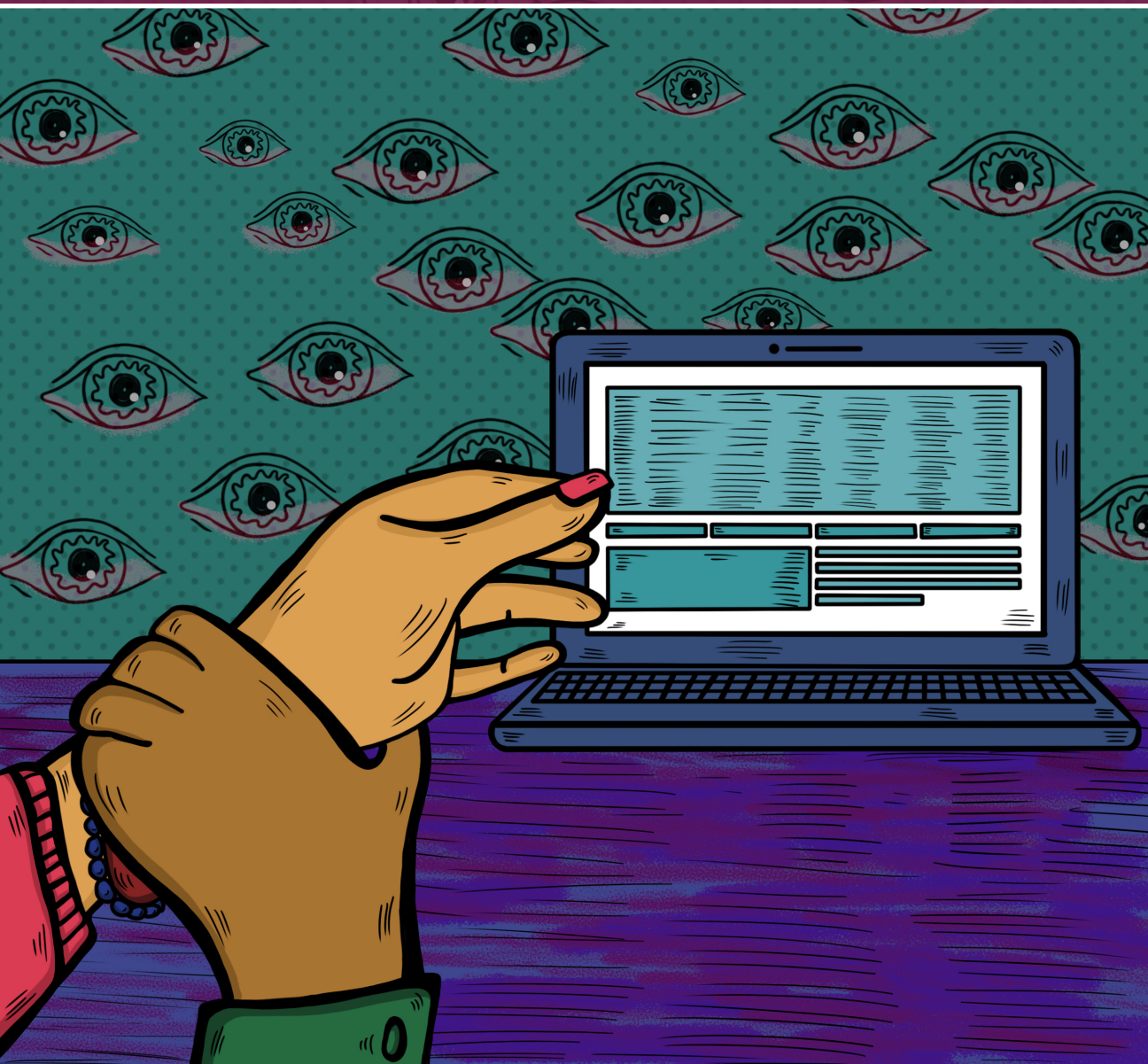




DigitalRightsFoundation
"KNOW YOUR RIGHTS"

Countering Digital Threats

Toolkit



Chapter 2

Interpreting PECA with Authorities: Comprehending Cyber Offences

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
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. How to Respond • 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.		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 How to Respond • 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'z

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>>



DigitalRightsFoundation
"KNOW YOUR RIGHTS"



@DigitalRightsFoundation



@digitalrightsfoundation



@digitalrightsfoundation



@digitalrightsfoundation



@DigitalRightsPK



@DigitalRightsPK