



CYBER SAFE GIRL

Beti ko Bachao, Cyber Crime Se

15 eye-opening sketches
to ensure online safety of girls



Dr. Ananth Prabhu G, is an Author, Software Engineer, Motivational Speaker and Cyber Security Expert. Currently serving as the Advisor for Vikas group of institutions, Professor in Sahyadri College of Engineering and Management. He is also the trainer at Karnataka Police Academy, Mysore and Police Training School, Gulbarga for Cyber Law, Cyber Terrorism and Security.



Mr. Vivek Shetty, is an entrepreneur and social activist.

CYBER SAFE
GIRL

Beti ko Bachao, Cyber Crime Se

• 15 eye-opening sketches •
• to ensure online safety of girls •

First Published in India in 2019

Copyright (C) Campus Interview Training Solutions 2019

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

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

Designed and printed by
Tarjani Communications Pvt. Ltd, Mangaluru

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

Credits



Sanjay Sahay, IPS



Dr. Murugan, IPS



Arun Chakravarthy, IPS



Roopa D, IPS



Dr. Vedamurthi CB, IPS



Uma Prashanth, KSPS



Reena Suvarna, KSPS



Yogesh Kumar, PI



Savithra Tej, PI



Prashanth Jhala
Cyber Law Consultant &
Cyber Crime Investigator



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



Naga VRK Basava
SEO Guru

Special Thanks to



Krishna J Palemar



Manjunath Bhandary



J Koragappa



B Poornajith Rai



Shafeeq Kallangadi



Waseem Shan
Web Designer



Artist
Anudeep Karkera





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 and Vivek Shetty for coming out with this wonderful booklet depicting 15 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!**

With respectful regards,

Hanumantharaya IPS
DCP L & O
Mangalore City Police



Index

MOBILE RECHARGE SHOP

DEBIT CARD CLONING

KEYLOGGER

SMS SPOOFING

CALL SPOOFING

RANSOMWARE

CYBER STALKING

PICTURE MORPHING

PROFILE HACKING

ONLINE GAMES

JOB CALL LETTER

DEEPPAKES

DATING WEBSITE

CAMERA HACKING

SOCIAL TROLLING

MOBILE RECHARGE SHOP

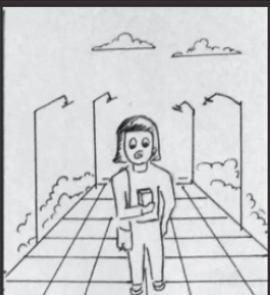
A Mobile Recharge Shop is a place where scamsters can gain access to your cellphone number because you have provided it to the recharge vendor. This number is then misused to call or text you and exploit your ignorance or even emotionally manipulate you.



MEENA GOES TO MOBILE SHOP TO RECHARGE HER PHONE WITH 50 RS CREDIT



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.



SHE GOES TO THE SHOP TO INFORM. WHEN SHE SAYS SHE HAS NO MONEY TO PAY RS 450, HE SAYS ITS OK, LET'S SEE NEXT TIME.



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



AKHIL CONVINCES HER ONE DAY AND TAKES HER TO THE LODGE. AFTER A DAY, HE BREAKS UP WITH HER.



HE BLACKMAILS HER TELLING IF SHE REVEALS TO ANYONE, HE WOULD MAKE HER PICTURES AND VIDEO VIRAL. MEENA IS DEPRESSED

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.



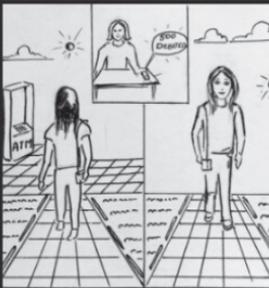
MEENA'S BOYFRIEND ARJUN IS A DRUG ADDICT. HE ALWAYS ASKS HER FOR MONEY.



MEENA HOPED THAT ONE DAY ARJUN WOULD CHANGE. BUT HE WOULD TALK ABOUT BREAKING UP AND BORROWING MONEY.



MEENA ASKS REENA FOR ₹500 . REENA GIVES HER ATM AND PIN.



MEENA COMES BACK AFTER FIFTEEN MINS. ₹ 500 DEBITED MESSAGE COMES IN REENAS PHONE



AFTER A WEEK, ₹ 5000 DEBITED ALERT COMES IN REENAS PHONE. REENA IS SHOCKED.



ON THE DAY MEENA HAD BORROWED ATM, ARJUN WAS WAITING OUTSIDE. HE TOOK THE ATM CARD



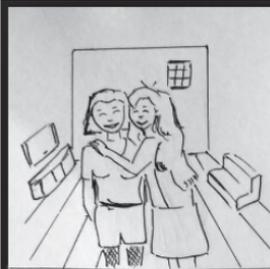
WITH A SKIMMING DEVICE HE REPLICATED THE CARD AND AFTER A WEEK WITHDREW MONEY FROM ATM AS HE HAD THE PIN



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 in 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



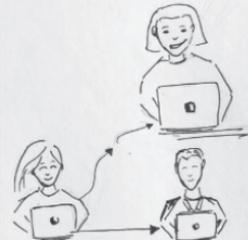
WITHOUT WASTING ANY TIME, POOJA PROPOSES VIVEK AND HE ACCEPTS. THEY START DATING EACH OTHER.



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



ONE DAY, ANUSHA LOGS ON TO POOJA'S LAPTOP AND INSTALLS KEYLOGGER PROGRAM, A SPYWARE WHICH WOULD RECORD AND MAIL A COPY OF ALL THE ACTIVITIES.



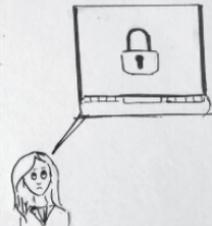
POOJA IS UNAWARE THAT HER PASSWORDS, PHOTOS SHARED, PRIVATE CHATS, EMAILS AND BROWSING HISTORY IS NOW AVAILABLE TO ANUSHA.



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

Shopping Online has to be done keeping guidelines in mind, or else one can become a victim of phishing from fake websites and message spoofing from unscrupulous elements.



CALL SPOOFING

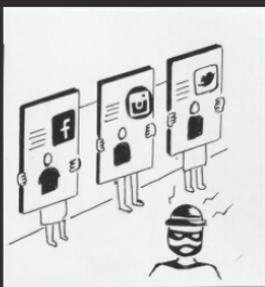
Call spoofing happens through apps that enable a person with criminal intent to change one's number and voice to impersonate another to defraud the receiver.



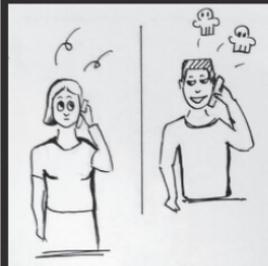
SHABANA IS A WIDOW. SHE LIVES ALONE IN HER INDEPENDENT HOUSE.



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 SHE COULD SEE SOME MUTUAL FRIENDS.



ONE DAY, SHE GETS A CALL FROM HER SON, WHEREIN HE SAYS, URGENTLY TRANSFER 1 LAKH TO HIS FRIENDS ACC, AS HIS ACC IS BLOCKED. HE ALSO SENDS THE ACC DETAILS.



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 REALIZED 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.

RANSOMWARE

Ransomware is a type of malicious software that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. It gains access to data through being downloaded as an attachment in a mail.



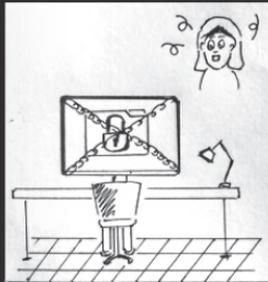
ALISHA IS AN ENTREPRENEUR. HER COMPANY HAS 50 EMPLOYEES AND 60 SYSTEMS.



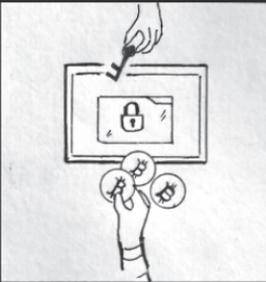
ONE DAY, SHE RECEIVES AN EMAIL FROM HER VENDOR HAVING AN ATTACHMENT.



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



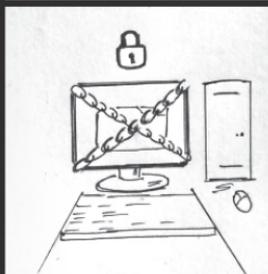
UPON OPENING THE FILE, HER SYSTEM GETS LOCKED AND ALL FILES ARE ENCRYPTED. UNABLE TO ACCESS.



AN ALERT MESSAGE ON SCREEN DEMANDS ₹ 1 LAKH TO BE PAID IN BITCOIN TO UNLOCK THE SCREEN.



ALISHA MAKES THE PAYMENT TO THE BITCOIN WALLET ADDRESS MENTIONED.



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



HER COMPANY'S MANAGER TELLS ALISHA, THE EMAIL SHE RECEIVED WAS A PHISHING EMAIL WITH RANSOMWARE



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

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.

		
<p>JUVERIYA IS AN NRI, COMPLETED HER SCHOOLING FROM THE US AND IS NOW IN INDIA TO PURSUE HER ENGINEERING. SHE LIVED HER LIFE TO THE FULLEST.</p>	<p>WHATEVER SHE DID, HAD TO GET UPLOADED ON SOCIAL MEDIA. OH YES, SHE HAD MORE THAN 10K FOLLOWERS.</p>	<p>SHE USED THE CHECK IN FEATURE ON FACEBOOK TO INFORM HER FRIENDS AND FOLLOWERS ABOUT HER WHEREABOUTS. HER LIFE HAD MINIMUM PRIVACY.</p>
		
<p>ONE DAY SHE DECIDES TO GO TO GOA ON A SOLO TRIP. SHE UPDATES HER PLANS ON HER WALL WITH ITINERARY.</p>	<p>KIRAN, A STALKER USED TO KEEP TRACK OF ALL HER DETAILS. HE WAS A HABITUAL OFFENDER AND WAS OUT ON BAIL RECENTLY.</p>	<p>HE TAKES A BUS TO GOA AND TEXTS JUVERIYA FROM HIS HOTEL ROOM AND EXPRESSES HIS DESIRE TO MEET HER.</p>
		
<p>AFTER CHECKING OUT HIS PROFILE, JUVERIYA BLOCKS HIM, UNAWARE ABOUT WHAT FATE HAD PLANNED FOR HER SHORTLY.</p>	<p>AS KIRAN HAD HER ITINERARY, HE FOLLOWS HER TO THE BEACH AND MOLESTS HER WHEN THERE WAS NO ONE AROUND. KIRAN ESCAPES.</p>	<p>JUVERIYA IS FEELING TERRIBLE AND REGRETS FOR NOT LIMITING HER IMAGES, CHECK IN DETAILS AND OTHER RELATED POSTS ON SOCIAL MEDIA.</p>

PICTURE MORPHING

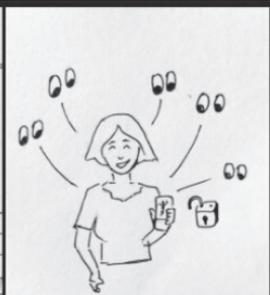
Morphing the face of a person to the body of another and publishing it to blackmail or otherwise intimidate the person is one of the ways by which people who upload photos on social networking sites can be exploited.



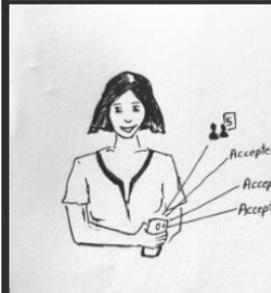
AISHWARYA IS A HAPPENING GIRL. 18 YEARS OLD, LIVING IN MUMBAI



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



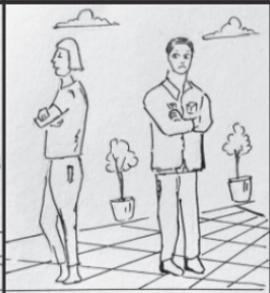
SHE USED TO GET THOUSAND LIKES AND HUNDRED COMMENTS FOR EVERY PIC POSTED.



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



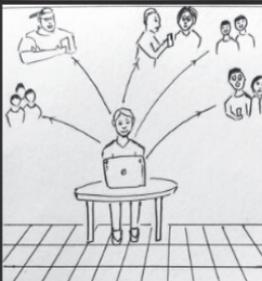
THE GUY, ARYAN FOLLOWS HER WHILE SHE IS ON HER WAY TO COLLEGE AND PROPOSES HER



AISHWARYA OUTRIGHTLY REJECTS HIS PROPOSAL AND SHOUTS AT HIM



ARYAN GOES BACK HOME, DOWNLOADS HER PICTURES, MORPHS IT WITH NAKED WOMEN.



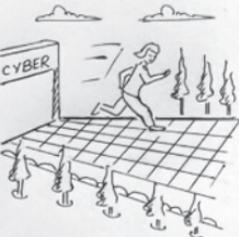
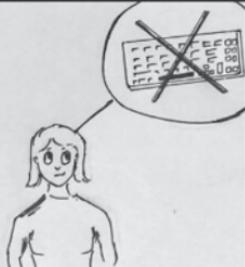
HE SENDS IT TO HIS FRIENDS AND UPLOADS ON RANDOM WEBSITES WITH HER PHONE NUMBER



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

PROFILE HACKING

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

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

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 GET INSIDE A 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?



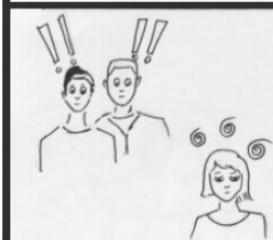
DEVIKA WAS EXCITED TO PLAY THIS GAME. IT HAD FIFTY LEVELS. EACH LEVEL HAD A TASK TO BE EXECUTED.



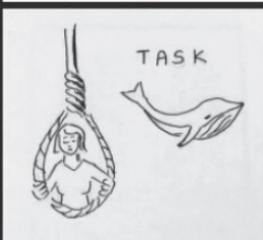
AFTER COMPLETING EACH TASK, SHE GOT APPRECIATION FROM THE ADMIN. THIS MADE HER FEEL GOOD, AS MORE AND MORE DOPAMINE WAS RELEASED INSIDE HER. SHE GOT ADDICTED.



DANGEROUS TASKS LIKE TATTOOING WHALE ON HER BODY WITH KNIFE, WALKING ON EDGE OF THE TERRACE, MIDNIGHT GRAVEYARD WALKS WERE FEW OF THE TASKS SHE COMPLETED.



HER CLASSMATES SAW A LOT OF CHANGES IN HER. SO DID HER TEACHERS. BUT NO ONE BOTHERED TO ASK HER. SHE HAD BY NOW SURRENDERED TO HER ADMIN.



THE FINAL TASK WAS TO HANG HERSELF AND COMMIT SUICIDE AT 1 AM. WITHOUT ANY REGRET OR FEAR, DEVIKA WROTE A SORRY LETTER TO HER PARENTS AND HANGED HERSELF. ONE PRECIOUS LIFE LOST.



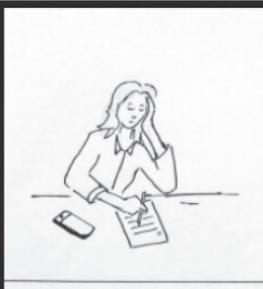
THE LETTER READ, I WISH PEOPLE CARED FOR ME, LOVED ME AND INCLUDED ME IN THEIR CIRCLES. I WAS TOTALLY IGNORED AND SECLUDED. WHAT IS THE POINT IN LIVING?

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.



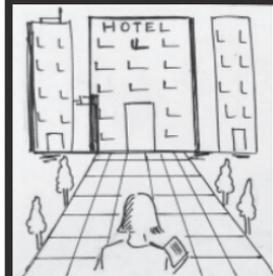
NISHITA COMPLETED HER ENGINEERING WITH FIRST CLASS. BUT SHE WAS NOT ABLE TO SECURE CAMPUS PLACEMENT



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 5 STAR HOTEL IN THE CITY. NISHITA TOOK AN AUTO AND REACHED THE HOTEL.



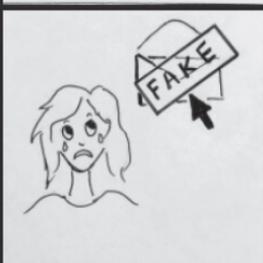
SHE WAS DIRECTED TO A SUITE ROOM, WHERE SHE SAW MANY JOB ASPIRANTS DOING THEIR LAST MINUTE PREPARATIONS



IT WAS NISHITA'S 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 THE 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

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.



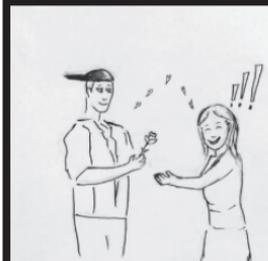
JANET IS A FINAL YEAR MBBS STUDENT. SHE IS IN A THREE YEAR LONG RELATIONSHIP WITH JOHN.



SHE WAS A REGULAR CONTENT CREATOR ON TIKTOK AND INSTAGRAM. USED TO UPLOAD ATLEAST TWO POSTS PER DAY.



BECAUSE OF SOME MISUNDERSTANDINGS, JANET STARTS AVOIDING JOHN. HER SENIOR ARJUN HAD A CRUSH ON HER FOR A LONG TIME.



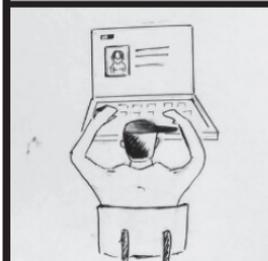
ARJUN TAKES THE OPPORTUNITY AND PROPOSES JANET. SHE AGREES. BUT LATER REGRETS FOR DUMPING JOHN.



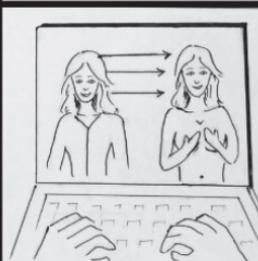
WITHIN A WEEK, SHE BREAKS UP WITH ARJUN AND GETS BACK TO JOHN AFTER SEEKING FORGIVENESS.



INFURIATED ARJUN WANTS TO TEACH JANET A LESSON FOR PLAYING WITH HIS FEELINGS.



WITH INSTAGRAM PHOTOS AND TIKTOK VIDEOS AS INPUT, ARJUN CREATES DEEPPAKES USING ARTIFICIAL INTELLIGENCE AND OTHER TOOLS



THE DEEPPAKE VIDEO CREATED SHOWED JANET INDULGING IN ADULTRY 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

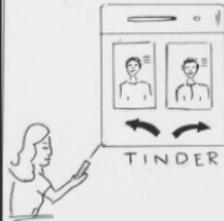
Females can be emotionally manipulated by smooth talkers on dating sites. Any private pictures or texts that they send across to probable dating companions on such sites are fair game for unscrupulous persons who can then blackmail them.



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 BEING A SMOOTH TALKER, HE IMPRESSES RASHMI WITH HIS CHARMS AND THEY START TEXTING, LATE NIGHT CALLS AND FINALLY DECIDE TO MEET THE NEXT DAY.



SHAKS TAKES HER TO THE BEST HOTEL IN TOWN FOR A CANDLE LIGHT DINNER. RASHMI KNOWS FOR SURE, THIS GUY IS HER PRINCE CHARMING.



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 ALSO REGRETS FOR TRUSTING THIS STRANGER SHE CAME ACROSS ON THE DATING SITE AND SENDING HIM PRIVATE PICTURES AND VIDEOS.

CAMERA HACKING

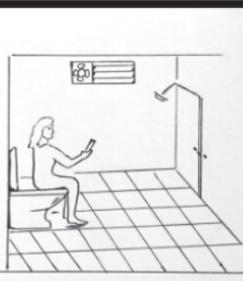
Camera hacking happens when photographs of a person are taken without consent, through malware that got downloaded with an attachment. Phones with no camera guard can be exploited for such criminal activities.



MANISHA IS THE MOST 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.



UNWARE 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 PUTTING A MOBILE FLIP CASE AND CAMERA COVER.

SOCIAL TROLLING

Social Trolling is posting inflammatory messages or visuals about a person or organisation in an online community with the express purpose of causing humiliation or nuisance to the object of trolling.



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



EVERYDAY THEY USED TO PULL SHRUTHIS LEGS, CALL HER 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 GAINED COURAGE AND TOLD HIM TO GET LOST AND MIND HIS BUSINESS.



IRRITATED ROHAN GOES BACK HOME AND EDITS ADULT JOKES WITH SHRUTHIS NAME AND FORWARDS TO HIS FRIENDS.



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



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

BONUS TIPS

Women and Cyber Crimes

1. Social Engineering: It is easy to hack into the mind of a person using a communication device or a computer system rather than hacking into the communication device or computer system that he or she is using.

Since we are wired to talk and give out information even to strangers, we fall prey to this modus operandi adopted by criminals. We get calls from Banks for cards and loans, Insurance Companies, Holiday Home providers, IT department, RBI, online market places etc but do we really check the credentials of the caller? We trust the caller and give out information that goes into our profiling for which the very call was made to us!

Preventions: It is said 'Speak Less than you Know and Have more than you Show'. Thus 'Tell Less about you and Know More about a few'.

2. Revenge Porn: Pictures and photos clicked in good times with your friends and acquaintances inadvertently may come to haunt you in future when the relationships get sour or when there is a family feud.

Preventions: Click less pictures with friends and acquaintances and follow the rule of 'Beware'.

3. Voyeurism: Privacy breach is biggest concern with advent of pin hole cameras and latest spy cams that can be hidden and are not easily detectable. Could be hidden in shopping malls, changing rooms, washrooms, hospitals and diagnostic centers, and also in offices and washrooms located in private offices.

Preventions: Though no concrete solution for this crime, but a random check on suspicious objects like window blinders, curtain and curtain rods, flower pots, murals, photo frames, bulbs, night lamps, drawers and any hanging objects on the walls may be carried out.

4. Cyber Stalking: Stranger following you on various social media platforms, chatrooms, messengers etc and causing you to fear and raise an alarm against them.

Preventions: Avoid interacting with strangers. Do not agree with them but do not be rude with them because some cases observed revealed that the stalking was done due to ego clashes.

5. Cyber Bullying: Sending tormenting post, harassing messages, threatening contents to a minor to cause mental harassment and depressive or suicidal state of mind to the recipient of such messages.

Preventions: Share those messages and posts with your Parents or teachers who are matured enough to understand the gravity of the matter and act accordingly. Do not keep on facing or enduring these troubles.

6. Photo editing Apps: These apps that you use to beautify yourself are also known to retain your original copy of the photo you have uploaded and even the copy of the edited version is saved on their servers. You can only wonder what next would they do with the copy of your photos!

Preventions: Use reputed apps that you should be downloading from secured App stores. The fake photo editors may cause you harm and edit your lifestyle if used by them with criminal intent.

7. Free Downloads: With every free downloads of music, videos, games, file sharing sites, software's, apps, e-books etc please also be ready to receive computer contaminates by way of worms, virus, trojans, malwares,

spywares, key loggers etc for FREE. Your communication device or your computer systems gets Freely compromised due to your Free downloads.

Preventions: Verify the Apps, Tools, Websites, Portals, Online Market Place, File sharing sites, Gaming sites from which you are downloading stuffs by carrying out reasonable searches using prudence.

8. 'I accept', 'I agree': It is easy to accept the terms and conditions before downloading that app or software or game or e-book or music or video that you want it on your digital devices. But before that, understand at what cost are you giving permissions!

Preventions: 'Look before you Leap' and so 'Read before you Tread' just before hitting on the 'I accept' or 'I agree' tab.

9. Password/Passphrase: Password may be a single word but a combination of more words would be a Passphrase. A Passphrase is more secured than a Password. Since you are being asked to create the Passwords, use all that is available on a keyboard to create one. Change it often. Use different passwords for different accounts.

Preventions: Passwords having a dictionary meaning are easy to crack. You are the creator of your own destiny thus create a complex password that is also easy to remember thereby safeguarding your online destiny. Never Share it with anyone Ever.

10. Webcams may reveal privacy: 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 his/her pictures and moments of privacy were clicked and uploaded online on porn sites.

Preventions: Use a masking tape on the camera of the web cam on your laptops/desktops. As for your mobile phones, keep a piece of cloth or a

handkerchief or a newspaper because they have cameras on both the sides.

11. Social Media Platforms: Do you meet and entertain a stranger in your real life? Why interact and entertain them in the virtual world too? Cheats, fraudsters, cyber criminals are waiting for you to accept their friends request. Investigations have also revealed that most of the time a request coming from a young female turns out to be a male. Anonymity is a biggest boon for cyber criminals. Also keep a tab on what you share and with whom you share with on these platforms.

Preventions: Care before you Share. Remember that Offline destiny is created by Daring but Online destiny is created by Sharing. Your Offline and Online values should match. Also remember 'Rock with your Friends but Block the ones who Offends!'

12. Use licenced operating systems: use a licenced version on your devices and not cracked versions. They enable great amount of security which is the outcome of strong research and development that is adhered to by these providers. Update the operating system with latest patches and versions.

13. Use licenced Antivirus: Just as there are Antibiotics for curing diseases in a human body, so we have Antiviruses for curing diseases in digital devices. Update the antivirus by downloading patches. Just as 'Catches wins Matches' so also 'Patches wins Glitches' (in your digital devices).

14. 'The Time is Ticking' but it shall Tick faster with disaster by wrong 'Clicking': so click less pictures and videos, click less on unknown links, click less on executable files, click less on free downloads, click less on personal details (while sharing), click less on apps that you do not

intend to use, click less on suspicious sites or unknown sites, click less on posts that offers you huge discounts, click less on images, messages and posts that are not useful to you. Ideally you should be averse on Clicking on all above.

15. Report: a cybercrime of any nature and gravity should be reported at the police station or Cyber Cell. It is always advisable to place it on records with the authorities concerned. This will not only help the police to investigate the crime that you have faced but will also help them to understand and analyse the modus operandi of the criminals and take corrective actions for preventions and detections.

Article by:

Advocate Prashant Jhala is a Cyber Lawyer from Mumbai. He is 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.

Cyber safety is an immeasurably important set of guidelines/rules/ideas to follow when interacting with people or websites on a computer, typically through the internet. When you use the internet you are making connections to strangers, as well as their servers, so it is extremely important to understand the risks of online behavior. If you are not careful you can very easily end up having your identity stolen, your credit ruined, and your files gone forever.



I am glad that Dr. Ananth Prabhu and Mr Vivek Shetty have come out with this wonderful eBook - #CyberSafeGirl which would definitely help millions of girls browsing the internet. Taking my father G H Ramachandra jis dream forward of ensuring a safe and inclusive society, I promise to extend my full support for this noble cause.

With regards and best wishes.

Jagdish R Chandra

Don't be a victim of
cyber crime.
Be a #CyberSafeGirl

Beti Ko

Bachao...
Cyber Crime Se...

