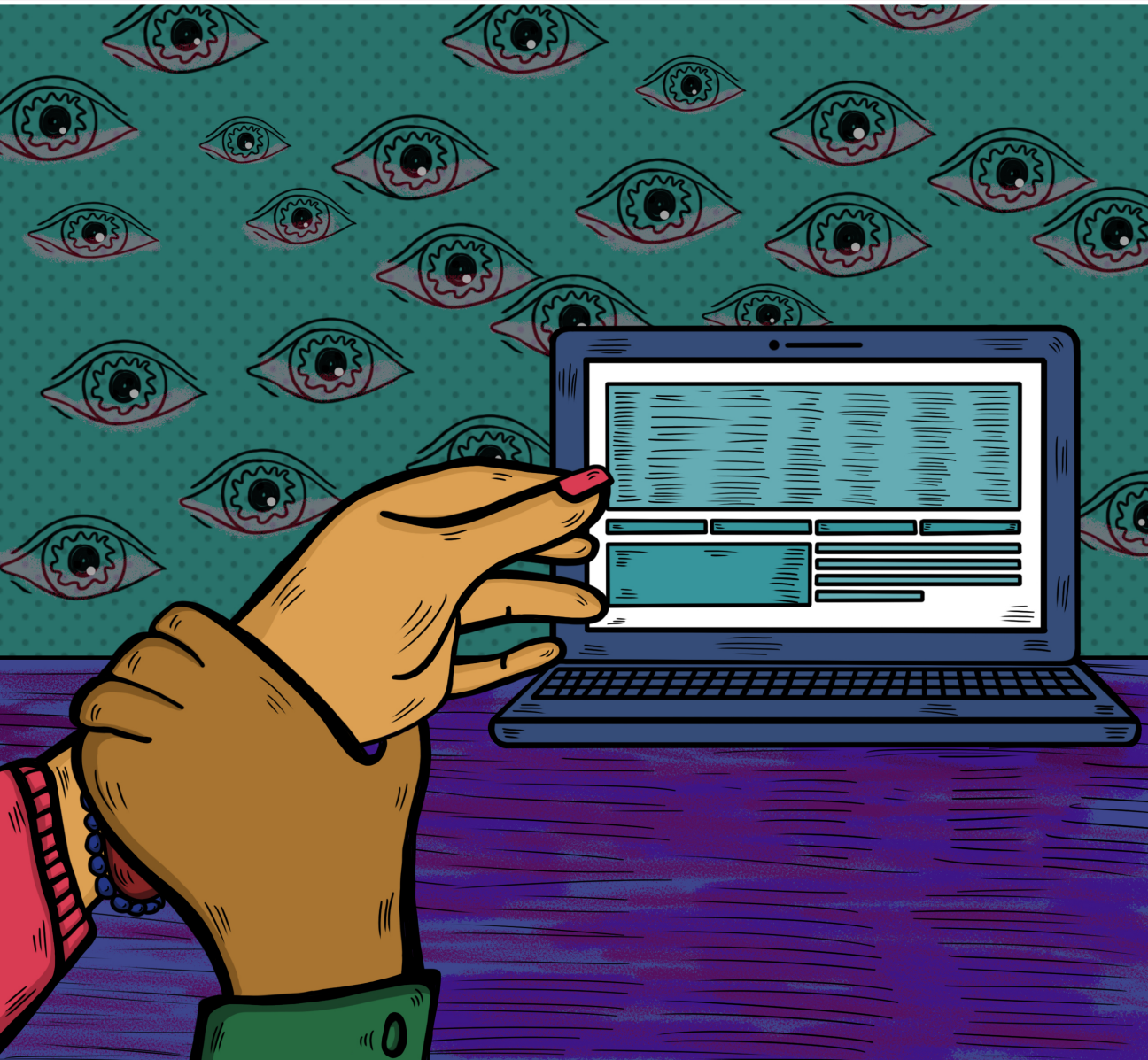




DigitalRightsFoundation
"KNOW YOUR RIGHTS"

Countering Digital Threats

Toolkit



Acknowledgment

We would like to express our sincere gratitude to all the people who contributed to the development of this toolkit on countering cyber threats. This toolkit aims to provide practical guidance and resources for individuals and organizations who face cyber risks and challenges in their daily activities. We hope that this toolkit will help them to enhance their cyber resilience and security.

First and foremost, we would like to express our sincere gratitude to our Executive Director, Ms. Nighat Dad, who reviewed the work of her team and provided valuable insights into the technical aspects of the toolkit. Secondly, we acknowledge the efforts and dedication of our legal intern, Ali Abbas Gilani, who utilized his research skills to develop this toolkit on countering cyber threats. We greatly appreciate his commitment and enthusiasm for the project.

Furthermore, we are also grateful for the crucial ideas and input from the legal department of the Digital Rights Foundation, which played a pivotal role in authoring this toolkit. The realization of this toolkit would not have been possible without the efforts of Ms. Irum Shujah (Advocate High Court), Ms. Shafia Imran (Advocate), Ms. Aqsa Javed (Advocate), and Ms. Minahil Farooq (Advocate). Their expertise and insights were invaluable in shaping the content and direction of this toolkit. Additionally, the Communications, Research, and Helpline departments of the Organization provided valuable input for the completion of this product.

We hope that this toolkit will serve as a useful resource for anyone who wants to learn more about cyber threats and protecting themselves online. We welcome any feedback or suggestions for improving the toolkit in the future. Thank you for your interest and support.

Table of Contents

Chapter 1 - The Do's and Don'ts of Internet Safety: Some Preventive Measures

Internet Safety: Dos and Don'ts	1
Don'ts	1
DO's	4
Procedure to Remove Unlawful Online Content	4

Chapter 2 - Interpreting PECA with Authorities: Comprehending Cyber Offences

Legal Avenues to Handle Cyber Offences	7
Law	7
Rules	7
Authority	8
Interpreting Prevention of Electronic Crimes Act 2016	8
Hacking	8
Glorification of an Offence	9
Cyber Terrorism	10
Hate Speech	11
Electronic Frauds	12
Javad Khan vs. State	13
Sheraz Khan vs. State	14
Offences against modesty of a natural person and minor	15
Child Pornography	16
Umer Khan vs. State	17
Hassan Nawaz vs State	18
Adil Nadeem vs. State	19
Cyber Stalking	20
Identity Theft	21

Chapter 3 - Punitive Measures for the Violations under PECA	23
Offences Under the Prevention of Electronic Crimes Act, 2016	23
Chapter 4 - Cyber Crime Wing - FIA	26
Cybercrime Wing Offices	26
Procedure to Submit a Complaint with the FIA	27
SCHEDULE 4 ANNEX-A FORM	28
From Complaint to Raid	30
SCHEDULE V-SEIZURE MEMO - (FORM-I)	31
Chapter 5 - DRF Cyber Harassment Helpline	33
What We Offer?	33
System and Procedures	34
What is Consent?	35
Chapter 6 - Safety Measures that the User can take	37
Some General Tips	37

Chapter 1

THE DO'S AND DON'TS OF INTERNET SAFETY: SOME PREVENTIVE MEASURES

In the ever-evolving digital landscape, it is important to understand the fundamentals of online safety and security. This requires taking an in-depth look into the legal framework laid down by the Prevention of Electronic Crimes Act (PECA) 2016, viewed through the lens of established practices and precedents set by relevant authorities in Pakistan.

Internet Safety: Dos and Don'ts

In today's digital age, understanding the dos and don'ts of internet usage is important to ensure a safe, productive, and meaningful online experience. Following are some key points to consider as preventive measures and guidelines that everyone should be aware of in order to make informed choices while using the digital platform.



Don'ts

- **Online Content:**

Do not ignore the impact of online content. Anything uploaded and shared online, such as a photo, video, or text, is called online content. While much of this content is positive and informative, a plethora of content has the potential to cause distress, emotional, and psychological harm to individuals who come across it. Moreover, it is important to recognize that predators and other bad actors are unprecedentedly using online spaces to accelerate illegal and harmful activity. Therefore, it is important for your safety and security to be careful while sharing internet content.

- **Unlawful Content:**

Do not engage in uploading unlawful content. It is against the law to upload unlawful content on the internet. Therefore it is important to understand what constitutes unlawful content in Pakistan. Unlawful content includes any such content that is harmful, hateful, pornographic, incites violence, or content that goes against established regulations and laws. To have a comprehensive understanding of what constitutes unlawful online content as per Pakistani law, refer to Chapter 5 of this toolkit.

- **Blasphemous Content:**

Do not participate or engage in uploading content that targets religious sentiments. Content with the intent to insult “the religion of any class of persons” and is against the “glory of Islam” is considered a serious offense under Chapter XV of the Pakistan Penal Code, 1860 (“PPC”). To ensure the online and offline safety of an individual, it is important to refrain from sharing or uploading such materials as uploading such content is not only against the law but also has the potential to create public, societal, and local conflicts in the country.

- **Hate Speech:**

Do not engage in hate speech online as it contributes to a harmful online environment, and causes legal consequences. Hate Speech refers to any verbal, written, or behavioral act that singles out or disparages an individual or a group of individuals because of their gender, religion, color, ethnicity, race, orientation, bodily features, identity, or nationality. Under the PECA, hate speech is defined as ‘...information through any information system or device that advances or is likely to advance interfaith, sectarian or racial hatred’.

- **Immoral/ Indecent Content:**

Do not engage with immoral or indecent content online. Content in music videos, movies, online games, or advertisements that are pornographic /sexually explicit in nature can send negative & harmful messages such as:

- Lack of consent.
- Depraved & violent behavior towards women or minors.
- Unrealistic relationship expectations.

It's important to note that not only is this type of content morally objectionable, but it is also an offense to “produce”, “distribute”, or

“transmit” photos and videos of children being sexually abused and exploited (also known as child pornography).

- **Defamation:**

Do not upload, or share any false information that damages the reputation of any person. Defamation, as it applies on the internet, is “intentionally and publicly” exhibiting, displaying, or transmitting any information that is false and “intimidates or harms” the “privacy of person” (Section 20 of PECA). Online attacks of such kind are against the law, and can also profoundly impact young people and their reputations.

- **Fake News:**

Do not share or upload fake news stories that are distorted, or misleading but are presented online as if they are accurate and truthful. The dissemination of fake news can occur both intentionally and unintentionally, with two distinct terms used to differentiate between them: misinformation and disinformation. Misinformation is false information that is spread regardless of the intent to mislead. Disinformation is false information that is spread deliberately to deceive. To illustrate, if someone shares a fake news story on social media without knowing it is fake, they spread misinformation. But if someone creates or shares a fake news story to influence people’s opinions or actions, they spread disinformation. Fake news websites and pages mimic legitimate news sites using technology and social media. They also use bots and software to create social media accounts, sharing manipulated stories. Sometimes, misleading fake news gets so much popularity that it can deceive journalists, making it difficult to ascertain the facts.

- **Anti-State Content:**

Do not engage in sharing or promoting anti-state content. According to PECA, uploading/sharing content against the “integrity, security or defence of Pakistan or public order” is unlawful. While Article 19 of the Constitution of Pakistan 1973 guarantees freedom of expression, it is important to note that this freedom is subject to reasonable restrictions. This means that inciting violence, promoting hate speech, and false information threatening public order cannot be permitted and protected under the ambit of freedom of speech.

DO's

To check any information that you see online, please use the following ESCAPE mechanism developed by the Witness organization;¹

The infographic consists of six vertical colored bars, each representing a letter of the word 'ESCAPE'. Each bar contains a title, a question, and a list of items to check. The colors are: Evidence (purple), Source (green), Context (blue), Audience (red), Purpose (dark blue), and Execution (orange).

E	S	C	A	P	E
EVIDENCE	SOURCE	CONTEXT	AUDIENCE	PURPOSE	EXECUTION
DO THE FACTS HOLD UP?	WHO MADE THIS, AND CAN I TRUST THEM?	WHAT'S THE BIG PICTURE?	WHO IS THE INTENDED AUDIENCE?	WHY WAS THIS MADE?	HOW IS THIS INFORMATION PRESENTED?
Look for information you can verify.	Trace who has touched the story.	Consider if this is the whole story and weigh other forces surrounding it.	Look for attempts to appeal to specific groups or types of people.	Look for clues to the motivation.	Consider how the way it's made affects the impact.
<ul style="list-style-type: none">• Names• Numbers• Places• Documents	<ul style="list-style-type: none">• Authors• Publishers• Funders• Aggregators• Social media users	<ul style="list-style-type: none">• Current events• Cultural trends• Political goals• Financial pressures	<ul style="list-style-type: none">• Image choices• Presentation techniques• Language• Content	<ul style="list-style-type: none">• The publisher's mission• Persuasive language or images• Moneymaking tactics• Stated or unstated agendas• Calls to action	<ul style="list-style-type: none">• Style• Grammar• Tone• Image choices• Placement and layout

Procedure to Remove Unlawful Online Content²

After carefully following/implementing the recommended ESCAPE mechanism as a safety measure for a better, safe, and secure internet experience, if you still encounter issues regarding online safety and security, law enforcement agencies are available to help. To seek assistance and address any online-related matters, one can report or file a complaint with these authorities.

1. <https://blog.witness.org/>

2. Ibid

i) Intimating PTA and FIA

If you become a victim of any of the above cybercrime(s), or even suspect that you might be a victim, you can take immediate action by:

- Reporting it to the Cyber Crime Wing - Federal Investigation Agency

 **Helpline:** 1991

 **Email:** helpdesk@nr3c.gov.pk

 **Website:** <https://www.fia.gov.pk/ccw>

- Filing a complaint to PTA regarding unlawful online content for blocking via the email address content-complaint@pta.gov.pk or through the Complaint Management System (CMS): <https://complaint.pta.gov.pk/RegisterComplaint.aspx>. As well as via PTA CMS mobile app. Upon receipt of a complaint, PTA processes the link for blocking/removal. The complainant is also informed of the end result.

ii) Reporting on Social Media Platforms

Many platforms have a reporting feature where users can report profiles, videos, pictures, and comments that are harmful, offensive, violent misleading, etc.


Sometimes, social media platforms might ask you to respond to personal questions. For example, if you report someone impersonating you or someone you know, they might ask you to send a scanned identification to confirm the identity.

Below are links from the most popular social media platforms to report something that is against community guidelines:

Facebook	https://www.facebook.com/help/181495968648557
Instagram	https://help.instagram.com/519598734752872
Twitter	https://help.twitter.com/en/rules-and-policies/twitter-report-violation#specific-violations
TikTok	https://support.tiktok.com/en/safety-hc/report-a-problem/report-a-video
YouTube	https://support.google.com/youtube/answer/2802027?hl=en&co=GENIE.Platform%3DAndroid
Snapchat	https://support.snapchat.com/en-US/i-need-help
Discord	https://support.discord.com/hc/en-us/requests/new

iii) **Contacting Relevant NGOs**

You can also contact the Digital Rights Foundation for support and guidance.

 **Helpline:** 0800-39393

 **Email:** helpdesk@digitalrightsfoundation.pk

 **Website:** <https://digitalrightsfoundation.pk/>

Chapter 2

INTERPRETING PECA WITH AUTHORITIES: COMPREHENDING CYBER OFFENSES

1. Legal Avenues to Handle Cyber Offences

A. Law:

The Prevention of Electronic Crimes Act, 2016 (PECA) was promulgated on August 22, 2016. It is a law on electronic crimes to prevent unauthorized acts, and describes related offences as well as mechanisms for their investigation, prosecution, trial and international cooperation, etc¹

Prevention of Electronic Crimes Act, 2016 (PECA)	
Description	Relevant Information
Name of statute	Prevention of Electronic Crimes Act 2016
Preamble	Mechanism for i. investigation ii. prosecution iii. trial and iv. international cooperation with respect to electronic crime
Total sections	Fifty - five (55)



Scan the code to access the
Prevention of Electronic Crimes Act 2016

B. Rules:

Removal and Blocking of Unlawful Online Content (Procedure, Oversight, and Safeguards) Rules, 2021, commonly referred to as Social Media Rules, were gazette notified on October 12, 2021. It provides a mechanism for the registration of significant Social Media Companies and a procedure for handling complaints, steps for blocking access, and removal of unlawful online content on the matter provided in PECA 2016.

1. PTA, 'ONLINE SAFETY GUIDE - SAFE USE OF SOCIAL MEDIA'

C. Authority:

Under section 37 of PECA, PTA is mandated to block the access or removal of unlawful online content(s)/information disseminated through any information system in Pakistan, which among other things includes content(s)/information against integrity, security or defence of Pakistan (anti-state), against the glory of Islam (blasphemous), hate speech (public order), decency and morality (pornography), contempt of court and defamation/impersonation.²

2. Interpreting Prevention of Electronic Crimes Act 2016

PECA comprehensively lists all offences and their respective punishments in Chapter II. For a better understanding, of certain cyber crimes and the law about those following is a breakdown with relevant legal jurisprudence:

A. Hacking

Hacking is gaining unauthorized access to data in a system or computer.³ Hacking can be done for various reasons, such as stealing information, disrupting services, or gaining notoriety. Hacking can also be done for ethical purposes, such as testing the security of a system or exposing vulnerabilities.

Hacking can be done through various techniques, such as:⁴

- **Social engineering:** This is when a hacker tricks a user into revealing sensitive information or opening a malicious link or attachment by pretending to be someone trustworthy or legitimate.
- **Password cracking:** This is when a hacker tries to guess or break a password by using brute force, dictionary, or algorithm methods.

2. Ibid

3. 'Hacking' (hacking noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com) <<https://www.oxfordlearnersdictionaries.com/definition/english/hacking>> accessed 4 August 2023

4. Kaspersky, 'What Is Hacking? And How to Prevent It' (www.kaspersky.com, 30 June 2023) <<https://www.kaspersky.com/resource-center/definitions/what-is-hacking>> accessed 4 August 2023

- **Malware infection:** This is when a hacker installs malicious software on a user's device or network by exploiting a vulnerability or using phishing or spamming methods.
- **Network sniffing:** This is when a hacker intercepts and analyzes the traffic on a network by using special tools or devices.

B. Glorification of an Offence:

Section 9 of PECA addresses the offence of glorifying an offence relating to terrorism, individuals convicted of terrorism-related crimes, or the activities of proscribed organizations or individuals or groups. Here's a detailed explanation of this section:

Subsection 1:

The subsection specifically outlines the offense of glorifying an offense related to terrorism or any person convicted of a crime related to terrorism. It also covers the glorification of activities conducted by proscribed organizations, individuals, or groups. Glorification, in this context, refers to the act of preparing or disseminating information, through any information system or device, with the intent to depict these offenses or activities in a positive or desirable manner. This includes any form of praise or celebration.

Penalties for Glorification:

This provision underscores the serious nature of glorifying terrorism-related offenses and aims to deter individuals from promoting or celebrating such actions through any electronic means. The penalties for glorification include imprisonment for a term that may extend to seven years, a fine that may extend to ten million rupees or both.

C. Cyber Terrorism:

Section 10 deals specifically with the offense of cyber terrorism, which is a serious crime involving various aspects of cybercrimes and cyber threats. Section 10 addresses individuals who commit or threaten to commit certain offenses under sections 6, 7, 8, or 9 of PECA, but with specific intent. These sections pertain to unauthorized access to critical infrastructure, unauthorized copying or transmission of critical infrastructure data, interference with critical infrastructure information systems or data, and the glorification of offenses. The central element of Section 10 is the intent behind committing or threatening these offenses, which includes specific objectives to:

- a. Coercion, Intimidation, Fear, Panic, or Insecurity: The first objective is to coerce, intimidate, and create a sense of fear, panic, or insecurity in various entities such as the government, the public, specific communities, sects, or society as a whole.
- b. Advancing Inter-Faith, Sectarian, or Ethnic Hatred: The second objective is to advance inter-faith, sectarian, or ethnic hatred. This involves using cyber means to promote hatred and hostility among different religious, sectarian, or ethnic groups.
- c. Advancing the Objectives of Proscribed Organizations or Individuals or Groups: The third objective is to advance the objectives of organizations or individuals or groups that have been proscribed or banned under the law. This includes using cyber tactics to support and further the agenda of such entities.

Penalties for Cyber Terrorism:

Individuals found guilty of committing cyberterrorism under Section 10 are subject to severe penalties. Penalties for cyber terrorism include imprisonment for a term that may extend to fourteen years, a fine that may extend to fifty million rupees or both. These penalties are meant to act as a strong deterrent against individuals who engage in cyber-terrorism activities that pose significant threats to national security, public safety, and social harmony.

D. Hate Speech:

Section 11 of PECA addresses the offense of hate speech, specifically focusing on individuals who prepare or disseminate information through any information system or device that promotes or is likely to promote interfaith, sectarian, or racial hatred. Section 11 targets individuals who engage in the dissemination of information, whether in the form of text, audio, video, or any other medium, with the intent to advance or likely advance hatred based on factors such as interfaith differences, sectarian divisions, or racial distinctions. The key element of this offense is the promotion of hatred, which includes content that is designed to create animosity, hostility, or antagonism among individuals or groups belonging to different faiths, sects, or racial backgrounds.

Penalties for Hate Speech:

Penalties for hate speech include imprisonment for a term that may extend to seven years, a fine, or both. These penalties are intended to deter individuals from engaging in hate speech activities, which can lead to social discord, conflicts, and tensions.

E. Electronic Frauds

Section 14 of PECA acknowledges the evolving landscape of financial crimes in the digital age. This Section aims to combat electronic fraud by holding individuals accountable for wrongful financial gain achieved through deceptive or unauthorized means. Section 14 states that anyone who intentionally interferes with or uses an information system, device, or data with the intent for wrongful gain, can be penalized. The section includes the following key components:

- **Intent for Wrongful Gain:**

The section specifies that the offender must have the intent for wrongful gain. In legal terms, this means that the individual's actions were motivated by the desire to acquire financial or material benefits through fraudulent means.

- **Interference with Information Systems, Devices, or Data:**

The provision covers a broad range of actions that can be considered electronic fraud. This includes any intentional interference with information systems, devices, or data. In the context of electronic fraud, this interference typically involves unauthorized access, manipulation, or disruption of electronic systems or data.

- **Inducing a Relationship or Deception:**

The section also addresses actions aimed at inducing someone into a relationship or deceiving them. This encompasses tactics where the offender uses fraudulent means to establish a relationship of trust with the complainant. Such deception can lead to financial harm to the victim or others.

- **Likelihood of Damage or Harm:**

The provision emphasizes that the act or omission must be likely to cause damage or harm to the victim or others. This highlights the importance of the potential consequences of electronic fraud in determining whether an offence has occurred.

Penalties for Electronic Frauds:

Once proven guilty, one can face imprisonment for a term that may extend up to two years, and a fine may extend up to ten million rupees.

Javad Khan vs. State **2023 PCrLJ 1092**

Facts: The Petitioner sought the quashment of FIR filed under Section 14 of the PECA along with Sections 419 and 420 of the P.P.C.

Arguments: The Petitioner's counsel contended that the offences under the P.P.C. could not be tried alongside offences under the PECA by a Court that had jurisdiction to try offences under the PECA in view of section 237 of the Code of Criminal Procedure, 1898, read together with section 26 of the General Clauses Act, 1897.

Excerpt: “At the heart of the controversy are three questions: (i) does the FIA as an investigation agency notified for the purpose of section 29 of the PECA have jurisdiction to investigate the offences defined under P.P.C.; (ii) in the event that FIA has jurisdiction to investigate offences under P.P.C. where such offences are made out from actions that constitute an offence under PECA, would inclusion of cognizable offences under P.P.C. authorized the investigation agency to register an FIR in relation to a non-cognizable offence under PECA without seeking prior permission from a Court of competent jurisdiction; and, (iii) can a special Court designated under section 44 of PECA conduct a joint trial of offences under PECA as well as offences under P.P.C.” (Para 4)

Decision: The Islamabad Court ruled that the FIA, as the designated investigative agency under Section 29 of the PECA, lacked the jurisdiction to investigate allegations falling under offences defined by the P.P.C. Therefore, the joinder of such offences with those under the PECA was not permissible. The court held that FIR against the Petitioner was liable for quashment. However, this action did not prevent the FIA from seeking the appropriate court permission to pursue charges under Section 14 of the PECA. Furthermore, for offences attributed to the PPC, the complainant retained the right to file a complaint with the police authorities.

Sheraz Khan vs. State 2022 PCrLJ 203

Facts: The case was registered against Petitioner under Sections 13, 14, and 16 of the PECA read with Sections 109, 419, 420, 468, and 471 of P.P.C.

Arguments: Petitioner's counsel contended that offences of P.P.C could not be investigated by FIA along with offences under PECA, 2016 nor could they be tried by the court constituted under the said Act. Therefore, the application of Sections 419, 420, 468, 471, and 109 of P.P.C in FIR was not legally justifiable.

Excerpt: "We all know that internet technology is progressing thick and fast and we are all benefiting by it in almost all fields of life but at the same time it has multiple disadvantages as well. Unless we exhibit maximum maturity and protect ourselves by self-imposed restrictions, we can easily fall victim of this latest technology and chances of being misled or even defrauded become more obvious when personal spite, selfishness or greed take charge of our social activities, whereas, a strong selfish desire of having more and more of something, especially the money is so damaging that it can destroy everything in a man's life and take away even what is his hard-earned." (Para 4)

Decision: As per the rule of consistency, the Lahore High Court granted bail to the Petitioner and directed the learned trial court to proceed with the trial expeditiously in accordance with the law.

F. Offences against modesty of a natural person and minor

Section 21 of PECA aims to address offences against the modesty and dignity of individuals. The section with a specific subsection for minors and adults focuses on protecting minors from online harassment. Here's a detailed breakdown of this legal provision:

Subsection 1:

This subsection targets individuals who intentionally and publicly exhibit, display, or transmit information through an information system with the following intentions:

1. Superimposing a photograph of an adult person's face over any sexually explicit image or video.
2. Including a photograph or video of an adult person engaged in sexually explicit conduct.
3. Intimidating an adult person with any sexual act or sexually explicit image or video.
4. Cultivating, enticing, or inducing an adult person to engage in a sexually explicit act.

The purpose of these actions is to harm the individual or their reputation, take revenge, create hatred, or blackmail them. If proven guilty of a crime under this subsection, the perpetrator will face imprisonment for up to five years, a fine of up to five million rupees, or both.

Subsection 2:

This subsection specifically targets offences against minors (individuals under the age of 18). Offences described in subsection 1, when committed against a minor, result in more severe penalties. Offenders can be punished with imprisonment for up to seven years and a fine of up to five million rupees.

G. Child Pornography

Child pornography under Section 22 of the PECA, refers to the intentional production, distribution, transmission, or possession of material in an information system that visually depicts:

1. A minor (a person who has not completed the age of eighteen years) engaged in sexually explicit conduct.
2. A person who appears to be a minor engaged in sexually explicit conduct.
3. Realistic images representing a minor engaged in sexually explicit conduct.
4. Disclosure of the identity of the minor involved in such content.

Section 22 is a stringent legal framework designed to combat the heinous crime of child pornography, and involves the sexual exploitation of minors and the creation, distribution, or possession of explicit materials featuring minors.

Penalties for Child Pornography:

Those found guilty of child pornography offences under PECA can face severe penalties, including imprisonment for a minimum of fourteen years, which can be extended up to twenty years, a fine not less than one million rupees, or both.

Umer Khan vs. State 2022 SCMR 216

Facts: A case was registered against the Petitioner under Section 22(1) of PECA. The petitioner was accused of sharing child pornographic content on Facebook through his mobile.

Arguments: The counsel for the Petitioner contended that there was no direct evidence to show that the Petitioner had shared the content on Facebook. Counsel also contended that no victim had been associated in the present case, and that the offence did not fall within the prohibitory clause.

Excerpt: “We have noticed that one of the most alarming social evil prevailing in the society is child pornography. It has created a havoc in society as it contains a great threat to morality and the future of children. One of the reason for the rise of child abuse/rape cases is squarely because of child pornographic content. The concerns regarding child sexual abuse and exploitation have been prevailing in the society in the past also. However, due to various factors, the gravity and impact of the offense of child pornography is increasing at an alarming rate and this menace needs to be curbed with iron hands.” (Para 5)

Decision: The court refused the bail and directed the trial court to proceed with the trial expeditiously.

Hassan Nawaz vs State
2022 YLRN 211

Facts: An FIR under Sections 21 and 22 of PECA along with Section 109 P.P.C was registered against Petitioner. The FIR stated that the Petitioner, with criminal intentions and ulterior motives, illegally and unauthorizedly created and operated the Instagram and WhatsApp accounts/groups to obtain, share, consume, possess, sell, and disseminate pornographic and sexually explicit pictures of minors.

Arguments: Petitioner's counsel argued that the Petitioner was implicated falsely in the case and that the absence of a private complainant in the case was enough to entitle the Petitioner to bail.

Decision: The Court held that Petitioner had successfully made out a prima facie case for his release on bail. Consequently, bail was allowed.

Adil Nadeem vs. State
2021 PCrLJ 1457

Facts: The Applicant sought post-arrest bail in a case registered under Section 22(1) of PECA against him. The undercover operation was launched by the cybercrime unit in Milan to fight the diffusion of child sexual abuse material through groups on Telegram and WhatsApp in which 351 foreign numbers were investigated. The Interpol coordinated with the cybercrime wing of the FIA, given that one cell number was of Pakistani origin. FIA conducted its inquiry and discovered that the Applicant used the number.

Arguments: The Applicant's counsel argued that the FIR was lodged after 3 years of the reported incident and the images/videos had been uploaded and saved on hard drive by the applicant's brother, who died back in 2016.

Excerpt: "Section 497, Cr.P.C. divided non-bailable offences into two categories i.e. (i) offences punishable with death, imprisonment of life or imprisonment for ten years; and (ii) offences punishable with imprisonment for less than ten years. The principle to be deduced from this provision of law is that in non-bailable offences falling in the second category (punishable with imprisonment for less than ten years), the grant of bail is "a rule and refusal an exception". (Para 5)

Decision: The Karachi High Court dismissed the bail petition and decided that the heinous nature of child pornography could not be taken lightly.

H. Cyber Stalking

Section 24 of PECA specifically addresses cyberstalking, which is a form of online harassment or intimidation. Cyberstalking involves the use of digital means to coerce, intimidate, or harass another person. Here's an in-depth explanation of this section:

Subsection 1:

Cyberstalking is defined as an offence in which a person, with the intent to coerce, intimidate, or harass another person, utilizes various electronic means of communication, including information systems, information system networks, the internet, websites, electronic mail, or similar channels, to engage in the following actions:

1. **Following or Repeatedly Attempting to Contact:** This includes following a person or making repeated attempts to contact them, even when the target has clearly expressed disinterest.
2. **Monitoring Electronic Communications:** It involves monitoring a person's use of the internet, electronic mail, text messages, or other forms of electronic communication.
3. **Spying or Surveillance:** This relates to observing or spying upon a person in a manner that causes fear of violence or serious alarm or distress in the mind of the victim.
4. **Unauthorized Photography or Video:** This refers to taking photographs or videos of a person without their consent and subsequently displaying or distributing them in a manner that causes harm to the individual.

Subsection 2:

1. Individuals found guilty of committing cyberstalking offences under subsection 1 are subject to penalties. The severity of the penalties depends on the circumstances, especially if the victim is a minor.

Penalties for cyberstalking include imprisonment for a term of up to

2. three years or a fine of up to one million rupees or both.

If the victim of cyberstalking is a minor, the punishment can be more

3. severe, with imprisonment extending up to five years, a fine of up to ten million rupees, or both.

I. Identity Theft

Identity theft is a cybercrime in which a malicious actor obtains and misuses another person's personal/sensitive information to impersonate them and commit frauds/scams using the stolen identity. The main motive of this crime is usually financial gain. The cybercriminal accesses the person's information by stealing their e-mail credentials, hacking into computer databases, intercepting network traffic, or using other methods. Identity thefts can involve various techniques, such as phishing, smishing, vishing, skimming, and spoofing. NR3C has successfully investigated many cases of identity theft.⁵

To protect yourself against Identity Theft, you must follow the steps below:

1. **Ask questions before giving out your Personal Information (e.g., CNIC or any other identifying information).**
 - Why do you need it?
 - How will you protect it?
 - Can you use a different identifier?
2. **Protect your information from scammers online and on your phone.**
 - Use strong passwords when creating an account.
 - Add multi-factor authentication to secure your account further.

5. Ibid

Phishing	Smishing	Vishing
Phishing is an attack that uses fraudulent emails to lure victims into clicking on malicious links, opening malicious attachments, or providing sensitive information.	Smishing is a type of phishing attack that uses SMS messages to trick victims into clicking on malicious links or providing sensitive information.	Vishing is a type of phishing attack that uses phone calls or voice messages to trick victims into providing sensitive information or performing fraudulent actions.
How to Respond	How to Respond ⁶	How to Respond
Do not click anything unsolicited in an email.	Be suspicious of SMSs claiming to come from a reputable organization such as a bank or TV channel.	Do not trust phone calls that say they are from a trustworthy organization like a bank, government agency or TV network.
If the suspicious email is from someone you know, contact them through phone or text message to inquire about its legitimacy.	Please do not respond to text messages requesting personal information without independently verifying that they are from a genuine source.	Avoid giving or verifying any personal/financial information on the phone without first verifying that it is from a genuine source.
Inform the service provider about the number and ask them to block it.	Do not click on any links embedded within unknown SMS or call any given numbers.	Remember that a government organization, bank or TV channel will not email asking for your sensitive data.
Set up two-factor or multi-factor authentication and never disable it.	Report the number to the concerned service provider for blocking.	
SKIMMING		SPOOFING
<p>Skimming is a type of fraud that involves stealing credit or debit card information using a device attached to a card reader, such as an ATM or a gas pump.</p> <p>How to Respond</p> <ul style="list-style-type: none"> • Before using your credit or debit card at the ATM, look for cameras, loose parts or any contraption that can be used to record your PIN. • Regularly review your bank statements and see if there is any suspicious activity. • Contact your respective bank immediately if you see any anomalous transaction. 		<p>Spoofing is a type of attack that involves impersonating a legitimate person, organization, or device by falsifying the sender's address, phone number, or IP address – often just by changing one letter, symbol, or number – to convince that you are interacting with a legitimate person or a company.⁷</p> <p>How to Respond</p> <ul style="list-style-type: none"> • Always verify the identity of the sender or caller before responding to any requests for information or action. • You should also avoid clicking on any links or attachments in suspicious emails or text messages. • Use strong passwords and two-factor authentication for your online accounts. • Contact the relevant office or person to verify if the sender is a legitimate source and not a disguise.

6. PTA, 'ONLINE SAFETY GUIDE - SAFE USE OF SOCIAL MEDIA'

7. 'Spoofing and Phishing' (FBI, 17 April 2020) <<https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing>>

Chapter 3

Punitive Measures for the Violations under PECA

The PECA lists the offenses and their respective punishments in Chapter II.

* Represents the recent amendments made under the Criminal Laws (Amendment) Act, 2023.

OFFENCES UNDER THE PREVENTION OF ELECTRONIC CRIMES ACT, 2016 (PECA)					
No	Provision	Description of Offence	Sentence Under PECA		
			Fine (up to)	Imprisonment	
1	Section 3	Unauthorized access to information system or data	Fifty thousand	Three months	Or With Both
2	Section 4	Unauthorized copying or transmission of data	One hundred thousand	Six months	Or With Both
3	Section 5	Interference with information system or data	Five hundred thousand	Two years	Or With Both
4	Section 6	Unauthorized access to critical infrastructure information system or data	One million	Three years	Or With Both
5	Section 7	Unauthorized copying or transmission of critical infrastructure data	Five million	Five years	Or With Both
6	Section 8	Interference with critical infrastructure information system or data,	Ten million	Seven years	Or With Both
7	Section 9	Glorification of an offence	Ten million	Seven years	Or With Both
8	Section 10	Cyber Terrorism	Fifty million	Fourteen years	Or With Both

9	Section 11	Hate Speech	Not given	Seven years	Or With Both
10	Section 12	Recruitment, funding and planning of terrorism	Not given	Seven years	Or With Both
11	Section 13	Electronic Forgery	Two hundred fifty thousand	Three years	Or With Both
12	Section 14	Electronic Fraud	Ten million	Two years	Or With Both
13	Section 15	Making, obtaining or supplying device for use in offence	Fifty thousand	Six months	Or With Both
14	Section 16	Unauthorized use of identity information	Five million	Three years	Or With Both
15	Section 17	Unauthorized use of SIM cards	Five hundred thousand	Three years	Or With Both
16	Section 18	Tampering, etc. of communication equipment	One million	Three years	Or With Both
17	Section 19	Unauthorized interception	Five hundred thousand	Two years	Or With Both
18	Section 20	Offences against dignity of a person	One million	Three years	Or With Both
19*	Section 21(1)	Offence against modesty of a natural person and minor	Five million	Five years	Or With Both
20*	Section 22	Child pornography	Not less than one million rupees	Fourteen years that may be extended up to twenty years	Or With Both
21*	Section 22A	Online grooming, solicitation and cyber enticement	Five hundred thousand that may be extended up to ten million	Five years that may be extended up to ten years	Not given

22*	Section 22B	Commercial sexual exploitation of children	Not less than one million	Fourteen years that may be extended up to twenty years	Not given
23	Section 22C	Use of information system for kidnapping, abduction or trafficking of minor	Not less than one million	Fourteen years that may be extended up to twenty years	Not given
24	Section 23	Malicious code	One million	Two years	Or With Both
25*	Section 24	Cyber Stalking	One million	Three years	Or With Both
26	Section 24A (1)	Cyberbullying	One hundred thousand that may be extended up to five hundred thousand	One year that may be extended up to five years	Not given
27	Section 25	Spamming	Fifty thousand that may be extended up to five million	Three months	Or With Both
28	Section 26	Spoofing	Five hundred thousand	Three years	Or With Both

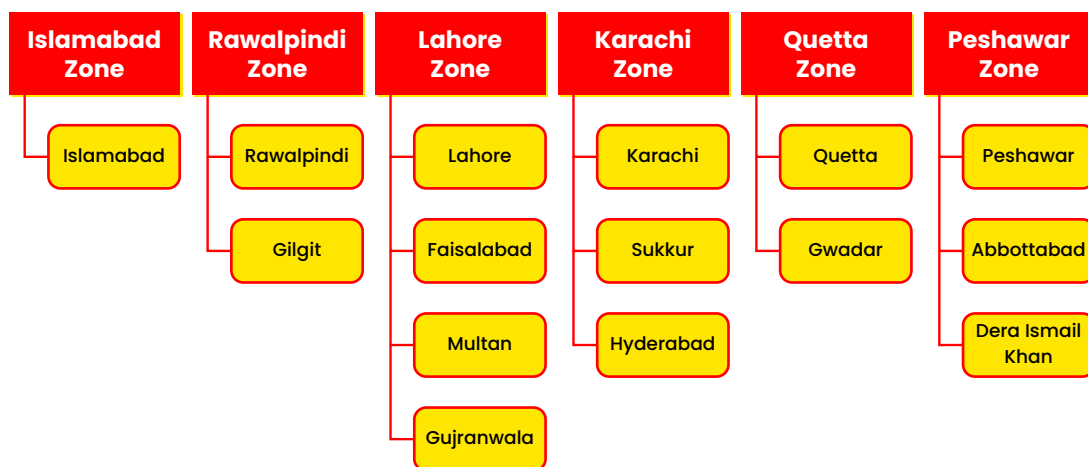
Chapter 4

CYBER CRIME WING - FIA

After an individual has recognized an instance of cybercrime, the complainant may file a formal complaint by visiting the nearby Cybercrime Reporting Centers' helpdesk or by submitting an online complaint with the Cybercrime Complaint Registration Form (<https://complaint.fia.gov.pk/>) which is available at the website FIA.

Cybercrime Wing Offices

The Cybercrime Wing is distributed into six zones and fifteen Cybercrime Reporting Centers:



Procedure to Submit a Complaint with the FIA

To file a complaint successfully, the following steps must be followed;

- Visit the nearby CCW Center, or submit an online complaint.
- Submit a written complaint at the Helpdesk, set up within the CCW Center.
- The circle in charge registers the case and assigns a complaint number.
- Once the complaint number has been registered, the complainant gets a verification code on their cell phone.
- Once the complaint is verified by the Verification Officer, an Investigation Officer (“IO”) gets marked.¹
- The IO shall chalk out an investigation work plan that needs the approval of the circle in charge (see Schedule 4 Annex-A Form below).²
- The IO shall submit an investigation report within six days.³
- In case a cognizable offence has been committed under the Act, the circle in-charge, after seeking legal opinion, shall order the registration of such case subject to the prior approval of the Additional Director in the zone.⁴
- In case of a non-cognizable offence under the Act, the circle in charge shall seek the permission of the competent Court for investigation under section 155 of the Code.⁵

NOTE:

It is highly advisable to file an in-person complaint by visiting your nearby Cybercrime Reporting Centers (CCRCs).

1. Section 7, paragraph 1 of PECA Rules, 2018

2. Section 7, paragraph 2 of PECA Rules, 2018

3. Section 7, paragraph 3 of PECA Rules, 2018

4. Section 7, paragraph 4 of PECA Rules, 2018

5. Section 7, paragraph 5 of PECA Rules, 2018

SCHEDULE 4 ANNEX-A FORM

INVESTIGATION WORK PLAN	
Case No:	
Implicated Persons:	
Investigation Plan date:	
Name of Investigator	
Allegations	(A brief summary of the reported complaint, including circumstances relevant to the matter being investigated)
Applicable legal norms	(State applicable laws (PECA 2016, PPC, etc) pertaining to the reported crime)
Implicated person	State name(s) of persons involved in the complaint and complete address and contact details.

WORK PLAN STEPS AND TIMELINES	
Investigate Action	{Identify interviewees, their contact details and a tentative schedule. Also, address issues of availability, order of interviews and special needs (e.g. interpreter, guardian)}

PROPOSED INTERVIEWS

No.	Name	Status (complainant, accused, witness, victim)	Contact Info (phone and e-mail)	Purpose of Interview	Tentative date/availability

EVIDENCE / RECORDS PRESERVATION AND COLLECTION

No.	Evidence/ Records to be Collected	Means of Collection/ Contact Point	Date Completed

Travel/ mission plan

{Proposed travel in connection with investigation - Include travel dates, length, purpose, location(s), number of investigator(s)/support required, and an estimation of costs}

RESOURCES

EQUIPMENT/INVESTIGATION TOOLS

{List required equipment for investigation, including laptop computer; portable printer; external hard drive; flash drive; digital camera; digital audio recorder; hard disk cloning software; SIM card reader/back-up; evidence bags/seals}

FORENSICS / EXTERNAL EXPERTISE

{List any forensic/external support or specialized forensic equipment required for the investigation}

Type of Evidence	Explanation	Date Obtained

Name and signature of assigned investigator: _____

Date: _____

Investigation Plan approved by: _____

(Circle in-Charge, Investigation)

From Complaint to Raid

- After a successful lodging of a complaint, the IO shall conduct a search and seizure in accordance with the provisions of PECA, 2016.⁶
- The IO must also obtain a prior warrant from the Court if required.⁷
- The case property that is seized must be handled properly and kept in good condition according to the Act and Schedule V, which describe the steps to follow.⁸

6. Section 8, paragraph 1 of PECA Rules, 2018

7. Ibid

8. Section 8, paragraph 2 of PECA Rules, 2018

SCHEDULE V

SEIZURE MEMO - (FORM-I)

Case Number:

Item:

Date of seize:

Time: Location:

Details of Person:

Details of Person from whom item(s) seized:

Address / Telephone Number / E-mail:

Description of item(s)

Description of item seized:	
Make/Model:	
Serial numbers:	
Colour:	
Condition:	
Number of pages (if documents):	
Any other identifying marks:	

	Name	Signature
Investigator		
Witness 1		
Witness 2		

Chapter 5

DRF CYBER HARASSMENT HELPLINE

What We Offer?




DRF's Cyber Harassment Helpline is the region's first helpline dedicated to addressing cyber violence and online harassment. It provides confidential and gender-sensitive support through a team of trained and qualified support officers who offer assistance in digital security, legal advice, and escalations with social media platforms. It is the primary goal of the helpline team to provide specialized assistance to the gendered marginalized communities, vulnerable professions, women, minors, and minorities affected by cyber-attacks.¹

OUR TIMINGS

The support officers are dedicatedly working from 9 AM to 5 PM, from Monday to Friday on toll-free calls, emails, and social media platforms.

In July 2022, DRF collaborated with Pakistan's National Commission of Human Rights to establish a Complaint Cell for Journalist Protection, with particular emphasis on resolving human rights issues that affect women journalists, thereby ensuring the freedom of the press.

CONTACT US (Monday to Friday | 9:00 AM to 5:00 PM)

Toll-Free Number	E-mail	Social Media		
		Instagram	Facebook	Twitter
0800-39393	helpdesk@digitalrightsfoundation.pk	 https://www.instagram.com/digitalrightsfoundation/	 https://www.facebook.com/DigitalRightsFoundation	 https://twitter.com/digitalrightsPK

1. 'Cyber Harassment Helpline' (digitalrightsfoundation.pk)<<https://digitalrightsfoundation.pk/cyber-harassment-helpline/>>

System and Procedures

- **Before inducting the Helpline Staff, the Organization shall ensure that:**
 - Helpline Staff undergo training that covers dealing with survivors, counselling skills, self-care, gender sensitization, cyber security, cyber harassment, cyber law in Pakistan, law enforcement mechanisms, operating a helpline, and simulation-based exercises.²
 - The staff members shall be vetted for gender sensitivity and subject to a rigorous interviewing and selection process before being hired, given the highly sensitive nature of their job.³
- **Duties of the Helpline Staff include the following:**
 - When assisting survivors of online abuse and harassment, the Helpline staff is directed to be non-judgmental and empathetic. The Helpline staff is also cautioned against imposing their own beliefs and preconceived notions of a situation onto the survivor and must act as facilitators, rather than controllers.⁴
 - For security and safety purposes, the Helpline staff shall not disclose their real names on calls and will instead use “counselling pseudonyms”.⁵
 - The Staff shall not coerce the survivor to provide evidence unless it’s given willingly with consent.⁶ However, the Support Staff must guide the survivor(s) to safely and securely store the evidence.⁷

NOTE:

All personally identifiable information (PII) will be obtained and shared through informed, active and withdrawable consent.⁸

2. Digital Rights Foundation, ‘Cyber Harassment Helpline Policy’ Section 2.12.2

3. Digital Rights Foundation, ‘Cyber Harassment Helpline Policy’ Section 2.12.3

4. Digital Rights Foundation, ‘Cyber Harassment Helpline Policy’ Section 2.12.4

5. Digital Rights Foundation, ‘Cyber Harassment Helpline Policy’ Section 2.12.6

6. Digital Rights Foundation, ‘Cyber Harassment Helpline Policy’ Section 3.6

7. Digital Rights Foundation, ‘Cyber Harassment Helpline Policy’ Section 3.5

8. Digital Rights Foundation, ‘Cyber Harassment Helpline Policy’ Section 3.1



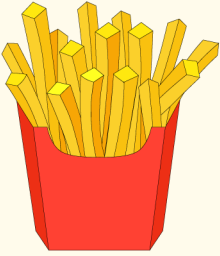
Scan the code to access the
Prevention of Electronic Crimes Act 2016

https://digitalrightsfoundation.pk/wp-content/uploads/2020/06/DraftPolicy_1.8_02.06.2020.pdf

What is Consent?

In simpler words, consent means nothing less than an enthusiastic YES!

CONSENT



- Freely Given*
- Reversible*
- Informed*
- Enthusiastic*
- Specific*

DO YOU GET CONSENT?

CONSENT IS

- ✓ ESSENTIAL
- ✓ GIVEN FREELY
- ✓ COMFORTABLE
- ✓ RETRACTABLE
- ✓ ACTIVE

CONSENT IS NOT

- ✗ ASSUMED
- ✗ PRESSURED
- ✗ SILENT
- ✗ RELUCTANT
- ✗ UNCONSCIOUS

CONSENT IS FOR EVERYTHING
AND EVERYONE...

REMINDER:

**CYBER
HARASSMENT
KNOWS NO
BOUNDARIES**

— — — — —

REPORT IT ON
TOLL-FREE NUMBER
0800-39393

 **DIGITAL HELP-DESK**
helpdesk@digitalrightsfoundation.pk

 Digital Rights Foundation
"YOUR VOICE MATTERS"

 **ہمارا
INTERNET**

NOTE:

The Helpline may refer the case to a relevant authority (e.g., FIA) by first obtaining consent from the survivor.

Chapter 6

SAFETY MEASURES THAT THE USER CAN TAKE

Some General Tips

Following are some of the safety guidelines that an individual can adopt to create a safe cyberspace around them:¹

- **Strong passwords:** Create unique, and strong passwords by keeping more than 10 characters with letters (uppercase and lowercase), numbers, and symbols. Your passwords must not include personal information or common words.
- **Change passwords frequently:** Use different passwords for each account and change your passwords frequently. The new password should be different from the old one and should be unique, avoid repetition of any words from old passwords.
- **Two-Factor Authentication (2FA):** Activate 2FA on your accounts. This creates an extra layer of security by requiring a second verification code.
- **Privacy Settings:** Review and adjust your social media accounts' privacy settings. Be cautious while sharing information online and keep your personal data as private as possible. Be careful before you share or post anything online – it might not go away, and someone could use it to hurt you in the future.
- **Keep personal data private:** Do not reveal too much information on your account, especially personal details like your address, phone number, where you live or stay, or your relatives' names. Hide your phone number. You can make your phone number "secret" so that

1. 'Cyber-Harassment: Self-Protection Tips | Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD)' (United Nations) <<https://www.unitad.un.org/content/cyber-harassment-self-protection-tips>>

when you call someone, they will see “private number” or “caller ID not available” on their phone. This can help you protect your personal data.

- **Use safe platforms:** Think about using Signal instead of WhatsApp. Signal offers more privacy. Also, use a Virtual Private Network (“VPN”) for better security when doing sensitive online business.
- **Avoid using public Wi-Fi connection:** Do not use the free public WiFi for your online activity.
- **Update Software Frequently:** Keep your operating system, antivirus program, and applications up to date.
- **Educate yourself:** Only add people you know to your personal social networks. Do not accept requests from strangers who want to be your friend. Tell your friends and people you know not to post any personal information about you. Do not post pictures of your home that might show where it is. Learn how to use the privacy settings of your social media apps, including who can see your information and how to block or hide content. Always check what is in the background of your videos or photos before you publish them.
- **Block and report:** Do not hesitate to block and report abusive users/accounts to social media platforms and websites. Block and report any accounts that are suspicious or threatening, and a person who is harassing you.
- **Create separate accounts:** Keep your private and business accounts separate.



DigitalRightsFoundation
"KNOW YOUR RIGHTS"



@DigitalRightsFoundation



@digitalrightsfoundation



@digitalrightsfoundation



@digitalrightsfoundation



@DigitalRightsPK



@DigitalRightsPK