

SURE PASS

**CYBER
PATRIOT**



Indian Cyber
Institute

Supported by



Information Security
Education & Awareness

Cyber Safe Girl

4.0

40 eye-opening infotoons
to ensure online safety of netizens

Ananth Prabhu G PhD, Post Doctoral Fellow

www.cybersafegirl.com

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



Dr Ananth Prabhu G

BE, MBA, MTech, DCL, PhD, Post Doctoral Fellow is an Author, Software Engineer, Motivational Speaker and Cyber Security Expert. Currently serving as Professor and Principal Investigator of Digital Forensics and Cyber Security COE at Sahyadri College of Engineering and Management and Director of SurePass Academy. He is also the Cyber Law and Security Trainer at the Karnataka Judicial Academy and Karnataka Police Academy. Dr Prabhu was recognized by India Today magazine as one among the 30 unsung heroes of our country in 2019.

☎ +91 89515 11111

✉ info@ananthprabhu.com

🌐 www.facebook.com/educatoranant

Co-Authors



Adv. Prashanth Jhala

He is the Founder of ICL Advocates (www.icladvocates.com) a Law Firm based out in Mumbai and also a Co-Founder of Indian Cyber Institute (indiancyberinstitute.com) which runs educational and training programs in the field of Cyber Crime Investigation, Computer Forensics, Ethical hacking and Information Security, Cyber Law etc. He has been instrumental in training the law enforcement agencies across the country. He is a regular speaker and trainer at various banking forums, the Defence Forces and workshops/events/seminars organised by Information and Technology stake holders.

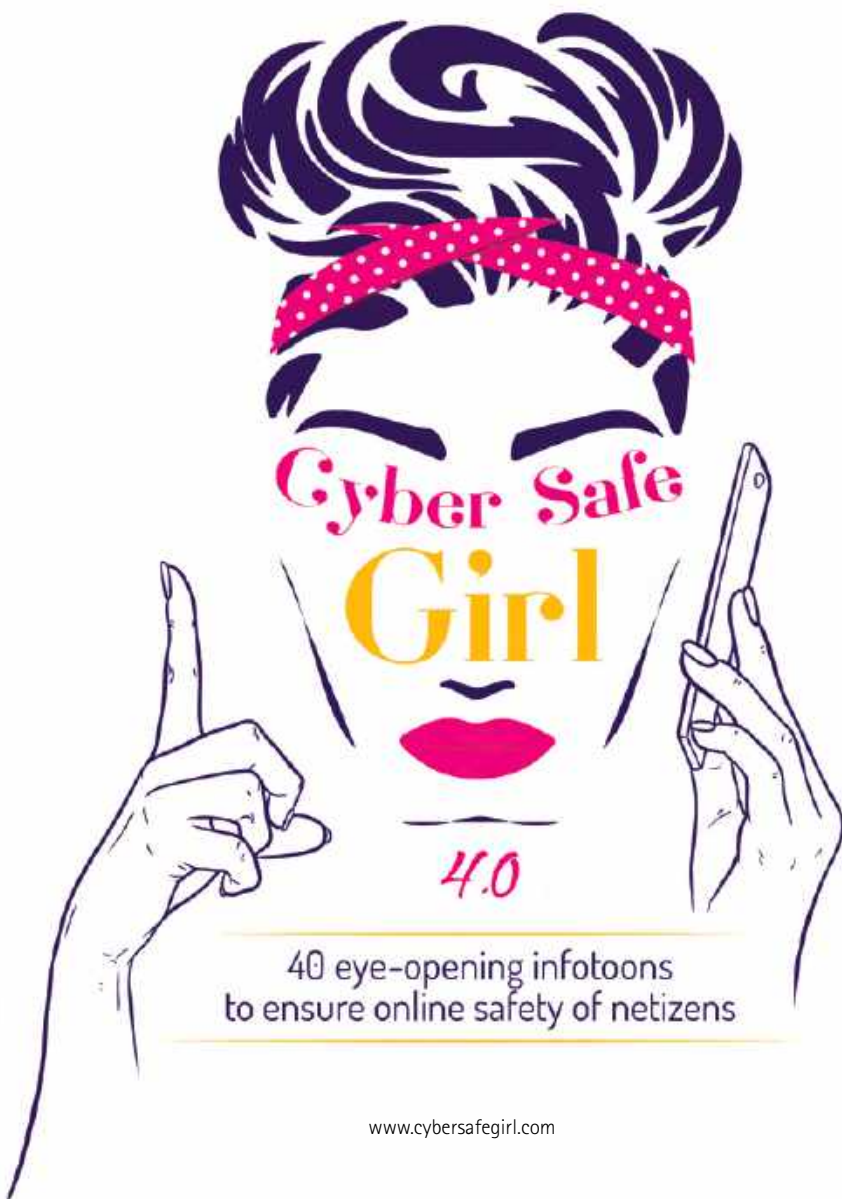
☎ +91 98691 84691 ✉ prashant@icladvocates.com



Yashavantha Kumar K N

He is a Police Officer in Karnataka State, Currently Serving as the Deputy Superintendent of Police in the CID. Mr Kumar has a MTech degree and is passionate in the field of Cyber Security and Forensics. He is an adjunct faculty in many training schools of the Law Enforcement Agencies of our country. He was recognized by DSCI(Data Security Council of India) as Cyber Cop of the year 2021.

☎ +91 94482 46483 ✉ yashvass@gmail.com



40 eye-opening infotoons
to ensure online safety of netizens

Title: Cyber Safe Girl

Version: Fourth

Publisher: Dr Ananth Prabhu G

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

First Published in India in 2018

Copyright (C) Campus Interview Training Solutions 2021

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
info@ananthprabhu.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



Ramachandra Rao
IPS



Arun Chakravarthy
IPS



Dr Murugan
IPS



Roopa D
IPS



N Shashi Kumar
IPS



Dr Vedamurthi
IPS



Hariram Shankar
IPS



Reena Suvarna
KSPS



M C Kavitha
KSPS

Special Thanks to _____



Manjunath
Bhandary



Ch A S Murty
ISEA Team



Dr Varadraj G



Vivek Shetty



Ravishankar B S



Vaikunt Prabhu



Paritosh Vyas



Gopalkrishna K



Naveen Kumar



Dr Mustafa B
Tech Resource



Rohan Don
Web Architect



Tapan J Mehta



Akash M



Anudeep Karkera
Artist



Do you want to invite
Dr Ananth Prabhu G
to address the students of your school /
college or employees of your organisation..?

.....

contact
+91 89515 11111
info@ananthprabhu.com

.....

to follow his regular updates
like the page



www.facebook.com/educatorananth



Topics

MOBILE RECHARGE SHOP

CYBER VULTURES

DEBIT CARD CLONING

APP TRAPS

KEYLOGGER

JUICE JACKING

SMS SPOOFING

WIFI HACKING

CALL SPOOFING

ONLINE RADICALIZATION

RANSOMWARE

HONEY TRAP

CYBER STALKING

QR CODE SCAM

PICTURE MORPHING

RFID CLONING

PROFILE HACKING

DRONE SURVEILLANCE

ONLINE GAMES

SEARCH ENGINE
RESULTS SCAM

JOB CALL LETTER

IDN HOMOGRAPH ATTACK

DEEPFAKES

SCRATCH CARD SCAM

DATING WEBSITE

SIM SWAP

CAMERA HACKING

CRYPTOJACKING

SOCIAL TROLLING

VIDEO CONFERENCE
SCAM

PONZI SCHEME

KIDS MOBILE PHONE

FAKE MATRIMONIAL
PROFILE

SMART HOMES

MOBILE REPAIR SHOP

MICRO LOANS

FAKE REVIEWS

BLUE SNARFING

FAKE PROFILE WITH
SEXTORTION

STOLEN PHONE



FOREWORD

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



If you are not responsible, you can very easily end up having your identity stolen, credit ruined and your files gone forever, to name a few.

Therefore, it is quintessential to follow the best practices to stay Cyber Safe and browse the internet responsibly.

I am glad that #CyberSafeGirl Version 4.0 has come out very well and it would definitely help millions of girls and netizens. The 40 info toons are very simple and easy to comprehend. I am sure, it would benefit any one from 9 to 99 years of age!

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

Warm Regards,

Smt. Rekha Sharma

Chairperson

National Commission for Women, New Delhi

THE IMPORTANCE OF CYBER SAFETY!

In today's world of cyber era, where there is an ever increasing cyber crimes and cyber thefts taking place, we need to be alert and ever conscious of every small act related to our personal activities on online social media.

Cyber hygiene is not a choice anymore, it is a necessity for a safe and secure lifestyle. Like a house that protects you from the external environment, cybersecurity protects you from external intruders interested in stealing or snatching your confidential information for various ulterior motives, often monetary and data! After all, Data is the new Oil. In this globally connected world, cyber safety is interlinked with the safety of everyone and not just one person/system.



As the dependency on the internet is growing, the importance of cyber safety is also growing significantly. Learning how to protect our devices and information from falling prey to malicious intruders has become imperative. Cyber safety matters to everyone as most of our crucial data is online.

To have a successful implementation of cyber hygiene, follow the 3 steps

Stop – Before using the internet or sharing any data, take time to understand the risks involved. Learn how to tackle potential risks.

Think – Watch for warning signs before accessing anything online. Consider the safety of others and analyze the importance of sharing the information.

Connect – Always connect to authorized and safe internet connections.

Am sure, this book will be of service to all the netizens of our country.

#JaiHind

Smt. Shyamala S Kundar

Member

National Commission for Women

MOBILE RECHARGE SHOP

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

Sections Applicable

IPC Sections (to be applied to the Shop Keeper)

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

IPC Section 354C - Voyeurism

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

IPC Section 503 - Criminal Intimidation

IPC Section 506 - Punishment for Criminal Intimidation

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

IT Act:

IT Act Section 66E - Punishment for violation of privacy

Mobile Number Sale to Stalkers by Recharge Shop:

IPC Sections (to be applied to the Shop Keeper)

IPC Section 109 - Punishment for abetment

IPC Section 114 - Abettor present when offence is committed

IPC Section 120B - Punishment for Criminal Conspiracy

IPC Section 406 - Punishment for Criminal Breach of Trust

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



DEBIT CARD CLONING

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

Sections Applicable

IT Act for cloning

- IT Act Section 66** – Computer related offences
- IT Act Section 66C** – Punishment for Identity Theft
- IT Act Section 66D** – Punishment for cheating by personation using computer resource

Money Transaction followed by cloning:

- IPC Section 419** – Punishment for cheating by personation
- IPC Section 420** – Cheating

IT Act

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

Cloning may blow up your Earnings!



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.

Sections Applicable

Key logger installation: IT Act Section 66

- Computer Related Offences

Stealing personal information: IT Act Section 66C

- Punishment for Identity Theft

Creating fake profile & posting private conversation : IT Act

IT Act Section 66C - Punishment for Identity Theft

IT Act Section 66D - Punishment for cheating by personation by using computer resources

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

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

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

IPC Sections:

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

If in hard copy, IPC Sections 292, 293 & 294

Keylogger may empty your Coffer!



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 POOJA'S 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, when you send an SMS, your handheld device sends the message with your phone number as the originator where in you as the sender cannot alter that number.

Sections Applicable

Act of hoax or trick or deceive a communication

IPC Section

IPC Section 465 – Making a false document(FORGERY)

IPC Section 419 – Punishment for cheating by personation

IT Act

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

SMS are Spoofed by Cyber Crooks!



CALL SPOOFING

Call spoofing happens through apps that enable a person with criminal intent to change his number and voice to impersonate another to defraud.

Sections Applicable

Act of hoax or trick or deceive a communication

IPC Section

IPC Section 465 – Making a false document(FORGERY)

IPC Section 419 – Punishment for cheating by personation

IT Act

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

Call Spoofing is always with criminal intent!



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 REQUEST, IF SHE COULD SEE SOME MUTUAL FRIENDS.



SHABANA'S 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 ONE PHONE NUMBER CAN BE FAKED FOR CALLS AND SMS. SCAMSTERS USE THIS TECHNIQUE TO TRICK PEOPLE. YOU 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. Users are shown instructions as to how to pay a fee to get the decryption key. The costs can range from a few hundred rupees to thousands, payable to cybercriminals in bitcoin.

Sections Applicable

Unauthorised access, Denial, Encryption :

IT Act Section 66 – Computer related offences

Demand without payment :





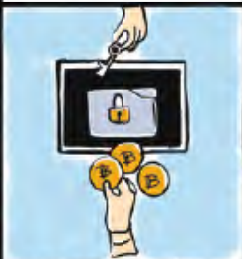




IPC Section 384 – Extortion

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

Demand & payment :

IPC Section 384 – Extortion.

Sensitize your Hardware and Software to avoid Ransomware!

		
<p>ALISHA IS AN ENTREPRENEUR. HER COMPANY HAS 50 EMPLOYEES AND 60 SYSTEMS.</p>	<p>ONE DAY, SHE RECEIVES AN EMAIL FROM HER VENDOR HAVING AN ATTACHMENT.</p>	<p>ALISHA DOWNLOADS THE ATTACHMENT. HER ANTIVIRUS WAS NOT UPDATED, SO NO ALERTS.</p>
		
<p>UPON OPENING THE FILE, HER SYSTEM GETS LOCKED AND ALL FILES ARE ENCRYPTED. UNABLE TO ACCESS.</p>	<p>AN ALERT MESSAGE ON SCREEN DEMANDS RS. 1 LAKH TO BE PAID IN BITCOIN TO UNLOCK THE SCREEN.</p>	<p>ALISHA MAKES THE PAYMENT TO THE BITCOIN WALLET ADDRESS MENTIONED</p>
		
<p>THE HACKER DOES NOT SEND THE PRIVATE KEY. THE FILES REMAIN ENCRYPTED AND INACCESSIBLE.</p>	<p>HER MANAGER QUIPS THAT THE EMAIL SHE RECEIVED WAS A PHISHING EMAIL WITH RANSOMWARE</p>	<p>ALISHA REGRETS FOR NOT DELETING THE EMAIL AND OPERATING HER SYSTEM BY NOT UPDATING HER ANTIVIRUS SOFTWARE. UPDATE ANTIVIRUS S/W ALWAYS</p>

CYBER STALKING

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

Sections Applicable

Offline :

IPC Section 354 D – Stalking

Online :

IPC Section 354 D – Stalking

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



PICTURE MORPHING

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

Sections Applicable

IPC Sections

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

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

IPC Section 469 – Making false electronic document for causing defamation

IPC Section 507 – Criminal Intimidation by an Anonymous communication

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

IT Act

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

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

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

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

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

Morphing is used for Defaming!



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 HER



AISHWARYA OUTRIGHTLY REJECTS HIS PROPOSAL AND SHOUTS AT HIM



ARYAN GOES BACK HOME, DOWNLOADS HER PICTURES AND MORPHS HER PICTURE 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 profile is accessed by a probable stalker who then compromises it.

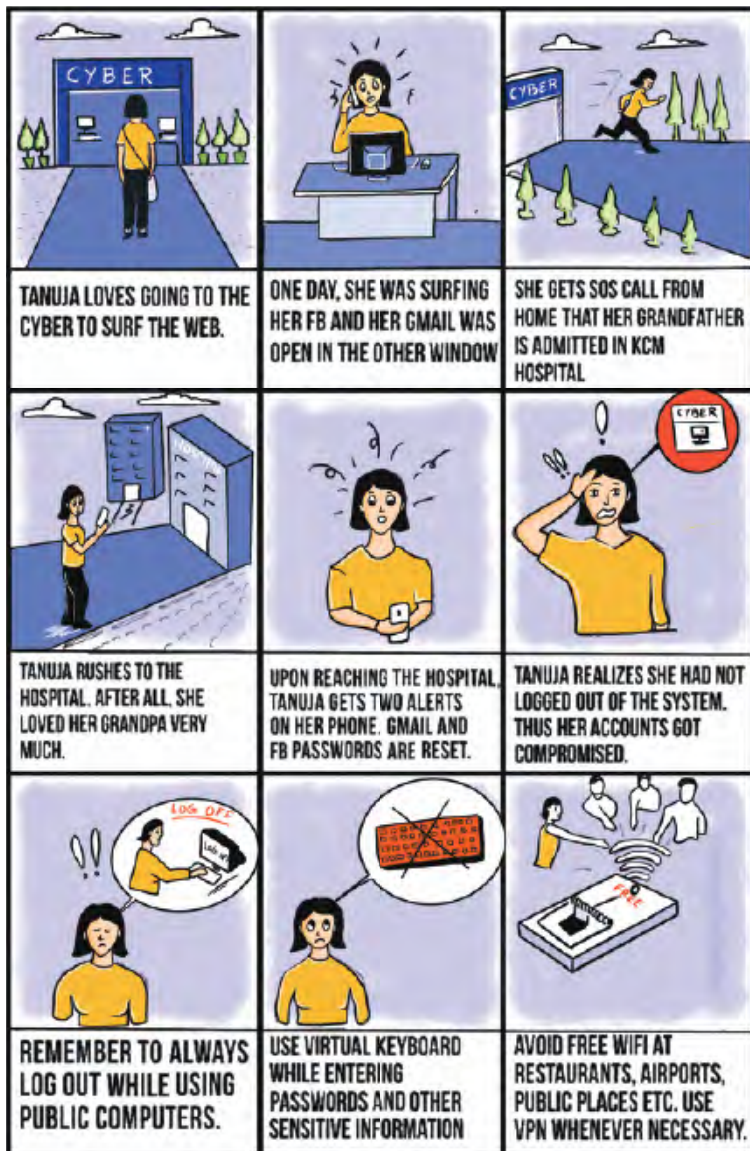
Sections Applicable

IT Act

IT Act Section 66 – Computer related offences

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

Profile Hacking means Security is Lacking!



ONLINE GAMES

Girls who are vulnerable to loneliness, low self-esteem and clinical depression can fall prey to dangerous online games that may become addictive and further harm them. Some dangerous online games like the blue whale challenge even end in the victim ending her life. This is a personal as well as social challenge for the others around.

Sections Applicable

IPC Sections

The site

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

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



JOB CALL LETTER

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

Sections Applicable

Fake account / ID:

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

Impersonation for cheating:

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

IPC Section 419 – Punishment for cheating by personation

IPC Section 420 – Cheating

IPC Section 465 – Making a false document (DEFINITION SECTION)

IPC Section 468 – Forgery for cheating

IPC Section 471 – Using forged document as genuine

IPC Section 474 – Procession of forged document

IPC Section 120-B – Punishment for Criminal Conspiracy

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

Abatement for offence

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

b. Remotely: IPC Section 109 – Punishment for abetment

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



DEEPPFAKES

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

Sections Applicable

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

Impersonation for cheating :

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

IPC Section 419 – Punishment for cheating by personation

IPC Section 420 – Cheating

Publishing online:

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

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

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

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

IPC Section 465 – Making a false document

Section 507 – Criminal Intimidation by an Anonymous communication

SEC 509 – Insulting modesty of women

Stalking: : IPC Section 354 D – Stalking Offline

: IPC Section 354 D – Stalking Online

IPC Section 120–B – Punishment for Criminal Conspiracy

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

Abatement for offence:

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

b. Remotely: IPC Section 109 – Punishment for abetment

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



DATING WEBSITE

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

Sections Applicable

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

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

IPC Section 419 – Punishment for cheating by personation

IPC Section 420 – Cheating

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

IPC Section 354C – Voyeurism

Stalking : Offline : IPC Section 354 D – Stalking

Online : IPC Section 354 D – Stalking

Publishing online

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

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

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

IPC Section 507 – Criminal Intimidation by an Anonymous communication

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

IPC Section 465 – Making a false document

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

		
<p>RASHMI IS A FIRST YEAR MBBS STUDENT. SHE WAS RECENTLY CROWNED AS MISS FRESHER..</p>	<p>SHE USED TO ALWAYS TALK TO HER FRIENDS ONLINE. BUT SHE WAS BORED OF TALKING TO THE SAME PEOPLE.</p>	<p>ONE DAY SHE REGISTERS ON TINDER AND STARTS SWIPING LEFT AND RIGHT.</p>
		
<p>SHE HAPPENS TO COME ACROSS SHAKS, A VERY GOOD LOOKING GUY, CLASSY, HAS LUXURIOUS CARS, PARTIES, TRAVELS ETC.</p>	<p>SHAKS WAS SMOOTH TALKER. HE INSTANTLY IMPRESSED RASHMI AND GOT LUCKY TO TAKE HER OUT.</p>	<p>HE TOOK HER FOR A CANDLE LIGHT DINNER. RASHMI FEELS, HE IS THE ONE FOR HER!</p>
		
<p>AFTER A COUPLE OF DAYS, SHAKS TELLS RASHMI THAT HE URGENTLY NEEDS 2 LAKHS AS HIS OFFICERS HAVE FROZEN HIS ACCOUNT. SHE SELLS HER GOLD CHAIN AND GIVES HIM THE MONEY.</p>	<p>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.</p>	<p>SHE REGRETS TRUSTING THIS STRANGER THRU' DATING SITE AND FOR SENDING HER PRIVATE PICS & VIDEOS. STAY ALERT</p>

CAMERA HACKING

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

Sections Applicable

Hacking–

IPC Section 66 – Computer related offences

Capturing photograph/video:

IPC Section 354C – Voyeurism

IT Act Section 66E – Punishment for violation of privacy

Creating Fake ID in social media

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

IPC Section 419 – Punishment for cheating by personation

Online Sexual harassment to a woman

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

Stalking : Offline : IPC Section 354 D – Stalking

Online : IPC Section 354 D – Stalking

Publishing online

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

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

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

IPC Section 507 – Criminal Intimidation by an Anonymous communication

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

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



SOCIAL TROLLING

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

Sections Applicable

- IPC Section 507** – Criminal Intimidation by an Anonymous communication
- IPC Section 509** – Word, gesture or act intended to insult modesty of a woman

Stalking:

Offline: IPC Section 354 D – Stalking

Online : IPC Section 354 D – Stalking

Are you Trolling, the law may be soon following!



PONZI SCHEME

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

Sections Applicable

Sections 3, 4, 5, 6 of Prize Chits and Money Circulation Schemes (Banning) Act, 1978

Also look up at State Acts eg

Section 9 of the Karnataka Protection of Interest of Depositors In Financial Establishments Act, 2004

Section 3, 4 of Maharashtra Protection of Interest of Depositors In Financial Establishments Act, 1999 etc.

IPC Section 120-B – Punishment for Criminal Conspiracy

IPC Section 406 – Punishment for Criminal Breach of Trust

IPC Section 420 – Cheating

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

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

		
<p>NEHA IS A GIRL FROM LOWER MIDDLE CLASS FAMILY.</p>	<p>SHE ALWAYS WANTED TO HAVE ALL THE LUXURIES IN LIFE.</p>	<p>ONE DAY SHE COMES ACROSS A WEBSITE THAT PROMISES BMW CARS, FOREIGN TOURS FOR ONLY RS.9999/-</p>
		
<p>SHE ENROLLS FOR A COUNSELING SESSION. GETS AN INVITE TO A 5 STAR HOTEL.</p>	<p>THEY TELL HER TO ENROLL AND INVITE 2 PEOPLE TO JOIN, LEFT AND RIGHT BRANCH OF TREE. SHE GETS COMMISSION OF RS.500</p>	<p>THE COMMISSION INCREASES AS THOSE WHOM SHE HAD ENROLLED, ALSO INDUCTS NEW PEOPLE</p>
		
<p>INITIALLY SHE RECEIVED SOME COMMISSION. WHEN ENROLLMENTS REDUCED, SHE INVESTS MORE FOR SELF ENROLLMENTS</p>	<p>ONE DAY THE WEBSITE IS NOW FUNCTIONAL AND NONE OF THE HELPLINE NUMBERS ARE WORKING. MEDIA REPORTS THE PROMOTERS ARE ABSCONDING.</p>	<p>ENROLLED MEMBERS ARE NOW DEMANDING MONEY. SHE HAS ALSO LOST BIG TIME. DO NOT FALL PREY.</p>

FAKE MATRIMONIAL PROFILE

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

Sections Applicable

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

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

FAKE MATRIMONIAL PROFILE



MOBILE REPAIR SHOP

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

Sections Applicable

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

Publishing online

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

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



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.

Sections Applicable

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

Fake Reviews may give you wrong Overviews!



FAKE PROFILE WITH SEXTORTION

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

Sections Applicable

Capturing photograph/video:

IPC Section 354C – Voyeurism

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

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

IPC Section 419 – Punishment for cheating by personation

IPC Section 354A – Sexual Harassment and punishment for Sexual

IPC Section 507 – Criminal Intimidation by an Anonymous communication

Publishing online

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

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

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

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

A Fake Profile can cause unimaginable consequences!



CYBER VULTURES

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

Sections Applicable

IT Act Section 66 – Computer related offences

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

Impersonation as financial company:

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

Fetching personal/ Banking/wallet details:

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

IPC Section 420 – Cheating

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



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 WILL 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.

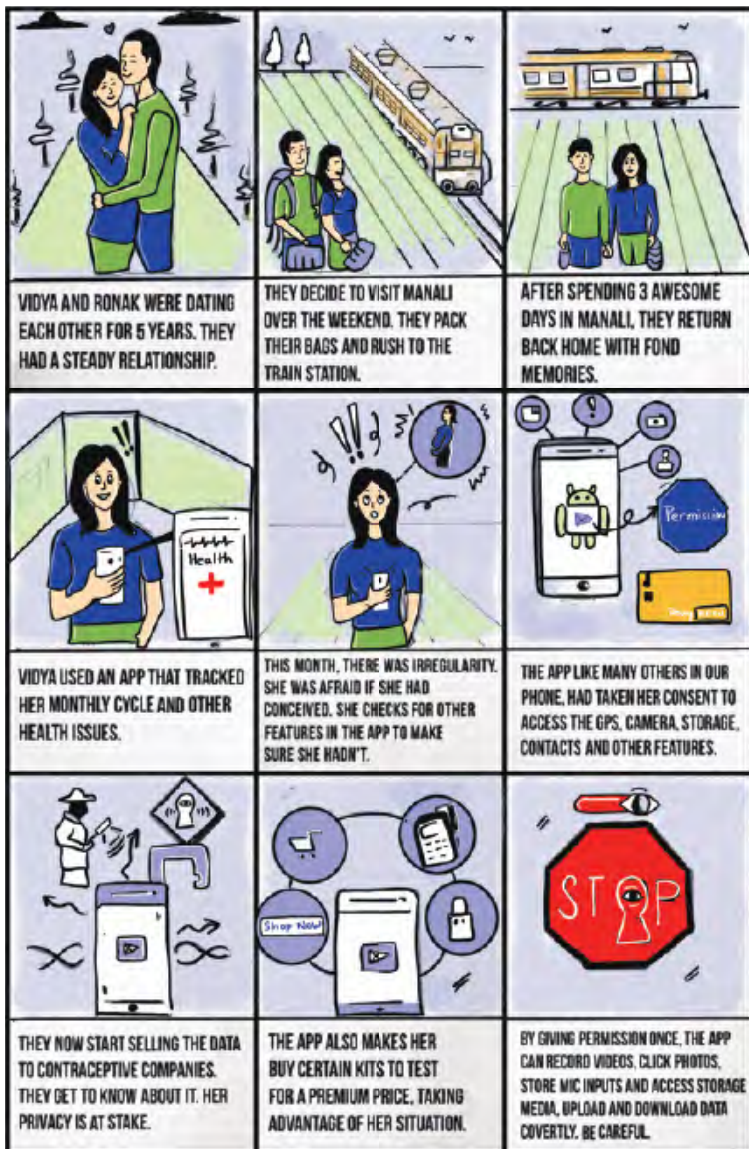
APP TRAPS

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.

Sections Applicable

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

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



JUICE JACKING

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

Sections Applicable

IT Act Section 66 – Computer Related Offences

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

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



WIFI HACKING

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

Sections Applicable

IT Act Section 66 – Computer Related Offences

Wrongful gain, wrongful loss of internet data:

IPC Section 420 – Cheating

Mischief by internet utility:

IPC Section 425/426 – Mischief

Publishing online

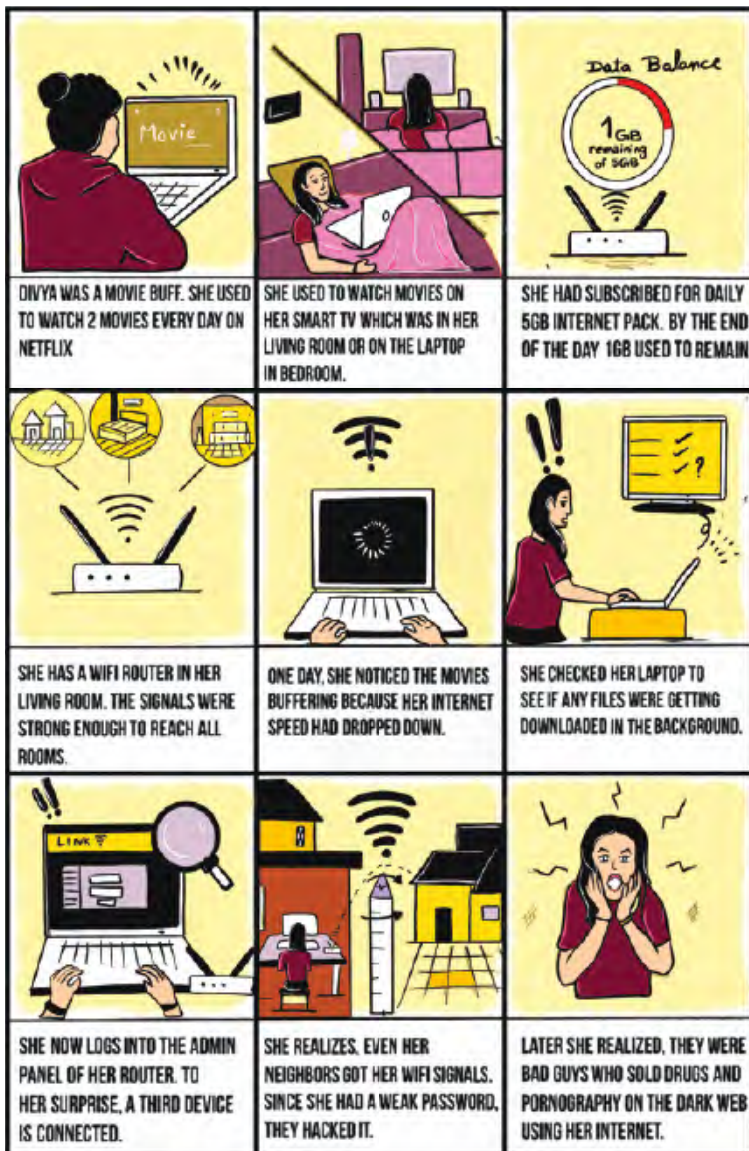
IT Act Section 67 – Punishment for publishing or transmitting obscene material in electronic form

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

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

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

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



ONLINE RADICALIZATION

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

Sections Applicable

- IT Act Section 66F** – Punishment for Cyber Terrorism
- IPC Section 120B** – Punishment of Criminal Conspiracy
- IPC Section 121** – Waging or attempting to wage war, or abetting waging of war, against the Government of India
- IPC Section 121A** – Conspiracy to commit offences punishable under Section 121A
- IPC Section 122** – Collecting arms, etc., with intention of waging war against the Government of India
- IPC Section 124A** – Sedition

Don't get Radicalized, rather be Rationalized!



RESHMA 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

HONEY TRAP

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

Sections Applicable

Capturing Picture/Video Over Online:

IPC Section 354C – Voyeurism

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

IT Act Section 66E – Punishment for violation of privacy

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

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

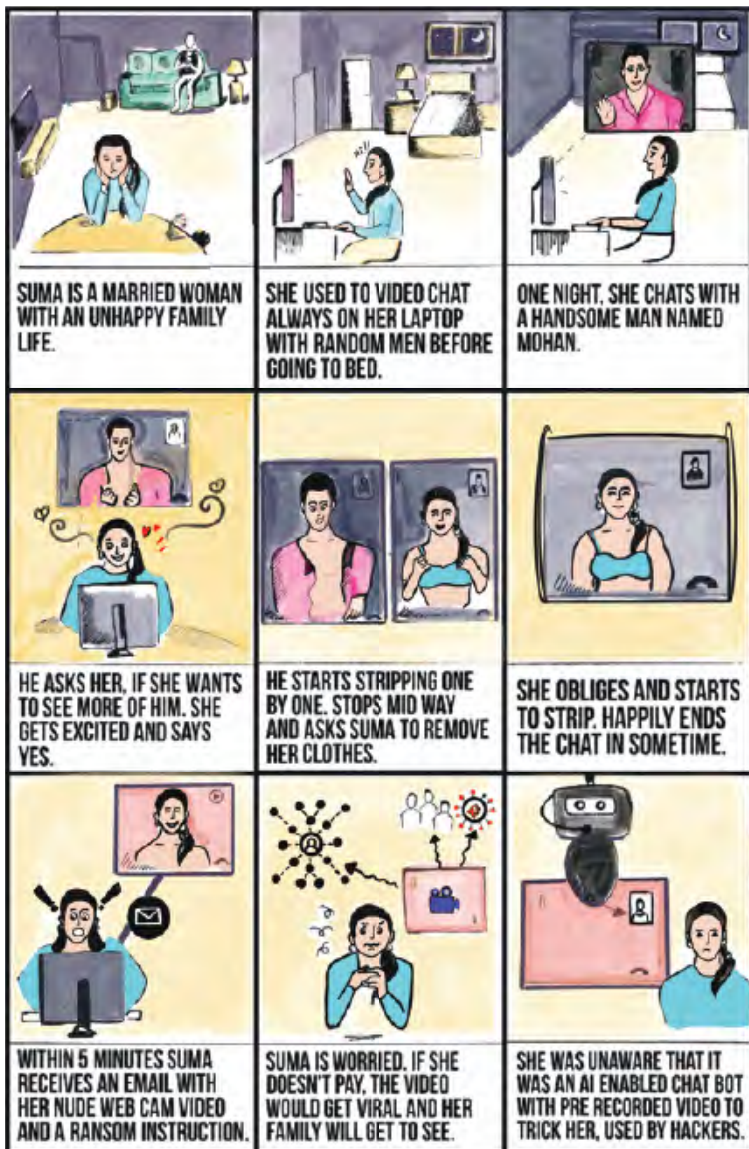
IT Act Section 67B – Punishment for publishing or transmitting of material depicting children in sexually explicit act etc., in electronic form & sections of POCSO

Demand for ransom (attempt):

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

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

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



QR CODE SCAM

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

Sections Applicable

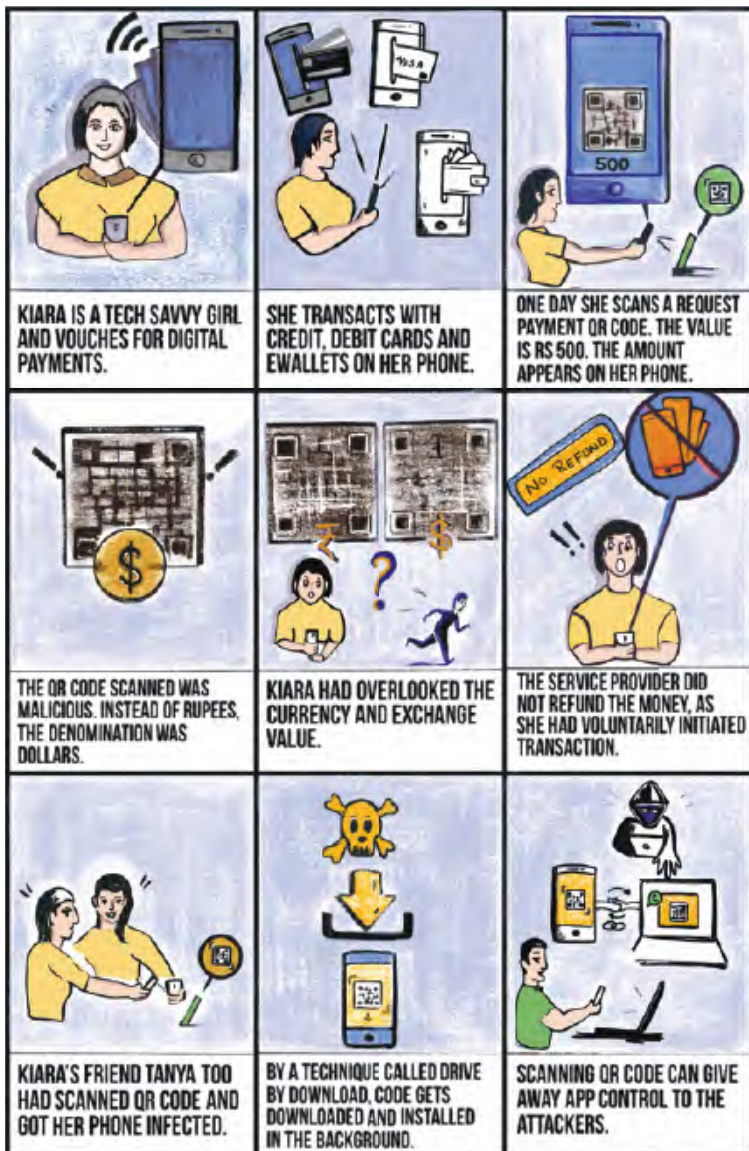
IPC Section 406 – Punishment for Criminal Breach of Trust

IPC Section 420 – Cheating

Unauthorised Access by installing malware in the background:

IT Act Section 66 – Computer related offences

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



RFID CLONING

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

Sections Applicable

IT Act Section 66 – Computer Related Offences

Stealing RFID data / RFID Cloning:

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

Retaining stolen data & Selling Credit Card Details:

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

IPC Section 420 – Cheating

Creating Replica of Digital ID & accessing server by impersonation:

IT Act Section 66 – Computer Related Offences

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

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

IPC Section 419 – Punishment for cheating by personation

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



AYESHA IS AN IT EMPLOYEE. SHE USED HER RFID TAG FOR DOOR ACCESS.



SHE USED TO PLACE THE RFID CARD IN HER WALLET AND FLASH THE WALLET AT THE READER.



SHE HAD A HABIT OF KEEPING HER WALLET ON THE DESK, EVERYTIME.



ONE DAY, SHE FORGOT TO TAKE THE WALLET WITH HER WHILE SHE LEFT HER DESK TO GO TO THE WASHROOM



A COLLEAGUE, JOHN WHO WAS JEALOUS OF AYESHA'S SUCCESS SCANS HER WALLET USING A RFID READER.



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



THE CREDIT CARD DETAILS ARE SOLD IN THE DARK WEB FOR MONEY BY JOHN.



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



USING THAT ID, JOHN ENTERS THE SERVER ROOM AND HACKS THE SYSTEMS. AYESHA GETS BLAMED FOR NO FAULT OF HER.

DRONE SURVEILLANCE

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

Sections Applicable

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

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

IPC Section 354C – Voyeurism

IPC Section 354D – Stalking

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

IT Act Section 66E – Punishment for violation of privacy

Unauthorised access to WI FI by DRONE:

IT Act Section 66 – Computer Related Offences

Stealing personal information via WI FI Cracker:

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

Dropping hazardous materials to house via DRONE:

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

You are profiled day in and day out without doubt.



ANURADHA, A MEDICAL STUDENT LIVED IN THE 33RD FLOOR OF HER APARTMENT.



SHE USED TO KEEP ALL HER WINDOWS OPEN AS THERE WERE NO TALLER BUILDINGS NEARBY WHO COULD VIEW HER PLACE.



SHE USED TO ROAM INDOORS WITH MINIMAL CLOTHES AS SHE NEVER SHARED HER HOME WITH ANYONE.



AKSHAY, HER EX BOYFRIEND USED A DRONE TO SNOOP ON HER IN MANY WAYS.



HE SENT THE DRONE ALL THE WAY UP TO RECORD HER BEDROOM AND LIVING ROOM VIDEOS COVERTLY.



THE DRONE USED TO KEEP TRACK OF IN AND OUT MOVEMENTS FROM HER HOUSE.



IT ALSO HAD A WIFI CRACKER IN IT, TO INTERCEPT ALL THE DATA, TO SNOOP ON HER.



HE COULD ALSO DROP HAZARDOUS MATERIALS/ WEAPONS TO HER HOUSE USING THE DRONE.



SHE COULD HAVE TRACKED THE DRONE IN THE VERY BEGINNING HAD SHE INSTALLED A CC CAMERA WITH MOTION SENSOR

SEARCH ENGINE RESULTS SCAM

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

Sections Applicable

IT Act Section 66 – Computer Related Offences

Replacing Original Contact Details by Fraudster Details:

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

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

IPC Section 419 – Punishment for cheating by personation

IPC Section 420 – Cheating

IPC Section 465 – Making a false document

IPC Section 468 – Forgery for the purpose of cheating

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

SEARCH ENGINE RESULTS SCAM

		
<p>AKSHATA HAD BOOKED A FLIGHT TICKET TO MANGALORE.</p>	<p>TWO DAYS BEFORE THE JOURNEY SHE GETS AN EMAIL STATING HER TICKETS ARE CANCELLED.</p>	<p>SHE GOOGLES THE HELPLINE NUMBER AND CALLS THE NUMBER WHICH APPEARED IN THE RESULTS.</p>
		
<p>THE CUSTOMER CARE ASKS HER CARD DETAILS FOR VERIFICATION. SHE GIVES ALONG WITH CVV.</p>	<p>SHE LOSES RS10000 FOR 5 CONSECUTIVE TIMES. TOTAL RS 50000.</p>	<p>THE MAIL SHE HAD RECEIVED WAS SPOOFED. NOT FROM THE AIRLINE.</p>
		
<p>THE CALL CENTER NUMBER IN THE SEARCH WAS INJECTED BY HACKERS. A FAKE NUMBER TO TRICK PEOPLE.</p>	<p>THOUGH SHE HADN'T SHARED OTP, FOREIGN GATEWAYS DO NOT NEED OTP FOR TRANSACTION.</p>	<p>AKSHATA HAD NOT DISABLED INTERNATIONAL USAGE ON HER CREDIT AND DEBIT CARD.</p>

IDN HOMOGRAPH ATTACK

An IDN homograph attack is similar to another type of domain name spoofing known as typosquatting. Both techniques attempt to deceive users by using a new domain name that's similar to an established name, although they exploit different types of similarities.

Sections Applicable

- IT Act Section 66** – Computer related offences
- IT Act Section 66C** – Punishment for Identity Theft
- IT Act Section 66D** – Punishment for cheating by personation using a computer resource

- IPC Section 419** – Punishment for cheating by personation
- IPC Section 420** – Cheating

Crackers replacing Letters & Characters to commit frauds.

		
<p>SUCHETA WANTS TO SEND MONEY TO HER MOTHER, WHO LIVES IN ANOTHER CITY</p>	<p>SHE RECIEVES A MESSAGE FROM HER BANK</p>	<p>THE MESSAGE WHEN OPENED READ AS FOLLOWS</p>
		
<p>EXCITED, SHE CLICKS ON THE LINK AND ENTERS HER LOGIN CREDENTIALS.</p>	<p>THE PAGE DID NOT LOAD UPON PRESSING SUBMIT. INSTEAD, SHE GOT THE LOGIN PAGE AGAIN.</p>	<p>SHE ONCE AGAIN ENTERS AND DOES A SUCCESSFUL TRANSACTION.</p>
		
<p>INSTEAD OF GIFT VOUCHER, SHE GETS A SHOCK TO SEE RS 10000 DEBITED FROM HER ACCOUNT</p>	<p>SUCHETA WAS A VICTIM OF IDN HOMOGRAPH ATTACK WHERE FAKE DOMAINS ARE CREATED THAT MIMIC REAL ONES</p>	<p>HAD SHE UPDATED HER BROWSER SHE WOULD HAVE GOT AN ALERT MESSAGE OF THE FAKE CYRILLIC DOMAIN, THAT MIMICS THE LATIN DOMAIN.</p>

SCRATCH CARD SCAM

A user receives a message with a link to a third-party website with a promise of winning guaranteed money. When the user clicks on the link, it redirects to a website with a scratch card mimicking the design of popular Pay Wallets scratch card.

Sections Applicable

- IT Act Section 66** – Computer related offences
- IT Act Section 66C** – Punishment for Identity Theft
- IT Act Section 66D** – Punishment for cheating by personation using a computer resource

- IPC Section 419** – Punishment for cheating by personation
- IPC Section 420** – Cheating

Sharing sensitive Credentials will bring about losses that would be Substantial



SIM SWAP










A SIM swap scam (also known as port-out scam, SIM splitting, Smishing and simjacking, SIM swapping) is a type of account takeover fraud. The fraud exploits a mobile phone service provider's ability to seamlessly port a telephone number to a device containing a different SIM. This feature is normally used when a customer has lost or had their phone stolen, or is switching service to a new phone.

Sections Applicable

- IT Act Section 66** – Computer related offences
- IT Act Section 66C** – Punishment for Identity Theft
- IT Act Section 66D** – Punishment for cheating by personation using a computer resource

- IPC Section 419** – Punishment for cheating by personation
- IPC Section 420** – Cheating

Swapping of Sim could lead you to a situation thats Dim

		
<p>ARPITHA HAD LINKED HER MOBILE NUMBER FOR AUTHENTICATION ON MANY APPS THAT SHE USED ON HER CELL PHONE.</p>	<p>FEW OF THEM WERE MOBILE WALLETS, 2FA FOR EMAIL, BANK ACCOUNTS, SOCIAL MEDIA ETC.</p>	<p>ONE NIGHT ARPITHA GETS A CALL FROM A CYBER CRIMINAL WHO PRETENDS TO BE CALLING FROM HER CELL PHONE COMPANY.</p>
		
<p>HE CONVINCES HER TO KEEP HER PHONE OFF FOR 2 HOURS, FOR A BONUS 5G ACTIVATION ONLY TO LIMITED CUSTOMERS.</p>	<p>ARPITHA SWITCHES OFF HER PHONE AND GOES TO SLEEP. NEXT MORNING WHEN SHE WAKES UP, THERE IS NO NETWORK.</p>	<p>THE HACKER HAD SUBMITTED HER DOCUMENTS AND OPTED FOR NEW SIM. AS THE NEW SIM GETS ACTIVATED, THE OLD ONE BECOMES USELESS.</p>
		
<p>USING FORGOT PASSWORD AND OTP VERIFICATION OPTIONS, THE HACKER GAINS CONTROL OF ALL HER ACCOUNTS.</p>	<p>HE ALSO GETS CONTROL OF HER WHATSAPP, MAKING HIM ACCESS HER PRIVATE CHATS/PHOTOS, TO BLACKMAIL HER.</p>	<p>VIA VISHING/SMISHING/PHISHING HACKERS ALSO REQUEST OTP TO HACK INTO WHATSAPP AND OTHER ACCOUNTS WITHOUT SIM SWAP.</p>

CRYPTOJACKING

It is a type of cyberattack in which a hacker co-opts a target's computing power to illicitly mine cryptocurrency on the hacker's behalf. Cryptojacking can target individual consumers, massive institutions, and even industrial control systems. It slows down infected computers, as the mining process takes priority over other legitimate activities.










Sections Applicable

- IT Act Section 66** – Computer related offences
- IT Act Section 66C** – Punishment for Identity Theft
- IT Act Section 66D** – Punishment for cheating by personation using a computer resource

- IPC Section 419** – Punishment for cheating by personation
- IPC Section 420** – Cheating

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

Cryptojacking helps hackers in Money Making

		
<p>ROOPA IS A SOFTWARE DEVELOPER AND WORKS FROM HOME.</p>	<p>SHE USES 2 HIGH END LAPTOPS TO EXECUTE HER CODE WHICH ARE RESOURCE INTENSIVE.</p>	<p>OFF LATELY, SHE NOTICED HER SYSTEMS TO BE MUCH SLOWER THAN USUAL.</p>
		
<p>ALSO, THE POWER USAGE OF THE SYSTEM HAD GONE UP DRASTICALLY.</p>	<p>UPON OPENING THE PROCESS MANAGER, SHE COULD SEE SOME UNKNOWN APPS RUNNING.</p>	<p>THESE APPS WERE CRYPTOJACKING APPS THAT CONSUMED HER RESOURCES TO MINE BITCOINS.</p>
		
<p>SHE HAD CLICKED ON AN UNKNOWN LINK THROUGH WHICH THIS APP WAS INSTALLED.</p>	<p>USING HER SYSTEMS RAM AND PROCESSOR, THE CYBER CRIMINAL EARN A LOT OF MONEY BY MINING.</p>	<p>HAD SHE INSTALLED A GOOD PAID ANTIVIRUS AND BROWSER EXTENSION TO BLOCK COIN MINING, THE SYSTEM WOULD HAVE BEEN SAFE.</p>

VIDEO CONFERENCE SCAM

There has been a mass adaptation of online platforms to conduct meetings, online classes, conferences without giving much consideration to the security settings of these platforms. This has paved the way for cyber criminals to take advantage of loopholes for malicious purposes.

Sections Applicable

- IT Act Section 66** – Computer related offences
- IT Act Section 66C** – Punishment for Identity
- IT Act Section 67** – Publishing or transmitting obscene content
- IT Act Section 67A** – Publishing or transmitting sexually explicit acts or conduct

Theft

- IT Act Section 66D** – Punishment for cheating by personation using a computer resource
(as per the facts of the case)
- IPC Section 419** – Punishment for cheating by personation
- IPC Section 420** – Cheating (as per the facts of the case)

Inference of who's attending such virtual Conference needs to made

VIDEO CONFERENCE SCAM



AMRITA WORKS FOR A MNC AS A TEAM LEAD. OFF LATELY, SHE HAD OPTED FOR WORK FROM HOME.



SHE USED TO REGULARLY HOST ONLINE MEETINGS TO COORDINATE WITH HER TEAM MEMBERS.



EVEN THE CLIENTS AT TIMES USED TO INTERACT VIA VIDEO CONFERENCE TO CHECK FOR PROGRESS AND SUGGEST CHANGES.



ONE MORNING, DURING THE CLIENT MEETING, A RANDOM USER LOGS IN AND POSTS A PORN CLIP.



EMBARRASSED BY THE EVENT, AMRITA LOGGED OFF.



SHE HAD MADE THE MISTAKE OF POSTING THE MEETING ID AND PASSWORD IN THE SAME MESSAGE IN A DISCUSSION FORUM.



A DISGRUNTLED EMPLOYEE FROM THE CLIENTS SIDE LOGGED IN WITH A PROXY NAME.



THE WAITING ROOM WAS NOT ENABLED TO SCREEN THE PARTICIPANTS.



PERMISSION TO SHARE SCREEN AND FILE SHARE WAS NOT DISABLED FOR ALL THE PARTICIPANTS.

KIDS MOBILE PHONE

Children are using devices at a younger age and it's a tricky situation for most parents since they do not want their child to come across adult, abusive, or violent content on the internet. Thus, it's important to consider setting controls on the devices they use. Responsible mobile phone use is about managing costs, sticking to family rules, keeping phones safe and being respectful.

Sections Applicable

If Gambling is involved:

The acts may attract Provisions of

Section 69A – IT Act for blocking illegal gambling websites.

The Public Gambling Act, 1867.

The Foreign Exchange Management Act, 1999 (FEMA).

The Lotteries Regulation Act of 1998.

A few States have made provisions for laws on Gambling.

Exceptions:

1. Horse racing is legal in India
2. Lottery system (in few States)
3. The Public Gambling Act of 1867 exempts skill-based games from the definition of gambling.

Online games may bring about losses, disrepute and shame

		
<p>SUMAN IS A SINGLE MOTHER. LIVES WITH HER 9 YEAR OLD SON ARNAAV.</p>	<p>SHE WORKS AS A BEAUTICIAN AT A PARLOUR CLOSE TO HER HOUSE.</p>	<p>BECAUSE OF THE PANDEMIC, ALL THE CLASSES ARE ONLINE. ARNAAV ATTENDS CLASSES VIA HIS MOTHERS MOBILE PHONE.</p>
		
<p>INSTEAD OF ATTENDING CLASSES, ARNAAV PLAYS VIDEO GAMES.</p>	<p>HE ALSO DOWNLOADS PAID APPS FROM THE PLAY STORE USING THE CREDIT CARD WHICH IS STORED.</p>	<p>SOMETIMES, HE EVEN BUYS COINS IN THE VIDEO GAMES TO COMPLETE THE LEVEL FASTER.</p>
		
<p>HE DELETES THE TRANSACTION MESSAGE RECEIVED VIA SMS SO THAT HIS MOTHER DOES NOT FIND OUT.</p>	<p>SUMAN WAS SHOCKED TO SEE RS 14000 SWIPED AT PLAY STORE IN HER MONTHLY CREDIT CARD BILL.</p>	<p>HAD SHE ENABLED PARENTAL CONTROLS ON IOS/ANDROID, ARNAAV COULD USE THE PHONE ONLY FOR ACADEMIC PURPOSES.</p>

SMART HOMES

Smart-home devices hold a treasure trove of personal information, from your birth date to credit card details, that cybercriminals can steal via hacking if the devices lack robust protections to thwart attacks. They can then use the stolen data to launch targeted attacks to rope you into shady deals.

Sections Applicable

- IPC Section 354** – Sexual harassment
- IPC Section 354C** – Voyeurism
- IPC Section 509** – Outraging modesty of women

- IT Act Section 66** – Computer related offences
- IT Act Section 66E** – Punishment for violation of privacy

Digital outreach may lead to Privacy Breach



MICRO LOANS

Fly-by-night micro lending illegal app-based financiers are thriving. These moneylenders target younger customers who look for quick loans for consumption purposes. Those failing to pay up will have their photos shared in their family and workplace social media groups, a tactic that has driven many to desperation.

Sections Applicable

- IPC Section 420** – Cheating
 - IPC Section 503/506** – Criminal Intimidation
 - IPC Section 383** – Extortion
 - IPC Section 306** – Abetment of Suicide
 - IPC Section 499/500** – Defamation
 - IPC Section 120B** – Criminal Conspiracy
 - IPC Section 34** – Common Intention
- Sections of Reserve Bank of India Act, 1934
(as per the facts of the case)

App based micro loans are Unsecured and the borrower becomes Insecure



BLUE SNARFING

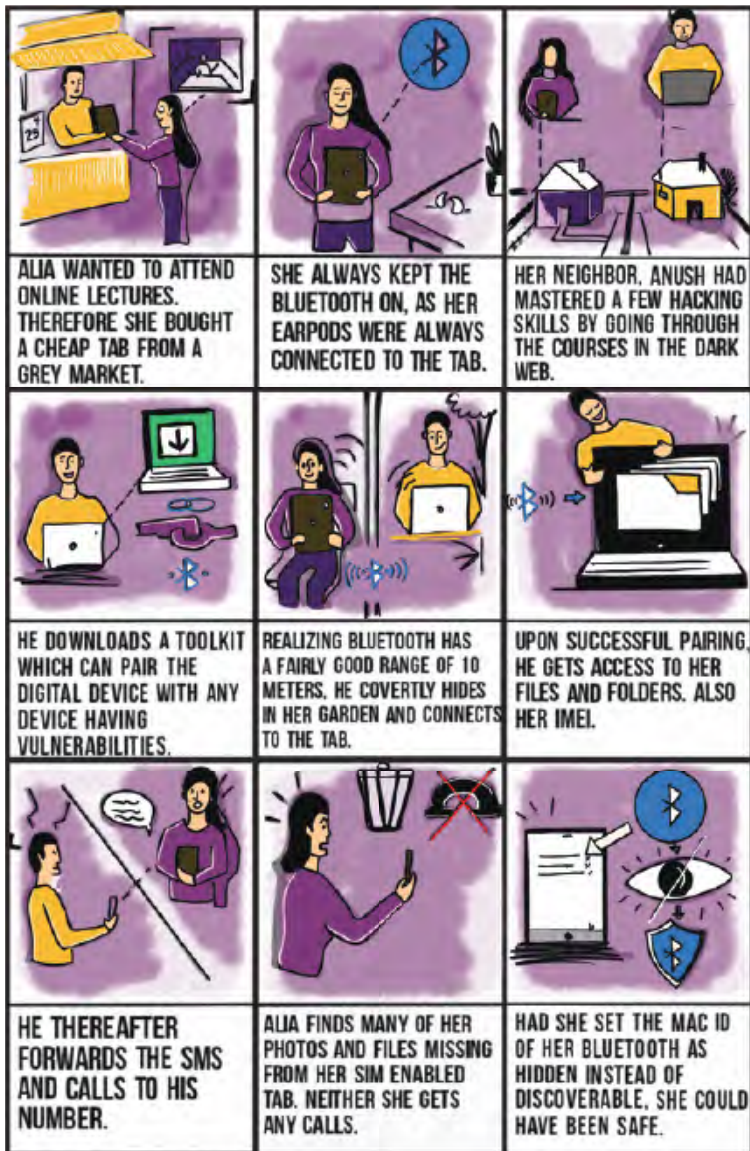
It is a device hack performed when a wireless, Bluetooth-enabled device is in discoverable mode. Bluesnarfing allows hackers to remotely access Bluetooth device data, such as a user's calendar, contact list, emails and text messages. This attack is perpetrated without the victim's knowledge.

Sections Applicable

- IT Act Section 66** – Computer related offences
- IT Act Section 66C** – Punishment for Identity Theft
- IT Act Section 66D** – Punishment for cheating by personation using a computer resource
(as per the facts of the case)

- IPC Section 419** – Punishment for cheating by personation
- IPC Section 420** – Cheating (as per the facts of the case)

Hacker may use your Bluetooth to route your information and cause you blues



STOLEN PHONE

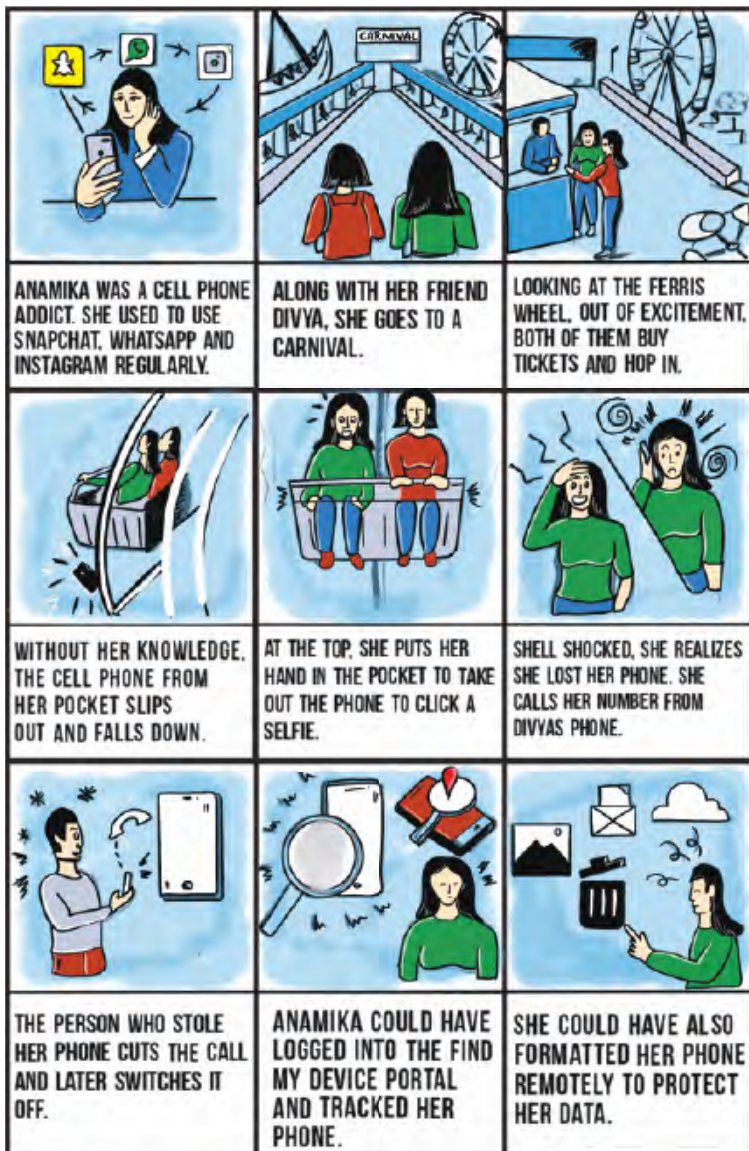
A stolen phone can leave you feeling helpless and scrambling. Mobile phones and the data they hold are very valuable to thieves. And for similar reasons – they hold so much important personal information of real and sentimental value – a theft can be a huge loss for the owner.

Sections Applicable

IPC Section 378/379 – Theft

IT Act Section 66 – Computer related offences

Lost cell phone, it may affect your cells and hormone



INFOTOONS EXPLAINED!

By Adv. Prashanth Jhala

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.

2. DEBIT CARD CLONING:

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

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

3. KEYLOGGER:

Precautions: Keyloggers may in the form of a hardware that could be attached to your computer system or to an ATM Machine 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 provideers, use licensed software's, do not click on suspicious links and the links that originate from unknown source, do not download free songs, movies, videos,

software's, applications, games etc., for a keylogger could be embedded in them and you may end up downloading one for free. Make sure to enable Two Factor Authentication for an additional layer of security, use virtual keyboard to enter the username and password and install a good antivirus on your system to stay cyber safe.

4. SMS SPOOFING:

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

5. CALL SPOOFING:

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

Also, never give credit card information to someone who calls you. You may also use Google reverse lookup or Truecaller for assistance.

6. RANSOMWARE:

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

7. CYBER STALKING:

Precaution: Cyberstalking is a serious crime, and no one wants to become a victim. One way to help protect yourself is to keep your personal information private on the internet. That's a start. Be careful about allowing physical access to your computer and other web-enabled devices like smartphones. Cyberstalkers can use software and hardware devices (sometimes attached to the back of your PC without you even

knowing it) to monitor their victims. Be sure you always log out of your computer programs when you step away from the computer and use a screensaver with a password. Delete or make private any online calendars or itineraries — even on your social network — where you list events you plan to attend. That information could allow a cyberstalker to know where and when you're planning to be somewhere. A lot of personal information is often displayed on social networks, such as your name, date of birth, where you work, and where you live. Use the privacy settings in all your online accounts to limit your online sharing with those outside your trusted circle. You can use these settings to opt out of having your profile appear when someone searches for your name. You can block people from seeing your posts and photos, too. If you post photos online via social networks or other methods, be sure to turn off the location services metadata in the photo. The metadata reveals a lot of information about the photo — where and when it was taken, what device it was taken on, and other private information. Most often, metadata comes from photos taken on a mobile phone. You can turn this off — it's usually a feature called geo-tagging — in your phone's settings.

8. PICTURE MORPHING:

Precautions: Morphing has become a child's play 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 pictures of her were circulated online by an accused. Care before you Share.

9. PROFILE HACKING:

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

10. ONLINE GAMES:

Precautions: Very recently it was reported that fake versions of online games (including Temple Run, Free Flow and Hill Climb Race) that are popular and have huge number of downloads were uploaded on play stores

as free downloads. Innocent people not able to distinguish between the real and the fake versions, downloaded the fake version and ended up in sharing entire personal data that resided on their devices. The 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. 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. Many parents do not see the details of the statements and pays up the amount online thereby giving their children a good cover for their forbidden acts. A few games were allegedly displaying inappropriate pictures that could cloud the innocent minds of children. Parents need to keep a tab on what their children are downloading or playing online by examining their browsing history and it is a point to worry if the browsing history is cleared regularly by children because that means they are hiding their footprints. Parental controls should come into play.

11. JOB CALL LETTER:

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

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

12. DEEP FAKES:

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

13. DATING WEBSITES:

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

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

14. CAMERA HACKING:

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

breach. Always use a masking tape on the webcam of your laptops to avoid breach of your privacy. As for mobile phones, put a piece of cloth on it when you are not using it. Remember that the mobile phones have cameras on both the side so precaution has to be adopted accordingly.

15. SOCIAL TROLLING:

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

16. PONZI SCHEMES:

Precautions: Schemes that offers to make you rich and wealthy without much efforts are often dubious. Remember such schemes offer high returns on your investment and may never return the money that you had invested. Unfortunately, both literate and illiterate 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 savings and make you poor. There have been enough Ponzi schemes being reported and investigated by the law enforcement agencies but despite that new Ponzi schemes are floated and people fall prey to such schemes. Study the entire project and cross verify, make your own research before entrusting your money to someone or investing it into any such schemes. Do not trust agents who promotes such schemes

because they are appointed to paddle wrong information and paint a fake picture of the scheme that would attract your attention and make you not think rationally.

17. FAKE MATRIMONIAL SITES:

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

18. MOBILE REPAIR SHOP:

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

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

19. FAKE REVIEWS:

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

20. FAKE PROFILES WITH SEXTORTION:

Precautions: An upward trend in these crimes have been observed. Pictures and videos clicked with or without consent in the moments of privacy are used later to blackmail and or extort females for further gratification, to extort money or to get them indulged into commission of other crimes or getting them involved in criminal activities. Pictures and Videos clicked in your good times comes to haunt you when the relationship turns sour. Never ever allow anyone to click a picture or a video that you may feel

would go against you someday. Also called Revenge Porn.

21. CYBER VULTURES:

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

22. APP TRAPS:

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

23. JUICE JACKING:

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

24.WIFI HACKING:

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

25. ONLINE RADICALIZATION:

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

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

26. HONEY TRAP

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

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

27. QR HACK

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

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

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

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

For receiving money, no OTP is ever generated.

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

28. RFID CLONING

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

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

confessed that he had a device which could store 10 virtual keys and that copying the data of the keys was as easy as tapping on the actual key.

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

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

29. DRONE SURVEILLANCE

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

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

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

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

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

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

30. SEARCH ENGINE FRAUD

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

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

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

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

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

RBI has now provided and enabled an added feature as a Security measure for Cards wherein you can now only make use of your cards at ATMs and on Point of Sale (POS) devices within the Country.

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

31. IDN HOMOGRAPH ATTACK

The Internationalised Domain Name (IDN) homograph attack is a way a malicious party may deceive computer users about what remote system they are communicating with, by exploiting the fact that 26 alphabets of English language have different look alike representation and carries different relevance as against the actual 26 alphabet in English language.

For example, a regular user of example.com may be lured to click a link where the English alphabet "a" is replaced with the Cyrillic character

Attackers can register their own domain names that are similar to the existing web addresses using the above technique.

Attackers can send "α" homographic URLs via email and social networks and they will look legitimate until the link is clicked on.

In order to best protect your device and network against phishing and malware, it is advised to use solutions that protect against IDN homograph attacks such as supporting web browsers (e.g., Firefox or Chrome) and carefully inspecting domain names for suspicious lookalike characters. Moreover, the use of network security solutions that scan traffic to identify and block IDN homograph attacks is another layer of defense that reduces the risk of accidentally accessing these potentially malicious domains.

The above mentioned frauds are very sophisticated and needs browsers to be updated and extensions to be in place. Sucheta would have been incapacitated to recognise and avert this crime as this one requires minute observations and tech support.

32. SCRATCH CARD SCAM:

This modus operandi has been in use for quite some time now but people who are not tech savvy or not literate enough to understand how technology works fall prey to such crimes.

By use of Wallets, either one can pay/transfer money (also known as push money) or alternatively one can call/request money (also known as pull money) from the person to whom such request could be sent via QR Codes.

Amrin failed to understand that the money that she thought would be paid to her was in fact a request for her to pay to the criminal.

Logically, you do not need your pin to receive money into your own account. The fraudsters do ask victims to use pin to send the money that they have sent (which actually is a request to pay money to the criminal) to transfer the amount show in the QR Code.

Golden Principle:

If you apply or use your wallets pin for any transactions, that logically means that you are making a payment to someone.

For receiving money into your account, you do not require to use your wallets pin.

So also if an OTP is generated and sent to you by your bank on your registered mobile number, that ideally means that you are going to make a payment. For receiving money, no OTP is required.

33. SIM SWAP:

SIM swap lets you move your number to a replacement SIM if your old SIM is lost, stolen or damaged, or if you need a different size SIM for your new device.

A sim is a veritable key to all your online transactions and is linked to

your banks and all your apps as well.

This fraud displays human weakness which justifies this statement, 'When ones Greed overpower ones Need', one may end up loosing something in bargain.

In order to avail the benefits of 5G connection meant only for privileged few as projected by the criminal, Arpitha fell for that bait/trap and shut her mobile for a couple of hours. The fraud was committed within that time and a new sim with forged documents was procured by the criminals. Naturally when criminal have the newly procured sim, all related and linked activities can be controlled by the criminal as the original sim is blocked. A criminal can gain unauthorised access in an authorised manner due to the new sim that's available with him.

Practically all accounts (banks, social media, apps, email etc) can be accessed and used by the criminals post initiation of 'reset password or pins'.

Despite users adopting best practices for information security, this modus operandi defeats all those purposes.

'Due Diligence' needs to adhered to by these mobile service providers before blocking the original sim and issuing a duplicate or new sim and verification should be done with the sim owner before processing any request. Time and again authorities have lambasted the acts of mobile service providers but SIM cards are yet being issued without proper verification.

Control on WhatsApp also can be initiated because now the 6 digit verification code will be sent to the new sim which the criminals have.

Sim Swap also can be initiated through IVR (Interactive Voice Response) facilities that the mobile service providers use for services. The sim owner is asked to key in digits that will allow Sim Swap through the use of IVRs and thus they loose control over their sim.

34. CRYPTOJACKING

Cryptojacking is the unauthorized use of someone else's computer to mine cryptocurrency. The unsuspecting victim's system may get compromised by clicking on malicious links or by infecting a website or online ad that may be loaded in victims browser with execution codes.

These crypto mining activities happen in background n hence are in a stealth mode.

Cryptojacking allows the infected machines to work for the hacker to mine cryptocurrency.

Raid consumption of power or electricity, excessive use of RAM and CPUs compared to regular usage are symptomatic and indicators that mining may be happening in the background.

Preventions:

Not clicking on links in an email or SMS originating from unknown source. Keeping an eye on processing speed of the system and also on rising electricity bills.

Install an ad-blocking or anti-cryptomining extension on web browsers.

Keep your web filtering tools up to date.

Use anti malware protection that is capable of detecting known crypto miners. Many of the anti malware vendors have added crypto miner detection to their products.

Use a mobile device management (MDM) solution to better control what's on users' devices.

35. VIDEO CONFERENCE SCAM

Preventions:

Neither host nor attendees of such meetings should share the meeting credentials in public or unknown forms.

Enable file sharing, screen sharing, video and audio communication mode and session recording option to required set of meeting participants and not all meeting participants.

In case if the number of meeting participants is high, ensure to provide a standard naming method to easily identify and avoid unwanted people from getting into the meeting.

In case of back to back meeting's enable waiting room to keep the meeting sessions separated and thereby avoid participants from entering into any session not meant for them.

36. KIDS MOBILE PHONE:

Due to pandemic, we have all been introduced to a new concept of working ie. Work From Home and so also children have to attend online lectures arranged by their schools.

This culture has forced quite a few families to share their device's, mostly mobiles, with their immediate family members for logging on to internet to attend meetings, transact business, do online banking and also children use these devices for attending online classes. After a point of time, children tend to deviate from their studies and start playing online games that give them enjoyment and thrill. The games are designed to be played for free for certain time by the providers and then once a child gets addicted, he/she would want to continue by paying for playing such games.

These games offer the winner points, stars, coins etc that could be won or bought and used to play further advance levels of those games, also would make the winner eligible to play other new games. Most of the parents have their debit/credit cards or wallets linked directly to their online bank accounts which makes it easier for a child to make payments using those links and because they have the control on the mobiles at that time, they would get the OTP for those transactions which they would smartly delete from logs after use.

Only when the parents get a bill or a bank statement, they would come to know their children's deeds.

Preventions:

Do not keep your banks accounts linked to debit/credit cards or wallets.

Opt the features of 'enable or disable' available on your devices very meticulously.

Disable features available on your cards to make international transactions and also disable it for use on POS machines (Point Of Sale) or ATM machines outside India.

Do use parental control software's and privacy settings available on Android/IOS devices.

Parents may prohibit/restrict access to particular sites by setting up filters on their devices.

Apart from virtual security, human surveillance and checks & balances should be adopted to control child's activity.

37. SMART HOMES

Ensure that you do not share the device credentials with strangers.

Always ensure to change the default device credentials.

Device firmware needs to be updated to latest versions.

Hidden cameras in bulbs etc could breach privacy of the user who would be unaware of such a crime being committed against them.

Buy products from trusted sources/platforms/portals/dealers to avoid commission of such crimes.

Privacy is a Fundamental Right and is an integral part of the right to life and liberty which is guaranteed under the Constitution.

38. MICRO LOAN

Also known as App based instant-loan or online-lending firms through which small amounts of loans are provided for short term without documents or verification of the borrower and involves high or exorbitant interest rates that are payable.

In December 2020, 3 centres in Hyderabad who had employed nearly 600 tele-callers were raided, these companies took instructions from their heads in Jakarta.

In a swift action, the police of Hyderabad and Cyberabad arrested 17 people, including several heads of app-based instant loan companies, for their role in lending money at a high interest rate and harassing the defaulters through coercive methods.

Tele-callers were used to persuade, harass and intimidate loan defaulters at various stages.

Loan collection agents or even rowdy recovery agents were sent to threaten, bully, manhandle or insult the defaulters.

Amongst others who were arrested, a CEO of an app-based instant loan company was arrested too for 'illegal' operation and cheating borrowers.

In Hyderabad, in a case of harassment by micro loan app organisers, a 28 year old techie died by suicide. When he could not repay the loan, they began harassing him and his family members by demanding repayment and even circulated his pictures and details to all his contacts, branding him as a fraud. He could not endure the humiliation and thus ended his life.

When you apply for such loans, they ask you to install their app as it is an app based instant-loan that is being offered.

Once you install, the app asks for certain permissions and in the guise of doing so, they gain access to lots of information in the background.

The app companies also collect sensitive data such as contacts, photos,

locations and phone memory from the mobile phones of the customers and are used to defame or blackmail the customers to get the repayment. Failing to repay will encourage these providers of loans to defame the defaulter by calling up his contacts, friends, families and also post defamatory statements on their social media platforms.

Preventions:

Never download personal loan apps which are unauthorised and always check users rating and review before downloading. Before signing or accepting the terms of the loan, check your EMI using a personal loan EMI calculator and compare it with the EMI amount given by the lender.

These loan providers are not registered with the RBI.

The App may be unverified and fake.

Terms & Conditions may be vague or misleading.

They do not verify borrowers credentials and asks for processing fees before disbursement of the loan amount.

Customers should not be lured by scams and instead should opt for well-known and reputed financial institutions to ensure that they are not a victim of personal loan scams.

39. BLUESNARFING

Preventions:

Always keep the Bluetooth of your devices in 'Switched Off' mode when not required.

In case of frequent usage of the Bluetooth, manually configure the discovery of your Bluetooth device so that the in other nearby Bluetooth devices your device name is not exhibited.

Keep your Bluetooth software's and drivers updated.

Bluetooth device should be titled in a way that would not reveal your identity.

Ensure to verify every incoming request on your bluetooth device rather than accepting all incoming requests.

40. STOLEN PHONE

Remember: Our cell phone has become as important as other cells in our body.

Upon realising that either you have misplaced your cell phone, forgot your phone or maybe it got stolen, there are a few actions that one needs to take.

Firstly Block you SIM card.

Inform the local police, in case your phone is lost, forgotten or misplaced, the police will issue a Loss Certificate mentioning relevant details of your cell phone.

If the phone has been stolen and if there are enough proofs and evidence to that fact, the police will register an FIR of Theft.

On your phone, always keep the Phone Finder facility 'On', so in case of above mentioned circumstances, you may be able to locate your device by logging into your computer and using the app you may be able to track down where your phone is currently located. Though accuracy differs when it comes to location finding and not all phones are to be found by such technology easily.

The other way is to use your computer and remotely delete data or block access to your phone.

Approaching the police and informing them is required to absolve yourself from any liabilities originating from that device once it was out of your possession.

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 with regards to 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.

NOTE FROM A POLICE OFFICER

By Yashavantha Kumar K.N, DySP

1. Steps to secure home wifi

Wifi hacking is also one of the attacks which come under wireless hacking. What happens here is that the information you share over your wifi could be captured, interpreted, and modified

Sender A: " hello how are you " over a wifi network

Now if the wifi is not secure an attacker could see the message and also could modify the message

How to secure:

- 1. Change the default Configuration:** Whenever we buy a wifi device it has a default username and password which will be common for everyone. So once we have the device we have to change the username and password and keep it unique. if default attackers can use it and get into your wifi routers
- 2. Configure Encryption:** Wifi routers purchased from vendors, by default will have network encryption default, This has to be enabled by the user. use WPA2 which is the most recommended encryption standard.
- 3. Disable Broadcasting feature:** This feature is usually used on public wifi networks, Enabling these in-home networks could increase the attack surface so disabling broadcasting is a better option.
- 4. Check for router updates:** Whenever there are a loophole in the system the vendor updates and releases patches, So make sure your router software is up to date.
- 5. Use VPN for remote access:** While remotely accessing your network make sure VPN is used so that your communication is tunneled and additional encryption is established.

2. How to Enable parental controls in Android

Parental controls permit you to manage what your children look out on search engines. Parents have control over what could be downloaded, viewed on google play store (Android Devices) based on the maturity and age- restrictions.

Steps to Enable parental Control

- ▶ In Apps , Open Google Play Store .
- ▶ On the top right find your profile icon and click on it
(Circle shaped icon)
- ▶ Tap on the option settings
- ▶ Click on Family , Select Parental Control
- ▶ Turn off Parental Control.Once you turn on you will be asked to enter a key through which you will be able to change the parental controls.
- ▶ Select the age restrictions for Apps & games , Films Separately .

3. How to Enable Parental Controls in IOS

Parental controls permit you to manage what your children look out on search engines. Parents have control over what could be downloaded, viewed based on the maturity and age- restrictions .

Steps to Enable parental Control

(Multiple times passcode might be asked)

- ▶ Click on settings and tap Screen Time.
- ▶ Tap Continue, then choose "This is My [Device]" or "This is My Child's [Device]."Create a passcode to protect the changes made or to modify it later
- ▶ Tap and turn on Content and Privacy Restrictions
- ▶ Tap iTunes & App Store Purchases. To prevent your child from deleting or downloading apps .
- ▶ Click on allowed apps option , To have restriction on apps your child is supposed to use

- ▶ Tap on content restrictions and restrict the content which is not necessary
- ▶ Under the same category you can also select web content and select limit adult sites .
- ▶ Under this category you can control siri web search and Game control features.

4. Best Antivirus Apps for Mobile and Laptop

Antivirus software is designed to detect, prevent and take action against malicious software in your computer, including viruses, It is a part of good security strategy.

▶ For Mobile devices (Available for both free and Paid Subscription)

1. Avira
2. Avast Antivirus
3. AVG Antivirus
4. Bitdefender Free Antivirus
5. Kaspersky Mobile Antivirus
6. McAfee
7. Norton
8. 360 Security

▶ For laptop or desktop

1. McAfee AntiVirus
2. Norton AntiVirus
3. Kaspersky Anti-Virus
4. Bitdefender Antivirus Plus

5. How to file a complaint regarding a cyber crime

Offline Mode: Cybercrime can be registered through an FIR in the nearest local police station, Cybercrime will be considered irrespective of the jurisdiction.

Online Mode:

1. Visit "<https://cybercrime.gov.in/> and click on file a complaint button
2. Accept the terms and conditions.
3. The complainant will not have to provide any personal information and the complaint will be registered anonymously.
4. Required information :

Incidental details: Category of the cybercrime, Date and time of the incident, State and district, Platform where the incident occurred, Upload evidence, Suspect's details : Suspect name, Suspect's identity

6. Details to preserve while complaining about Email received.

If a user comes across a mail which looks suspicious or if the user feels the mail is inappropriate it is recommended to register a complaint .

Details to preserve .

1. The moment you receive the mail forward the mail to your other personal ID or someone's mail you trust. So the content of the mail is safe with us.
2. In specific note down the senders email id, Approximate date and time, Attachments if any (Only in sandbox)
3. Check the forwarding which has happened with respect to the mail received.
4. Bills if any transaction has occurred.

7. Details to preserve regarding messages on social media messenger.

Social Media upholds one of the highest attacks surfaces. If any of the users feels threatened on social media , with respect to content , messages , comments etc . Preserve the following details.

Details to preserve:

1. Any social media platforms for that concern if you feel there is any inappropriate content have the snapshot of the content and keep it safely.

2. Note down the username, email id (If available)
3. Approximate date and time of the event .
4. Also keep track of previous conversations or interactions with the attacker.

8. What to do if a fake profile is created

Fake profile also known as impersonating on social media is increasing exponentially in today's generation for various reasons ,

Steps to be followed if impersonated :

Instagram :

1. Find the account which is pretending to be your account on instagra, Visit the profile .
2. Click on the three dots on the top corner and choose a report , You can ask your trusted people to report that account .
3. Reporting can also be done at web portal of Instagram help centre : <https://help.instagram.com/contact/636276399721841>
4. On the web portal you will be asked to provide your official ID proof to verify the report.

Facebook :

1. Find the account which is pretending to be your account on Facebook, Visit the profile .
2. Click on the three dots on the top corner and choose a report , You can ask your trusted people to report that account .
3. Reporting can also be done at web portal of Facebook help centre under the category Report an imposter account <https://www.facebook.com/help/contact/169486816475808>

9. Things to know before flying a Drone

Any person purchasing or flying drones should follow the guidelines provided by India's Ministry of Civil Aviation.

1. There are mainly 3 categories of drones :

- ▶ **Nano drones** : These drones weigh less than or equal to 250 grams, No license and or permit is required.

- ▶ **Micro or Small Drones**: These drones weigh more than 250 grams and less than 25 kg , They have to follow UAOP-1 and DGCA guidelines

- ▶ **Medium and Large Drones**: Drones weighing more than 25 kg should follow UAOP-2 and DGCA guidelines , Prior clearance from air traffic and air defence control must be taken.

- ▶ **Micro Drone** : Maximum Height allowed - 60 meters ,
Max Speed - 25 m/s

- ▶ **Small drone** : Maximum Height allowed - 120 meters ,
Max Speed - 25 m/s

Guidelines :

All drone operations should take place only after prior permission has been received for a flight or series of flights through the Digital Sky online platform.

A drone pilot is liable for the protection of any data gathered during a drone operation.

Restricted Zones :

- ▶ Within a distance of 5 km from the perimeter of international airports at Mumbai, Delhi, Chennai, Kolkata, Bengaluru, and Hyderabad
- ▶ Within a distance of 3 km from the perimeter of any civil, private, or defense airports
- ▶ Within 25 km from the international border which includes Line of Control (LoC), Line of Actual Control (LAC), and Actual Ground Position Line (AGPL)
- ▶ Within 3 km from the perimeter of military installations/facilities without clearance

- ▶ Within 5 km radius from Vijay Chowk in Delhi
- ▶ Within 2 km from the perimeter of strategic locations/vital installations notified by the Ministry of Home Affairs, unless clearance is obtained
- ▶ Within a 3 km radius of State Secretariat Complex in State Capitals
- ▶ Beyond 500 mt (horizontal) into the sea from the coastline, provided the location of the ground station is on a fixed platform on land

10. Safety tips while using smart devices

Every device is smart nowadays. When said smart , they are connected to the internet ,and if they are connected to the internet they are hackable .

Safety tips :

1. Keep very strong and Unique passwords for all your devices.
(Do not use the same passwords).
2. Use network encryption enabled wifi devices.
3. Use trusted service providers to purchase your smart devices.
4. Keep all your devices' firmware uptodate.
5. Change default usernames and Passwords of your device .
6. Default the unnecessary features such as remote access.
7. Enable two-factor authentication , (Can use Google Authenticator).

11. TAKE THE ONLINE PRIVACY TEST

The first step to taking control is a privacy check-up. Follow these instructions now, and don't panic if you find something online you didn't expect:

1. Google your name using quotation marks, like "Reena Suvarna" (and be sure to check the Images tab).
2. Google your phone number.
3. Google your home address.
4. Google your PAN or AADHAR.
5. Do a Google reverse image search of your most-recently shared photos.

Don't blame yourself for what companies like Facebook, LinkedIn, Google, online advertising companies, and data brokers have done to your privacy. And don't panic if you see something you didn't realize was public: what's online doesn't have to stay visible forever. You can send a request to the website administrator to take down the content which you feel should not be present. You may contact us for any assistance.

12. EIGHT PRIVACY TIPS TO USE RIGHT NOW

Every three months, do a privacy check-up that includes searching for your name, phone number, and address, as well as online accounts such as Facebook, Twitter, Google, and your bank. But you can take some actions immediately to make yourself safer online and, hopefully, improve what you see in those check-ups.

1. Use different email addresses for different online accounts. You can set them up to forward email to the address you actually check.
2. View your Facebook, LinkedIn, and Google+ profiles as someone else, and then adjust the privacy settings.
3. Tape over your webcam. This is very important. Or invest in a camera cover.
4. Activate the password lock on your phone, laptop, and tablet.
5. Never sign in on someone else's phone, computer, or tablet.
6. Use VPN. Preferably, a paid version.
7. Consider getting a post office box that you can use in place of your home address to minimize the risk of identity theft, stalking, and other dangers.
8. Install two or three anti tracking plug-ins and extensions : in your browser, such as AdBlock Plus, Disconnect, Abine's Blur, or Ghostery.

If you want to be extra vigilant or if you have known enemies online, you can also set up a Google Custom Alert at <http://google.com/alerts/>.

When you do, you'll get an email notification whenever your name, email address, or phone number is added to Google's searched sites. Note that Google Alerts sends you only the newly indexed results for your search since the last time it checked, not every result there is. You can set up as many alerts as you like, and enter multiple words for each search. Try to use specific search terms so you don't end up with frustratingly general results. To search for an exact phrase, put quotes around your words (like "Kavita Kariappa"), and finish up by selecting the areas you want Google to cover (News, Blogs, and so on) and how often you want the results delivered. Once you're done, bookmark the Google Alerts page so you can go back and manage your Alerts or edit them to work better for you.

13. What To Do When You've Been Attacked

There are two main ways you can be the victim of malicious hacking: you can be personally targeted, or you can be the victim of a company that follows bad security practices.

NOTE To see if your information was released in a recent breach of a company's website, visit <http://www.haveibeenpwned.com/>.

If you think your accounts have been attacked, try to access those accounts. If you're able to log in, reset the passwords if possible, and check all settings carefully in case an attacker added a forwarding address for all of your email or changed your security questions. Check everything.

In particular, if your email account is attacked, follow these steps:

- 1.** Change your password.
- 2.** Change your username if possible.
- 3.** Look through your inbox for unusual activity.
- 4.** Check sent email for suspicious activity, and see what you find in the Trash.
- 5.** See if any users or email addresses have been added to the account and delete any you don't recognize.

6. Look for email forwarding. If you didn't turn it on, turn it off.
7. Check every single setting. If you're not sure what a particular setting means, search for it online. Also look for settings that just look wrong or out of place.
8. If any of your contacts have been sent emails that were not from you, contact them immediately. Warn them that your account has been compromised and not to respond to or click anything in those emails. Let them know too that you have the situation under control.

Follow any relevant steps in the list above for all of the accounts you can access. You may still be locked out of some accounts at this point, but don't panic. You can get them back.

14. Leaked Password

Search online and you'll find long lists of things to do to help make your passwords stronger and attack-proof. If you decide to use a password manager, these great little apps can generate really strong passwords for you whenever you need one. You can also use password generators on trusted websites, such as LastPass (<http://lastpass.com/generatepassword.php>) or Norton (<http://identitysafe.norton.com/password-generator/>).

Follow these rules and you'll get better passwords:

1. Make strong passwords that are at least 12 to 16 characters long.
2. Don't use pet or family names.
3. Don't use your address, Social Security number, birth date, or other personal information.
4. Never recycle or reuse a password-not even once.
5. Change your passwords every 10 weeks to 90 days.
6. Don't let Chrome, Firefox, Safari, or any other browser save passwords for you.

7. Use password phrases (usually six or more words long) for the best security.
8. Include capital letters, numbers, and symbols if the app or site allows it.

Once you've created and saved complex passwords for every site, protect them:

Block shoulder surfing by covering your screen as you enter a password and making sure that no one's observing you.

1. Don't tell anyone your password.
2. Create passwords that are hard to guess.
3. Password protects your phone, tablets, phablets, and computers.
4. Use a password manager.

Password managers like LastPass and 1Password save all of your passwords safely in a vault and encrypt everything. That way, you have them all in one place, no one can accidentally discover them, and you can make really complicated passwords, because the manager will keep track of them (and remember them) for you. You use one master password to other accounts; otherwise an attacker could use that connection to get into those accounts.

15. Recover Your Accounts and Data

Contact websites for which you're unable to reset passwords, and follow their account-recovery processes. Many, like Twitter and Google, will have online forms you can fill out or other procedures to follow when you've been locked out of your account.

For example, Google will ask you questions that only you can answer, like which five people you email most often. After a day or so, you should receive an email that sends you to a page where you have to answer more questions about your Google account, such as the names of your folders, when you started using different Google services, and so on.

Getting your Google account back can take at least 48 hours, often longer.

Google may not be known for customer service, and neither is Yahoo!, Hotmail, or any other "free" online business. But you'll have to put up with them to get your accounts back, and here's a short list of forms and phone numbers to get you started. (For help finding direct phone numbers that may save you a ton of time, check out <http://gethuman.com/>.)

1. Amazon: Use Help Contact Us.
2. Apple: Reset your Apple ID password at <http://iforgot.apple.com/password/verify/appleid/>, or find your Apple ID at <http://iforgot.apple.com/appleid/>.
3. eBay: Call 1.866.961.9253. Tell them you'd like to talk about "Account-someone has used your account."
4. Facebook: <http://facebook.com/hacked/>
5. Google: <http://google.com/accounts/recovery/>
6. Microsoft (Outlook, Xbox, Hotmail, and so on): [http:// account.live.com/acsrf/](http://account.live.com/acsrf/)
7. PayPal: 1.888.221.1161 (Outside the United States, call 1.402.935.2050.)
8. Twitter: <http://support.twitter.com/forms/hacked/>
9. Yahoo!: <http://help.yahoo.com/kb/helpcentral/> or 1.800.318.0612

You'll have to look hard to find support for some websites, and others may have nothing to help you. If you don't see what you need in the list here, search online for "[website] account verification form" or "[website] account hacked," or go to the website's help or contact page.

25 POPULAR CYBER ATTACKS

By Dr. Ananth Prabhu G

Difficulty Level : Medium

1. Cross-site scripting (XSS) : This is a type of computer security vulnerability typically found in web application makes it possible for attackers to inject malicious code (e.g. JavaScript's) into the victim's web browser. This malicious code is used by the attackers to steal the victim's credentials, such as cookies. The access control policies (i.e., the same origin policy) employed by the browser to protect those credentials can be bypassed by exploiting the XSS vulnerability. This kind of vulnerabilities have been exploited to craft powerful phishing attacks and browser exploits.

2. SQL injection : The SQL injection attack is one of the most common attacks on web applications. It is a code injection technique that exploits the vulnerabilities in the interface between web applications and database servers. The vulnerability is present when user's inputs are not correctly checked within the web applications before being sent to the back-end database servers. Many web applications take inputs from users, and then use these inputs to construct SQL queries, so the web applications can get information from the database. Web applications also use SQL queries to store information in the database. These are common practices in the development of web applications. When SQL queries are not carefully constructed, SQL injection vulnerabilities can occur.

3. Buffer Overflow Attack : The memory storage regions that temporarily hold data while it is being transferred from one location to another are known as Buffers. A buffer overflow (or buffer overrun) occurs when the volume of data exceeds the storage capacity of the memory

buffer, which results in the program attempting to write the data to the buffer to overwrite adjacent memory locations making it vulnerable. This vulnerability arises due to the mixing of the storage for data (e.g. buffers) and the storage for controls (e.g. return addresses): an overflow in the data part can affect the control flow of the program, because an overflow can change the return address. Such vulnerability can be utilized by a malicious user to alter the flow control of the program, even execute arbitrary pieces of code. Buffer overflows can affect all types of software. They typically result from malformed inputs or failure to allocate enough space for the buffer. If the transaction overwrites executable code, it can cause the program to behave unpredictably and generate incorrect results, memory access errors, or crashes.

4. Sniffing : The practice or technique of monitoring, gathering, capturing, and logging some or all data packets passing through a given computer network is called sniffing or packet sniffing. A packet sniffer is composed of two parts namely, a network adapter and software that is used by a network to observe or troubleshoot network traffic. These sniffers are used by attackers to seize data packets that contain valuable information and analyze the network traffic. Sniffing is categorized into active sniffing and passive sniffing. The sniffing in which there is the constant activity by the attacker to obtain information and sniff the traffic from the switch network is called Active sniffing. In passive sniffing, the attacker is hidden and sniffs through the hub.

5. Spoofing : When an attacker masquerades as an authentic user or as a device to secure something beneficial or crucial information for their gain is called spoofing. There are various kinds of spoofing such as website spoofing, IP spoofing and E-mail spoofing. Other common methods include ARP spoofing attacks and DNS server spoofing attacks. An E-mail spoofing targets the user whereas, IP spoofing is predominantly

targeted at a network.

In an IP spoofing attack, the attacker attempts to obtain illicit and illegal access to a network through messages with a bogus or spoofed IP address to deceive and show it off as a message from a trusted source. This is achieved by using a genuine host's IP address and varying the packet headers led from their personal system to mimic it as an original and a trusted computer's IP address.

6. ARP Cache Poisoning : The ARP (Address Resolution Protocol) is a very simple protocol. It is a communication protocol used for discovering the link layer address, such as a MAC address, given an IP address and it does not implement any security measures. The ARP cache poisoning attack is a common attack against the ARP protocol. Under such an attack, attackers can fool the victim into accepting forged IP-to-MAC mappings. This can cause the victim's packets to be redirected to the computer with the forged MAC address.

7.Meltdown Attack : The Meltdown vulnerability represents a special genre of vulnerabilities in the design of CPUs. The vulnerabilities allow a user-level program to read data stored inside the kernel memory. Such access is not allowed by the hardware protection mechanism implemented in most CPUs, but a vulnerability exists in the design of these CPUs that makes it possible to defeat the hardware protection. Because the flaw exists in the hardware, it is very difficult to fundamentally fix the problem, unless we change the CPUs in our computers. These were discovered in 2017 and publicly disclosed in January 2018. The Meltdown exploits critical vulnerabilities existing in many modern processors, including those from Intel and ARM. Along with the Spectre vulnerability, they provide an invaluable lesson for security education.

8. Spectre Attack : Discovered in 2017 and publicly disclosed in January 2018, the Spectre attack exploits critical vulnerabilities existing in many modern processors, including those from Intel, AMD, and ARM. The vulnerabilities allow a program to break inter-process and intra-process isolation making it possible for the malicious program to read the data from the area that is not accessible to it. Such access is not allowed by the hardware protection mechanism (for inter-process isolation) or software protection mechanism (for intra-process isolation), but a vulnerability exists in the design of CPUs that makes it possible to defeat the protections. It is very difficult to fundamentally fix the problem because the flaw exists in the hardware, unless we change the CPUs in our computers.

9. DNS Rebinding Attack : DNS rebinding is a commonly used form of computer attack by the method of manipulating resolution of domain names. The attacker registers a domain (such as attacker.com) and delegates it to a DNS server that is under the attacker's control. The server is configured to respond with a very short time to live (TTL) record, preventing the DNS response from being cached. When the victim browses to the malicious domain, the attacker's DNS server first responds with the IP address of a server hosting the malicious client-side code. For instance, they could point the victim's browser to a website that contains malicious JavaScript or Flash scripts that are intended to execute on the victim's computer.

The malicious client-side code makes additional access to the original domain name (such as attacker.com). These are permitted by the same-origin policy. However, when the victim's browser runs the script, it makes a new DNS request for the domain, and the attacker replies with a new IP address. For instance, they could reply with an internal IP address or the IP address of a target somewhere else on the Internet.

"Pharming" is a variety of attack type in which the attacker hijacks

the network address (either IP address or domain name) of a target application for the purpose of intercepting all end-user interaction with the target application. The attacker can then make use of this interception to compromise sensitive information or distribute malware, including back doors and Trojans.

10. BGP Hijacking Attack : The BGP (Border Gateway Protocol) is used to direct traffic across the Internet, allowing networks to exchange "reachability information" to facilitate reaching other networks. BGP hijacking is a form of application-layer DDoS attack that allows an attacker to impersonate a network, using a legitimate network prefix as their own. When this "impersonated" information is accepted by other networks, traffic is inadvertently forwarded to the attacker instead of its proper destination.

11. Botnet Attack : An Internet bot is a software application that runs automated tasks over the internet. Tasks run by bots are typically simple and performed at a much higher rate compared to human Internet activity. Some bots are legitimate—for example, Googlebot is an application used by Google to crawl the Internet and index it for search. Other bots are malicious—for example, bots used to automatically scan websites for software vulnerabilities and execute simple attack patterns. A botnet is a collection of internet-connected devices infected by malware that allow hackers to control them. Botnet owners can have access to several thousand computers at a time and can command them to carry out malicious activities.

Cyber criminals use botnets to instigate botnet attacks, which include malicious activities such as data theft, credentials leaks, unauthorized access and DDoS attacks. They initially gain access to these devices by using special Trojan viruses to attack the computers' security systems. Then by implementing command and control software, they carry out

malicious activities on a large scale. These activities can be automated to encourage as many simultaneous attacks as possible.

Different types of botnet attacks can include:

- ▶ Distributed Denial of Service (DDoS) attacks that cause unplanned application downtime
- ▶ Validating lists of leaked credentials (credential-stuffing attacks) leading to account takeovers
- ▶ Web application attacks to steal data
- ▶ Providing an attacker access to a device and its connection to a network.

12. TCP SYN flood Attack : (a.k.a. SYN flood) is a type of Distributed Denial of Service (DDoS) attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.

Essentially SYN flood DDoS, the offender sends TCP connection requests faster than the targeted machine can process them, causing network saturation, often using a fake IP address. The server, unaware of the attack, receives multiple, apparently legitimate requests to establish communication. It responds to each attempt with a SYN-ACK packet from each open port.

During this time, the server cannot close down the connection by sending an RST packet, and the connection stays open. Before the connection can time out, another SYN packet will arrive. This leaves an increasingly large number of connections half-open – and indeed SYN flood attacks are also referred to as “half-open” attacks. Eventually, as the server's connection overflow tables fill, service to legitimate clients will be denied and the server may even malfunction or crash.

13. Phishing Attack : Phishing is a type of social engineering attack. It is used to steal user data, including login credentials and credit card

numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. An attack can have devastating results.

Phishing is often used to gain a foothold in corporate or governmental networks as a part of a larger attack, such as an advanced persistent threat (APT) event. In this scenario, employees are compromised to bypass security perimeters, distribute malware inside a closed environment, or gain privileged access to secured data.

For individuals, this includes unauthorized purchases, the stealing of funds, or identity theft.

14. Backdoor Attack : Backdoor installation is achieved by taking advantage of vulnerable components in a web application. It is a malware type that negates normal authentication procedures to access a system. As a result, remote access is granted to resources within an application, such as databases and file servers, giving perpetrators the ability to remotely issue system commands and update malware. Once installed, detection is difficult as files tend to be highly obfuscated.

Web Server backdoors are used for a number of malicious activities, including:

- ▶ Data theft
- ▶ Website defacing
- ▶ Server hijacking
- ▶ The launching of distributed denial of service (DDoS) attacks
- ▶ Infecting website visitors (watering hole attacks)
- ▶ Advanced persistent threat (APT) assaults

15. Drive By Download : In a Drive-by-Download attack, the web application is tampered (i.e. injected with HTML code) that instructs a visitor's browser to download malware located in an attacker's controlled server. Usually the malware is Trojan horse software that takes control of the victim's machine, making it part of a larger botnet. Most often innocent victims are unaware of the background download operation since tampering is not visually apparent to visitors. If any warning appears it is usually dismissed as victims believe it to be part of the original application.

16. Site Scanning : It is the initial phase of any attack on Web applications. It is also known as probing. Target Web sites are scanned for known vulnerabilities in infrastructure software (such as IIS) as well as unknown vulnerabilities in the custom code developed for the specific target application. The attacker gathers information about the structure of the Web application (pages, parameters, etc.) and the supporting infrastructure (operating system, databases, etc.).

First, the attacker detects the operating system installed on the server which is done using automatic tools like nmap, by identifying the Web Server type in the HTTP Request (for example, IIS runs on Windows-based sites) or by guessing according to file extensions. (Usually, Windows-based sites use ".htm" and ".jpg" files, whereas UNIX sites use .html and .jpeg files).

Identifying which Web server runs on the target machine is very useful to the attacker. Knowing the specific type of Web server (and by extension its default configuration), an attacker may try to exploit known vulnerabilities, access sample files and try default user accounts. There are three common ways of detecting the Web server: by using automatic tools such as Nikto, by identifying the Web server type in the HTTP Request, or by guessing according to files suffixes (ASP Pages normally indicate an IIS Server whereas PHP Pages normally indicate

an Apache server).

After analyzing the infrastructure, the entire application can be scanned. Application scanning provides a map of the entire site including: all pages, parameters used by dynamic pages, cookies used by the site and transactions flow. This information leads the attacker to an understanding of the application's authentication, authorization, logic, and transactional mechanisms. This body of information provides the basis of a strategy to attack the target site.

17. Supply Chain Attack : Supply chain attacks can damage organizations, individual departments, or entire industries by targeting and attacking insecure elements of the software supply chain.

Here is an example of a sophisticated supply chain attack:

An attacker discovers large organizations using an open-source component built by a certain group of developers. The attacker identifies a developer who is not actively working on the project and compromises their GitHub account. Using the compromised GitHub account, the attacker commits innocent-looking code to the project, which in fact contains a backdoor. The backdoor is packaged into the next release. When one of the target organizations updates the open-source component to the new, compromised version, they are owned by the attacker.

18. HTTP Parameter Pollution : HTTP Parameter Pollution (HPP) is a Web attack technique that allows an attacker to craft a HTTP request in order to manipulate or retrieve hidden information. This evasion technique is based on splitting an attack vector between multiple instances of a parameter with the same name. Since none of the relevant HTTP RFCs define the semantics of HTTP parameter manipulation, each web application delivery platform may deal with it differently. In particular, some environments process such requests by concatenating

the values taken from all instances of a parameter name within the request. This behavior is abused by the attacker in order to bypass pattern-based security mechanisms.

19. Command Injection : It is a cyber attack that involves executing arbitrary commands on a host operating system (OS). Typically, the threat actor injects the commands by exploiting an application vulnerability, such as insufficient input validation. Command injection takes various forms, including direct execution of shell commands, injecting malicious files into a server's runtime environment, and exploiting vulnerabilities in configuration files, such as XML external entities (XXE).

For example, a threat actor can use insecure transmissions of user data, such as cookies and forms, to inject a command into the system shell on a web server. The attacker can then leverage the privileges of the vulnerable application to compromise the server.

Command Injection vs Code Injection

Command injection typically involves executing commands in a system shell or other parts of the environment. The attacker extends the default functionality of a vulnerable application, causing it to pass commands to the system shell, without needing to inject malicious code. In many cases, command injection gives the attacker greater control over the target system.

Code injection is a generic term for any type of attack that involves an injection of code interpreted/executed by an application. It is made possible by a lack of proper input/output data validation. This type of attack takes advantage of mishandling of untrusted data inputs.

A key limitation of code injection attacks is that they are confined to the application or system they target. If an attacker can inject PHP code into an application and execute it, malicious code will be limited by PHP functionality and permissions granted to PHP on the host machine.

20. Google Hacking : It involves an attacker submitting queries to Google's search engine with the intention of finding sensitive information residing on Web pages that have been indexed by Google or finding sensitive information with respect to vulnerabilities in applications indexed by Google.

As search engines crawl their way through web applications with the intent of indexing their content they stumble upon sensitive information. The more robust and sophisticated these crawlers become the more coverage they get of a server exposed to the web and any information, accidentally accessible through a web server or a web application will quickly be picked up by a search engine. Sensitive information may be on the personal level such as security numbers and credit card numbers and passwords, but it also encompasses technical and corporate sensitive information such as client files, the company's human resources files, or secret formulas put accidentally on a server. In addition to this the search engine picks up information that may expose application vulnerabilities such as error messages contained in the server's reply to the search engine's request, directory listings and so on. All this sensitive information is available for anyone to see through the appropriate search terms.

Google Hacking is by no means confined to searching through the Google search engine but can be applied to any of the major search engines including Yahoo!, Ask.com, LiveSearch and others.

21. Website Defacement Attack : Most websites and web applications store data in environment or configuration files, that affects the content displayed on the website, or specifies where templates and page content is located. Unexpected changes to these files can mean a security compromise and might signal a defacement attack. In this type of an attack malicious parties penetrate a website and replace content on the site with their own messages. The messages can convey

a political or religious message, profanity or other inappropriate content that would embarrass website owners, or a notice that the website has been hacked by a specific hacker group.

Common causes of defacement attacks include:

- ▶ Unauthorized access
- ▶ SQL injection
- ▶ Cross-site scripting (XSS)
- ▶ DNS hijacking
- ▶ Malware infection

22. Fork Bomb Attack : A fork is a system call used in Unix and Linux systems that takes an existing process (a.k.a, a parent) and replicates it, forming a new process (a.k.a, a child). This allows both processes to carry out unique tasks simultaneously.

A fork bomb (also known as a "rabbit virus") is a denial of service (DoS) attack in which the fork system call is recursively used until all system resources execute a command. The system eventually becomes overloaded and is unable to respond to any input.

In a fork bomb attack, self-replicating child processes consume system resources, blocking legitimate programs from running and preventing the creation of new processes. During an attack, keyboard inputs (e.g., logout attempts) are ignored, essentially locking the system.

Because a fork loop consumes CPU and memory, system resources are typically depleted long before an operating system reaches the maximum allowed processes. This results in "kernel panic", i.e., the core operating system (the kernel) cannot cope and crashes.

For the majority of systems, a freeze lasts until a machine is restarted, and often a hard reboot is required to regain control. Data loss is highly likely. Some kernels might have pre-set limits that eventually allow an administrator access to the system.

23. LAND Attack : It is a Layer 4 Denial of Service (DoS) attack. Here the attacker sets the source and destination information of a TCP segment to be the same. A specially crafted TCP SYN packet is created such that the source IP address and port are set to be the same as the destination address and port, which in turn is set to point to an open port on a victim's machine. A vulnerable machine would receive such a message and reply to the destination address effectively sending the packet for reprocessing in an infinite loop. Thus, machine CPU is consumed indefinitely freezing the vulnerable machine, causing a lock up, or even crashing it due to the packet being repeatedly processed by the TCP stack.

24. Web Scraping : Web scraping is used in a variety of digital businesses that rely on data harvesting. It is the process of using bots to extract content and data from a website.

Unlike screen scraping, which only copies pixels displayed onscreen, web scraping extracts underlying HTML code, and, with it, data stored in a database. The scraper can then replicate entire website content elsewhere.

Scraper tools and bots

Web scraping tools are software (i.e., bots) programmed to sift through databases and extract information. A variety of bot types are used, many being fully customizable to:

- ▶ Recognize unique HTML site structures
- ▶ Extract and transform content
- ▶ Store scraped data
- ▶ Extract data from APIs
- ▶ Legitimate use cases include:
 - ▶ Search engine bots crawling a site, analyzing its content and then ranking it.
 - ▶ Price comparison sites deploying bots to auto-fetch prices and product

descriptions for allied seller websites.

► Market research companies using scrapers to pull data from forums and social media (e.g., for sentiment analysis).

Web scraping is also used for illegal purposes, including the undercutting of prices and the theft of copyrighted content. An online entity targeted by a scraper can suffer severe financial losses, especially if it's a business strongly relying on competitive pricing models or deals in content distribution.

Since all scraping bots have the same purpose—to access site data—it can be difficult to distinguish between legitimate and malicious bots.

25. Brute Force Attack : A brute force attack involves 'guessing' username and passwords to gain unauthorized access to a system. It is a popular cracking method by some accounts. It accounted for five percent of confirmed security breaches. Brute force is a simple attack method and has a high success rate. Attacker motivation may include stealing information, infecting sites with malware, or disrupting service.

Attackers use applications and scripts as brute force tools. These tools try out numerous password combinations to bypass authentication processes. In other cases, attackers try to access web applications by searching for the right session ID.

While some attackers still perform brute force attacks manually, today almost all brute force attacks today are performed by bots. Attackers have lists of commonly used credentials, or real user credentials, obtained via security breaches or the dark web. Bots systematically attack websites and try these lists of credentials and notify the attacker when they gain access.

Types of Brute Force Attacks

Simple brute force attack—uses a systematic approach to 'guess' that doesn't rely on outside logic.

Hybrid brute force attacks—starts from external logic to determine which

password variation may be most likely to succeed and then continues with the simple approach to try many possible variations.

Dictionary attacks—guesses usernames or passwords using a dictionary of possible strings or phrases.

Rainbow table attacks—a rainbow table is a precomputed table for reversing cryptographic hash functions. It can be used to guess a function up to a certain length consisting of a limited set of characters.

Reverse brute force attack—uses a common password or collection of passwords against many possible usernames. Targets a network of users for which the attackers have previously obtained data.

Credential stuffing—uses previously-known password-username pairs, trying them against multiple websites. Exploits the fact that many users have the same username and password across different systems.

OFFENCES AND RELEVANT PENAL SECTIONS

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

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

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

24	Failure to Block Web sites, when ordered	Section 69A of ITAA 2008 imprisonment up to 7 years and fine	
25	Sending threatening messages by e-mail		Section 506 IPC 2 years or fine or both
25	Word, gesture or act intended to insult the modesty of a woman		Section 509 IPC 1 years or fine or both – IPC as applicable
26	Sending defamatory messages by e-mail		Section 500 IPC 2 years or fine or both
27	Bogus Web sites, cyber frauds	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 419 IPC 3 years imprisonment or fine Section 420 IPC 7 years imprisonment and fine
28	E-mail Spoofing	Section 66C of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC 2 years or fine or both Section 468 IPC 7 years imprisonment and fine
29	Making a false document	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 465 IPC 2 years or fine or both
30	Forgery for purpose of cheating	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section 468 IPC 7 years imprisonment and fine
31	Forgery for purpose of harming reputation	Section 66D of ITAA 2008 3 years imprisonment and fine up to Rupees one lakh	Section. 469 IPC 3 years and fine
32	E-mail Abuse		Sec. 500 IPC 2 years or fine or both
33	Punishment for criminal intimidation		Sec. 506 IPC 2 years or fine or both – if threat be to cause death or grievous hurt, etc. – 7 years or fine or both
34	Criminal intimidation by an anonymous communication		Sec. 507 IPC 2 years along with punishment under section 506 IPC
35	Copyright infringement	Section 66 of ITAA 2008 3 years imprisonment or fine up to Rupees five lakh or both	Sec. 63, 63B Copyrights Act 1957
36	Theft of Computer Hardware		Sec. 379 IPC 3 years imprisonment or fine or both
37	Online Sale of Drugs		NDPS Act
38	Online Sale of Arms		Arms Act

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

GLOSSARY

A

Antivirus

Antivirus software is used to monitor a computer or network, to detect cyber security threats ranging from malicious code to malware. As well as alerting you to the presence of a threat, antivirus programs may also remove or neutralise malicious code.

Artificial Intelligence (AI)

(AI) refers to the simulation of human intelligence in machines that are programmed to think like humans and mimic their actions. Unfortunately, that same technology can be deployed by cybercriminals, which has forced cybersecurity experts to work even harder to stay ahead of the latest attack strategies.

Authentication

The process of verifying the identity or other attributes of a user, process or device.

B

Backdoor

An undocumented, private, or less-detectible way of gaining remote access to a computer, bypassing authentication measures, and obtaining access to plaintext.

Bitcoin

Cryptocurrency, a form of electronic cash created by Satoshi Nakamoto.

Blacklist

A list of entities (users, devices) that are either blocked, denied privileges or access.

Blockchain

A blockchain is a write-only database, dispersed over a network of interconnected computers, that uses cryptography to create a tamperproof public record of transactions. Because blockchain technology is transparent, secure and decentralized, a central actor cannot alter the public record.

Bot

A computer connected to the Internet that has been compromised with malicious logic to undertake activities under the command and control of a remote administrator.

Botnet

A network of infected devices, connected to the Internet, used to commit coordinated cyber attacks without their owner's knowledge.

Breach

The unauthorised access of data, computer systems or networks.

Bring your own device (BYOD)

A strategy or policy whereby an organisation permits employees to use their personal devices for work purposes.

Brute force attack

An attack in which computational power is used to automatically enter a vast quantity of number combinations in order to discover passwords and gain access.

Bug

A relatively minor defect or flaw in an information system or device.

CAPTCHA

A test that distinguishes between robots and humans using a website where you have to “prove you’re human”.

Catfishing

Creating a fake identity on a social network account, usually a dating website, to target a specific victim for deception.

CISO

Acronym for Chief Information Security Officer is a senior-level executive job in a company, in the IT or cyber security department. A CISO's responsibilities include ensuring and maintaining adequate protection for the company's assets and technology, in terms of both strategy and development, to mitigate and manage cyber security risks. CSO (Chief Security Officer) is another name used for the same job.

Cookie

A segment of data sent by an Internet server to the browser that is returned to the browser every time it accesses the server. This is used to identify the user or track their access to the server. Initially, cookies were used to stay logged in but are now commonly used for tracking.

Cryptography

The study of encoding. Also, the use of code/cipher/mathematical techniques to secure data and provide authentication of entities and data.

Cyber attack

Deliberate and malicious attempts to damage, disrupt or gain access to computer systems, networks or devices, via cyber means.

Cyber incident

A breach of a system or service's security policy.

Data breach

The unauthorised movement or disclosure of information, usually to a party outside the organisation.

Data integrity

The quality of data that is complete, intact, and trusted and has not been modified or destroyed in an unauthorized or accidental manner.

Data loss

No longer having data, whether because it has been stolen, deleted, or its location forgotten

Data security

The measures taken to protect confidential data and prevent it from being accidentally or deliberately disclosed, compromised, corrupted or destroyed.

Darkweb

The dark web refers to websites and online content that exists outside the reach of traditional search engines and browsers. This content is hidden by encryption methods (in most cases, these sites use the Tor encryption tool to hide their identity and location) and can only be accessed with specific software, configuration settings or pending approval from their admins. The dark web is known for being a hub for illegal activities (drug and crime transactions, dark hat hacking and so on).

Decryption

The process of deciphering coded text into its original plain form.

Denial of service (DoS)

This is a type of cyber attack that prevents the authorised use of

information system services or resources, or impairs access, usually by overloading the service with requests.

Dictionary attack

Known dictionary words, phrases or common passwords are used by the attacker to gain access to your information system. This is a type of brute force attack.

Digital Signature

A digital signature is a technique used to encrypt and validate the authenticity and integrity of a message, software or digital document. The digital signature is difficult to duplicate by a hacker, that's why it is important in information security.

Distributed denial of service (DDoS)

A denial of service technique where multiple systems are used to perform the attack, overwhelming the service.

Download attack

Malicious software or a virus that is installed on a device without the user's knowledge or consent – sometimes known as a drive-by download.

E

Electronic warfare (EW)

The use of energy, such as radio waves or lasers, to disrupt or disable the enemy's electronics. An example would be frequency jamming to disable communication equipment.

Encode

The use of a code to convert plain text to cipher text.

Encryption

The use of a cipher to protect information, making it unreadable to anyone who doesn't have the key to decode it.

Endpoint

A collective term for internet-capable computer devices connected to a network – for example, modern smartphones, laptops and tablets are all endpoints.

Ethical hacking

The use of hacking techniques for legitimate purposes – i.e. to identify and test cyber security vulnerabilities. The actors in this instance are sometimes referred to as 'white hat hackers'.

Exfiltration

The transfer of information from a system without consent.

Exploit

The act of taking advantage of a vulnerability in an information system. Also used to describe a technique that is used to breach network security.

F

Firewall

A virtual boundary surrounding a network or device that is used to protect it from unwanted access. Can be hardware or software.

G

Gateway

An intermediate system that is the interface between two computer

networks. A gateway can be a server, firewall, router, or other device that enables data to flow through a network.

GDPR

General Data Protection Regulations. European legislation designed to prevent the misuse of data by giving individuals greater control over how their personal information is used online.

H

Hacker

Someone who breaks into computers, systems and networks.

Hashing

Using a mathematical algorithm to disguise a piece of data.

Honeypot (honeynet)

A decoy system or network that serves to attract potential attackers, protecting actual systems by detecting attacks or deflecting them. A good tool for learning about attack styles. Multiple honeypots form a honeynet.

I

Incident

Any breach of the security rules for a system or service. This includes attempts to gain unauthorised access, the unauthorised use of systems for the processing or storing of data, malicious disruption or denial of service, and changes to a system's firmware, software or hardware without the owner's consent.

Incident response plan

A predetermined plan of action to be undertaken in the event of a cyber incident.

Indicator

A signal that a cyber incident may have occurred or is in progress.

Insider threat

A malicious threat to a group or organization that comes from someone within, like an employee, contractor, or business associate, who has insider information regarding the organization's data, computer systems, or security measures.

Internet of things (IoT)

The ability of everyday objects, such as kettles, fridges and televisions, to connect to the internet.

Intrusion Detection System/Intrusion Detection and Prevention (IDS/IDP)

Hardware or software that finds and helps prevent malicious activity on corporate networks.

IP address

Also known as an Internet Protocol address, is the string of numbers used to identify each computer using the internet on a network.

IP spoofing

A tactic used by attackers to supply a false IP address in an attempt to trick the user or a cyber security solution into believing it is a legitimate actor.

J

Jailbreak

The removal of a device's security restrictions, with the intention of installing unofficial apps and making modifications to the system. Typically applied to a mobile phone.

Javascript

A language used to create and control the content on a website, allowing you to program the behavior of web pages to do a specified action.

K

Key

The numerical value used to encrypt and decrypt cipher text.

Keylogger

A type of software or hardware that tracks keystrokes and keyboard events to monitor user activity.

L

Logic bomb

A piece of code that carries a set of secret instructions. It is inserted in a system and triggered by a particular action. The code typically performs a malicious action, such as deleting files.

M

Malicious code

Program code designed for evil. Intended to hurt the confidentiality,

integrity or availability of an information system.

Malvertising

The use of online advertising to deliver malware.

Malware

Short for malicious software. Any viruses, Trojans, worms, code or content that could adversely impact organisations or individuals.

Man-in-the-middle Attack (MitM)

Cyber criminals interpose themselves between the victim and the website the victim is trying to reach, either to harvest the information being transmitted or alter it. Sometimes abbreviated as MITM, MIM, MiM or MITMA.

Mitigation

The steps taken to minimise and address cyber security risks.

Mobile Device Management (MDM)

Mobile device management (MDM) is a type of security software, specifically for monitoring, managing and securing mobile, tablet and other devices, allowing remote administration and management of the device.

N

Netiquette

(short for network etiquette) is a collection of best practices and things to avoid when using the Internet, especially in communities such as forums or online groups. This is more of a set of social conventions that aim to make online interactions constructive, positive and useful. Examples include: posting off-topic, insulting people, sending or posting spam, etc.

Obfuscation

In cyber security, obfuscation is a tactic used to make computer code obscure or unclear, so that humans or certain security programs (such as traditional antivirus) can't understand it. By using obfuscated code, cyber criminals make it more difficult for cyber security specialists to read, analyze and reverse engineer their malware, preventing them from finding a way to block the malware and suppress the threat.

Packet sniffer

Software designed to monitor and record network traffic. It can be used for good or evil – either to run diagnostics and troubleshoot problems, or to snoop in on private data exchanges, such as browsing history, downloads, etc.

Passive attack

Attackers try to gain access to confidential information in order to extract it. Because they're not trying to change the data, this type of attack is more difficult to detect – hence the name 'passive'.

Password sniffing

A technique used to harvest passwords by monitoring or snooping on network traffic to retrieve password data.

Patching

Applying updates (patches) to firmware or software, whether to improve security or enhance performance.

Payload

The element of the malware that performs the malicious action – the cyber security equivalent of the explosive charge of a missile. Usually spoken of in terms of the damaging wreaked.

Penetration testing

A test designed to explore and expose security weaknesses in an information system so that they can be fixed.

Personally Identifiable Information (PII)

The data that enables an individual to be identified.

Pharming

An attack on network infrastructure where a user is redirected to an illegitimate website, despite having entered the right address.

Phishing

Mass emails asking for sensitive information or pushing them to visit a fake website. These emails are generally untargeted.

Proxy server

A go-between a computer and the internet, used to enhance cyber security by preventing attackers from accessing a computer or private network directly.

Q

Quantum computing

A quantum computer can process a vast number of calculations simultaneously. Whereas a classical computer works with ones and zeros, a quantum computer will have the advantage of using ones, zeros and “superpositions” of ones and zeros. Certain difficult tasks

that have long been thought impossible for classical computers will be achieved quickly and efficiently by a quantum computer.

R

Ransomware

Ransomware is a type of malware (malicious software) which encrypts all the data on a PC or mobile device, blocking the data owner's access to it.

ReCAPTCHA

A service from Google that works to protect websites from spam and abuse caused by robots. A user is presented with a Turing test to distinguish them from a robot.

Red team

A group authorised and organised to emulate a potential adversary's attack or exploitation capabilities against an enterprise's cyber security posture.

Redundancy

Additional or alternative systems, sub-systems, assets, or processes that maintain a degree of overall functionality in case of loss or failure of another system, sub-system, asset, or process.

Remote Access Trojan (RAT)

Remote Access Trojans (RATs) use the victim's access permissions and infect computers to give cyber attackers unlimited access to the data on the PC.

Rootkit

A set of software tools with administrator-level access privileges installed on an information system and designed to hide the presence

of the tools, maintain the access privileges, and conceal the activities conducted by the tools

S

Secret key

A cryptographic key that is used for both encryption and decryption, enabling the operation of a symmetric key cryptography scheme.

Security Operations Center (SOC)

A central unit within an organisation that is responsible for monitoring, assessing and defending security issues.

Smishing

Phishing via SMS: mass text messages sent to users asking for sensitive information (eg bank details) or encouraging them to visit a fake website.

Social engineering

Manipulating people into carrying out specific actions or divulging information that is of use to an attacker. Manipulation tactics include lies, psychological tricks, bribes, extortion, impersonation and other type of threats. Social engineering is often used to extract data and gain unauthorised access to information systems, either of single, private users or which belong to organisations.

Software as a service (SaaS)

Describes a business model where consumers access centrally-hosted software applications over the Internet.

Spam

The abuse of electronic messaging systems to indiscriminately send unsolicited bulk messages.

Spear phishing

Spear phishing is a cyber attacks that aims to extract sensitive data from a victim using a very specific and personalised message designed to look like it's from a person the recipient knows and/or trusts.

Spoofing

Faking the sending address of a transmission to gain unauthorised entry into a secure system.

Spyware

Spyware is a type of malware designed to collect and steal the victim's sensitive information, without the victim's knowledge.

SQL injection

This is a tactic that uses code injection to attack applications that are data-driven. The maliciously injected SQL code can perform several actions, including dumping all the data in a database in a location controlled by the attacker. Through this attack, malicious hackers can spoof identities, modify data or tamper with it, disclose confidential data, delete and destroy the data or make it unavailable. They can also take control of the database completely.

SSL / Secure Sockets Layer

This is an encryption method to ensure the safety of the data sent and received from a user to a specific website and back. Encrypting this data transfer ensures that no one can snoop on the transmission and gain access to confidential information, such as card details in the case of online shopping. Legitimate websites use SSL (start with https). Users should avoid inputting their data in websites that don't use SSL.

Steganography

A way of encrypting data, hiding it within text or images, often for malicious intent.

Symmetric key

A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt plain text and decrypt cipher text, or create a message authentication code and to verify the code.

T

Threat analysis

The detailed evaluation of the characteristics of individual threats.

Threat assessment

The product or process of identifying or evaluating entities, actions, or occurrences, whether natural or man-made, that have or indicate the potential to harm life, information, operations, and/or property.

Threat hunting

Cyber threat hunting is the process of proactively searching across networks and endpoints to identify threats that evade existing security controls.

Threat management

There is no silver bullet to prevent 100% of cyber threats. Successful threat management requires a multi-layered approach encompassing prevention, detection, response and recovery.

Threat monitoring

During this process, security audits and other information in this category are gathered, analysed and reviewed to see if certain events in the information system could endanger the system's security. This is a continuous process

Tracking cookie

This type of cookies are places on users' computers during web browsing sessions. Their purpose is to collect data about the user's browsing preferences on a specific website, so they can then deliver targeted advertising or to improve the user's experience on that website by delivering customized information.

Trialware

Software that can only be run for a limited amount of time before it expires.

Trojan horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorisations of a system entity that invokes the program.

Two-factor authentication (2FA)

The use of two different components to verify a user's claimed identity. Also known as multi-factor authentication.

U

Unauthorised access

Any access that violates the stated security policy.

URL injection

A URL (or link) injection is when a cyber criminal creates new pages on a website owned by someone else that contain spam words or links. Sometimes, these pages also contain malicious code that redirects your users to other web pages or makes the website's web server contribute to a DDoS attack. URL injection usually happens because of vulnerabilities in server directories or software used to operate the website, such as an outdated WordPress or plugins.

V

Virtual Private Network (VPN)

An encrypted network often created to allow secure connections for remote users, for example in an organisation with offices in multiple locations.

Virus

Programs that can self-replicate and are designed to infect legitimate software programs or systems. A form of malware.

Visual Hacking

Also called "shoulder surfing" or "screen snooping," visual hacking occurs when someone steals sensitive information or credentials by physically looking at someone's screen. This could involve glancing at a computer monitor or picking up an unattended smartphone or tablet. While there are many security measures designed to combat conventional cyberattacks, visual hacking requires innovative strategies like screen protectors or continuous biometric authentication.

Vulnerability

A weakness, or flaw, in software, a system or process. An attacker may seek to exploit a vulnerability to gain unauthorised access to a system.

W

Wabbits

A wabbit is one of four main classes of malware, among viruses, worms and Trojan horses. It's a form of computer program that repeatedly replicates on the local system. Wabbits can be programmed to have malicious side effects. A fork bomb is an example of a wabbit: it's a form

of DoS attack against a computer that uses the fork function. A fork bomb quickly creates a large number of processes, eventually crashing the system. Wabbits don't attempt to spread to other computers across networks.

Water-holing (watering hole attack)

Setting up a fake website (or compromising a real one) in order to exploit visiting users.

Whaling

Highly targeted phishing attacks (masquerading as a legitimate emails) that are aimed at senior executives.

White team

A group responsible for refereeing an engagement between a Red Team of mock attackers and a Blue Team of actual defenders of information systems.

Whitelist

A list of entities that are considered trustworthy and are granted access or privileges.

Worm

A self-replicating, self-propagating, self-contained program that uses networking mechanisms to spread

X

Xafecopy

Malware particularly found embedded in a variety of mobile apps, most commonly in battery optimizers, without the knowledge or consent of the user, ultimately subscribing the phone to a number of services which charge money directly to the user's mobile phone bill.

XSS Attack

An abbreviation of cross-site scripting, Cross-Site Scripting attacks is a method in which malicious scripts are injected into an otherwise trusted web site. An attacker can use XSS to send a malicious script to an unsuspecting user.

The user's browser has no way to know that the script should not be trusted, and will execute the script since it thinks the script came from a trusted source.

Y

Y2K

Stands for "year 2000". This abbreviation is well known today because of the term "the Y2K problem" or "the millennium bug". The Y2K problem stemmed from fears of computer programs that store year values as two-digits figures—"97" to mean the year 1997, for example—would cause problems as the year 2000 rolls in.

Z

Zero-day

Recently discovered vulnerabilities (or bugs), not yet known to vendors or antivirus companies, that hackers can exploit.

Zombie

A zombie computer is one connected to the Internet that, in appearance, is performing normally, but can be controlled by a hacker with remote access to it who sends commands through an open port. Zombies are mostly used to perform malicious tasks, such as spreading spam or other infected data to other computers, or launching DoS (Denial of Service) attacks, with the owner being unaware of it.



HELPLINE NUMBERS

Cyber Helpline : 155260 (Delhi & Rajasthan) 24x7

National Emergency Number : 112

Police : 100

Women Helpline : 1091

Mental Health Helpline : 1800-599-0019

iCall Suicide Helpline : 9152987821

Fire : 101

Ambulance : 102

Disaster Management Service : 108



Are you Certified?

“

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

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

”



www.cybersafegirl.com

SURE PASS

CYBER
PATRIOT



Indian Cyber
Institute

Supported by



Information Security
Education & Awareness

Beli Bachao Cyber Crime Se...



Don't be a victim
of cyber crime.

www.cybersafegirl.com

Be a #CyberSafeGirl