INDIAN JOURNAL OF LEGAL REVIEW

(P) Volume I and Issue I of 2023

ISBN - 978-81-961097-8-3

Published by

Institute of Legal Education

https://iledu.in

# Cyber Crime- Types & Remedies

**Author** - Areej Khalid, Student at Jitendra Chauhan College of Law

**Best Citation** - Areej Khalid, Cyber Crime- Types & Remedies, Indian Journal of Legal Review (IJLR), 1 (1) of 2023, Pg. 42-47, ISBN - 978-81-961097-8-3.

***ABSTRACT***

*The paper focuses on the emerging trend of online crimes and frauds. Any crime that involves a computer and a network is called computer crime also popularly known as cybercrime. Therefore, a crime which involves network and computer or is done through any digitalised platform is known as Cybercrime. There are four most common cybercrime Phishing Scam, Identity Theft, Salami Attack and Ransomware attack. The Government of India has looked into the rising rates of cybercrimes and has provided its citizens with respective legal remedies. Therefore, if a person gets victimised by these attacks there are certain legal remedies for the same that the person can seek.*

**INTRODUCTION**

The term Cybercrime has been established after the immense growth of digital works or computerisation. Cybercrime from the word itself can be figured out as a crime done digitally or a crime which involves internet or computer. Cybercrimes are considered to be very risky and dangerous as these crimes effect major data loss and financial loss and also failure of expensive software.

Cybercrime can be defined as "The illegal usage of any communication device to commit or facilitate in committing any illegal act". It may include many types of profit making activities like ransomware attack, phishing, identity fraud etc. In cybercrime criminals target victim's personal information to attempt theft.

The Council of Europe Convention on Cybercrime, to which the U.S. is a signatory, defines cybercrime as a wide range of malicious activities, including the illegal interception of data, system interferences that compromise network integrity and availability, and copyright infringements. Warren Buffett describes cybercrime as the "number one problem with mankind" and said that it "poses real risks to humanity.

There are many privacy concerns surrounding cybercrime when confidential information is intercepted or disclosed, legally or otherwise. Cybercrime when comes to international level and becomes a matter of nation-state is then referred to as cyber warfare.

**BREIF OF INFORMATION TECHNOLOGY ACT, 2000**

Information Technology Act, 2000 was enacted the parliament of India in the year June, 2000. The act came into effect from October 17th, 2000. In 2000, the word Information Technology was limited to electronic documents, digital and e signatures and authentication of records as there was no social media or OTT platform in those days. But with expansion of internet all over the world, IT Act was introduced to regulate all the internet related activities.

**Objectives of IT ACT**

IT Act has come into force with the primary objective to establish and protect cyber laws and also to facilitate electronic functions for the purpose of transactions, e-commerce, etc. Other objectives of the act are as follows:-

1. Grant legal recognition to digital signatures
2. Use of digital signature for legal authentication

INDIAN JOURNAL OF LEGAL REVIEW

(P) Volume I and Issue I of 2023

ISBN - 978-81-961097-8-3

Published by

Institute of Legal Education

https://iledu.in

3. To facilitate electronic filing of documents relating to Government agencies and govt. departments.
4. To provide legal sanction and facilitate the electronic transfer of funds between banks and other financial institutions.
5. Grant legal recognition to Bankers under RBI Act and Indian Evidence Act.

**Features of the Act are as follows:-**

- Under this Act, security measures are also provided for electronic records and digital signature.
- Procedure for appointment of Adjudicating officer is also mentioned under this act. Adjudicating officers will be appointed to hold enquiries pertaining to matters under IT Act.
- Provisions regarding establishment of Cyber Regulatory Appellate is also mentioned under the act. This tribunal will handle all appeals against the order of controller or adjudicating officer
- Appeal against the award of adjudicating officer is possible only through High Court.

**Cyber Security under IT Act**

The provisions relating to cyber security under IT Act are dealt in section 2(1) (nb). According to section 2(nb) cyber security means protecting information, equipment, devices computer, computer resource, communication device and information stored therein from unauthorised access, use, disclosure, disruption, modification or destruction. [76]

**PHISHING SCAM**

In general, phishing scam is when someone pretends to be someone else (i.e. known to the target) with the intention to perform fraud. It is a type of online scam which targets the audience by sending them e-mail and that email appears to be from a well-known source. For example an email from a friend, company, bank, etc. It asks the target audience to share personal details, which then the scammers use to get access to the accounts or to open new accounts. One of the most common examples for phishing scams is asking for OTP.

However there are certain ways in which the audience can save themselves from such scams. One of the most relevant methods is by not responding to such mails that ask for personal or financial information. Now the question arises how to spot phishing scam emails or texts?

1. The official mail that the company sends ends with "@google.com", whereas the scammers' uses public email domain such as "@gmail.com" or "@yahoo.com".
2. Sometimes the domain name is spelled wrong. For example if the mail is sent from Microsoft it can be spelled as miscrosfot. This also indicates that the mail is not genuine.
3. Very often the mail is not written correctly. This means that the mail has many grammatical errors or spelling mistakes. This also indicates that these mails are sent by the scammers.
4. The phishing mail also contains the sense of urgency. It is stated as ACT NOW, RESPOND IMMEDIATELY etc.

**Legal Remedies for Phishing**

There are two aspects for phishing,

1. ***Criminal Aspect of Phishing-*** As we all know that phishing is a criminal act that involves leaking data of the victim using internet, it comes under cybercrime and is hence dealt under the Information and Technology Act, 2000. The provisions dealing with phishing were incorporated in 2008. These provisions are :-
   - ***Section 43 of IT ACT-*** **Section** 43 of IT Act deals with Penalty and compensation for damage to computer, computer system etc.
     If any person without permission of the owner or any other person who is in charge of a computer, computer

[76] Information Technology Act, 2000

INDIAN JOURNAL OF LEGAL REVIEW
(P) Volume I and Issue I of 2023
ISBN - 978-81-961097-8-3
Published by
Institute of Legal Education
https://iledu.in

system or computer network, or computer resource —

a) accesses or secures access to such computer, computer system or computer network;
b) downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
c) introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
d) disrupts or causes disruption of any computer, computer system or computer network;
e) denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means; (g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act, rules or regulations made thereunder
f) Charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system, or computer network, he shall be liable to pay damages by way of compensation to the person so affected.
g) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;
h) steel, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

- ***Section 66 of IT Act-*** deals with dealing with phishers who steal victim's account. It states that "-If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both."[77]

  ***Explanation of the Act-*** For the purpose of this act, the word 'dishonesty' shall have the meaning assigned to it in section 24 of IPC

  The word fraudulently shall have the meaning assigned to it under section 25 of IPC.
- ***Section 66 C of IT Act-*** Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine with may extend to rupees one lakh. [78]

Another common attack to that of Phishing is Cyber Espionage

**CYBER ESPIONAGE**

It is a cyber-attack in which the unauthorised user attempts to access sensitive or classified data or intellectual property for economic gain. Cyber espionage attacks can be motivated by monetary gain; they may also be deployed in conjunction with military operations or as an act of cyber terrorism or cyber warfare. The impact of cyber espionage, particularly when it is part of a broader military or political campaign, can lead to disruption of public services and infrastructure, as well as loss of life.[79]

[77] IT Act, 2000
[78] IT Act,2000
[79] https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/

INDIAN JOURNAL OF LEGAL REVIEW

(P) Volume I and Issue I of 2023

ISBN - 978-81-961097-8-3

Published by

Institute of Legal Education

https://iledu.in

**CYBERSQUATTING**

Cybersquatting is unauthorised use of internet domain names that are much the same of actual companies or website names. Cybersquatting registrant obtains and uses the domain name with the bad intent to profit from goodwill of the actual trademark owners.[80] For example, a goodwill website is www.bluepink.com but cybersquatting registrants might name their site as www.bluep1nk.com . The intent of doing this is to gain profit from the name of another company by fooling the audience.

**Laws regulating Cybersquatting**

The cybersquatting is dealt under Anti cybersquatting Consumer Protection Act, 1999.

The Internet Corporation for Assigned Names and Numbers (ICANN) established the Uniform Domain Name Dispute Resolution Policy (UDRP) to solve disputes over registration of internet domain name. India since is under signatory touch with WIPO, it is mandatory to follow UDRP. Therefore, India has started Indian Domain Name Dispute Resolution Policy (INDRP). Following are the certain standards set by INDRP:-

a) Appointment of arbitrator with regard to domain names
b) Manage Arbitration proceedings according to Arbitration and Conciliation Act, 1996
c) The Arbitration in the case should pass reasonable award within 60 days from the beginning of the proceedings
d) Arbitrator shall give reasons for the award

**CYBERSTALKING**

In cyberstalking the person targets an individual to keep an eye on their daily routine with the intent to cause harm. This harm can be mental or emotional or physical harm. In cyberstalking the person keeps harassing their target through mails or text messages. It is an activity of using internet to stalk or harass someone. Offences like defamation, false accusations, and threats via mail or texts all of these can come under cyberstalking if done via Internet. For example, making fake social media profile to follow the victim.

**Laws regulating Cyberstalking**

- ***Section 67 of Information Technology Act, 2000*** deals with punishment regarding cyberstalking. It states that *Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.*[81]

**CYBER BULLYING**

Cyber bullying covers sending or posting negative or harmful about someone. These content comprise of personal information with the intent to cause embarrassment or humiliation to the victim. Some cyber bullies act to an extent to make the act unlawful. It includes defaming any person publicly.

Since the word cyber is connected with the word bullying, cyber bullying usually happens in social media platforms or other online websites. It is simply bullying on digital platform.

[80] https://www.winston.com/en/legal-glossary/cybersquatting.html

[81] Information Technology Act, 2000.

INDIAN JOURNAL OF LEGAL REVIEW

(P) Volume I and Issue I of 2023

ISBN - 978-81-961097-8-3

Published by

Institute of Legal Education

https://iledu.in

According to some, cyber bullying is less harmful type of bullying as it is not physical. But this opinion is false. Although the effect of cyber bullying is not physical but it effects the mental health of the victim.

**Legal remedy for Cyber bullying**

The word 'Bullying' is not mentioned in IPC (Indian Penal Code).

**EMAIL SPOOFING**

It is a type of activity that picks out emails of business by using email with false sender address. Because the receiver trusts the source they are more likely to open the links or attachments and become a target of the same.

**Legal remedy for email spoofing**

***Section 66(D)*** deals with Punishment for cheating by personation by using computer resources. Whoever, by means of any communication device or computer resource cheats by personation, shall be punished with

• Imprisonment of either description for a term which may extend to three years and

• shall also be liable to fine which may extend to one lakh rupees

**HACKING**

Hacking is a process where a person gets unauthorised access to the computer system or data of other individual or the company. There are three types of Hackers;-

- **Black Hat Hackers-** black hat hackers perform hacking with the bad intent. They hack others system with the intention to get unlawful financial gains. These hackers are very dangerous as the hacking process can damage whole system.
- **White Hat Hackers-** In order to prevent the actions of black hat hackers, white hat hackers have evolved. These hackers have the good intent to hack. The techniques used by black hat hackers are similar to white hat hackers but the only difference is that white hat hackers are hired by specific companies or organisations to discover loop holes in their respective systems.
- **Grey Hat Hackers-** Actions of Grey Hat Hacker are for benefit for the society as a whole. These hackers hack with the intent to provide common good. They belong in between of white hat hackers and black hat hackers.

**MALWARE**

Malware is software designed in such a way to destroy or harm any programmable device, service or network. Main motive of cybercriminals to use this is to reduce data that can benefit them financially.

**RANSOMWARE**

In ransomware, the wrongdoers steal something of considerable worth and to return it, they demand great value. Commonly this involves stealing of Company data.

If a company is hit by ransomware, the business comes to halt and the employees cannot perform their jobs. It is a kind of virus that has evolved into a great malware and is slowly becoming a major threat for big organisations. It often comes into the form of phishing emails or fake software etc.

**Legal remedies for Ransomware**

These malware attacks are clear case of "extortion". According to section 384 of IPC "Whoever intentionally puts any person in fear of any injury to that person, or to any other, and thereby dishonestly induces the person so put in fear to deliver to any property or valuable security, or anything signed or sealed which may be converted into a valuable security, commits 'Extortion'."

Ransomware as Tortuous Liability- Under tortuous liability, the act is covered under *trespass to chattels* commonly known as trespass to goods.

INDIAN JOURNAL OF LEGAL REVIEW

(P) Volume I and Issue I of 2023

ISBN - 978-81-961097-8-3

Published by

Institute of Legal Education

https://iledu.in

Ransomware under IT Act- under information technology act the following sections can be used against the wrongdoers

- Section 65- Tampering with computer source documents
- Section 66-
- Section 67- Publishing or transmitting obscene information in electronic form
- Section 70- Unauthorised access to protected system.
- Section 72- Penalty for breach of confidentiality and privacy.
- Section 73- Penalty for publishing false electronic signature.

**SALAMI ATTACK**

When several minor cyber-attacks are combined to create a hefty attack it is known as Salami attack. It is a cybercrime which is used to commit financial frauds. This attack has an awful change. A banker inserts a program into the bank's database which then deducts a low amount of cash from every account holder.

There are two types of Salami Attack

- Salami Slicing- it happens when the hacker gets the information of the customers online and deducts a slight amount of cash from every account which is invisible to the customer but when these amount joined together it makes a very huge amount.
- Penny Shaving- it happens when the hacker steals money in small account but by rounding to the closest within the transactions. The change is so small that nobody can deduct this.

**Legal Remedies for Salami Attack**

Salami attack is the type of crime in which the hacker steals money in small amount. However, if a person gets convicted of this act the person can be imprisoned under **section 66 of IT Act**.

**CONCLUSION**

We now live in an era where technology is advancing and digitalisation is spreading in a vast area. With the increase use of internet, the rate of cybercrime is also increasing, for which, however the legal remedies are present. The Govt. of India has come up with Information Technology Act, 2000 to regulate such cyber-criminal activities.

There are four main types of cyber-attacks. These are as follows, Phishing Scam, Ransomware attack, identity theft and Salami attack. Other common cyber-attacks include email spoofing, cyber bullying, cyber espionage and many others. All of these are very dangerous in nature and cause serious financial and emotional damage to people.

The print media should educate the users and youngsters about the dangerous effect of cybercrimes. It should educate people with the precautions one should take to avoid themselves from getting into such situations. Cybercriminals have the capacity to paralyse large parts of communication network, cause financial meltdown and unrest in the society. Therefore it is necessary to take note of this.

**REFERENCES**

Websites Referred

1. https://www.crowdstrike.com/cybersecurity-101/cyberattacks/cyber-espionage/
2. https://www.geeksforgeeks.org/what-is-salami-attack/amp/
3. https://indiankanoon.org/doc/132073018/
4. https://www.bluevoyant.com/blog/cybercrime-types-and-prevention
5. https://cybertalents.com/blog/what-is-cyber-crime-types-examples-and-prevention
6. https://www.ftc.gov/news-events/topics/identity-theft/phishing-scams
7. https://www.mondaq.com/india/data-protection/1219182/a-glance-at-online-fraud--phishing

Books Referred

1. Information Technology Act By Amar Law Publications.
2. Professional's IT Act, 2000 Bare Act.