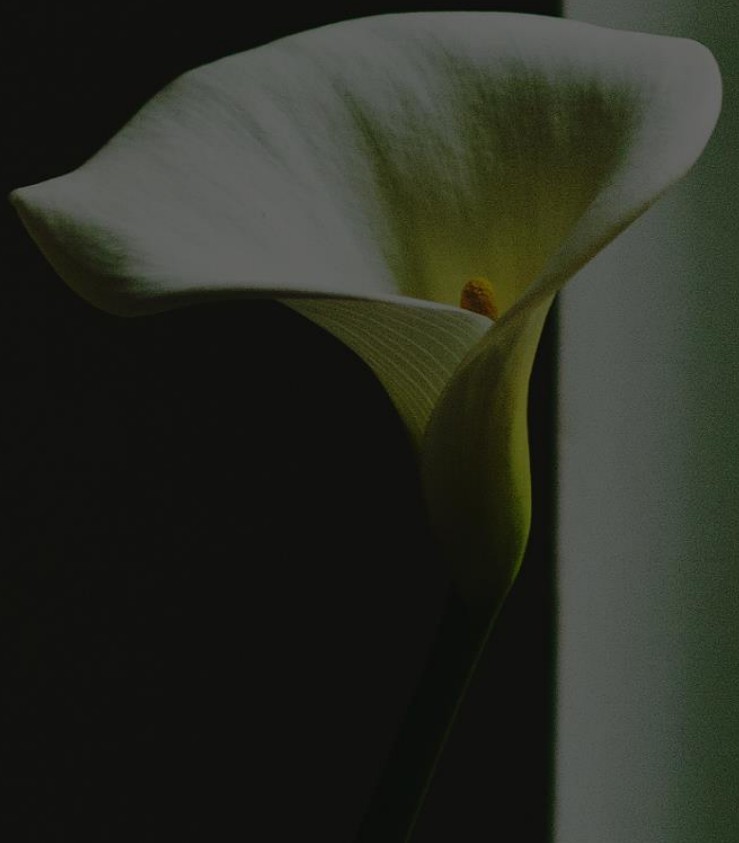


# CYBER CRIME AND ONLINE SAFETY

FOR THE PEOPLE BY THE PEOPLE

In The "Regards Of Victims"



### Introduction Of Cybercrime and Online Safety

Cyber Crime is an illegal activity that involves use of electronic device such as computer, laptop, mobile, etc for stealing someone's privacy.

India a country in peace or places?

Almost every day thousands of crimes related to cyber bullies, harassment is reported.

Technology is a been as well as curse, it however, becomes a platform for online cybercrimes.

Emphasizing on females, they undergo at the most. They face sexual harassment, Rape threats and other online scams including email bombings.

Even, many suicide cases are due to harassment as they lead to depression.

Though world is becoming modern but one should not forget basic life valued enrol themselves into such activities blackmailing via fake accounts, threatening about misuse of private photos and even fake edits promoting nuisance.

They are not only ruining their lives but also of victims. Victim prefers silence and remaining voiceless due to the society. However, victims are always blamed at the end.

A part than feminism, males are too not safe on social platforms. Since there is every kind of human, 6 women empowerment is also misused by women. 'Security is a Myth for both Genders.'

Unable to combat depression, Suicide is given priority. Teenagers, due to losing relationship, ego cantered talk on such paths.

*“As cybersecurity leaders, we have to create our message of influence because security is a culture and you need the business to take place and be part of that security culture”*



### What is Cyber Security?

Cyber Security is the practice of defending computers, servers, mobile devices, electronic systems, networks, and data. It's also known as information technology security.

### Types Of Cyber Security

We divide cyber security into three parts. first Cloud Security, second Network Security, and third Application Security. Let's explain one by one.

1. **Cloud Security:** Cloud security, also known as cloud computing security. Cloud security is the protection of data stored online via cloud computing platforms from theft, leakage, and deletion. The users of the latest technologies and security techniques protect your data, application and infrastructure with cloud computing. There are three types of Cloud Computing:
  - a. Public
  - b. Private
  - c. Hybrid
2. **Network Security:** It is a process to protect your network and data from breach, intrusion and other threats. It is important for the home network as well as the business world.
3. **Application Security:** It includes hardware, software, and all tasks that introduce a secure web server, software development. That aim is to prevent data or code within the application.

### Skills Required for Cyber security expert

- Computer Knowledge
- Operating System
- Networking

- Command line
- Cyber Laws
- Virtualization Technology
- Cryptography
- Programming
- Creative Thinking
- Anonymity
- Problem Solving
- Social Engineering
- Reverse Engineering
- Information Gathering

### What is Cyber Crime?

Cybercrime, also called computer crime or online crime. This involves a computer, mobiles and a network, the use of a computer to further, trafficking in child pornography, stealing identities, violating privacy, Identity fraud, Theft of financial or card payment data.



### Common Cyber Crime

1. Phishing: Using fake websites or email messages to get personal information from internet users.
2. Social Network Fraud: Fraudsters use social media sites to advertise various scams to a large audience, posts might include anything from investment opportunities to items or services for sale.



3. Cyberbullying/Cyber Harassment: It is bullying that takes place over digital devices like cell phones, computers, and tablets. includes sending, posting, or sharing negative, harmful, false.
4. Cyber Extortion: Cybercriminals demand payment through malicious activity, such as ransomware, DDoS attacks and steal confidential corporate data and threaten to expose it. The most common form of cyber extortion.
5. Identity Theft: When an unauthorized person uses your personally identifying information, such as your name, address, Social Security Number (SSN), or credit card or bank account information to assume your identity in order to commit fraud or other criminal acts.

### Cyberterrorism



The use of the Internet to conduct violent acts that result in, or threaten, the loss of life or significant bodily harm, in order to achieve political or ideological gains through threat or intimidation.

#### Who are the cyber terrorists?

Premeditated, politically motivated attack against information, computer systems, computer programs, and data which results in violence against non-combatant targets by subnational groups or clandestine agents.

#### Types of Cyber Terrorism Attack

There are various types of cyber terrorism attack that are deployed by cyberterrorists.

According to the Centre for the Study of Terrorism and Irregular Warfare at the Naval Postgraduate School in Monterey, California, cyber terrorism capabilities can be group into three main categories; “simple-unstructured”, “advance-structured” and “complex-coordinated”.

1. Simple-Unstructured: to conduct basic hacks against individual systems using tools created by other people.
2. Advanced-Structured: to conduct more sophisticated attacks against multiple systems or networks and possibly, to modify or create basic hacking tools.
3. Complex-Coordinated: The terrorists have the ability to create sophisticated hacking tools. They are also highly capable of conducting target analysis and command and control.

There are five main types of cyber terrorism attack which are incursion, destruction, disinformation, denial of service and defacement of web sites.

### What is Cyber Law



Cyber Law also called IT Law is the law regarding Information-technology including computers and internet. Cyber law is one of the newest areas of the legal system. Cyber law provides legal protection to people using the internet. This includes both businesses and every citizen. Every action and reaction in cyberspace have some legal and cyber legal angles. The major motive of this law is to protect people from online fraud. Cyber Law to prevent online fraud. IT law prevents credit card theft, identity theft, and other money-related crimes that are bound to happen online. People who commit online fraud, face state criminal charges.

### Cyber Crime Under the IT ACT

1. Sec. 65, Tampering with Computer Source Documents.
2. Sec. 66, Hacking Computer Systems and Data Alteration.
3. Sec. 67, Publishing Obscene Information.
4. Sec. 70, Unauthorized Access of Protected Systems.
5. Sec. 72, Breach of Confidentiality and Privacy.
6. Sec. 73, Publishing False Digital Signature Certificates.

### Special Laws and Cybercrimes Under the Ipc Include

1. Sending Threatening Messages by Email, Indian Penal Code (IPC) Sec. 503.
2. Sending Defamatory Messages by Email, Indian Penal Code (IPC) Sec. 499
3. Forgery of Electronic Records, Indian Penal Code (IPC) Sec. 463
4. Bogus Websites & Cyber Fraud, Indian Penal Code (IPC) Sec. 420
5. Email Spoofing, Indian Penal Code (IPC) Sec. 463
6. Web-Jacking, Indian Penal Code (IPC) Sec. 383
7. Email Abuse, Indian Penal Code (IPC) Sec. 500

### Some Case in Cyber Cell



#### Case 1 **BANK FRAUD**

Victim complains that Rs.4.25 lacs have been fraudulently stolen from his/her account online via some online Transactions in 2 days using NET BANKING.



#### Case 2 **IDENTITY THEFT**

Victim complaints that his Debit/Credit card is safe with him still somebody has done shopping/ ATM transactions on his card.



#### Case 3 **PHISHING MAIL**

Somebody sent an Email from Income Tax Department and asked for all the bank information and after that 40,000/- has been fraudulently taken away from her account.





### **Case 4** **LOTTERY SCAM**

Got an email that you are a lucky winner for a big amount of prize money and asked to deposit an amount to claim that prize.



### **Case 5** **JOB FRAUD**

Received an Email for a JOB Notification for a VERY BIG ORGANISATION and ask to deposit X amount and come for the interview with the Pay Slip.



### **Case 6** **DATA THEFT**

A Corporate Complained that his crucial data has been stolen and has been misused against his organization.



### **Case 7** **WEBSITE HACKING**

Somebody hacked into the Website and posted very defamatory content on his/her website.



### **Case 8** **ONLINE TRANSACTIONS FRAUDS**

In such matters, the complainant alleges that some unknown person had withdrawn money/ made transactions through his/her credit/debit cards through online purchasing. In most of these cases purchasing is done by using following crucial information of the credit/debit card:

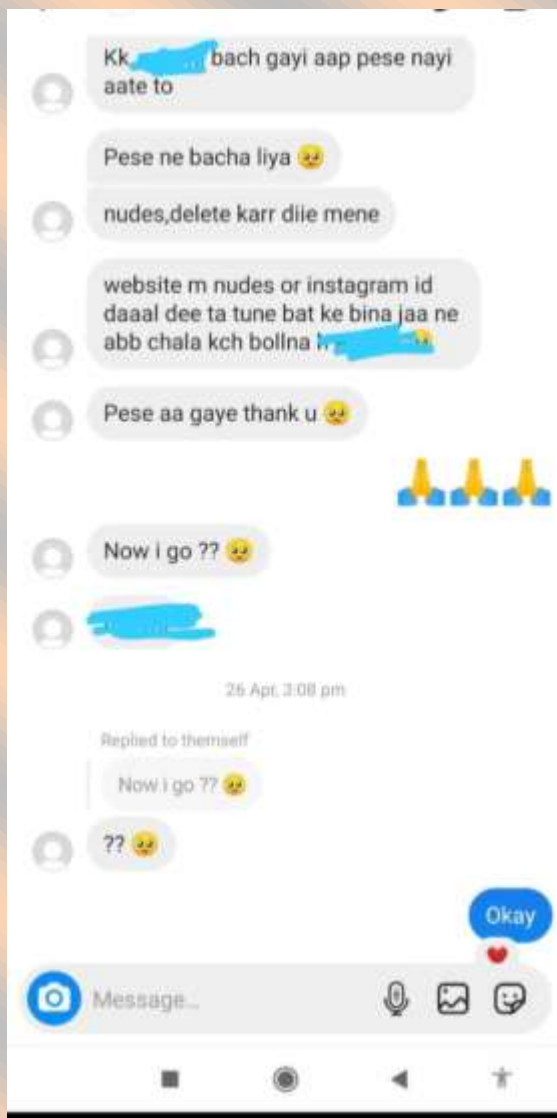
1. The 16 Digit Credit/Debit Card Number
2. The validity of the Credit/Debit card
3. The 3-digit confidential Card Verification Value (CW) or the One-Time-Password (OTP) sent on the registered mobile number of the Debit Card holder.

While it may be that the Card Number and the validity of the card is made available to the fraudsters through an insider in the bank, the OTP is procured by them by deceiving the account holder to share the OTP on the pretext that it is required for account verification, etc.



## Case 9

Below attached screenshots are real based on victims., How they have been troubled and blackmailed. One guy stalked a girl's account and with fake id texted her to be her girlfriend otherwise he will edit her pictures (simple) into nudity using his skill!! Later, the girl was supported by her boyfriend and the guy apologised and left!! Other case, the girl was asked to pay otherwise the guy would leak her photos into porn sites. the helpless girl paid him anyhow. Considering revenge kind, a girl was blackmailed with screenshots of chats of her with her ex-boyfriend and was blackmailed to send them to her family. The girl used to pay. the boy returned again and asked for more money she kept paying him. He got her into stage of depression, anxiety and stress even the girl became victim of asthma too. Later, at her worst stage she shared the incident to her brother and finally she came out of the matter. Victims should not scare of such threats. If u r not wrong no power in world can pull u down! They should even not think to commit suicide. Or even they should not pay.



## Cyber Awareness

### Computer devices Awareness

- Keep your operating system, browser, mobile application, and all installed software up-to-date.
- Do not use pirated software. Besides being a crime, it makes your computer vulnerable to cyber-attacks.
- Use a good antivirus and firewall solution.
- Regularly backup your data on an external hard disk or USB drive. Additionally, consider backing up on a cloud service.
- Be careful before connecting USB devices to your computer. They may contain malware.
- Be careful before downloading email attachments. They may contain malware.
- Use a strong password. Your password should be complex and difficult to guess. Ideally, they should be at least 12 characters long & should have capital, small letters, numbers and special characters.
- Consider using full disk encryption or at least encrypted pen-drives for securing your data.
- When connecting to Wi-Fi, ensure you are connecting to the correct network.
- Don't connect to public Wi-Fi.
- Avoid clicking banner ads.
- Never click unexpected pop-up windows that offer to remove spyware or viruses from your computer.



### Social media Awareness

- Learn about and use the privacy and security settings on your social networking.
- Photos clicked using a smartphone may have geolocation embedded. Remove this before posting/sharing the photos and videos.
- If someone is harassing, bullying or threatening you first report them to the police and take a screenshot then remove them from your friends list.

### Phone Security Awareness


- Use a strong password instead of a 4-digit pin.
- Ensure that the device automatically locks itself if unused for more than a minute.
- Download the app only from a trusted location.
- Carefully read reviews about an app before downloading it.




- Check the permission the app requests.
- Ensure you download and install all operating system and app updates.
- Turn off automatic WIFI connections
- Turn off Bluetooth when not required.




## SAFE SOCIAL MEDIA USAGE FACEBOOK






Review the logged In devices



Unrecognized Login Alerts



Enable Two-factor Authentication



Hacked Facebook Account Recovery



Use Safe Password



Review App Permissions



### E-banking Awareness

- Connect to your website using a device that has the latest and updated security software, web browser and operating system.
- Take a printout of the transaction confirmation and store the printout till you cross check that transaction in your monthly statement.
- Check your account on a regular basis.
- Change your internet banking password at least once a week or month.
- Passwords should be complex.
- Do not access your internet banking account from a cyber cafe or when connected to public WIFI.
- To access your bank internet banking, always type in the correct URL into the browser and never click on a link in an email to visit your bank site.
- Never disclose your password or pin anyone, not even to bank employees





### Wi-Fi Security Awareness


- Make sure you actually need a Wi-Fi network.
- Change your router password every month or week.
- Regularly check your Wi-Fi router logs.
- Use WPA2 Security encryption
- Use a strong password


- Block unwanted sites.


SAFE  
**PUBLIC WI-FI USAGE**




  
Always activate Virtual Private Network (VPN) in your smartphone and computer

  
Enable two-factor authentication for email and social networking services

  
Remember to Turn Off, the network sharing

  
Always Make sure your operating system's Firewall is ON

  
Do not perform online banking using public wifi

## Prevention Of Cybercrime and Online Safety Tips



Ministry of Home Affairs has started "Citizen Financial Cyber Fraud Reporting and management System" for prevention of money loss in case of Cyber Financial Fraud, for immediate reporting, call 155260. (24\*7)

**Some online website for checking your password, website details, file (check file is inject any malicious software or not), Image Meta data, Cybercrime reporting website and some more.**

1. Whois Lookup  
It is popular domain name search tool that allows a wildcard search, monitoring of whois record and history caching.  
Website: <https://whois.domaintools.com/>
2. Password Meter  
To check the strength of a password based on multiple parameters.  
Website: <http://www.passwordmeter.com/>
3. Virus total  
A free server that analyses suspicious files and URL's the quick detection of viruses, worms, trojans, and all kinds of malware.  
Website: <https://www.virustotal.com/en/>
4. Online exif viewer and remover  
The online exif viewer and remover for viewing and removing exif data of pics  
Website: <https://www.verexif.com/en/>
5. Cyber Crime report portal  
Website: <http://www.cybercelldelhi.in/Report.html>



<https://cybercrime.gov.in/Accept.aspx>

6. Have I Been Pwned

It allows you to search across multiple data breaches to see if your email address or phone number has been compromised

Website: <https://haveibeenpwned.com/>

If you are victim then you can contact us [Nitin Pandey](#) , [Bhanu Sharma](#) and [Chetan Bansal](#)

## About the Author and Team

Nitin Pandey sir



This book has been written under the guidance of Nitin Pandey sir. He helped and guided us a lot to write these things especially in pointing out the major challenges in cybercrime and online safety. Nitin Pandey sir is a National Cyber Security Consultant, currently working as Cyber Consultant of Uttar Pradesh Cyber Crime, Police Headquarters Lucknow. He is a globally acknowledged person and has more than a decade's experience in the field of Cyber Security. We are heartily thankful to him

for his guidance and support to us for writing this book for public awareness.

Get in touch:

<https://in.linkedin.com/in/initinpandey1>

<https://twitter.com/initinpandey>

<https://www.instagram.com/initinpandey>

<https://nitinpandey.info/>

Bhanu Sharma



They plan to write this book. They guide me also and share mind map to write this book. Bhanu Sharma have own community (hackingmaster\_t56). He provides webinar and share tips and information about cyber security and awareness. He educates and spread awareness among the public about cybercrime, ethical hacking & cybersecurity. Their goal is to build a safer Cyber World. Focuses on Cyber Security and help new Cybersecurity Enthusiast to get familiar with the cyber world. They are also working on awareness programme to help people to be safe and secure. He pursuing

Diploma in Electrical Engineering at Rajasthan.

Get in touch:

<https://twitter.com/officiallybhanu>

[https://www.instagram.com/hackingmaster\\_t56/](https://www.instagram.com/hackingmaster_t56/)  
[https://linktr.ee/hackingmaster\\_t56](https://linktr.ee/hackingmaster_t56)

Chetan Bansal



I am author this book. Firstly, I thank you Nitin sir, Bhanu bro for guiding and helping me for this book. I'm currently handle three community. In this community I share some session regrading cyber security, helping each other to build skills and share cyber security resources. I am also working on teaching programme to help people to be secure and understand what is cybersecurity, how is work, need of cyber security excerpt. I am pursuing Diploma in Information

Technology Enabled Services & Management at Delhi.

Get in touch:

<https://www.linkedin.com/in/chetanbansal11/>  
<https://www.instagram.com/i.m.cbkali/>  
<https://github.com/cb-kali>  
<https://linktr.ee/i.m.cbkali>

**If guy's you're like this e-book please review this:**

**<https://forms.gle/7hvitgQmRo8EF5oQ8>**



# THANK YOU