VIPS
योगः कर्मसु कौशलम्
IN PURSUIT OF PERFECTION

VIPS Centre of Excellence for Cyber Law

VIVEKANANDA INSTITUTE OF PROFESSIONAL STUDIES

Affiliated to GGSIP University, Recognised by Bar Council of India
& Approved by AICTE Accredited Grade "A" Institution by NAAC,
Recognised under Section 2(f) by UGC.
An ISO 90001:2015 Certified Institution

VIVEKANANDA SCHOOL OF LAW AND LEGAL STUDIES

presents

Handbook on Cyber Security Awareness - Frequently Asked Questions (FAQs)

by The VSLLS Centre of Excellence for Cyber Law

Prof. (Dr.) R. Venkata Rao

CHAIRPERSON,
Vivekananda School of Law and Legal Studies,
Vivekananda Institute of Professional Studies

It delights me to note that the Centre of Excellence for Cyber Law, Vivekananda School of Law and Legal Studies, Vivekananda Institute of Professional Studies is bringing out 'A Handbook on Cyber Security Awareness'.

The importance of the Handbook cannot be overstated. It is an idea whose time has come.

The exponential pace at which technology is galloping and the advent of IoT (Internet of Things) thanks to the ushering in of the Fourth Industrial Revolution which is a 'System Revolution', have bedazzled everyone making us wonder as to what is happening around us.

Cyber Illiteracy, even among the most literate otherwise, has been making us vulnerable to the machinations of the cyber predators.

The 'Invisible Internet' is threatening to make us the victims of many a cyber crime like Cyber Bullying and Cyber Frauds.

The credo of Vivekananda School of Law and Legal Studies is that 21st Century Problems cannot be solved with a 20th Century mindset and 19th Century working tools.

The Handbook is a humble attempt to make the surroundings around us more cyber secure.

I am sure the Netizens will find the Handbook extremely useful as a Protective Shield.

Warm Regards

INTRODUCTION TO THE HANDBOOK

Cyber space is not new to anyone. People have adopted cyber space due to its advanced technology and user-friendly operations. Moreover, cyber space can be accessed without a training as its steps are fixed and certain to operate. Thus, its adaptability is evident amongst the public at large. However, this is only one side of the coin. On another side, victimisation is growing day by day. Every user of cyber space is a possible victim of the cyber-attack. This is due to unsecured access to cyber space and unawareness about cyber security. This vulnerability can be minimised and can be avoided with awareness about cyber security.

Each user uses cyber space for different purposes. Thus, the related threats are also of various kinds. It is natural that each user must be having different questions to keep him cyber safe. Considering this situation, the Center of Excellence for Cyber Law consisting of Vivekananda School of Law and Legal Studies (VSLLS) conducted a small research study. We collected the questions from around 200 cyber space users of various age groups. Out of the total collected questions, the research team selected frequently asked questions (FAQs) posed by the cyber users. The research team researched the same and found its answers. The researchers also researched the legal response of those questions. Thus, the research team studied cyber technology and law both to find answers to the FAQs.

The present Handbook titled as Handbook on Cyber Security Awareness: Frequently Asked Questions is the outcome of this research study. Total 15 areas of cyber threat are referred to in this Handbook with an average of 6 to 9 FAQs of each type of cyber threat. An exceptional care has been taken that as cyber space is user friendly, then its Handbook of FAQs must also remain user friendly. Thus, answers

to all FAQs are not lengthy and lucid language is used deliberately. This Handbook contains questions mainly relating to the meaning and scope of the cyber threat, legal response and punishment if any to the perpetrator. The Handbook of FAQs shall be useful for the probable victims. It is also observed that few users perpetrate cyber- attack due to unawareness of the gravity of the threat. For example, cyberstalking and bullying. Thus, a couple of questions – answers are given in each selected area to make ignorant attackers aware of legal consequences.

We are glad to present Handbook on Cyber Security Awareness: Frequently Asked Questions developed by students and faculty members of the Center of Excellence of Cyber Law, Vivekananda School of Legal Studies. We are indebted to the Management, Vivekananda Institute of Professional Studies who support us in all endeavours. Dr S.C. Vats, Chairman, Vivekananda Institute of Professional Studies inspire us to be relevant to society with innovative ideas. He always insists to go beyond the boundaries of the syllabus to make students learn. We are thankful to Prof (Dr.) R. Venkata Rao, Chairperson, Vivekananda School of Legal Studies and Prof (Dr). T. V Subba Rao, Professor Emeritus for their valuable guidance on each step.

Your feedback will make this humble attempt more meaningful.

Prof. (Dr). Rashmi Salpekar
Dean, Vivekananda School of Law and Legal Studies,
Vivekananda Institute of Professional Studies

RESEARCH TEAM

Nitin Dhatarwal, B.A.LL.B. (Semester III)

Riya Jaitly, B.B.A.LL.B. (Semester III)

Shivangi Kohli, B.B.A.LL.B. (Semester IX)

Arshia Jain, B.B.A.LL.B. (Semester V)

Dhrone Diwan, B.B.A.LL.B. (Semester V)

Barkha Tandon, B.B.A.LL.B. (Semester III)

Shubhanshi Phogat, B.A.LL.B. (Semester III)

Tarang Sehgal, B.A.LL.B. (Semester VII)

Suvarna Singh, B.A.LL.B. (Semester VII)

Katyaini Chamola, B.B.A.LL.B. (Semester VII)

Shweta Shukla, B.B.A.LL.B. (SemesterVII)

Isha Singh, B.B.A.LL.B. (Semester III)

Jigyasa Joshi, B.A.LL.B. (Semester IX)

Yukta Batra, B.A.LL.B. (Semester VII)

Sakshi Komal Dubey, B.A.LL.B. (Semester III)

CONTENTS

CONTENTS

CYBER SECURITY- NEED OF THE HOUR

Cyberspace is a virtual and border less space making it prone to be abused by the mischievous individual, groups or entities. The radical use of cyberspace at present has brought forth concerns like cyber threats ranging from identity theft, online harassment, Cheating, data theft to the infringement of privacy and so on. Reasons such as anonymity of the offender's identity, Jurisdiction issues, diversity in laws regulating cyberspace in different jurisdictions put the offender at more advantageous place and the victims more vulnerable.In the light of these facts cyber security is the need of the hour to protect the privacy and identity of the user, security of the systems and safeguarding the interest of the society at large.

> "Identity theft, Harassment, Misrepresentation, Cheating are methods of attacking your system."

FREQUENTLY ASKED QUESTIONS

Q1: Should cyber security be my concern?

Ans: Yes, depending on the awareness and exposure to the Internet and social media, cyber security becomes a concern for people. Cybersecurity is the practice of protecting critical systems and sensitive information from digital attacks.

Q2: Should the same password be used for logging in to various websites?

Ans: No, for different accounts, it is preferable to use different passwords. A simple reason behind this is that in case your account gets hacked access to only that account will be done, other data will not leak.

Q3: Should I save the passwords or my location when websites ask for permission for the same?

Ans: Never save passwords or locations when websites ask permission to do so, If the website gets hacked, your data will be leaked very easily.

Q4: What is the meaning of sensitive information? Should I restrict access to my sensitive information?

Ans: Sensitive information is the personal information and important credentials like phone number, credit/debit card details, Adhaar card number etc. It may also include the sexuality, gender, political opinion of a person. Access to sensitive information and exploitation of the same comes within the ambit of the processing of information done by the Artificial Intelligence of the company. The Government has proposed the Personal Data Protection Bill,2020 to tackle this issue.

Q5: Is there awareness about famous social media scams like the Nigerian prince scam or other cyber frauds? What are other common cybercrimes netizens are vulnerable to?

Ans: In the Nigerian prince scam, a person receives an email in which the alleged Nigerian prince will ask for some donation to feed the poor. Other cyber frauds are 419 scams and advance-fee scams. Other cybercrimes are Hacking, Chatroom Abuses, Cyber Bullying, Software Piracy, Virus Dissemination, Child Pornography, Cyber Terrorism, Voyeurism, Tampering with Computer sources or Data, Data Mining and Cyber-Stalking.

Q6: What should be my recourse if ever encountered cybercrime of any form?

Ans: The recourse depends on the nature of cybercrime a person has encountered, for instance, social media websites have their reporting mechanisms to ensure the user's safety. Presently, Chapter 11 of Information Technology Act, 2000deals with cyber crimes in India, in case a person becomes the target of a serious offence.

Q7: What are the preventive measures I can take to improve my cyber security?

Ans: The preventive methods if inculcated can help in preventing one from becoming a victim of cybercrime to a certain extent. Some of the ways are mentioned as follows:

1. Profiles can be blocked from public searches.
2. Restricting who can find me via online search can prove to be an essential life-saver.
3. Logging out after each session ensures avoidance of mistakes such as not logging out the id at a place like cybercafé . Social media credentials with strangers should not be shared.
4. Requests from unknown persons should not be accepted as it increases the risk and vulnerability for cyber attacks.
5. Do not click on suspicious links received through messages, either online or offline.
6. The privacy setting of social media accounts should be at the most restricted levels. While sharing anything online apply maximum caution. This step will up to a certain extent ensure that your data is not collected by the offender.

HACKING

Accessing a computer or mobile system without the express or implied consent of the owner is known as hacking. It is a criminal offence and is covered under "Computer related offences" defined under Section 66 of The Information Technology Act, 2000.The main objective of hacking is to break into device's system to steal, destroy, alter, misuse or misappropriate data. Hackers do so by secretly installing harmful malware into the system. This malware stealthily transfers the personal and financial information. Common hacking techniques include malvertising, worms, viruses, trojans, browser hijacks etc. Any mobile phone or a computer system connected to the internet is susceptible to the threat of getting hacked if appropriate safety measures are not taken.

"Common hacking techniques include malvertising, worms, viruses, trojans, browser hijacks etc."

FREQUENTLY ASKED QUESTIONS

Q1: What is hacking?

Ans: Accessing a computer or mobile system without the express or implied consent of the owner is known as hacking

Q2: How do hackers hack?

Ans: Hackers commonly create rootkits, worms, viruses, trojans, browser hijacks etc. that deposit malware into the device's system. Sometimes hackers also use manipulation techniques to lure unsuspecting users into clicking on a malicious attachment or providing personal data.

Q3: How do hackers find me?

Ans: Any mobile phone or a computer system connected to the internet is open to getting hacked if appropriate safety measures are not taken. Hackers try to access device's system and personal information directly if you are not protected by a firewall.

Q4: How can hackers affect me?

Ans: Once the system has been hacked, a hacker might be able to gain control over your usernames and passwords, steal money from your bank accounts, request new account Personal Identification Numbers (PINs), Make purchases on your name, use and abuse your Social Security number to open bank accounts, sell your information to other parties who will use it for illicit purposes, etc

Q5: What is the legal punishment for hacking?

Ans: Punishment for hacking is imprisonment up to 3 years or a fine which may extend to 2 lakh rupees or both.

Q6: How will I know if my computer or mobile system has been hacked?

Ans: You can look out for basic signs to know whether your computer or mobile system has been hacked like changes in passwords of personal accounts, debit cards, credit cards and documents, unexplained financial transactions, receiving suspicious login alert emails from online services you are using, being locked out of your online accounts, etc.

Q7: How can I protect my devices from hackers ?

Ans: Some of the basic measures you can take to protect yourself from hackers are as follows:

- Avoid visiting dangerous websites.
- Never download unsupported attachments. Never click on links in unfamiliar emails. Make your passwords long and complicated. Use antivirus protection.
- Use a 2-way firewall.
- Keep private and financial information out of online conversations.

Q8: What to do once a computer or mobile system has been hacked?

Ans: Reach out to your bank and email service provider as early as possible and request them to temporarily block the account for preventing its misuse by the hacker, send messages to all your contacts from alternative phone numbers or emails alerting them to not respond to emails and messages coming from that hacked account and lastly, file a complaint at your nearest police station detailing the complete incident.

REFERENCES

[1] https://hacked.com/how-to-check-if-youve-been-hacked/

[2] https://www.webroot.com/in/en/resources/tips-articles/computer-security-threats-hackers

[3] http://www.cybercelldelhi.in/emailfraud.html

PHISHING

In the age of the internet, every individual has come across emails with bi-lines/ subjects as 'Response Required' or 'Review your information.' Well, these emails are termed as Phishing.

Phishing is a sophisticated method of gathering personal information using deceptive emails and websites.

The entire gameplay revolves around making the receiver believe that the message is from a trusted entity such as their bank, a note from the company or employee they work with. Eventually, tricking the human victim into revealing sensitive information.

"Phishing is a sophisticated method of gathering personal information using deceptive emails and websites."

FREQUENTLY ASKED QUESTIONS

Q1: How can one recognize or suspect phishing?

Ans: Scammers use emails or SMS's to trick the victim into providing information. The goal of the attacker is to cause financial loss, data loss, malware into the electronic device and illegal use of user's details.

One can spot phishing scams through the following ways – The message is sent from the public domain

The domain name may be mis-spelt Email is not well crafted Suspicious attachments and links The message creates an urgency

Q2: What are the provisions envisaged under the Information Technology Act, 2000 w.r.t Phishing?

Ans: In the year 2008, the Information Technology Act was amended to include phishing under the Information technology Act, 2000. The sections that are applicable are Section 43,66, 66A, 66C,66D and 81.Under section 77B of the Information Technology Amendment Act, 2008 phishing scams have been included.

Q3: What are the different types of Phishing?

Ans: The different types of phishing are as follows- Email Content Injection Link Manipulation CEO Fraud

Mobile Phishing Spear Phishing Voice Phishing Session- hijacking Man–in-the-middle Evil–Twin-Wi-Fi Malvertising.

Q4: What are the ways to prevent phishing?

Ans: Following are the ways to prevent phishing:

Use of security software and updating it periodically. Mobile phones can be protected by setting software to update automatically.
These updates could give you critical protection against security threats.

Accounts can be protected by using multi-factor authentication. Some accounts offer extra security by requiring two or more credentials to login to your account.

Data can be protected by backing it up. Back up your data and make sure it is not connected to your home network

Q5: What amount of punishment can be rendered for the offence?

Ans: Phishing is punishable under section-43 of Information Technology Act, 2000 with a penalty up to Rs. 1 crore.

Q6: What's the difference between phishing, smishing, vishing and pharming ?

Ans: The goal is the same, only the manner of obtaining information is different Phishing – takes place via email. Vishing – happens via a phone call. Smishing – takes place through SMS. Pharming – through the DNS cacheon the end- user device or the network equipment of the provider.

Q7: What is Malware?

Ans: Malware takes place when a person clicks an email attachment and inadvertently installs software that mines the computer and network for information. Key logging is a type of malware that tracks keystrokes to discover passwords.

Trojan horse is another type of malware that is installed and tricks the person into entering his/ her personal information.

Q8: Under what sections of Indian Penal Code, 1860, is phishing punishable ?

Ans: Phishing is punishable under section - 415 (Cheating) ; section-425 (mischief); section-464 (Forgery) and section -107(Abetment).

Q9: How to report phishing?

Ans: The Ministry of Home Affairs and Indian Cyber Crime Coordination Centre has operationalized a helpline 155260 for reporting cyber crimes.

Q10: What is Malvertising?

Ans: Online-Advertisements or pop-ups that encourage victims to click on them. Leading to the installation of malware on the computer.

REFERENCES

[1] https://terranovasecurity.com/what-is-phishing/

[2] https://www.protectimus.com/blog/phishing-vishing-smishing-pharming/

[3] https://www.imperva.com/learn/application-security/phishing-attack-scam/

[4] https://www.csoonline.com/article/2117843/what-is-phishing-how-this-cyber-attack-works-and-how-to-prevent- it.html

PRIVACY BREACH

A privacy breach happens when an association or individual either purposefully or incidentally Provides unapproved or unplanned admittance to somebody's very own data. Discloses, adjusts, loses or obliterates somebody's very own data. A security break additionally happens when somebody can't get to their own data due to, for instance, their record being hacked. Privacy breaks can go from the low end when a solitary individual's data is influenced through to the very good quality when countless individuals are influenced. Security breaks can be unplanned or caused through the activities of pernicious entertainers. Privacy breach are a reality for associations that hold individuals'very own data.

> "Security breaks can be unplanned or caused through the activities of pernicious entertainers."

Organizations and associations can lose individual data through smugness, insufficient security, helpless strategies or unintentionally. In the event that a protection break occurs in your organization, realize how to oversee it. A security break can cause long haul and momentary ramifications for an association. Primer Assessment- For the situation of a break, promptly contain the break. Assign a suitable individual and group to explore and research the break.

FREQUENTLY ASKED QUESTIONS

Q1: What is a privacy breach?

Ans: A privacy breach happens when there is unapproved admittance to assortment, use or exposure of data. Probably the most widely recognized examples of a protection break happen when the individual data of a patient, client or customer is taken, lost or erroneously uncovered

Q2:How many types of privacy breach are there?

Ans: Distinguish Risks Associated with the Breach - To precisely decide the danger, the association should consider the individual data included, the people influenced by the break, the reason and degree of the break just as the conceivable damage from the break.

Warning - All at risk and implied parties should be educated regarding the break. Also, the association ought to recollect their legitimate and legally binding commitments and the dangers implied in the break.

Anticipation of Breaches - Outlined underneath are a couple of precaution estimates that can be taken to guarantee that a break isn't rehashed.

Q3: Whether privacy breach is legal or illegal?

Ans: Yes, breach of privacy without any permission is illegal. The breach of privacy is under the ambient of fundamental rights and comes under the right to life and liberty under article 21 of the Indian Constitution. For cyber security the privacy of an individual is of prime importance and hence cannot escape the legal scope.

Q4: What is a potential privacy breach?

Ans: A protection break happens when individual data is taken or lost or is gathered, utilized or uncovered without power. A protection break happens when individual data is taken or lost or is gathered, utilized or uncovered without power.

Q5: What are the ways to stop privacy breach?

Ans: Following are the ways to stop privacy breach:

Stay Alert. On the off chance that you have been important for an information break, the penetrated organization might send you a notification.

Initiate a Fraud Alert.

Monitor Your Financial Accounts. Monitor Your Credit Reports. Freeze or Lock Your Credit File.

Q6: What is a privacy violation?

Ans: With more and more private information being utilized by web applications, information security has become a critical issue. Incidents involving the harvesting of sensitive data take place on a constant basis all over the world. This stealing and manipulating of private information by malicious attackers is commonly known as a privacy violation.

Q7: What is the punishment for a privacy breach ?

Ans: Section 66E of the Information Technology, Act, 2000(Computer related offenses): Whoever, purposefully or intentionally catches, distributes or sends the picture of a private space of any individual without their assent, under conditions abusing the protection of that individual, will be rebuffed with detainment which might reach out to three years or with fine not surpassing two lakh rupees, or with both.

REFERENCES

[1] https://us.norton.com/internetsecurity-privacy-what-is-a-privacy-breach.html

[2] https://www.colleaga.org/tools/essentials-privacy-breach-management-protocol

SOCIAL MEDIA ACCOUNTS

Social media is a tool that has transformed the digital world with its inception. It has become quite popular these days due to its user-friendly database. In simpler words, the world is at our fingertips all thanks to social media. Because of the availability of internet access, the number of social media users in India has risen to 624 million in 2021, with Meta owned Facebook being the most popular among the general public. When it comes to the good effects of social media, the most important is that it is an excellent tool for education.

People have become more socially conscious of global challenges. Furthermore, it strengthens the bond with loved ones as the distance is no more a barrier due to social media.

> “Social media users in India have grown to a whopping 624 million in 2021 with Facebook as the most favourable.”

FREQUENTLY ASKED QUESTIONS

Q1: What is social media?

Ans: Social media is a web-based platform that allows us to connect, communicate, produce, and share material with individuals from all over the world.

Q2: What are the top three most popular social media apps?

Ans: In the race of popularity, Facebook stands at the first position followed by WhatsApp, Instagram, YouTube, Snapchat, Twitter, and many others.

Q3: How much time does the average person spend every week on media platforms?

Ans: According to a poll on social media usage performed in October and November 2020 across India, the majority of respondents from all generations spent more than six hours per week on social networking sites.

Q4: When did social media first become popular?

Ans: The Six Degrees, a social media site that allows users to submit their profiles, was the first social media platform for building relationships. It was created in 1997. The oldest app currently in use is LinkedIn, which was established in 2002.

Q.5: Is it safe to utilize social media platforms?

Ans: They are safe to use if they are used correctly. Users can manage what others can view about them by using security and privacy settings on most websites.

Q6: Which statutes governs ocial media privacy?

Ans: On the subject of online privacy and data protection, there is no formal legislation. The Information Technology Act of 2000, on the other hand, was passed to address social media privacy concerns. Even though it can't totally protect privacy, it can help to mitigate it.

Q7: What safeguards are in place to protect the user's privacy?

Ans: Sections 43, 66, 66F, and 67 of the Information Technology Act of 2000, as well as the Rules, are among the provisions. The IT Rules 2021 also provide a dual aspect (1) increasing the accountability of the social media platforms (such as Facebook, Instagram, Twitter etc.); and (2) empowering the users of social media by establishing a three-tier redressal mechanism for efficient grievance resolution.

Q8: What are fake and bogus accounts?

Ans: These accounts are set up for malicious purposes. They can be used to propagate false information as well as attempt to hack into other people's accounts.

Q9: How can I filter out such accounts from my list of accounts to follow?

Ans: When you receive follow requests from people you don't know, you can double-check to be sure they're genuine.

The following are two red flags for fake accounts:

- Look over their timelines and connections listings. Are there any accounts that you have in common?
- Do they keep posting the same information/links again?

REFERENCES

[1] https://online.maryville.edu/blog/evolution-social-media/

[2] https://www.toppr.com/guides/essays/essay-on-social-media/

[3] https://www.statista.com/statistics/278407/number-of-social-network-users-in-india/#:~:text=With%20the%20ease%20of%20internet,media%20pla tforms%20as%20of%202020.

[4] https://www.futurelearn.com/info/blog/50-social-media-faqs-answered

[5] https://sproutsocial.com/insights/social-media-questions/

IDENTITY THEFT

Identity Theft or Identity Fraud refers to "any type of crime in which someone wrongfully obtains another person's sensitive data in a way that involves fraud or deception, done for financial gain."

This is a millennium crime and with the advent of technology and the growing exposure to the internet, cyberspace gives easy access to steal an individuals' identity. This offence can be committed by stealing a person's sensitive information like their name, date of birth, debit/credit card details. You know your identity has been stolen if: the bank statement looks fishy, your cheque bounces, you lose your cellular services, unknown or unfamiliar use of your debit/credit card etc. However, you can prevent this by: setting up passwords, avoid using shady links/ websites, limiting our exposure and make sure that you keep your personal/ sensitive information to yourself.

"This is a millennium crime and with the advent of technology and the growing exposure to the internet, cyberspace gives easy access to steal an individuals' identity."

FREQUENTLY ASKED QUESTIONS

Q1: What exactly does Identity Theft mean?

Ans: Identity Theft refers to stealing someone's personal or sensitive information and then pretending to be them to commit offences/ indulge in illegal activities.

Q2: What are the different types of Identity Thefts? Ans: The different types of Identity Thefts are:

1. Financial Identity
2. Social Security Identity
3. Medical Identity
4. Synthetic Identity
5. Child Identity
6. Criminal Identity

Q3: What is meant by Synthetic Identity?

Ans: Synthetic Identity refers to when the criminal mixes original information with made-up facts which gives birth to a new set of facts or a new identity. For example, a criminal stole A's name and date of birth. He then stole B's address and his credit card number. After mixing all the stolen information, he presents himself as C- a person whose identity is not real.

Q4: (a) Can anybody steal my IP address and misuse it?
(b) Is stealing of IP address considered as Identity Theft?

Ans (a): Your IP Address can be stolen and it can be used to retrieve all your sensitive information which can further be misused in multiple ways. However, you can protect yourself (and your IP address) by

setting up a VPN (Virtual Private Network). It gives you privacy and anonymity by creating a private network from a public connection. So, by setting up a VPN, you can use the internet without revealing or exposing your IP address.

Ans (b): If the hacker is successful in retrieving all your personal information and then if they misuse it, then yes, it will be considered as identity theft. However, you can prevent it by setting up a VPN.

Q5: What is meant by identity theft on cyberspace?

Ans: Identity Theft on cyberspace is nothing but stealing of sensitive information from the internet.

Q6: How can I protect myself from being a victim of identity theft?

Ans: You can protect yourself from the menace of Identity Theft by-

- Protect your devices and data by using passwords.
- Don't share your personal information with random strangers or any random/shady site.
- Keep a tab on your transaction statement(s) and if you notice any suspicious activity, contact your bank immediately.
- Keep a check on your social media account(s).
- Be careful while using public wifi or any unsecured network.

Q7: Are there any legal provisions that dealwith identity theft?

Ans: Yes, Section 66C of the IT Act, 2000 deals with identity theft, 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.

Q8: How does the offence affect the victim?

Ans: The victim (of identity theft) can be arrested or detained or punished for the crimes that have been committed using their sensitive information. not only this but it makes them feel unsafe, affects them psychologically, mentally, emotionally and socially.

REFERENCES

1. https://blog.ipleaders.in/all-you-need-to-know-about- identity-theft-in-cyberspace-in-india/
2. https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud
3. https://www.robertmhelfend.com/federal-defense/identity-theft-laws/
4. https://www.businessinsider.in/tech/how-to/what-you-can-do-with-an-ip-address-and-how-to-protect-yours-from-hackers/articleshow/76165946.cms
5. https://us.norton.com/internetsecurity-id-theft-5-red-flags-of-identity-theft.html

BANKING FRAUD

On 20th October 2021, two persons lost 56 lakhs and 6 lakhs respectively in cyber fraud. The first victim was lured into investment in bitcoin trading whereas the second victim was lured with buying websites.

These are a few examples of what a bank fraud would look like. The advent of a cashless economy has also brought some vulnerabilities with it. Banking Fraud befalls when someone attempts to take funds, or is successful in taking funds and other assets from one's account illegitimately. The ambit of 'Bank Fraud' is wide, and it covers Ponzi-Schemes, Pyramid Schemes, Identity Fraud, Phishing, Card Fraud, Skimming, Fund Transfer Scams, and Fake Prizes.

"The advent of a cashless economy has also brought some vulnerabilities with it."

FREQUENTLY ASKED QUESTIONS

Q1: How can I save myself from bank fraud?

Ans: (a) Refrain from giving your account details or other security information to any person or website unless their identity and authenticity are verified. Such details may include One-Time Passwords (OTP), Indian Financial System Code (IFSC), Bank Account Number, ATM Pin.

(b) Refrain from giving your money to any person who offers to place it with a bank on your behalf for a rate of return higher than the prevailing rate.

(c) Do not be distracted when using your bank card.

(d) Exercise utmost care while using your card to make payments on the internet. Make sure that you disclose your Card Verification Value only on secure payment websites.

(e) Beware of calls, letters, e-mails asking for your help to place huge sums of money in an overseas bank.

(f) Do not reply to spam or unsolicited e-mails that promise you some benefit.

Do read the cyber brochure to secure yourself from cyber fraud by the Ministry of Home Affairs at https://cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20fina l.pdf

Q2: What do I do if I find an unauthorized transaction in my account?

Ans: (a) Immediately contact your bank. As per RBI regulations, if illegal transactions are reported immediately bank will pay back the lost amount if it finds there is no fault with the account holder.

(b) File a Police Report.

(c) Block your current account and move your money to your new account.

(d) Monitor your account and credit closely.

Q3: Where can I file such a cyber bank fraud complaint?

Ans: According to the Information Technology Act, 2000, a cybercrime comes under the purview of global jurisdiction. A cybercrime report can be registered in any cyber cell across the Indian territory; however, it is advisable to lodge your complaint online on https://cybercrime.gov.in/Webform/Crime_AuthoLogin.aspx.

Q4: Where can I get my complaint registered?

Ans:(a)Lodge an Online Complaint at https://www.cybercrime.gov.in/Accept.aspx.

(b) Lodge the Complaint at the nearest Police Station.

(c) Lodge the Complaint at District Cyber Cells.

Q5: Where can I register my complaint immediately?

Ans: The Union Home Ministry operationalised the national helpline number 155260 and reporting platform for preventing financial loss due to cyber fraud. An SMS will be sent to you with an acknowledgement number of the complaint with directions to submit complete details of the fraud on the national cybercrime reporting portal (https://cybercrime.gov.in/) within 24 hours.

Q6: What all documents I would be required to make a bank fraud complaint?

Ans: (a) Collect your bank statement for the last six months.

(b) Copy of SMSs received related to the alleged transactions.

(c) Copy of your ID proof and address proof as shown in the bank records.

(d) Print out the alleged email along with the full header of the email.

(e) Details of the alleged transaction made.

Q7: What all documents I would be required to make a bank fraud complaint pertaining to a bitcoin transaction?

Ans: (a) You shall inform the concerned authority about the complete facts about the incident.

(b) Address of Bitcoin.

(c) Amount of Bitcoin involved.

(d) Address from/to whom purchase/sale of Bitcoins is done.

Q8: How can I help if I am not a victim?

Ans: Register as 'Cyber Volunteer' on National Cybercrime Reporting Portal. The Cyber Crime Volunteer Program aims to bring together citizens having a passion to serve society in making cyberspace clean and safe.

REFERENCES

[1] Hyderabad Cyber Fraud: MNC staffers lose Rs. 60 lakh in two cases, THE NEW INDIAN EXPRESS (Oct. 20, 2021, 10: 37 AM), https://www.newindianexpress.com/cities/hyderabad/2021/oct/20/hyderabad-cyber-fraud-mnc-staffers-lose-rs-60-lakh-in-two-cases-2373402.html.

[2] 12 held by Delhi Police for attempts of unauthorized withdrawal from high-value NRI account, ANI NEWS (Oct. 19, 2021, 14:20 PM), https://www.aninews.in/news/national/general-news/12-held-by-delhi-police-for-attempts-of-unauthorised-withdrawal-from-high-value-nri- account20211019123416/.

[3] SECURE Online Financial Services!, MINISTRY OF HOME AFFAIRS, https://www.cybercrime.gov.in/pdf/Financial%20Fraud%20Brochures%20fi nal.pdf.

[4] Ashwini Kumar Sharma, What to do if you lose money to bank fraud, MINT (Sept. 16, 2021, 23:08 PM), https://www.livemint.com/money/personal-finance/what-to-do-if-you- lose-money-to-a-bank-fraud-1568654707964.html.

[5] CYBER CRIME UNIT, DELHI POLICE, http://www.cybercelldelhi.in/Report.html.

[6] Govt. launches national helpline no. to report cyber crime; all you need to know, MINT (Jun. 7, 2021, 23:07 PM), https://www.livemint.com/news/india/govt-launches-national-helpline- no-to-report-cyber-crime-all-you-need-to-know-11623950388095.html.

[7] NATIONAL CYBER CRIME REPORTING PORTAL, https://www.cybercrime.gov.in/Webform/FAQ.aspx.

[8] Parliament Proceedings| Cyber volunteer programme rolled out for 'cyber hygiene promotion', Home Ministry informs Parliament, THE HINDU (Mar. 09, 2021, 20:01 PM), https://www.thehindu.com/news/national/parliament-proceedings-cyber-volunteer-programme-rolled-out-for-cyber-hygiene-promotion-home-ministry-informs-parliament/article34029289.ece.

PORNOGRAPHY DISTRIBUION

The act of creating, publishing, displaying or distributing pornographic content constitutes pornography distribution. The use of cyberspace to do so is called cyber pornography and is punishable in India under section 67, Information Technology Act, 2000. The easy accessibility of such content has adverse effects on young minds. Moreover, it leads to the sexual exploitation of women and children. Witnessing the ill effects of pornographic content on society, India banned porn websites in 2013, 2015 and then again in 2018. Various sections of the Information Technology Act, 2000 and the POCSO Act, 2012 deals with pornography. However, more measures need to be taken to eliminate such content from all platforms and make cyberspace more resourceful.

“The act of creating, publishing, displaying or distributing pornographic content constitutes pornography distribution.”

FREQUENTLY ASKED QUESTIONS

Q1: What is Pornography?

Pornography is a representation of sexual behaviour in books, pictures, statues, films, and other media that is intended to cause sexual excitement. The distinction between pornography (illicit and condemned material) and erotica (which is broadly tolerated) is largely subjective and reflects changing community standards.

Q2: What does the distribution of pornography mean?

Ans: Pornography distribution includes publishing, transmitting, creating and displaying pornographic content. This is punishable under Sections 67, 67A and 67B of the Information Technology Act, 2000.

Q3: Why is pornography distribution bad?

Ans: The creation of pornographic content leads to the sexual exploitation of individuals. It also promotes paedophilic behaviour. Not only this, but porn also propagates immoral practices such as the objectification of women, normalization of sexual activity without or even against consent, etc. A number of victims of human trafficking also end up as sex workers for the porn industry.

Q4: If porn websites are banned in India, does it mean that I am liable to be punished for watching porn on my devices?

Ans: No, watching porn on a personal device is not illegal in India. However, watching or storing pornographic content which depicts child pornography or rape or violence against women is an offence even if it is being watched in a private space.

Q5: What can I do to prevent pornography distribution?

Ans: Anyone can report a case of pornography distribution through the helpline number: 155260. One can also become a cyber volunteer for the government through the website https://cybercrime.gov.in

Q6: What is CSAM?

Ans: Child Sexually Abusive Material (CSAM) refers to material containing sexual image in any form, of a child who is abused or sexually exploited. Section 67 (B) of the IT Act, 2000 states that "it is punishable for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form".

Q7: Whom should I inform if I see any content displaying the sexual exploitation of minors?

Ans: Child pornography is a serious offence against society. In order to track and take down cases of child porn, the Central government has created a centralised portal https://cybercrime.gov.in/Webform/Helpline.aspxand, a helpline number 155260 to register all such complaints. One can also dial 1098 to report cases of children in distress.

Q8: What should I do if I become a victim of cyber pornography?

Ans: A victim of cyber pornography can approach the police in 3 ways.

The exclusive website https://cybercrime.gov.in is founded just for specific offences related to cyberspace. One can easily file a complaint on the website regarding any cyber crime committed against him/her.

Secondly, the local police stations can be approached for filing complaints just as the cybercrime cells specially designated with the jurisdiction to register complaints.

Lastly, the provision of E-FIR is now available in many states across India. Anyone can file a complaint online by visiting the respective website of the state police.

Q9: Where can I learn more about cybercrimes in India?

Ans: You can learn more about cybercrimes and cyberlaw on www.cybercrime.in and www.mha.gov.in.

REFERENCES

[1] https://www.financialexpress.com/india-news/govt-defines-child-pornography-brings-digital-or-computer-generated-content-under-it/1641214/

PEDOPHILES

The anonymity, rapid transmission and unsupervised nature internet offers make cyberspace a playground for pedophiles. Such illegal activities can be categorised into two types, mainly, child sexual predating and child pornography, both of which are prohibited and punishable under the Indian law. The trend of using the internet to lure children is on the high rise as pedophiles can pose themselves in any way they want to. Furthermore, parents either do not have the technical knowledge about the darker side of the web or they feel hesitant talking about such threats due to its obscene nature. With the unprecedented growth of such activities all over the globe, awareness and regulation is the primary key to protect our children from such predators.

“Illegal activities can be categorised into two types, mainly, child sexual predating and child pornography.”

FREQUENTLY ASKED QUESTIONS

Q1: What is pedophilia and who are online pedophiles?

Ans: Pedophilia is the sexual preference for or a strong sexual interest in prepubescent or early pubescent children. People who view child pornography (online voyeurs), make and distribute child pornography and child sexual abusers who use the Internet to achieve their ends (online predators) are online pedophiles.

Q2. What are the ways in which pedophiles pose to lure in children online?

Ans: There are mainly two ways: those who pretend to be a young person with an intention to manipulate their potential victims to the point where they can befriend them and sexually abuse them and those who do not lie about their age or sexual interests and introduce themselves as a confidant or a mentor who will help the young person discover and explore.

Q3. What kind of children do the pedophiles target?

Ans: In terms of gender, approximately 75% of the victims are reported to be female. Children with low self-esteem who are often neglected socially and spend long periods of time online have been identified as high potential targets.

Q4. What are the common playgrounds used by pedophiles on the Internet?

Ans: Pedophiles target websites including chat rooms that feature subjects that attract children and teenagers, such as games, music, sports, or fashion. Some of them include Chatzy chat rooms, Omegle and Chathub where they can add such interest and pose as peers to

interact with children. Some also use popular social media sites to message children directly using fake and suspicious accounts.

Q5. How to detect online pedophiles?

Ans: Pedophiles usually take some time to form a bond with the potential child victim by asking questions that turn more private as they start to gain the child's trust over time. It starts with greetings before they ask simple questions related to age and interests, what the child looks like and the child's family relations. Then the conversation gradually becomes more explicit with the exchange of pictures and child pornographic videos before they suggest meeting face to face.

Q6. What law provides provisions related to prohibition and punishment of child-related offences online in India?

Ans: There are mainly two acts that cover the subject. The Information Technology Act, 2000 (IT Act) punishes child pornography, child grooming or exploitation and a person involved in such activities in any way is punishable with imprisonment for a term which may extend upto five years and imposed fine which may extend upto Rs.10 Lacs under the IT Act 2000. The Protection of Children from Sexual Offences Act, 2012 (POCSO) which provides legal protection against sexual assault, sexual harassment and child pornography punishes any person involved with imprisonment which can extend to five years and is liable to fine for first-time offenders and seven years for subsequent conviction.

Q7. What are some measures that can be taken by the parents to protect their children?

Ans: Educating children about the risks on the internet and how to avoid them should be the foremost priority of every parent. Parents should be understanding of their child's curiosity and should talk through it instead of straightaway blocking such talks. In addition, parents should be mindful of their children's behavioural patterns by monitoring their internet activity, setting up time limits and guidelines

to be followed and using child-friendly settings on browsers to block explicit websites.

Q8. What safeguards can be practiced as a society?

Ans: More aware we are of the problem, better will be the solutions we come up with. So, as a society, we should create more awareness about this issue not only for the children but their parents as well by talking more about it. Conducting topic related seminars and sessions for parents and inculcating it into the 'Stranger danger' curriculum in schools while giving the children a platform to share their feelings if they ever come across a potential threat are some ways to do so.

REFERENCES

[1] https://www.inspq.qc.ca/en/sexual-assault/fact-sheets/online-pedophilia-and-cyberspace

[2] https://ojjdp.ojp.gov/sites/g/files/xyckuh176/files/jjjournal/jjjournal1598/net.html

SEXUAL PREDATORS

Crimes through the internet that are against minors involve deceit and begin with communication between adults and minors over the internet with the objective of coercing them into illegal sexual activity. Chat rooms, instant messaging, Internet forums, social networking sites, cell phones, and even video game consoles, online areas like these attract predators because they permit them to make contact with the victims without drawing public attention. In fact, the minors are mostly confederate with offenders often using fake promises of love and romance to seduce victims to meet. Those who exploit others in a sexual manner may not be just seeking sex. Rather, they see sex as a form of dominance and control.

A parent who is accessible and has open communication with their children will be better able to protect them from predators. As children grow, they should be able to discern what is and isn't appropriate behaviour and express this openly with their families

> "Adults communicating with children over the Internet with the goal of coercing them into illegal sexual activity."

FREQUENTLY ASKED QUESTIONS

Q1: Are online predators available through social networking sites only?

Ans: No, these people are around you and can contact you through games and online sites also.

Q2: Is there any specific age of such criminals?

Ans: No, sexual predators can be of any age.

Q3: Should I trust people whom I meet through the internet?

Ans: No, till the point you are sure about their intentions.

Q4: Do social media platforms provide features to safeguard my privacy?

Ans: Yes, the privacy of your account is an essential feature.

Q5: Can I file a complaint against offensive or intimate remarks passed through the internet?

Ans: Yes, social media platforms provide us with the opportunity to report such messages and people.

Q6: How do these offences take place?

Ans: These offences take place through the internet.

Q7: Why do sexual predators stalk people and give intimate remarks?

Ans: They want to take advantage of you and fulfil their sexual desires by forcing their will on you.

Q8: Is this crime punishable under any legal statute?

Ans: Yes, it is punishable under the Indian Penal Code (IPC) as well as Information Technology (IT) Act. For instance, Sections 354 and 509 of the IPC and 66A and 67A of the IT Act.

REFERENCES

[1] https://indiankanoon.org/doc/1965344/#:~:text=The%20Information%20Technology%20Act%2C%202000&text=(1)%20This%20Act%20may%20be,outside%20India%20by%20any%20 person.

ONLINE GAMING ADDICTION

"Excessive of everything is bad." Video game addiction is compulsive or uncontrolled use of video games, in a way that causes problems in other areas of the person's life. Especially among the Gen Z, it has become much of a concern across the world.

It simply means spending more screen and gaming time sometimes even ignoring the things happening around. According to a study published by the Indian Journal of Public Health in September 2020, over half of the participants in a survey featuring students said they have been spending more time on gaming since the pandemic.

> "Excessive of everything is bad."

FREQUENTLY ASKED QUESTIONS

Q1: Is online gaming addiction a real problem and disorder?

Ans: Many countries consider it to be a real problem and even a gaming disorder, that results in significant impairment to an individual's ability to function in various life domains over a prolonged period of time.

Q2: Who is most likely to get addicted to online games?

Ans: It can be all ages but especially the age group of 12- 23 involving teenagers and students.

Q3: What kind of games can be an addiction to me?

Ans: The team games or massively multiplayer online role- playing games (MMORPGs) where you communicate with the members and get a sense of recognition when you perform well are considered the most addictive genre. For example; games like PUBG and Fortnite.

Q4: What causes such addiction?

Ans: The designing of video games by making them just challenging enough to keep you coming back for more but not so hard that the player eventually gives up, such causes addiction. In short, success acts like a gamer magnet.

Q5: How has the Covid pandemic led to an increase in such addiction?

Ans: The pandemic got the world to set an online platform for everything, for instance, online classes that have led to a rise in kids suffering from problems including screen or online gaming addiction happened.

Q6: What are the signs and symptoms of this addiction?

Ans: (a) Feelings of restlessness/irritation.

(b) Lack of concentration due to preoccupied mind.

(c) Isolation from people to spend more time to play.

(d) Fatigue.

(e) Migraine/eye strain.

(f) Poor personal hygiene.

(g) Unhealthy body.

Q7: What are the effects of online gaming addiction?

Ans: It causes physical, mental and psychological damage increasing anxiety, depression, high heartbeat and blood pressure due to too much excitement and stress in players. It can put you in danger as some games lack cyber safety and cause huge monetary loss as you (the player of the game) can misuse money in some futile game.

Q8: How can we or our parents help tackle this addiction?

Ans: (a) Individual Counselling can help you to address the various issues, and also help you to reduce your compulsions to play.

(b) Behaviour modification techniques can help you to recognise what the trigger points are for you to engage in excessive gaming, and also help you identify healthier alternatives.

(c) It is not a common occurrence for adults that are addicted to gaming to go into family therapy. However, if you are a teenager or a child, family therapy is highly advisable.

Q9: Are there any laws or norms regarding online gaming addiction?

Ans: No such policy is formulated yet for the protection of children from online gaming addiction as well as to constitute a regulatory authority to monitor and rate the content of both offline and online games. But in July'21, when an NGO filed a petition regarding the same, the Delhi High Court discussed that there is a need for a national policy that lays emphasis on the role of schools and the Cyber Cell in tackling the issue.

REFERENCES

[1] https://www.psychguides.com/behavioral-disorders/video-game-addiction/

[2] https://www.who.int/news-room/q-a-detail/addictive-behaviours-gaming-disorder

[3] https://www.thehindu.com/news/national/hc-asks-centre-to-decide-on-a-petition-seeking-a-policy-to-protect-children-from-gaming-addiction/article35597409.ece/amp/

[4] https://www.thehindu.com/sci-tech/health/gaming-disorder-increases-during-pandemic/article36812568.ece/amp/

CYBER CASINO

Online gambling is a mode of gambling facilitated by technological advancements and internet availability, including wagering and probability-based gaming activities offered through internet-enabled devices including computers, smartphones, tablets and other related devices. It is largely inclusive of automated activities that can be conducted in private, at the ease of one's home enabling instant bets and their outcomes by merely using high- speed internet connections. It is a rapidly growing phenomenon, with its ease to access, increasing participation, luring outcomes but along with increasing problems and risks. Thus, in the sheer public interest, such form of gambling spurs centralised laws for regulation or limitation.

"It is largely inclusive of automated activities that can be conducted in private, at the ease of one's home enabling instant bets and their outcomes by merely using high-speed internet connections."

FREQUENTLY ASKED QUESTIONS

Q1: What are the types of online gambling in India?

Ans: The internet has a wide variety of online gambling such as: Poker, Online Casino and Sports Betting.

Q2: Is online gambling legalised anywhere in India?

Ans: Yes, in India, Sikkim was the first state to legalize online gambling, other states that allow online gambling are- Nagaland, Goa, West Bengal, Daman.

Q3: What is the legal age for online gambling in India?

Ans: The legal age of online gambling as legalised by certain states is mostly 18 years in India.

Q4: Is skill based online gambling legal in India?

Ans: Yes, the Supreme Court of India in R.M.D. Chamarbaugwala v. Union of India, (1957) S.C.R 874 heldthat where there is a certain level of skill involved in a gameit would not be considered gambling. Game of skills refer to games where success depends upon superior knowledge, training, attention and adroitness of the player. Thus, the Supreme Court dismissed an appeal against Rajasthan High Court decision in Chandresh Sankhla v. State of Rajasthan, Civil Writ Petition No. 6653/2019 which held that online fantasy sport platform, Dream11,involves skill and thus is not gambling. Therefore, applications such as- Dream11, My Team11, My11 Circle, Fan fight Fantasy and many others are legally operational in India.

Q5: What is the legal status of online gambling in India?

Ans: Gambling in India is a state subject and entitles the state to formulate laws governing such activities. There is no stringent central law that directly regulates online gambling, though the Payment and Settlement Act, 2008 authorizes the Reserve Bank of India to operate a payment system for regulation of electronic payment mechanisms. Also, Foreign Direct Investment (FDI) policies restricted enterprises to involve in lotteries, gambling and betting activities. These activities are regulated by the IT Act, 2000 although there are no specific provisions that explicitly makes online gambling illegal within or outside India.

Q6. What are the consequences of online gambling convincing its ban?

Ans: The consequences of online gambling are signs of excessive addiction, increased suicidal deaths, easy accessibility, involvement of third-party loan companies, money laundering, invasion of privacy, access to personal details via online applications, absence of stringent laws etc. that demands for a ban on online gambling.

Q7: Will online gambling winnings be taxed in India?

Ans: Yes, when a person plays betting games on online gambling platforms such as – Rummy, a Tax Deducted at Source (TDS), tax is automatically deducted from their winnings at the source itself.

Q8: Whom to approach when duped in online gambling?

Ans: The aggrieved person should immediately register a complaint at a local police station or cyber crime authorities or other concerned agencies such as Economic offences wings.

REFERENCES

[1] R. M.D Chamarbaugwala v The Union of India 1957 AIR 628.

[2] Avinash Mehrota v the state of Rajasthan SLP(civil) 18478/2020.

[3] http://www.helplinelaw.com/immigration-appeal-and-others/GAMLSI/gambling-in-india.html.

[4] https://iclg.com/practice-areas/gambling-laws-and-regulations/india.

CYBER RADICALIZATION

With the advent of technology, spreading false propaganda and metanarratives to incite people against one another has never been easier. Social Media proves to be the main culprit which lured in the vulnerable crowd is drawn in with a promise of validation of their perspectives and subtly manipulated to a more alienated purview altogether. Instances of social media content being the inciting factor have often come to light in recent times with a prominent example being that of an environment activist Disha Ravi, who is accused of conspiracy against the Union of India due to her interaction with Khalistan Supporters through the virtual interface.

“Social Media proves to be the main culprit which lured in the vulnerable crowd is drawn in with a promise of validation of their perspectives and subtly manipulated to a more alienated purview altogether.”

FREQUENTLY ASKED QUESTIONS

Q1: What exactly does Cyber Radicalisation denote?

Ans: The meaning of Cyber Radicalisation can be derived by a simple dissection of its two components, wherein thus it means the use of information technology or computers for the propagation of narratives that radicalise an individual.

Q2: Which platforms are used commonly for cyber radicalisation?

Ans: Social media platforms have been a convenient interface for extremists to prey upon susceptible individuals prone to Radicalisation and further recruit them to extend their propaganda. Some examples of platforms thus commonly used include Meta owned Facebook, Whatsapp, Instagram, LinkedIn, YouTube, Twitter, etc.

Q3: Which tools are used to radicalise youth through electronic mediums?

Ans: The internet is used for propagating wrong information through mass texts, toolkits and videos that convey false and alienating metanarratives. This has further been financially backed by the exploitation of unregulated online payment methods as well.

Q4: Why does Cyber Radicalisation affect the youth more?

Ans: Although anyone can be radicalised, impressionable youth and children are more susceptible due to their extensive screen times and interaction with social media. The psychological vulnerability for radicalisation is the highest at this age.

Q5: When can any content found online be deemed to be radical?

Ans:Any communication which instigates violence, consists of instructions on how to cause violence, incites people against the Government or includes any divisive false information can be deemed to be radical.

Q6: How to recognise if someone is at risk of being radicalised?

Ans:Behavioral changes that can be used as cues to recognise if someone is being radicalised include a change in social circle, unwillingness to discuss opinions, comments that suggest hatred towards different factions and direct participation in the propagation of such hate.

Q7: What are the safeguards that can be undertaken to curb radicalisation through online mediums?

Ans: Some common precautions include limiting access to harmful content online in public buildings like schools, and ensuring appropriate action is taken to remove harmful content from the internet by a combined effort of citizens and the Government alike.

Q8: What specific initiatives have been taken by the Government to tackle the menace of Cyber Radicalisation?

Ans: Two new divisions, Counter-Terrorism and Counter Radicalisation Division and the Cyber and Information Security Division, were created in the Ministry of Home affairs in 2017, so as to give focused attention to the issues relating to counter radicalization, etc.

REFERENCES

[1] Archetti, C., Terrorism, Communication and New Media: Explaining Radicalization in the Digital Age, Perspectives on Terrorism, 9(1) (2015), available at http://www.terrorism analysts.com/pt/index.php/pot/article/vie w/401

[2] Prevent Strategy, HM GOVERNMENT (2011) (Pg 77), available at https://assets.publishing.service.gov.uk/government/ uploads/sy stem/uploads/attachment_data/file/97976/prevent-strategy- review.pdf

[3] Left Wing Extremism Division, MINISTRY OF HOME AFFAIRS, available at https://www.mha.gov.in/division_of_mha/left-wing- extremism-division.

[4] Creation of CTCR and CIS Divisions in MHA, Press Information Bureau (07 FEB 2018, 4:45PM), available at https://pib.gov.in/ Pressreleaseshare.aspx?PRID=1519500.

PORT SCANNING

Port scanning is one of the most popular forms of inspection ahead of a hack, helping attackers determine which ports are the easiest to hack into. Hackers use various port-scanning techniques for locating holes within specific computer ports. Intruders seek these opportunities and gain access to open ports and plan and attack. There are a total of 65,535 ports in each IP address, and hackers may scan each and every one of them to find any that are not secure.

As is often the case with computer security, the best offence is a good defence. If you have an openly accessible server, your organization framework will be helpless against port outputs.

> “There are about 65,535 ports in each IP address, and hackers may scan each one to find any that are not secure.”

FREQUENTLY ASKED QUESTIONS

Q1: How many ways are there for hackers to use port scanning?

Ans: The various kinds of port outputs that programmers use is -

1. Vanilla: The scanner attempts to associate with all 65,535 ports.
2. Strobe: A more engaged sweep, searching for known services to exploit.
3. Fragmented Packets: The scanner sends parcel parts as a way to sidestep packet filters in a firewall.
4. User Datagram Protocol (UDP): The scanner searches for open UDP ports.
5. Sweep: The scanner pings a similar port across more than one machine to see which computers are active.
6. FTP Bounce: The scanner goes through an FTP server to mask the source.
7. Stealth: The scanner blocks the scanned computer from recording the port sweep.

Q2: How does port scanning work?

Ans: Port sweeps send requests to each port, asking to interface to an organization. The output then, at that point, makes note of the ports that react and which seem unprotected.

Once the attacker has determined weak ports in a network, the scan will classify them into three categories: Open, closed, or filtered.

Q3: What information is shared with the hacker if my port has been scanned?

Ans: Port scanning provides the following information to attackers:

What services are running.

Which users own the services.

If anonymous logins are allowed.

What network services require authentication.

Q4: How to prevent port scanning?

Ans: If you have a publicly accessible server, your network system will be prone to port scans. However, there are several safety measures that may come in handy in preventing a port scan-

Install a Firewall: A firewall will facilitate forestall unauthorized access to your private network. It controls the ports that are unprotected and their visibility. Firewalls can also detect an ongoing port sweep and stop it immediately.

TCP Wrappers: TCP wrappers can give administrators the flexibility to allow or deny access to the servers based on their IP addresses or domain names.

Uncover Holes in the Network: Conduct your own internal port scan to find out if there are more ports open than required. Regularly check your system to determine present vulnerable points that could be exploited.

Q5: How to check which ports are open?

Ans: You can check which ports in your device are open or closed. There are different methods for Windows and Apple PCs to do so.

For Windows: https://www.howtogeek.com/howto/28609/how- can-i-tell-what-is-listening-on-a-tcpip-port-in-windows/

For IOS devices: https://wilsonmar.github.io/ports-open/ Q6: How long does it take to scan ports?

Ans: Scanning one port on 65,536 hosts at 1 second per host takes about 18 hours. If you scan one extra port on each of the 65,536 hosts

and allow 1 second per host, it would take an extra 18 hours to scan that extra port.

Q7: Is port scanning legal?

Ans: As such, no concrete law exists to ban port scanning. At the state and local levels, no clear guidelines are provided.

However, while it is not publicly illegal, port and vulnerability scanning without permission can get you into trouble.

Q8: Can you get arrested for port scanning?

Ans: The amount of risk that comes with the desire to scan a port is based on whether it is authorized. If you do not have permission, then you are at a greater risk of backlash. If you do have permission – then get it in writing and signed.

Civil lawsuits – The owner of a scanned system can sue the person who conducted the scan. Even if it is proven unsuccessful, the case can waste time and resources on legal costs.

Complaints to ISP – The owner of a scanned system can report the scanner's IP address to the associated ISP. Many ISPs prohibit unauthorized port scanning. Some will act in ways such as with reprimands or cancelling of service.

REFERENCES

[1] https://www.datto.com/blog/what-is-port-scanning

[2] https://www.techopedia.com/definition/4059/port-scanning

[3] https://www.varonis.com/blog/port-scanning-techniques/

[4] https://www.avast.com/en-in/business/resources/what-is-port-scanning#pc

CYBER BULLYING

The term Cyber Bullying is defined as bullying or exploitation of an individual by the means of the internet. This form of bullying has been seen significantly in the digital age. The term bullying in itself is derogatory and when it is done over the digital sphere it is more devastating for the victim. The most common places where cyberbullying occurs are:

- Social Media, such as Facebook, Instagram, Snapchat, and Tik Tok; Text messaging and messaging apps on mobile or tablet devices;
- Instant messaging, direct messaging, and online chatting over the internet;
- Online forums, chat rooms, and message boards, such as Reddit;
- Email;
- Online gaming communities.

The most vital issue of cyber bullying is that in many cases the identity of the bully is also unknown and hence actions cannot be taken against the bully. The main aspect of cyber bullying are - Online Sexual harassment and online stalking and the reports for the same have seen a significant rise in recent times.

“The main aspect of cyber bullying are - Online Sexual harassment and online stalking and the reports for the same have seen a significant rise in recent times.”

FREQUENTLY ASKED QUESTIONS

Q1: What is cyberbullying?

Ans: Like bullying in person, cyberbullying (also known as online bullying) is repeated, deliberate behaviour intended to tease, demean, or harass someone in a less powerful position. By contrast, cyberbullying uses electronic media and information technology as the means for carrying out the harassment. Since cyberbullying is online, it exposes the victim to harm 24 hours a day, can be made anonymously, and can potentially be broadcast to a far wider audience than in-person attacks.

Q2: How is cyberbullying different from in-person bullying? Ans:

Cyberbullying happens 24x7 and could happen in your home.

Cyberbullying is anonymous and potentially broadcast to wider audience. Posts can be difficult to remove and can last forever.

Cyberbullies don't have to confront people face-to-face, which makes it easier to do Cyberbullying is pervasive.

Q3: How can I prevent cyberbullying?

Ans: Some ways to prevent cyber bullying are-

Don't forget that even though you can't see a cyberbully or the bully's victim, cyberbullying causes real problems. If you wouldn't say it in person, don't say it online. Don't write it. Don't forward it.

Refuse to pass along cyberbullying messages Tell friends to stop cyberbullying

Block communication with cyberbullies Report cyberbullying to a trusted adult

Speak with other students, teachers and school administrators to develop rules against cyberbullying

Raise awareness of the cyberbullying problem in your community by holding an assembly and creating fliers to give to younger kids or parents

Q4: If a parent suspects their child is a cyberbully, what should they do?

Ans: The parent can start by teaching the child about social responsibility. Have the child imagine the situation in reverse. Cyberbullying can spiral to a massive level, even though cyberbullies may have just sent a post or text that initially started off as a joke. It is also important to teach this same lesson to cyberbully victims because many victims in turn can become cyberbullies themselves.

Q5: What can I do if my child is involved in online bullying?

Ans: Be supportive and responsive to all kids who have been involved in bullying situations, whether they are being bullied or are bullying others (or both).

Get the full story: Listen carefully and take it seriously. It may not be simple: the child or teen may be the target of bullying or maybe bullying someone as well. Recognize, too, that kids may be reluctant to talk about it.

Make a plan together. Ask what you can do to help, and make the child's answers the basis for the plan. Discuss what each of you will do. Get help. Find counsellors or other experts trained to deal with kids who have been bullied or have bullied others.

Q6: What are the legal provisions for safeguards for women against Cyber Bullying?

Ans: The Press release on 'Digital Exploitation of Children', by the Ministry of Women and Child Development states that sections 354A and 354D of the IPC provides punishment for cyber bullying and cyber

stalking against women. Cyber-stalking of women was recognised as an offence, subsequent to the insertion of section 354D in the IPC through the Criminal Law (Amendment) Act, 2013.

Q7: How can I prevent cyberbullying and stay cyber-safe?

Ans: You can refuse to pass along cyberbullying messages. Tell friends to stop cyberbullying, block communication with cyberbullies, and report cyberbullying to a trusted adult. To stay cyber-safe, never post or share your personal information online or your friends' personal information (this includes your full name, address, telephone number, school name, parents' names or credit card number). Never share your Internet passwords with anyone and never meet face-to-face with someone you only met online.

Q8. What are the cyberbullying helplines available for the victims?

Ans: Victims of cyber fraud can call the helpline number 155260, which is manned and operated by the state police concerned. Currently, the number would be operational in seven states and Union territories (Chhattisgarh, Delhi, Madhya Pradesh, Rajasthan, Telangana, Uttarakhand and Uttar Pradesh)

ABOUT

THE CENTRE OF EXCELLENCE FOR CYBER LAW

The Centre of Excellence For Cyber Law is one of the Centres of Excellence of Vivekananda School of Law and Legal Studies, Vivekananda Institute of Professional Studies. It is an initiative for appraising the ubiquity and dynamics of cyberspace; recognising the compelling need for a technologically neutral and uniform legal structure that deals with cyberspace and Information Technology. It also acknowledges the requirement of possessing cyberspace knowledge as an inescapable qualification in the era of Fourth Industrial revolution. Inevitably, cyber law has become an indispensible necessity working towards regulation of this borderless space in order to create a protected sphere which is capable of safeguarding the interest of various stakeholders.

In the light of the emerging contours of cyberspace, meteoric development in technology, diverse legal frameworks across the globe, the popping controversies surrounding the balancing of interests not only of individuals but also of nations, the Centre is proposed to function with a broad objective to explore techno-legal aspects of the critical and novel facets of cyberspace. Additionally, the Centre interprets the National and International developments in the field of Cyber law by integration of interdisciplinary approach through awareness, research and training programmes.

FACULTY COORDINATORS

Ms. Ritika Chauhan, Assistant Professor, VSLLS, VIPS
Dr. Nipun Gupta, Assistant Professor, VSLLS, VIPS
Ms. Ravneet Sandhu, Assistant Professor, VSLLS, VIPS

EXECUTIVE MEMBERS

Mr. Abhishek Singh, B.A.LL.B. (Semester IX)
Ms. Chetanya Goswami, B.B.A.LL.B. (Semester V)

EDITED & COMPILED BY

Ms. Ritika Chouhan,
Assistant Professor, VSLLS, VIPS
Ms. Manya Manchanda, B.A.LL.B. (Semester IX)

VIVEKANANDA INSTITUTE OF PROFESSIONAL STUDIES

AU-Block (Outer Ring Road), Pitampura, Delhi-110034

+91 11 27343402, +91 11 27343403 vipsedu@vips.edu