

# Safe Use of Social Media Online Safety Guide



Copyrights © 2022 Pakistan Telecommunication Authority

All rights reserved. Printed and bound in Pakistan. No part of this publication may be reproduced, or utilized in any form or by any means, electronic or mechanical, including photocopying, recording, or by any information of storage and retrieval system, or transmitted, without the prior written permission of the publisher.

**Published by**

Pakistan Telecommunication Authority  
Headquarters, F-5/1,  
Islamabad, Pakistan  
Website: [www.pta.gov.pk](http://www.pta.gov.pk)

**Cataloging-in-Publication Data**

Pakistan Telecommunication Authority  
PTA's Online safety guide: safe use of social media  
**ISBN: 978-969-8667-63-4**

**Acknowledgment:**

The Online Safety Guide was written by Ms. Tayyaba Iftikhar, Assistant Director PR, with support from the Cyber Vigilance Division, Law & Regulations Division and Web Analysis Division of PTA.



# Table of Content

## Why Internet Safety Matters

05

06

What is Online Content?

06

Unlawful Content

06

Blasphemous Content

06

Hate Speech

07

Indecent/Immoral Content

08

Anti-State Content

08

Defamation

08

Fake News

09

Harmful User Generated Content

09

What are Community Guidelines?

10

The Consequences of Breaking Guidelines

11

How to Report

12

The Internet & the Law in Pakistan

## Online Grooming

17

17

What is online grooming?

18

How does online grooming happen?

19

Where can online grooming happen?

19

Warning Signs

20

How to protect yourself from unwanted contact

## Online Reputation

23

24

How is it formed?

24

What is a positive digital footprint?

25

Consequences of Negative Online Reputation

26

Netiquettes ("Internet etiquettes")

## Privacy and Identity Theft

29

30

What is Personally Identifiable Information?

30

Who collects Data?

30

How is data being used?

31

How to Protect Your Privacy Online?

32

What is Identity Theft?

33

How to Protect Yourself Against Identity Theft

35

Report Identity Theft









# Why Internet Safety matters?

People use digital technologies for everyday activities. What happens online can just be just as real and important as what happens offline. This booklet offers guidance on the risks young people & children might face online, and some advice on how to stay secure & responsible and maintain a positive digital footprint.



## What is Online Content?

Anything that is uploaded and shared online such as a photo, video or text is content. While a lot of content online is positive in nature—there is a plethora of content that can cause distress or emotional harm. Online spaces are being used by predators and other bad actors to accelerate illegal and harmful activity in an unprecedented way.

## Unlawful Content

This part of the booklet guides young adults to recognize and avoid online content that is harmful, blasphemous, pornographic, etc. The list of online content that is unlawful as per Pakistani law is given ahead.

## Blasphemous Content

Just like in your offline life, when you're online you might come across something which is upsetting, outrageous and unconventional. Content with intent to insult "*the religion of any class of persons*" & is against "*glory of Islam*" is a cognizable offence under chapter – XV of Pakistan Penal Code, 1860 (Act XLV of 1860) ("PPC").

Moreover, under section 295 – C of PPC whoever, defiles the sacred name of the **Holy Prophet Muhammad** (ﷺ) shall be punished with death or imprisonment for life, and shall also be liable to fine.

## Hate Speech

Online hate can be defined as any hateful post about a person or community based on race, religion, ethnicity, sexual orientation, disability or gender. Prevention of Electronic Crimes Act 2016 (PECA), defines hate speech as '*...information through any information system or device that advances or is likely to advance interfaith, sectarian or racial hatred*'.

The law has been designed to protect the dignity of groups and communities. Young people are especially vulnerable to online hate if they are:

- Struggling with a sense of identity
- Experiencing family problems or traumatic event
- Experiencing discrimination pertaining to disabilities, race, sect or ethnicity

Given the anonymous nature of the internet, the effect of what has been said cannot be seen hence some users can act without restraint and leave unpleasant and hateful comments/reactions. This can have an adverse effect on the user who may be on the receiving end of such feedback.





# Indecent/Immoral Content

Content in music videos, movies, online games or advertisements that is pornographic /sexually explicit in nature can send negative & harmful messages such as:

✗ Unrealistic relationship expectations

✗ Lack of consent

✗ Depraved & violent behaviour towards women

It is an offence to “*produce*”, “*distribute*” or “*transmit*” photos and videos of children being sexually abused and exploited (also known as child pornography).





# Anti-State Content

Under PECA (2016), uploading/sharing of content against “*integrity, security or defence of Pakistan or against public order*” is unlawful.

Under Article 19 of the Constitution of Pakistan 1973, freedom of expression has been guaranteed (subject reasonable restrictions). However, groups and individuals inciting violence, promoting hate speech and false information that threaten public order etc. cannot be permitted to do so.

# Defamation

Defamation, as it applies on the internet, is “*intentionally and publicly*” exhibiting, displaying or transmitting any information which is **false** and “*intimidates or harms the reputation or privacy of person*” (Section 20 of PECA 2016).

Online attacks of such kind can have a deep impact on young people and their reputations. They are also not aware of their legal rights in such circumstances. If you are a victim of online aggression, start by:

- Taking screenshots of the image/video or textual post and reporting directly to the social media platform for removal of content.
- Report to the concerned law enforcement agency for investigation.

# Other Forms of Harmful Online Content

While the following type of content is not unlawful, its prevalence online makes it harmful and it might be helpful if you can quickly identify such content to avoid any inconvenience.

# Fake News

Fake news is the spreading of news stories online that are not true, misleading or distorted but made to look like an accurate representation of a situation.

Websites and pages propagating fake news use technology and social media to look like legitimate news sites. Some organizations may target you with ads that look like the news. Hackers use bots and software to create multiple social media accounts and use those to spread doctored narratives.

Sometimes, misleading information is also reported by journalists – which can make it difficult to ascertain the facts.

# Uncover the Truth

Ask critical questions of any news you consume and verify if the news is genuine or fake:

- What website is this from?
- Who wrote it (and when)?
- What does the whole article or video say?
- Which sources are they referring to?





# Harmful User Generated Content

It is easy to assume that the pictures and videos of other users you see on social media reflect their real life, when most of the time they are showing you a lifestyle that is merely smoke and mirrors.

Online personas are created by anyone and everyone to curate the best parts of life. The pressures from social media can negatively affect anyone – especially young people. Sometimes such content can persuade one to take up dangerous hobbies or perpetuate harmful stereotypes.

All social media platforms have community standards or guidelines with regards to dangerous or threatening pranks, videos depicting abuse or encouraging eating disorders, images or clips showing violence and hacking guides.

## What are Community Guidelines?

Community guidelines are a set of rules created by each social media platform that direct how users should behave on a platform to ensure a safe environment for all.

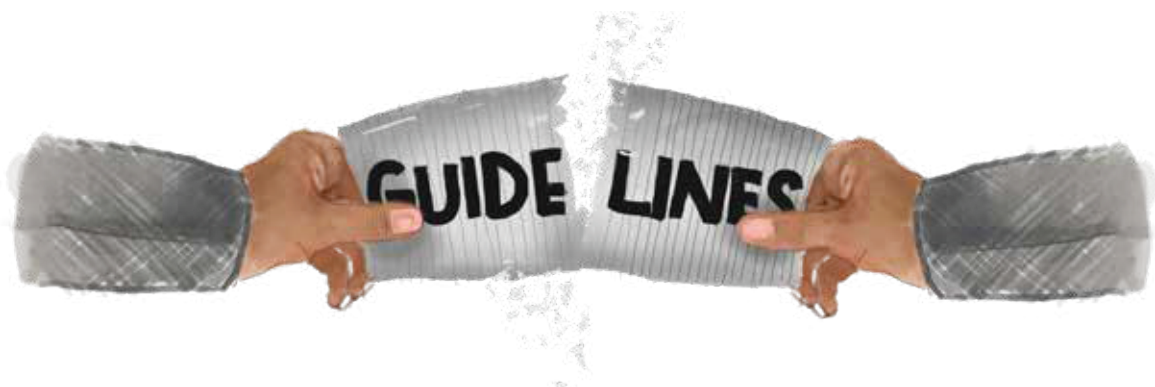
They tend to cover advice on what is prohibited, i.e. harmful behavior, violent/dangerous content, violation of intellectual property and other actions that can lead to accounts being suspended or permanently deleted.



# The Consequences of Breaking Guidelines

Consequences of breaking these guidelines could range from suspension of account or permanent deletion to referring the case to the authorities for taking action. To ensure that you adhere to the platform's guidelines, review them so you are aware of what content is considered acceptable before posting. Below are community guidelines\* from the most popular social media platforms for you to review:

<b>Instagram</b>	<a href="https://help.instagram.com/477434105621119">https://help.instagram.com/477434105621119</a>
<b>Facebook</b>	<a href="https://www.facebook.com/help/477434105621119/?helpref=uf_share">https://www.facebook.com/help/477434105621119/?helpref=uf_share</a>
<b>Snapchat</b>	<a href="https://snap.com/ur-PK/community-guidelines">https://snap.com/ur-PK/community-guidelines</a>
<b>Discord</b>	<a href="https://discord.com/guidelines">https://discord.com/guidelines</a>
<b>TikTok</b>	<a href="https://www.tiktok.com/community-guidelines?lang=ur">https://www.tiktok.com/community-guidelines?lang=ur</a>
<b>Youtube</b>	<a href="https://www.youtube.com/howyoutubeworks/policies/community-guidelines/">https://www.youtube.com/howyoutubeworks/policies/community-guidelines/</a>
<b>X</b> <small>(formerly known as Twitter)</small>	<a href="https://help.twitter.com/en/rules-and-policies/twitter-rules">https://help.twitter.com/en/rules-and-policies/twitter-rules</a>



\*These guidelines are subject to change.



# How to Report

## Block, delete and unfollow

If someone repeatedly sends you content you don't want to see; block, unfollow or delete them.

## 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 or misleading etc.

The identity of the person who is reporting is kept confidential. In some cases, social media platforms might ask you to respond to some personal questions. For example, if you are reporting someone impersonating you or someone you know, they might ask you to send a scanned piece of identification to confirm the identity.

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

<b>Facebook</b>	<a href="https://www.facebook.com/help/181495968648557">https://www.facebook.com/help/181495968648557</a>
<b>Instagram</b>	<a href="https://help.instagram.com/519598734752872">https://help.instagram.com/519598734752872</a>
<b>TikTok</b>	<a href="https://support.tiktok.com/en/safety-hc/report-a-problem/report-a-video">https://support.tiktok.com/en/safety-hc/report-a-problem/report-a-video</a>
<b>X</b> <i>(formerly known as Twitter)</i>	<a href="https://help.twitter.com/en/rules-and-policies/twitter-report-violation#specific-violations">https://help.twitter.com/en/rules-and-policies/twitter-report-violation#specific-violations</a>
<b>Youtube</b>	<a href="https://support.google.com/youtube/answer/2802027?hl=en&amp;co=GENIE.Platform%3DAndroid">https://support.google.com/youtube/answer/2802027?hl=en&amp;co=GENIE.Platform%3DAndroid</a>
<b>Snapchat</b>	<a href="https://support.snapchat.com/en-US/i-need-help">https://support.snapchat.com/en-US/i-need-help</a>
<b>Discord</b>	<a href="https://support.discord.com/hc/en-us/requests/new">https://support.discord.com/hc/en-us/requests/new</a>

# The Internet & the Law in Pakistan

## PECA 2016

The Prevention of Electronic Crimes Act 2016 (PECA) was promulgated and gazette notified on August 22, 2016. It provides the primary mechanism for online content regulation and the investigation and prosecution of cyber offences in Pakistan.

## Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules, 2021

The Rules commonly referred to as Social Media Rules were gazette notified on October 12, 2021 to deploy oversight mechanism, regulate content on social media in Pakistan, and mandate social media companies to localise presence in Pakistan.

## Role of PTA Under PECA 2016

Under Section 37 of Prevention of Electronic Crimes Act (PECA) 2016, PTA is mandated to block/remove unlawful online content in Pakistan including content against integrity, security or defence of Pakistan (anti state), against glory of Islam (blasphemous), hate speech (public order), decency and morality (pornography), contempt of court and defamation/impersonation.

## Procedure for Complaints

### For Blocking

Any person can lodge a complaint regarding unlawful online content for blocking via email address

content-complaint@pta.gov.pk or through Complaint Management System (CMS):

[https://complaint.pta.gov.pk/  
RegisterComplaint.aspx](https://complaint.pta.gov.pk/RegisterComplaint.aspx)

As well as via:

**PTA CMS mobile app**

Upon receipt of complaint, PTA processes the link for blocking/removal. Complainant is also informed of the end result.

PTA is also proactively blocking links pertaining to blasphemous content, pornography or against security and defence of Pakistan etc.

## For Criminal Investigation

Report to Cyber Crime Wing - Federal Investigation Agency for online crimes.

**Helpline:** 1991

**Complaint Form:** <https://complaint.fia.gov.pk/>

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



Scan the code to access more PTA  
online safety advice & other resources.



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

Offences in Prevention of Electronic Crimes Act, 2016 (PECA)				
No	Provision	Description of offence	Sentenced under PECA	
			Fine (up to)	Imprisonment
1	Section 3	Unauthorized access to information system or data	Fifty thousand	Three months
2	Section 4	Unauthorized copying or transmission of data	One hundred thousand	Six months
3	Section 5	Interference with information system or data	Five hundred thousand	Two years
4	Section 6	Unauthorized access to critical infrastructure information system or data	One million	Three years
5	Section 7	Unauthorized copying or transmission of critical infrastructure data	Five million	Five years
6	Section 8	Interference with critical infrastructure information system or data	Ten million	Seven years
7	Section 9	Glorification of an offence	Ten million	Seven years
8	Section 10	Cyber Terrorism	Fifty million	Fourteen years
9	Section 11	Hate Speech	Not given	Seven years





### Offences in Prevention of Electronic Crimes Act, 2016 (PECA)

No	Provision	Description of offence	Sentenced under PECA	
			Fine (up to)	Imprisonment
10	Section 12	Recruitment, funding and planning of terrorism	Not given	Seven years
11	Section 13	Electronic Forgery	Two hundred fifty thousand	Three years
12	Section 14	Electronic Fraud	Ten million	Two years
13	Section 15	Making, obtaining or supplying device for use in offence	Fifty thousand	Six months
14	Section 16	Unauthorized use of identity information	Five million	Three years
15	Section 17	Unauthorized use of SIM cards	Five hundred thousand	Three years
16	Section 18	Tampering etc. of communication equipment	One million	Three years
17	Section 19	Unauthorized interception	Five hundred thousand	Two years
18	Section 20	Offences against dignity of person	One million	Three years
19	Section 21	Offence against modesty of a natural person and minor <i>Previously convicted</i>	Five million Not provided	Five years Ten years
20	Section 22	Child pornography	Five million	Seven years
21	Section 23	Malicious code	One million	Two years
22	Section 24	Cyber Stalking	One million	Three years
23	Section 25	Spamming	Fifty thousand	Three months
24	Section 26	Spoofing	Five hundred thousand	Three years

### Sections of Pakistan Penal Code (PPC)

No	Section	Description	Punishments
1	Section 295 A	To outrage religious feelings	Up to ten years imprisonment or fine or both
2	Section 295 B	Defiling of copy of Holy Quran	Imprisonment for life
3	Section 295 C	Derogatory remarks against Holy Prophet Muhammad (PBUH)	Death or imprisonment for life and fine
4	Section 298, 298 A & B	Intent to harm religious feelings and derogatory remarks against Holy Personalities	Up to three years imprisonment or fine or both





# Online Grooming

There is a chance that you might meet people online that aren't who they say they are. Grooming is a word to describe the tactics abusers use via the internet to sexually exploit and manipulate young people and children.



# How does online grooming happen?

Young people can sometimes end up trusting abusers whose real identities they may not know.

*Online groomers may pretend to be someone else online*

Groomers use social media platforms popular with young people and pretend to be one of them. They select their victim based on perceived vulnerability and attempt to befriend them by pretending to share similar hobbies or interests, using someone else's pictures, offering gifts or followers and sharing "secrets".

*Building trust between themselves and their victim*

Once the groomer gains the victim's trust, they may ask for explicit pictures or videos from the young person. They will try to emotionally blackmail the victim and threaten to block them if they say no to such requests. The victim may feel helpless and end up sharing intimate pictures – which can be used for extortion later by the groomer.

*Groomer can be someone you already know*

Online groomer may be somebody the victim has already met through their family or through social circle. They will further use the internet to build a relationship with their victim. Groomers can pretend to be charismatic, kind and occasionally helpful and young people may not realize that they are being groomed.





# Where can online grooming happen?

Online predators will target children and young adults on platforms and apps that young people are most likely to use (including job forums and gaming sites). They may also appear to be the same age as their victim. The predator will often start a friendly conversation or offer advice to gain the victim's trust before asking them for their phone number to chat privately.

## Warning Signs

The person contacting you online could be a stranger or someone you already know or have met. They can be someone who is older or close to your age. Predators will also lie about their gender, where they live and their actual motivations. Here are some warning signs:

- **You feel uncomfortable**— predators will test boundaries and ask intrusive questions from their victim. Trust your instincts.
- **They tell you their webcam or video app is not working** — the online groomer might pretend to be someone else. They say that their webcam or video app is not working so you cannot see what they really look like.
- **They make inappropriate comments about your appearance or body**— and ask for personal pictures of you or those of your family members/friends. Be careful of anyone online who gives lots of compliments for no reason.
- **They contact you multiple times and in different ways** — for example, you meet them on Reddit then they ask for your phone number and start direct messaging you.
- **They insist on meeting** — they might say they want to see you in person and will act angry/distant or call you a “bad” friend if you don’t agree.
- **They want to keep it private** — people who want to harm you do not want other people to know about them. They may ask you to only contact them when you are alone.
- **They ask you for favors/money etc.** — Once trust has been established, the groomer might ask the victim for money or other favors. They will make false claims and promises about their relationship with the victim to get what they want.





# How to protect yourself from unwanted contact



## Make your accounts private

By adjusting your privacy settings, you can stay in control of who sees what you post online and who can contact you directly.



## Delete contacts

Go through your social media friends' and followers' list. Check if you actually know them. Delete contacts that look suspicious or have not posted in a while.



## Screenshot evidence

Take screenshots of messages, pictures, phone numbers etc. that make you uncomfortable.



## Report and block

Once you have all your screenshots, report the person directly to the platform and then block their account to prevent them sending you further messages.



## Report to police

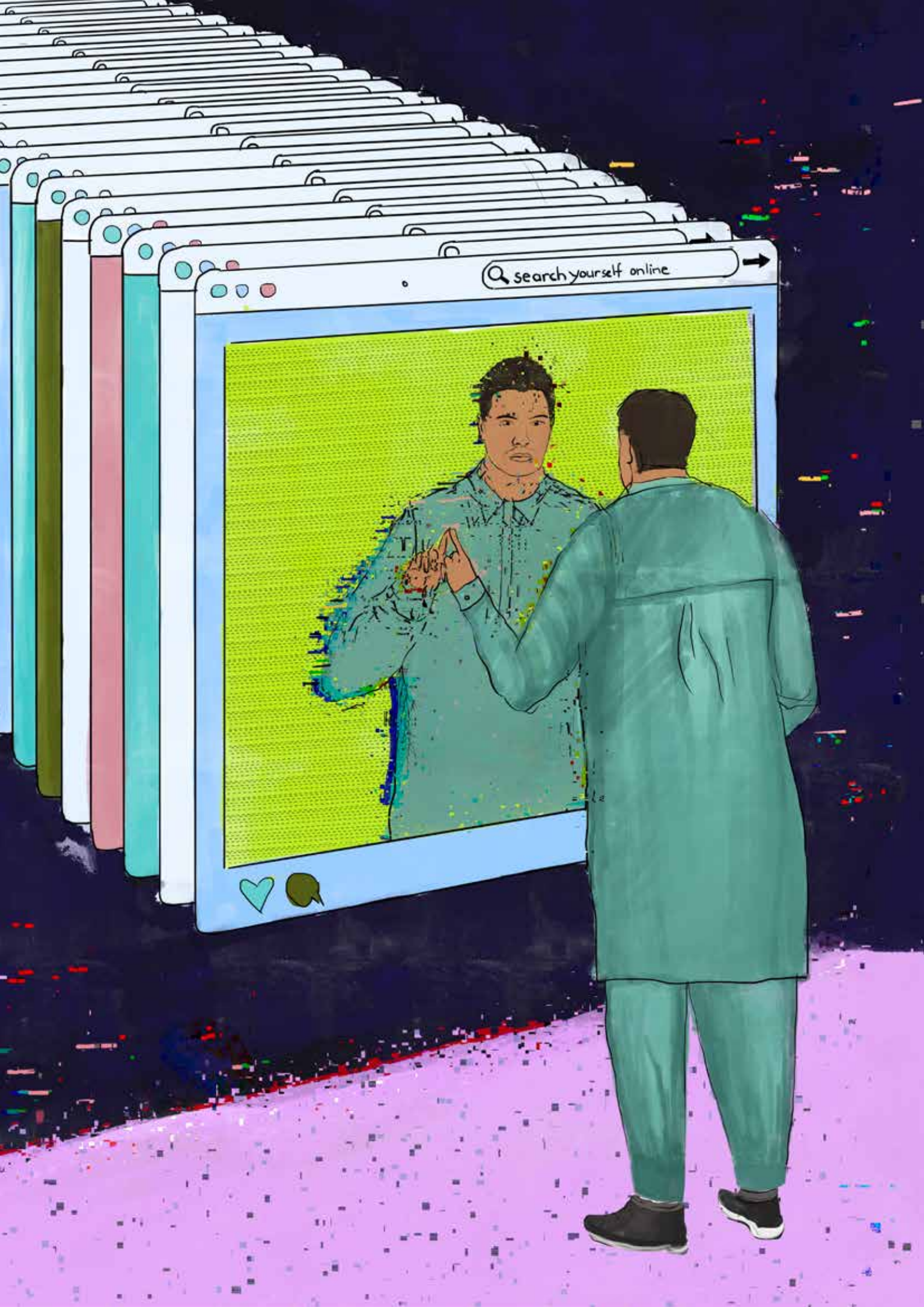
Report cyber-harassment or blackmailing to Cyber Crime Wing - Federal Investigation Agency.

Helpline: 1991

Complaint Form: <https://complaint.fia.gov.pk/>

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







# Online Reputation

A good reputation can propel someone to success. A stellar digital presence creates opportunities.

**Search yourself:**  
do you know what is  
online about you?



## How is it formed?

Your posts and actions on various online social platforms define your image— anyone (including potential employers, universities and others) can google your name or check your social media presence. Things that can form an online reputation include:

Images, videos, stories and opinions you post or share with others.

What you like or dislike and the people you follow online.

## What is a positive digital footprint?

Your digital footprint is any information that exists online for people to see. **Remember: the internet never forgets!** The more you share about yourself, the more a permanent and extensive record will exist about you.

Here are some ways to leave a positive digital footprint:

### Think Before You Post, Like or Share Something:

Building a positive digital presence requires that before posting, sharing or following a particular content/ content creator, you ask yourself if you really want your future employers, teachers, colleagues, family & friends to associate that content with you.

If the answer is no, consider posting/sharing something else that will not worry you in the future.

### Show Your Creativity:

Social media can be used as a medium to highlight your talents and achievements. Young people can publish their creative portfolio or résumé of accomplishments online on various websites or on their social media accounts.

### Create Positive Content:

Images, messages, tweets, videos and any written text on social media will establish your online reputation. Strive to create content that is not offensive or hurts the sentiments of a particular religion, group or community.

### Be Kind and Understanding:

Building a positive digital presence is as easy as liking a post online! Write constructive comments and seek out positive stories to share with friends and family. Take control of your digital reputation.



# Consequences of Negative Online Reputation:

## Impact on relationships

Sharing offensive or hurtful content may have a negative impact on your relationship with family and friends. Other people may also associate the hurtful or offensive content with your personality and may not wish to engage in meaningful relationships with you. As mentioned earlier in this booklet, some content – under PECA 2016 & PPC – is illegal to be uploaded and shared on the internet and you can risk violating the law in the process.

## Impact on educational and career prospects

Many employers and universities now search for candidates online before hiring them or giving them admission. Making a comment about something you disagree with is a reasonable action – however belittling, disparaging, and abusing someone or something may make you an unsuitable candidate.





# Netiquettes (“Internet etiquettes”)

Online reputation is also linked with internet etiquettes. The word is a combination of “Internet” and “etiquette”. Netiquette describes the rules of conduct and behavior for respectful and appropriate communication online. Without such etiquette rules, online conversations can spiral into misunderstanding.

- **Don’t assume everyone understands where you are coming from.** The internet hosts people from different countries, cultures, and ethnicities. With this in mind, review your comment before contributing to the conversation. Ask yourself, “Will everyone understand this?”
- **Don’t spam.** Do not forward unsolicited emails and links to your friends, colleagues and acquaintances.
- **Be Accurate and Factual** It is important to fact-check everything you view online and include sources when giving advice/ information or when simply sharing it on a platform or site. Why? Because false information has the potential to mislead and even harm people.
- **Remember, if it is on the internet, it’s everywhere.** Once information is on the internet, it stays there forever. It is important not to place every intimate detail of your life online – especially if it has the potential to become a security risk in the future.
- **Respect Others’ Opinions.** You will run into some disagreements while being on the internet. However, you can disagree with someone and respect their opinions at the same time. Treat people the way you would like to be treated, and you will avoid potential problems.



“ Fact-check everything and include sources when posting online ”







# Privacy and Identity Theft

Your personal information is a valuable commodity. It holds your digital & financial identity.



# What is Personally Identifiable Information?

Personally identifiable information is any data that can be used to identify someone. This includes information like name, date of birth, CNIC/passport number, phone number, email address and IP addresses etc.

It can also include search history, photos, purchases and locations. The list goes on.

## Who collects data?

Websites, social media platforms and apps track your online behavior. They collect information about your location, browsing habits, web history and more. This data gives a complete intimate picture of who you are, your life, your social circle etc. The websites you visit and the apps you download gather data that advertisers need to understand the type of person you are and which targeted advertisements to show you.

## How is data being used?

Companies use the data collected from connected products — fitness trackers to home automation devices — for financial benefit. Consumers have little awareness of how much of their personal data is being collected, who is looking at it, and its actual worth.

Data brokers or data service providers collect, analyze and sell consumer information – including **personal aspects of your life** such as social media connections, search engine queries, and online purchases – from various sources. They sell it to businesses and investors who monetize this data for business purposes and to capture new revenue streams. Such user data is also acquired by academic researchers to study human behavior.

You may think that the data present online about you is not an issue. After all, you have nothing to hide!

The information you share online: your preferences, shopping habits, relationships, location, religious beliefs, even the number of steps you take every day etc. are all being collected and analyzed by businesses and data brokers who profit from your data.





# How to Protect Your Privacy Online?

## Change Your Device Name

Perhaps, you have “named” your phone, Wi-Fi or Bluetooth as your actual name – “*Ahmed’s Wi-Fi*” - or maybe the name was automatically generated during setup. This means that everyone in the area can see your real name.

Change the name to something less personal through the ‘*Settings*’ of your device.

## Clear Your Location Footprints

Your location can reveal important details about you and your habits, where you live, where you work and where you like to meet family and friends. You may have your location switched off on your phone but several built-in apps may already be tracking your movements and activities. Why? Because this information is valuable to companies and data brokers.

Check the ‘*Settings*’ of your phone and review each app’s permissions and turn off location services - if that app does not need to know your location to provide you with any service.

## Remove Random Apps on Your Phone


The apps on your phone are interested in collecting your data. Review permissions assigned to apps and check your phone routinely to see if there are any apps that you are not using and remove them.

## Privacy Matters

Phones, tablets and computers tend to come pre-installed with browsers that may not prioritise your privacy. A secure browser helps you stay safe online and prevents your data from being exploited.

Search for a secure browser that suits your requirements while also protecting your privacy and shielding you from trackers. For protection, against malware, ads, and tracking, you can install extras known as “*add-ons and extensions*” (these are easy-to-install mini-programs for your browser that can make your online activity more private). Remember to install extensions from official web stores and pay attention to the permissions they require.

## Check if the App or Website is Safe

Make sure the website you are visiting and entering your data into is legitimate. To stay secure, look for Hypertext transfer protocol secure (HTTPS) URL and  icon, and make sure the URL in the address bar is correct. If your antivirus or browser flags a site as fraudulent or it shows you many pop-up ads, it is best to stay away! You can also check the reviews of the website or app online through a simple search online.

**Remember:** A browser extension or piece of software downloaded from a sketchy app or website can potentially create a privacy and security problem. Only download programs, apps and browser extensions directly from their makers and official app stores.



# What is Identity Theft?

Identity theft is when someone uses your personal or financial information without your permission.

They might steal your name and address, credit card, or bank account numbers etc. and use them to:

- Make unauthorized purchases/transactions
- Engage in various fraudulent/criminal activities

## How are identities stolen online?

Online identity theft occurs when users fall for tactics like opening unsolicited malicious email attachments; downloading malware onto their computers or smartphones; connecting to insecure wireless networks or sharing their passwords with other people.

## Malware & Spyware

**Malware** or “malicious software” includes viruses and spyware that can steal personal information, send spam and commit fraud. To trap users, criminals create fake websites resembling legitimate websites, compel users with desirable downloads and ad links that will download malware – especially on computers that don’t have adequate security software.

Spyware is a type of malware that can covertly monitor your online behavior. It may redirect users to unwanted malicious websites, send users pop-up

ads, monitor the websites they visit or record their keystrokes to steal personal information.

## Ransomware

Ransomware is a type of malware that accesses a victim’s files, locks and encrypts them and issues a warning to the victim that a ransom must be paid (through online payment methods) to get those files back. Cybercriminals use such tricks to try to get users to visit websites or click on attachments /links that appear legitimate but actually contain malicious code.

## Online Extortion Schemes

Online/cyber extortion refers to the gaining of cyber assets or money by force or threats. The threats can take various forms, but the most common threats include:

- Releasing personal information such as explicit photos
- Harming the person or their loved ones
- Damage to reputation & financial loss

## Sextortion (Sexual Extortion)

In a sextortion scam, the extortionist threatens to release the victim’s explicit pictures or videos to the victim’s friends and family in exchange for money or other favors. Instead of giving in to the blackmailer’s demands, consider support from a trusted friend/family member and report to concerned law enforcement agency.

## Email Extortion

- The extortionist emails the victims and claims to have hacked into their computer & webcam and recorded private activity.
- Threatens to release compromising information to the victim’s contact list unless payment is made, usually in the form of cryptocurrency.
- Once common tactic is to send an email to the victims about being in possession of their personal data. The criminals reveal a compromised account password from prior large-scale data breaches or hacks to the victim to ensure that the user believes them. These scams are targeted towards children, elderly or other vulnerable groups.



# How to Protect Yourself Against Identity Theft

## Ask questions before giving out your Personal Information

Some organizations need your CNIC/passport to identify you. Those organizations may include your bank, educational institute or your employer.

Other organizations that might ask you for your CNIC/passport might not really need it. Ask these questions before you give them critical personal information:

- Why do you need it?
- How will you protect it?
- Can you use a different identifier?

## Protect your information from scammers online and on your phone

If you're logging in to an online account, use a strong password. Use password manager to store all your passwords.

### Add multi-factor authentication.

Multi-factor authentication offers extra security by requiring two or more credentials to log in to your account. The additional credentials you need to log in to your account fall into two categories: something you have — like a passcode or something you are — like a scan of your fingerprint or your face. Multi-factor authentication makes it difficult for scammers to log in to your accounts if they do get your username and password.





### Vishing:

This where a scammer, posing as trusted sources, uses voice messages or phone calls to try to steal personal/financial information.

### How to Respond:

- Be suspicious of phone calls claiming to come from a reputable organization such as a bank, government organization or TV channel.
- Never share or confirm personal/financial details over the phone.
- Report the number to concerned provider for blocking.

### Smishing:

Scammers use SMS/text messages to trick a user into opening a malicious attachment or link.

### How to Respond:

- Be suspicious of SMSs claiming to come from a reputable organization such as a bank or TV channel.
- Do not respond to text messages that request personal information without first independently verifying that they are from a genuine source.
- Do not click on any links embedded within unknown SMS or call any given numbers.
- Report the number to concerned provider for blocking.

### Phishing:

Phishing is an online attack in which scammers use fake websites (that look legitimate), emails and links in hopes that some person will reveal their personal information such as account number, CNIC, passwords etc.

Often these websites & emails have **spelling mistakes** and **carry a sense of urgency** such as imploring you to claim a reward/free minutes or data/mobile phones etc before the time limit or threatening to suspend your account.

### How to Respond:

- Never give out personal information without first verifying that it is from a genuine source.
- If the suspicious email is from someone you know, contact them through phone or text message to inquire about it.
- Remember that a government organization, bank or a TV channel will not email asking for your sensitive data.



## Watch Out For Credit/Debit Card Skimming

Skimming is a type of theft that uses a device on an ATM to steal and store details from your transaction. 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.

## Check Your Transactions

Regularly review copies of bank and card statements for suspicious activity. Contact your bank immediately if you see transactions that you did not make.

# Report Identity Theft

If you become a victim of identity theft, or even suspect that you might be a victim, take immediate action.

Report identity theft to the Cyber Crime Wing - Federal Investigation Agency

**Helpline:** 1991

**Complaint Form:** <https://complaint.fia.gov.pk/>

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

The Cyber Crime Wing will collect the details of your situation.



