police Academy and Police Training College.

+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 25 topics described in the Cyber Safe Girl v2.0 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

Beti Bachao, Cyber Crime Se...

2.0

25 eye-opening sketches
to ensure online safety of girls

Title: Cyber Safe Girl

Version: Second

Publisher: Dr Ananth Prabhu G

Foreword by Mr .Vivek S hetty

First Published in India in 2018

Designed and printed by
Tarjani Communications Pvt. Ltd, Mangaluru

Credits

Sanjay Sahay, IPS

Dr. Murugan, IPS

Arun Chakravarthy, IPS

Roopa D, IPS

Dr. Vedamurthi CB, IPS

Hanumantharaya, IPS

Reena Suvarna, KSPS

Bharath S Reddy, KSPS

Dr. Devaraj B., KSPS

M.C Kavitha, KSP

Adv. Prashanth Jhala
Cyber Law Consultant &
Cyber Crime Investigator

Tapan J Mehta
Founder, Indian Cyber Institute
Cyber Crime Consultant and
Financial Crime Investigator

Special Thanks to

Krishna J Palemar

Manjunath Bhandary

J Koragappa

Manish Yadav

Vaikunt R Prabhu

Ganesh M Nayak
Outreach Head

Fazeel Ahmed
Web Developer

Waseem Shan
Web Designer

Prasad Patibandla

Artist

Anudeep Karkera

Vivek Shetty
Entrepreneur & Social Activist
twitter: @vivekshettym

FOREWORD

Cyber Crime is a global phenomenon which hampers the privacy and security of a person online. Women are often the soft targets. There are people who are on the lookout for personal information, like passwords, bank details, etc. Apart from that women are often harassed, stalked and threatened in the virtual world.

Your Facebook/Twitter status and photos say a lot about you. A determined person may already have found out that you're a woman, details about where you live and whether you are currently alone. With that post, the bad guy could set you up for a robbery or even a physical attack.

I congratulate Dr. Ananth Prabhu G for coming out with this wonderful booklet depicting 25 real time scenarios. Also, the safety measures to be taken for online safety would keep you protected from various crimes, helping you to build your protective cocoon online. After all, awareness is the key and everyone must engage in responsible internet surfing.

Remember, that prevention is better than cure. Be ready to fight this war against cyber crime. STAY SAFE ONLINE!

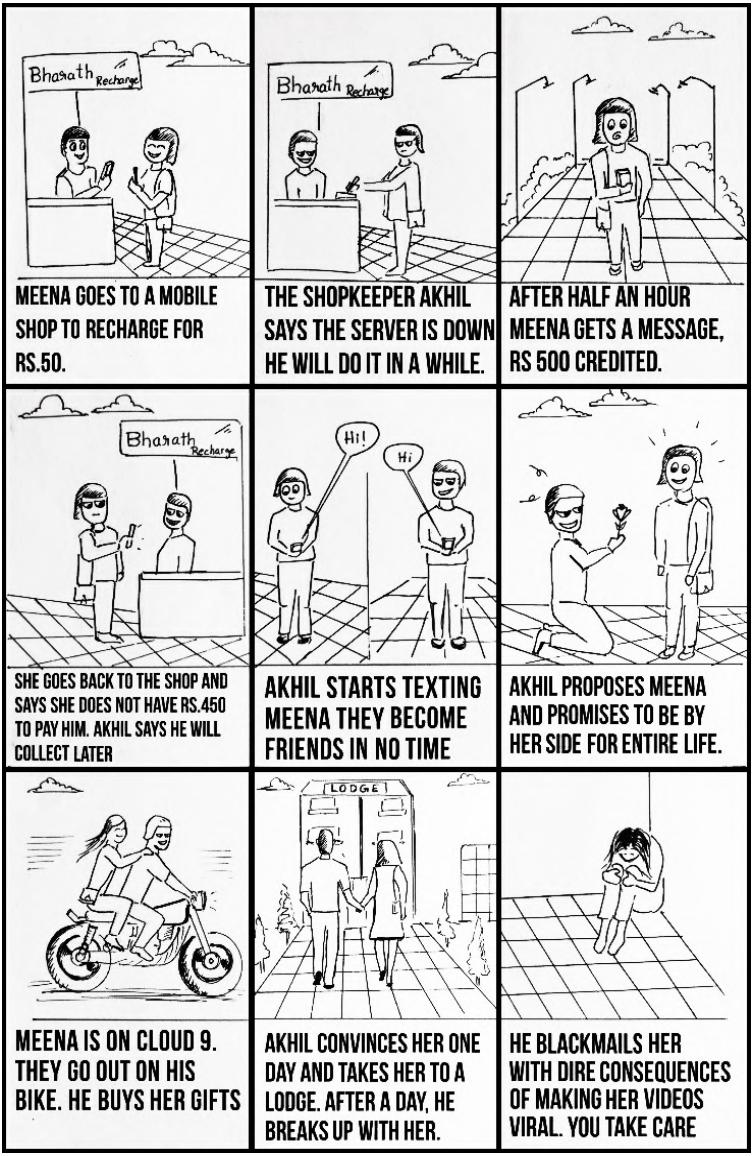
Warm Regards,

Vivek Shetty

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.


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

DEBIT CARD CLONING

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


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

KEYLOGGER

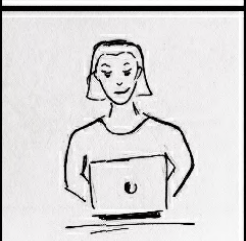
It is a malicious program that may be installed on the victim's computer for recording computer user keystrokes to steal passwords and other sensitive information. With Keylogger a scamster will be able to collect login details and other matter saved in the computer and have them mailed to a designated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

ANUSHA AND POOJA ARE BEST FRIENDS AND SHARE THE SAME ROOM IN THEIR PG. THEY WORK FOR THE SAME MNC

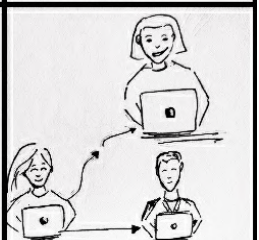
INCIDENTLY, BOTH OF THEM END UP HAVING A BIG TIME CRUSH ON THEIR BOSS VIVEK

WITHOUT WASTING ANY TIME, POOJA PROPOSES VIVEK AND HE ACCEPTS. THEY START DATING EACH OTHER.

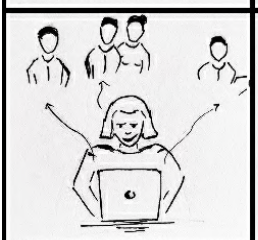
ANUSHA IS HEART BROKEN. SHE WANTS TO TEACH POOJA A LESSON THAT SHE WOULD REMEMBER FOR LIFE.



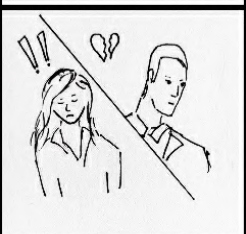
ANUSHA INSTALLS KEYLOGGER SPYWARE ON POOJAS LAPTOP, TO SNOOP ON HER ACTIVITIES.



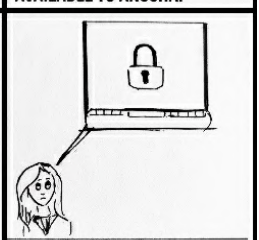
POOJA IS UNAWARE THAT HER PASSWORDS, PHOTOS SHARED, PRIVATE CHATS, EMAILS AND BROWSING HISTORY IS NOW AVAILABLE TO ANUSHA.



ANUSHA EMAILS THE PRIVATE CONVO TO POOJA'S PARENTS AND UPLOADS THEIR PRIVATE PHOTOS ON SOCIAL MEDIA VIA FAKE PROFILE.



VIVEK IS SHOCKED. THEY BREAK UP AND POOJA IS NOW ALL SHATTERED.



POOJA REGRETS FOR NOT LOCKING HER PC WITH A PASSWORD AND INSTALLING AN ANTI VIRUS PROGRAM WHICH WOULD HAVE PROTECTED HER.

SMS SPOOFING

Spoofing is being able to send a message by hiding or changing or using a completely different sender ID. Typically, 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.


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

CALL SPOOFING

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

SHABANA IS A WIDOW. SHE LIVES ALONE IN HER INDEPENDENT HOUSE.

TO KEEP HERSELF OCCUPIED, SHABANA SURFS THE INTERNET AND IS VERY MUCH ACTIVE ON SOCIAL MEDIA.

SHE WAS UNAWARE ABOUT SOCIAL ENGINEERING AND USED TO BEFRIEND ANYONE WHO SENT HER FRIEND REQUESTS, IF THEY HAD SOME MUTUAL FRIENDS.

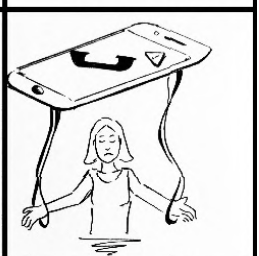
SHABANAS SON MAKES AN EMERGENCY CALL AND REQUESTS 1 LAKH TO BE TRANSFERRED TO HIS FRIENDS ACCOUNT.

SHABANA VERIFIES HER SONS NUMBER, IT'S VALID. THUS ADDS THE BENEFICIARY AND TRANSFERS THE AMOUNT.

UPON TRANSFER, SHE CALLS HER SON ON HIS NUMBER AND ASKS HIM IF THE AMOUNT IS REFLECTING IN HIS ACCOUNT.

HER SON, SHAFIQ IS SURPRISED AS HE HAD NOT CALLED HIS MOTHER AT ALL.

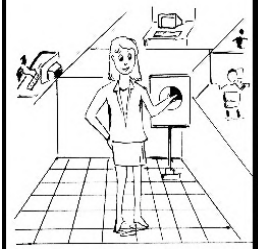
SHABANA REALISED THAT SHE HAD BECOME A VICTIM OF CALL SPOOFING AND ENDED UP TRANSFERRING MONEY TO A SCAMSTER.



USING CERTAIN APPS, ANY NUMBER CAN BE FAKED FOR CALLS AND SMS. SCAMSTERS USE THIS TECHNIQUE TO TRICK PEOPLE. BE CAREFUL

RANSOMWARE

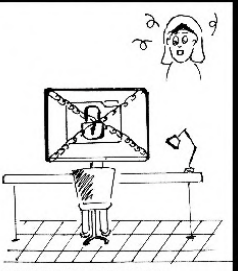
Ransomware is a form of malware that encrypts a victim's files. The attacker then demands a ransom from the victim to restore access to the data upon payment. Users are shown instructions as to how to pay a fee to get the decryption key. The costs can range from a few hundred dollars to thousands, payable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



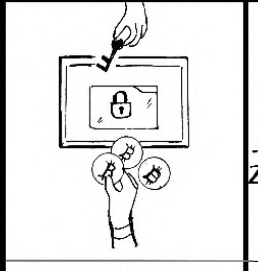
ALISHA IS AN ENTREPRENEUR. HER COMPANY HAS 50 EMPLOYEES AND 60 SYSTEMS.

ONE DAY, SHE RECEIVES AN EMAIL FROM HER VENDOR HAVING AN ATTACHMENT.

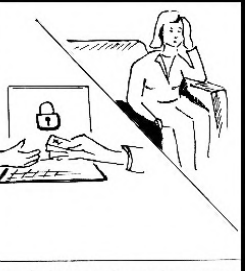
ALISHA DOWNLOADS THE ATTACHMENT. HER ANTIVIRUS WAS NOT UPDATED, SO NO ALERTS.



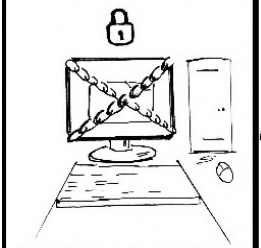
UPON OPENING THE FILE, HER SYSTEM GETS LOCKED AND ALL FILES ARE ENCRYPTED. UNABLE TO ACCESS.



AN ALTER MESSAGE ON SCREEN DEMANDS RS. 1LAKH TO BE PAID IN BITCOIN TO UNLOCK THE SCREEN.



ALISHA MAKES THE PAYMENT TO THE BITCOIN WALLET ADDRESS MENTIONED.



THE HACKER DOES NOT SEND THE PRIVATE KEY. THE FILES REMAIN ENCRYPTED AND INACCESSIBLE.

HER MANAGER QUIPS THAT THE EMAIL SHE RECEIVED WAS A PHISHING EMAIL WITH RANSOMEWARE

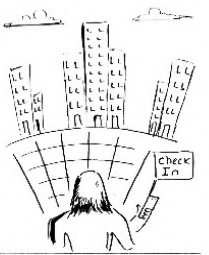
ALISHA REGRETS FOR NOT DELETING THE EMAIL AND FOR NOT UPDATING HER ANTIVIRUS SOFTWARE AND OPERATING SYSTEM.
UPDATE ANTIVIRUS ALWAYS

CYBER STALKING

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

JUVERIYA IS AN NRI, COMPLETED HER SCHOOLING FROM THE US AND IS NOW IN INDIA TO PURSUE HER ENGINEERING. SHE LIVES LIFE TO THE FULLEST

WHATEVER SHE DID, SHE WOULD UPLOAD ON SOCIAL MEDIA. OH YES! SHE HAD 10K PLUS FOLLOWERS

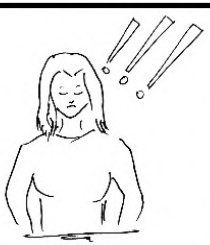


SHE USED THE CHECK-IN FEATURE TO UPDATE HER WHEREABOUTS. HER LIFE HAD MINIMUM PRIVACY

ONE DAY SHE DECIDES TO GO TO GOA ON SOLO TRIP. SHE UPDATES HER PLANS ON HER WALL WITH ITINERARY.

KIRAN, A STALKER USED TO KEEP TRACK OF ALL HER DETAILS. HE WAS A HABITUAL OFFENDER AND WAS OUT ON BAIL RECENTLY.

HE TAKES A BUS TO GOA AND TEXTS JUVERIYA FROM HIS HOTEL ROOM AND EXPRESSES HIS DESIRE TO MEET HER.



AFTER CHECKING OUT HIS PROFILE, JUVERIYA BLOCKS HIM, UNAWARE ABOUT WHAT FATE HAD PLANNED FOR HER SHORTLY.

AS KIRAN HAD HER ITINERARY, HE FOLLOWS HER TO THE BEACH AND MOLESTS HER WHEN THERE WAS NO ONE AROUND. KIRAN ESCAPES.

JUVERIYA IS FEELING TERRIBLE AND REGRETS FOR UPLOADS, UPDATES AND POSTS ON SOCIAL MEDIA. YOU TAKE CARE

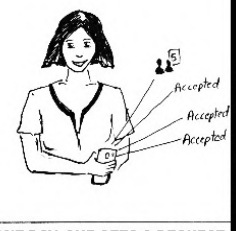
PICTURE MORPHING

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

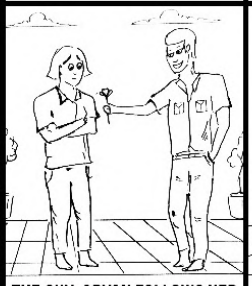
AISHWARYA IS A HAPPY GIRL. 18 YEARS OLD, LIVING IN MUMBAI

SHE ALWAYS CLICKED PHOTOS AND UPLOADED ON INSTA. ALSO, WAS CRAZY ABOUT TIKTOK

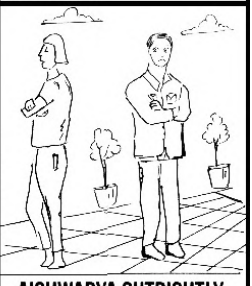
SHE USED TO GET THOUSAND LIKES AND HUNDRED COMMENTS FOR EVERY PIC POSTED.



ONE DAY, SHE GETS A REQUEST FROM A RANDOM GUY. SHE ACCEPTS.

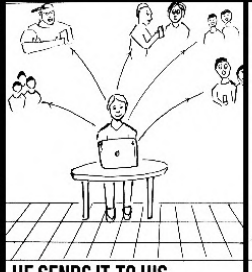


THE GUY, ARYAN FOLLOWS HER WHILE SHE IS ON HER WAY TO COLLEGE AND PROPOSES TO HER



AISHWARYA OUTRIGHTLY REJECTS HIS PROPOSAL AND SHOUTS AT HIM

ARYAN GOES BACK HOME, DOWNLOADS HER PICTURES, AND MORPHED HER WITH NAKED BODY



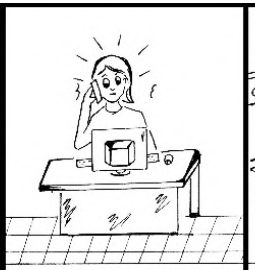
HE SENDS IT TO HIS FRIENDS AND UPLOADS ON RANDOM WEBSITES WITH HER PHONE NUMBER

AISHWARYA IS DEPRESSED AND REGRETS FOR UPLOADING HER CLEAR PHOTOS ON SOCIAL MEDIA AND ACCEPTING RANDOM REQUESTS. YOU BE VIGILANT

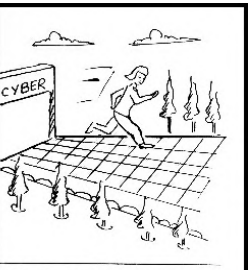
PROFILE HACKING

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

TANUJA LOVES GOING TO THE CYBER TO SURF THE WEB.



ONE DAY, SHE WAS SURFING HER FB AND HER GMAIL WAS OPEN IN THE OTHER WINDOW



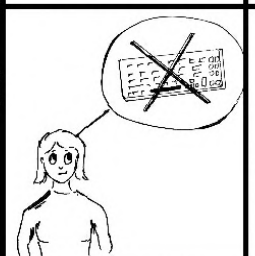
SHE GETS SOS CALL FROM HOME THAT HER GRANDFATHER IS ADMITTED IN KCM HOSPITAL

TANUJA RUSHES TO THE HOSPITAL. AFTER ALL, SHE LOVED HER GRANDPA VERY MUCH.

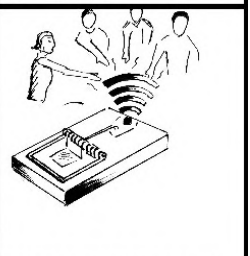
UPON REACHING THE HOSPITAL, TANUJA GETS TWO ALERTS ON HER PHONE. GMAIL AND FB PASSWORDS ARE RESET.

TANUJA REALIZES SHE HAD NOT LOGGED OUT OF THE SYSTEM. THUS HER ACCOUNTS GOT COMPROMISED.

REMEMBER TO ALWAYS LOG OUT WHILE USING PUBLIC COMPUTERS.



USE VIRTUAL KEYBOARD WHILE ENTERING PASSWORDS AND OTHER SENSITIVE INFORMATION



AVOID FREE WIFI AT RESTAURANTS, AIRPORTS, PUBLIC PLACES ETC. USE VPN WHENEVER NECESSARY.

ONLINE GAMES

Girls who are vulnerable to loneliness, low self-esteem and clinical depression can fall prey to dangerous online games that may become addictive and further harm them. Some 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.

DEVIKA IS A FIRST YEAR ENGINEERING STUDENT, HAILING FROM A REMOTE VILLAGE IN KARNATAKA.

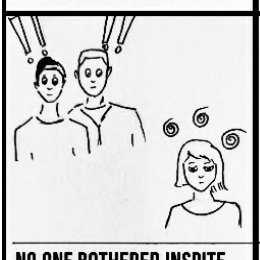
HER CLASSMATES USED TO IGNORE HER BECAUSE SHE WAS TOO SIMPLE TO GEL AMONG THE GROUP OF GIRLS. SHE HAD NO ONLINE FRIENDS EITHER.

BECAUSE OF LONELINESS, SHE ENDED UP CLICKING A LINK THAT SHE RECEIVED IN HER EMAIL, WHICH READ- THE BLUE WHALE GAME. ARE YOU READY?

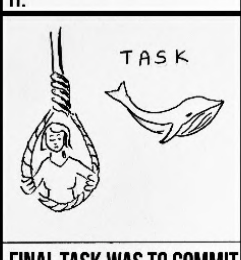
DEVIKA WAS EXCITED TO PLAY THIS GAME. IT HAD FIFTY LEVELS. EACH LEVEL HAD A TASK TO BE EXECUTED.

COMPLETING EACH TASK GAVE HER A BROWNIE POINT. SHE FELT GOOD. THE DOPAMINE RUSH GOT HER ADDICTED TO IT.

DANGEROUS TASKS LIKE TATTOOING ON BODY WITH KNIFE,GRAVEYARD WALKS WERE ASSIGNED.



NO ONE BOTHERED INSPITE OF SEEING CHANGES IN HER.



FINAL TASK WAS TO COMMIT SUICIDE BY HANGING. SHE WROTE AN APOLOGY TO HER PARENTS AND HANGED.

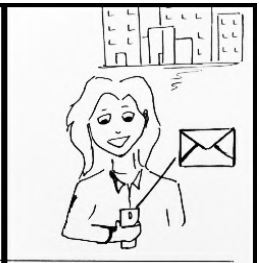
THE LETTER READ- I WISH PEOPLE LOVED ME. I WAS IGNORED. WHAT'S THE POINT IN LIVING.

JOB CALL LETTER

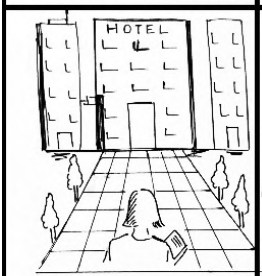
Websites offering jobs need to be checked for veracity and authenticity. Mails need to be double-checked and verified before one responds and acts on instructions provided, especially if one is asked to put in a personal appearance.

NISHITA COMPLETED HER ENGINEERING WITH FIRST CLASS. BUT SHE WAS NOT ABLE TO SECURE CAMPUS PLACEMENT

SHE USED TO ALWAYS UPLOAD HER RESUME ON NAUKRI.COM AND OTHER JOB CLASSIFIED WEBSITES, HOPING TO GET A GOOD JOB



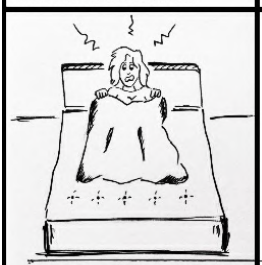
ONE DAY SHE RECEIVES A CALL LETTER FROM A REPUTED COMPANY. THE PAY PACKAGE READ 7 FIGURES.



THE INTERVIEW WAS SCHEDULED AT A 5STAR HOTEL IN THE CITY. NISHITA TOOK AN AUTO AND REACHED THE HOTEL.

SHE WAS DIRECTED TO A SUITE ROOM, WHERE SHE SAW MANY JOB ASPIRANTS DOING THEIR LAST MINUTE PREPARATIONS

IT WAS NISHITAS TURN. BEFORE THE INTERVIEW BEGAN, SHE WAS OFFERED A DRINK BY THE BUTLER. SHORTLY, SHE FELT DIZZY.



NISHITA DOES NOT REMEMBER ANYTHING THAT HAPPENED AFTER SHE DRANK. SHE WAS ON BED WITHOUT CLOTHES. SHE WAS EXPLOITED.

SHE LATER REALIZED THAT, IT WAS A PHISHING MAIL WHICH SHE RECEIVED. SHE DID NOT VERIFY THE DETAILS.

LIKE NISHITA, IN THE PRETEXT OF GETTING JOBS, LAKHS OF WOMEN GET EXPLOITED AND MANY GET ROBBED OF MONEY.
YOU TAKE CARE.

DEEPFAKES

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

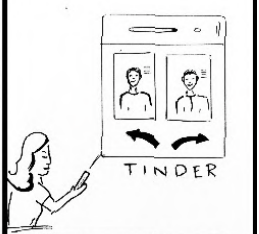

JANET IS A FINAL YEAR MBBS STUDENT. SHE AND JOHN ARE IN A RELATIONSHIP SINCE 3 YEARS.
SHE WAS A REGULAR CONTENT CREATOR ON TIKTOK AND INSTAGRAM. USED TO UPLOAD AT LEAST TWO POSTS A DAY.
JANET HAD A FIGHT WITH JOHN AND BROKE UP. HER SENIOR ARJUN GETS TO KNOW.
ARJUN TAKES THE OPPORTUNITY AND PROPOSES TO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

DATING WEBSITE

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

RASHMI IS A FIRST YEAR MBBS STUDENT. SHE WAS RECENTLY CROWNED AS MISS FRESHER..

SHE USED TO ALWAYS TALK TO HER FRIENDS ONLINE. BUT SHE WAS BORED OF TALKING TO THE SAME PEOPLE.



ONE DAY SHE REGISTERS ON TINDER AND STARTS SWIPING LEFT AND RIGHT.

SHE HAPPENS TO COME ACROSS SHAKS, A VERY GOOD LOOKING GUY, CLASSY, HAS LUXURIOUS CARS, PARTIES, TRAVELS ETC.

SHAKS WAS A SMOOTH TALKER. HE INSTANTLY IMPRESSED RASHMI AND GOT LUCKY TO TAKE HER OUT.

HE TOOK HER FOR A CANDLE LIGHT DINNER. RASHMI FEELS, HE IS THE ONE FOR HER!

AFTER A COUPLE OF DAYS, SHAKS TELLS RASHMI THAT HE URGENTLY NEEDS 2 LAKHS AS IT OFFICERS HAVE FROZEN HIS ACCOUNT. SHE SELLS HER GOLD CHAIN AND GIVES HIM THE MONEY.

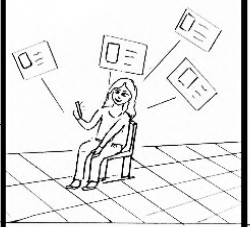
SHAKS BLOCKS HER. LATER, THROUGH ONE OF HER FRIENDS SHE GETS TO KNOW THAT SHAKS WAS A MARRIED MAN AND HE USED TO CON WOMEN LIKE THIS.

SHE REGRETS TRUSTING THIS STRANGER THRU' DATING SITE AND FOR SENDING HER PRIVATE PICS & VIDEOS. STAY ALERT

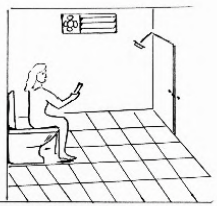
CAMERA HACKING

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

MANISHA IS THE COOLEST GIRL IN HER COLLEGE

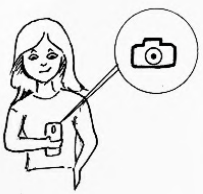


SHE USED HER PHONE TO CHECK MAILS, MANAGE SOCIAL MEDIA ACCOUNTS AND TRANSFER MONEY.



SHE USED TO CARRY HER PHONE TO THE WASHROOM ALL THE TIME.

SHE HAD NO IDEA ABOUT A FILE DOWNLOADED BY HER ON MESSENGER ONCE, WHICH WAS A TROJAN WITH MALWARE.



THE MALWARE SWITCHED ON FRONT AND BACK CAMERAS OF HER PHONE WITHOUT HER CONSENT, DISCREETLY CAPTURING VIDEOS.

UNAWARE ABOUT THE MALWARE, MANISHA KEPT HER PHONE ASIDE IN THE BATHROOM AND HAD SHOWER.

ONE DAY, HER FRIEND JOEL TELLS HER THAT, HE CAME ACROSS HER SHOWER VIDEO ON A PORN WEBSITE.

MANISHA IS SHATTERED. HER PHONE DID NOT HAVE AN ANTIVIRUS INSTALLED, WHICH PROTECTS THE PHONE.

SHE ALSO REGRETTED FOR NOT HAVING A MOBILE FLIP COVER AND CAMERA COVER. YOU TAKE CARE

SOCIAL TROLLING

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

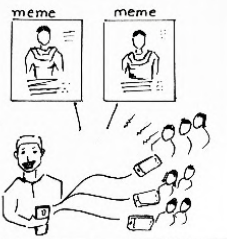
SHRUTHI IS A SIMPLE GIRL, HAILING FROM A MIDDLE CLASS FAMILY. SHE BELIEVES IN MORALS AND ETHICS.

THE STUDENTS IN COLLEGE WHERE SHE STUDIED WERE MOSTLY CAREFREE TYPES AND FASHION FREAKS

EVERY DAY THEY WOULD PULL HER LEGS, CALL HER BY NAMES AND MAKE HER FEEL MISERABLE.

ROHAN, THE MOST FAMOUS BOY IN THE COLLEGE CALLED SHRUTHI A GAWAR AND TOLD HER TO GO BACK TO HER VILLAGE.

SHRUTHI DECIDED TO PUT A FULL STOP TO THIS MENACE. SHE GAINS COURAGE AND ASKS HIM TO GET LOST AND MIND HIS BUSINESS.



IRRITATED ROHAN GOES BACK HOME AND EDITS ADULTS JOKES WITH SHRUTHI'S NAME AND FORWARDS IT TO HIS FRIENDS.

ALSO MAKES A TROLL PAGE OF SHRUTHI, UPLOADS MEMES AND FUNNY VIDEOS OF HER

SHRUTHI BECOMES A LAUGHING STOCK AND NOW WISHES TO DISCONTINUE HER STUDIES.

SHRUTHI LATER REALIZES SHE SHOULD HAVE INFORMED THE AUTHORITIES IN COLLEGE AND LODGED A COMPLAINT IN THE WOMENS POLICE STATION

PONZI SCHEME

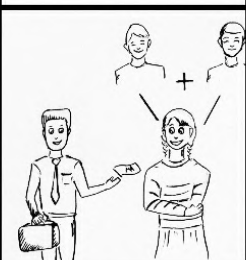
A Ponzi scheme is a fraudulent investing scam promising high rates of return with little risk to investors. Victims of such schemes are vulnerable to hackers with malicious intent and fall prey to their promises of recovery of their losses.

NEHA IS A GIRL FROM LOWER MIDDLE CLASS FAMILY.

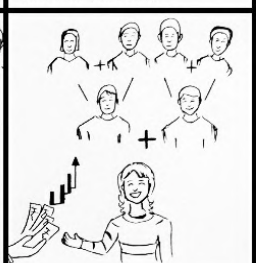
SHE ALWAYS WANTED TO HAVE ALL THE LUXURIES IN LIFE.

ONE DAY SHE COMES ACROSS A WEBSITE THAT PROMISES BMW CARS, FOREIGN TOURS FOR ONLY RS.9999/-

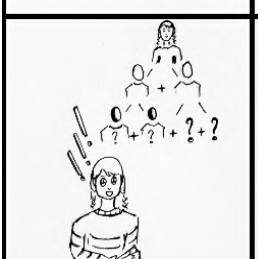
SHE ENROLLS FOR A COUNSELING SESSION. GETS AN INVITE TO A 5 STAR HOTEL.



THEY TELL HER TO ENROLL AND INVITE 2 PEOPLE TO JOIN, LEFT AND RIGHT BRANCH OF TREE. SHE GETS COMMISSION OF RS.500



THE COMMISSION INCREASES AS THOSE WHOM SHE HAD ENROLLED, ALSO INDUCTS NEW PEOPLE



INITIALLY SHE RECEIVED SOME COMMISSION. WHEN ENROLLMENTS REDUCED, SHE INVESTS MORE FOR SELF ENROLLMENTS

ONE DAY THE WEBSITE IS NON FUNCTIONAL AND NONE OF THE HELPLINE NUMBERS ARE WORKING. MEDIA REPORTS THE PROMOTERS ARE ABSCONDING.

ENROLLED MEMBERS ARE NOW DEMANDING MONEY. SHE HAS ALSO LOST BIG TIME.
DO NOT FALL PREY.

FAKE MATRIMONIAL PROFILE

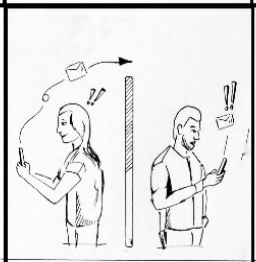
A fraudster may have registered on a matrimonial site with a fake profile. The details and profile pic may not be his. He can dupe a naive girl who falls for his practised charm and believes in the authenticity of supportive material that he provides to back up his identity.

FATHIMA A SPINSTER WORKS AS AN ENGINEER. HER PARENTS ARE ON THE LOOKOUT FOR A GROOM

SHE HAD REGISTERED ON MANY MATRIMONIAL SITES, HOPING TO FIND A GROOM.

SHE GETS AN INBOX MESSAGE FROM A 30 YEAR OLD MALE, EXPRESSING INTEREST

HER SEARCH REVEALS HIM AS AN INDIAN, IRS OFFICER WORKING IN BANGALORE AND HAILING FROM A WEALTHY FAMILY



THEY START EXCHANGING TEXTS, THEN CALL EACH OTHER. HE WAS A CHARMER AND SHE FALLS FOR HIM

TO MAKE HER BELIEVE, HE SHOWED HER HIS ID, LOGIN DETAILS ON THE WEBSITE, PHOTOS OF HIS FAMILY, FRIENDS ETC.,

ONE DAY HE TOLD HER, HE HAS GOT SUSPENDED FROM JOB BECAUSE SOME POLITICIANS NEVER LIKED HIM. HE WANTED MONEY TO GET BACK HIS JOB.

HE HANDS OVER HIS PASSPORT, ID AND OTHER DOCUMENTS FOR SAFE KEEPING. SHE TRANSFERS 5LAKHS TO HIS ACCOUNT, TO HELP HIM DURING HIS DIFFICULT TIMES.

A WEEK LATER, SHE READS IN THE NEWSPAPER, HE WAS ARRESTED FOR CHEATING MANY WOMEN THROUGH MATRIMONIAL WEBSITE. YOU BE SURE.

MOBILE REPAIR SHOP

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

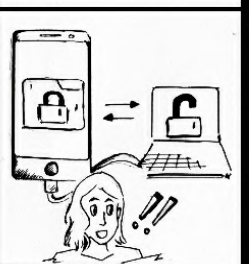
TANVI WAS A SELFIE ADDICT. SHE HAD THE LATEST FLAGSHIP ANDROID PHONE WITH EPIC CLARITY CAMERA.

SHE HAD CLICKED MANY CANDID PICTURES, SOME PRIVATE PHOTOS WITH HER BOY FRIEND AND FEW WITH ROOMMATES IN THE HOSTEL

ONE DAY SHE ACCIDENTLY DROPS THE PHONE AND SHE IS UNABLE TO SWITCH IT ON, INSPITE OF TRYING EVERYTHING POSSIBLE.

SHE VISITS AN UNAUTHORIZED MOBILE SHOP AND ASKS HIM TO REPAIR. SHE ALSO TELLS HIM NOT TO CHECK HER DATA, WHICH HE OBLIGES.

SHE THOUGHT, HER PHOTOS AND OTHER DATA ARE SAFE AS SHE HAD LOCKED THEM WITH A PATTERN CODE.



HARDLY DID SHE KNOW THAT PATTERN/PASSCODES CAN BE EASILY BROKEN WITH HACKING SOFTWARES.

THE SHOPKEEPER AFTER REPAIRING THE PHONE, ACCESSES HER GALLERY AND KEEPS A COPY OF THE PHOTOS.

AFTER A FEW DAYS, SHE GETS A CALL FROM ONE OF HER RELATIVE MENTIONING THAT HER PHOTOS ARE VIRAL AND GETTING SHARED IN MANY GROUPS.

TANVI REGRETS FOR CLICKING SUCH PHOTOS AND KEEPING THEM IN HER PHONE. SHE IS UNABLE TO FACE HER FAMILY AND SOCIETY NOW. YOU BE CAREFUL.

FAKE REVIEWS

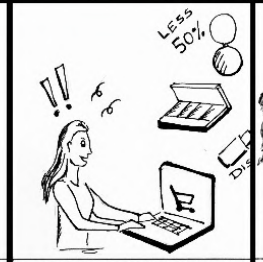
A website may dupe customers by putting up fake reviews of products. They plant glowing reviews and pay for perfect ratings that attract customers, especially backed by discounted prices. These products from dubious sites may cause untold harm if used.

NIKITA IS AN UNDERGRADUATE STUDENT AND ALSO AN UPCOMING MODEL.

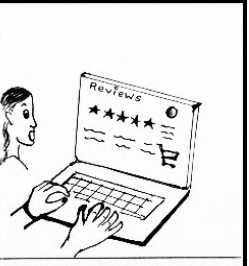
SHE USED TO ATTEND A LOT OF PAGE 3 PARTIES TO MAKE SURE SHE WAS IN THE LIMELIGHT.

THE COSMETICS AND PERFUMES THAT SHE WORE WERE VERY EXPENSIVE, WHICH LASTED LONG TILL THE END OF PARTY.

AS SHE STARTED ATTENDING MORE PARTIES, THE COSMETICS GOT OVER SOON. SHE STARTS EXPLORING OPTIONS TO BUY THEM ONLINE FOR CHEAP.



SHE COMES ACROSS A WEBSITE WHICH OFFERS THE SAME PRODUCTS FOR 50% LESS.



THOUGH IT LOOKS UNBELIEVABLE, SHE CHECKS THE VERIFIED REVIEWS. IT WAS 4 STARS ON AVERAGE.

SHE DECIDES TO BUY THE PERFUME AND COSMETICS. PAYS ONLINE. GETS AN SMS FOR ORDER CONFIRMATION.

SHE GETS THE PRODUCT HOME DELIVERED. UPON USING THEM, SHE GETS RASHES ON SKIN, WHICH WERE SO ACUTE, SHE HAD TO GET ADMITTED IN HOSPITAL

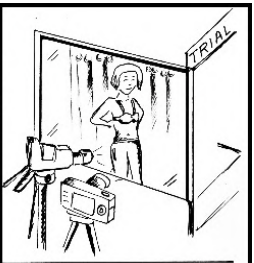
NIKITA GOT CARRIED AWAY BY FAKE REVIEWS. MANY WEBSITES ARE KNOWN TO PLANT GLOWING REVIEWS. YOU TAKE CARE OF WEBSITE & REVIEWS, ELSE WOULD PAY FOR THE MISTAKE.

FAKE PROFILE WITH SEXTORTION

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

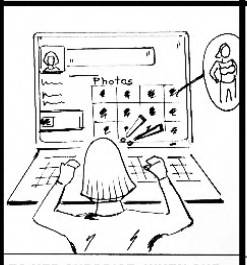
JHANVI WANTED TO BUY CLOTHES FOR HER BIRTHDAY. SHE VISITS A GARMENT SHOP WITH HER FRIEND.

SHE IS IN A DILEMMA AS TO WHICH ONE TO FINALIZE. SO SHE TAKES THEM ALL TO THE CHANGING ROOM.



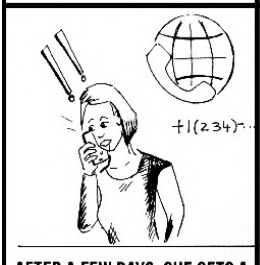
HARDLY DID SHE KNOW THAT, THE ROOM HAD 2 WAY MIRRORS WITH CAMERA FITTED ON THE OTHER SIDE.

A FEW DAYS LATER, HER FRIENDS CALL HER UP TO FIND OUT WHY SHE HAD OPENED ANOTHER FB ACCOUNT.

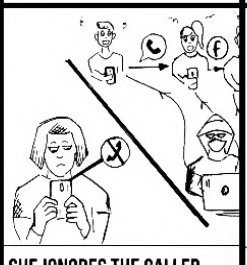


TO HER SURPRISE, WHEN SHE CHECKS THAT PROFILE, IT HAS HER REGULAR DP BUT INSIDE THE GALLERY, ALL HER PRIVATE PHOTOS.

SHE REPORTS THE PROFILE ONLINE AND IS NOT READY TO COMPLAIN TO THE POLICE. SHE WAITS, BUT ALL IN VAIN.



AFTER A FEW DAYS, SHE GETS A CALL FROM AN INTERNATIONAL NUMBER, ASKING HER TO MEET HIM OR FACE CONSEQUENCES.



SHE IGNORES THE CALLER, HE LATER STARTS SENDING HER PHOTOS TO HER FRIENDS AND FAMILY VIA THE FAKE ACCOUNT.

JHANVI NOW DECIDES TO REPORT TO THE POLICE. BUT THE DAMAGE HAS ALREADY BEEN DONE.
YOU TAKE CARE

CYBER VULTURES

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

MRS LOBO IS A WIDOW HAILING FROM A MIDDLE CLASS FAMILY. SHE HAS 2 DAUGHTERS.

ONE OF HER RELATIVES CONVINCED HER TO INVEST ALL HER SAVINGS AMOUNT INTO A PONZI SCHEME FOR HIGHER RETURNS.

SHE ALSO ENDED UP INVESTING HER HUSBAND'S INSURANCE AMOUNT INTO THE SCHEME.

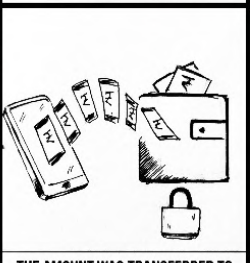
ONE DAY SHE REALIZES THE COMPANY DIRECTORS HAVE FLED AND SHE BELIEVES SHE HAS LOST ALL HER MONEY.

A HACKER MANAGES TO GET THE DATABASE OF ALL THOSE WHO HAD INVESTED BY GAINING ACCESS TO THE SERVER.

HE CALLS INVESTORS INDIVIDUALLY, ASSURES THEM THEY WIL GET THE AMOUNT BACK IF THEY GIVE HIM 30% OF THE AMOUNT RECEIVED.

MRS LOBO AGREES FOR THE OFFER. HE REQUESTS FOR UPI CODE, ATM AND ACCOUNT NUMBER.

MRS LOBO WAS SHOCKED TO SEE THE ONLY AMOUNT SHE HAD, RS 2 LAKHS WAS DEBITED BY THE HACKER, IN NO TIME.



THE AMOUNT WAS TRANSFERRED TO A SHADY EWALLET COMPANY, WHICH REFUSES TO COMPLY WITH THE INVESTIGATION AGENCIES. BE SURE OF RANDOM CALLERS.

APP TRAPS

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

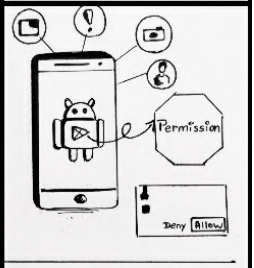
VIDYA AND RONAK WERE DATING EACH OTHER FOR 5 YEARS. THEY HAD A STEADY RELATIONSHIP.

THEY DECIDE TO VISIT MANALI OVER THE WEEKEND. THEY PACK THEIR BAGS AND RUSH TO THE TRAIN STATION.

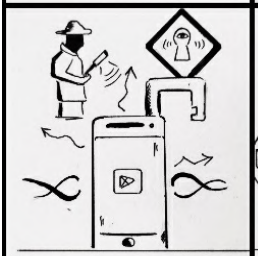
AFTER SPENDING 3 AWESOME DAYS IN MANALI, THEY RETURN BACK HOME WITH FOND MEMORIES.

VIDYA USED AN APP THAT TRACKED HER MONTHLY CYCLE AND OTHER HEALTH ISSUES.

THIS MONTH, THERE WAS IRREGULARITY. SHE WAS AFRAID IF SHE HAD CONCEIVED. SHE CHECKS FOR OTHER FEATURES IN THE APP TO MAKE SURE SHE HADN'T.

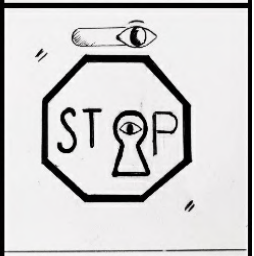


THE APP LIKE MANY OTHERS IN OUR PHONE, HAD TAKEN HER CONSENT TO ACCESS THE GPS, CAMERA, STORAGE, CONTACTS AND OTHER FEATURES.



THEY NOW START SELLING THE DATA TO CONTRACEPTIVE COMPANIES. THEY GET TO KNOW ABOUT IT. HER PRIVACY IS AT STAKE.

THE APP ALSO MAKES HER BUY CERTAIN KITS TO TEST FOR A PREMIUM PRICE, TAKING ADVANTAGE OF HER SITUATION.



BY GIVING PERMISSION ONCE, THE APP CAN RECORD VIDEOS, CLICK PHOTOS, STORE MIC INPUTS AND ACCESS STORAGE MEDIA, UPLOAD AND DOWNLOAD DATA COVERTLY. BE CAREFUL.

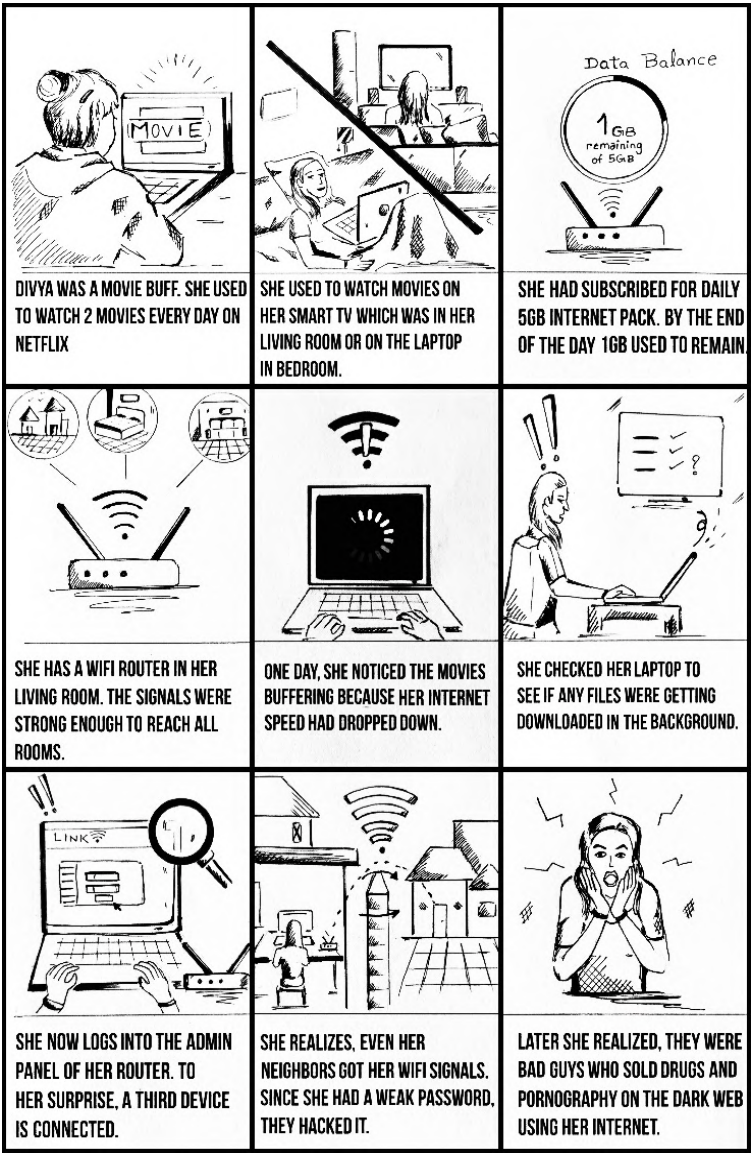
JUICE JACKING

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


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

WIFI HACKING

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



DIVYA WAS A MOVIE BUFF. SHE USED TO WATCH 2 MOVIES EVERY DAY ON NETFLIX

SHE USED TO WATCH MOVIES ON HER SMART TV WHICH WAS IN HER LIVING ROOM OR ON THE LAPTOP IN BEDROOM.

SHE HAD SUBSCRIBED FOR DAILY 5GB INTERNET PACK. BY THE END OF THE DAY 1GB USED TO REMAIN.

SHE HAS A WIFI ROUTER IN HER LIVING ROOM. THE SIGNALS WERE STRONG ENOUGH TO REACH ALL ROOMS.

ONE DAY, SHE NOTICED THE MOVIES BUFFERING BECAUSE HER INTERNET SPEED HAD DROPPED DOWN.

SHE CHECKED HER LAPTOP TO SEE IF ANY FILES WERE GETTING DOWNLOADED IN THE BACKGROUND.

SHE NOW LOGS INTO THE ADMIN PANEL OF HER ROUTER. TO HER SURPRISE, A THIRD DEVICE IS CONNECTED.

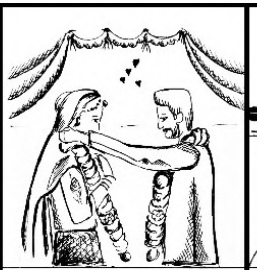
SHE REALIZES, EVEN HER NEIGHBORS GOT HER WIFI SIGNALS. SINCE SHE HAD A WEAK PASSWORD, THEY HACKED IT.

LATER SHE REALIZED, THEY WERE BAD GUYS WHO SOLD DRUGS AND PORNOGRAPHY ON THE DARK WEB USING HER INTERNET.

ONLINE RADICALIZATION

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

RESHMA WAS A SIMPLE GIRL. SHE HAD COMPLETED HER ENGINEERING.



HER PARENTS DID NOT WANT HER TO WORK AFTER HER STUDIES. THEY GOT HER MARRIED TO AN ENGINEER IN AFRICA

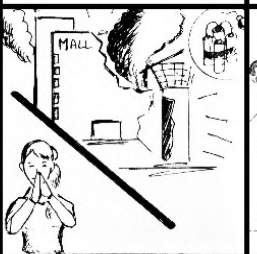
HER HUSBAND TOOK HER ALONG WITH HIM TO AFRICA. BUT SHE DID NOT GET A JOB THERE.

SHE WAS AT HOME ALL THE TIME WITH NO WHERE TO GO AROUND. SO SHE SPENT MOST OF HER TIME ONLINE.

ONCE SHE CAME ACROSS A POST. UPON CLICKING, SHE ENTERED INTO A WEBSITE WITH WEIRD IMAGES AND POSTS.

SHE RECEIVED EMAILS FROM THAT WEBSITE AND LATER STARTED REGULAR CONVERSATIONS WITH THEIR LEADER.

HE WAS SUCCESSFUL IN PLANTING THEIR IDEOLOGY INTO HER INNOCENT MIND. ALSO, DELIVERED THE WEAPONS TO HER HOME.



AFTER RECITING THE PRAYERS, THE NEXT DAY SHE EXPLODES HERSELF IN A MALL, IN SEEK OF HEAVEN.

HER HUSBAND AND FAMILY WERE SHELL SHOCKED. THEY WERE CLUELESS ABOUT THIS COVERT ONLINE RADICALISATION

BONUS TIPS

TIPS TO STAY CYBER SAFE

1. MOBILE RECHARGE:

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

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

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.

Debit Card Cloning: Cloning may blow up your Earning!

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.

Keylogger: Keylogger may empty your Coffer!

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.

SMS spoofing: SMS are Spoofed by Cyber Crooks!

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.

Call spoofing: Call Spoofing, Caller is Confusing!

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.

Ransomware: Sensitize your Hardware and Software to avoid Ransomware!

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.

Cyber Stalking: Cyber Stalking Means Someone is Watching!

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.

Picture Morphing: Morphing is used for Defaming!

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.

Profile Hacking: Profile Hacking means Security is Lacking!

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.

Online Games: 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).

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.

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

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.

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

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!

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

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.

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

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!

Social trolling: Are you Trolling, the law may be soon following!

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.

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

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.

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

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.

Mobile repair shop: If caution not adhered at such Shops, get ready to take big Hops!

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.

Fake reviews: Fake Reviews may give you wrong Overviews!

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.

Fake profiles with sextortion: A Fake Ex may levy a unforgiving Tax!

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.

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

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!

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

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.

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

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!

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

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.

Online Radicalization: Don't get Radicalized, rather be Rationalized!

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

He is the Founder of Indian Cyber Lawyers (indiancyberlawyers.in) 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@indiancyberlawyers.in

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.

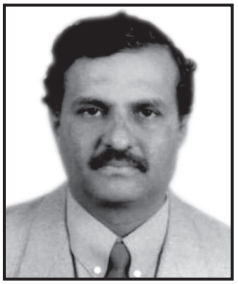
OFFENCES AND RELEVANT PENAL SECTIONS

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



HS Chandramouli
State Public Prosecutor
Government of Karnataka

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

If you are not careful, you can very easily end up having your identity stolen, credit ruined and your files gone forever.

Therefore, it is quintessential to follow the best practices to stay Cyber Safe.

I am glad that #CyberSafeGirl Version 2.0 has come out very well and it would definitely help millions of girls browsing the internet. The 25 info toons are very simple and easy to understand. I am sure, it would benefit anyone from 9 to 99 years of age!

To conclude, the 2 topics- Bonus Tips that highlight the precautionary measures and the various Sections of the IT Act, other relevant acts is a must read.

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

Warm Regards,

HS Chandramouli

Beti Bachao Cyber Crime Se...

www.cybersafegirl.com

Don't be a victim of cyber crime.

Be a #CyberSafeGirl