CIVIC ACTION TEAMS

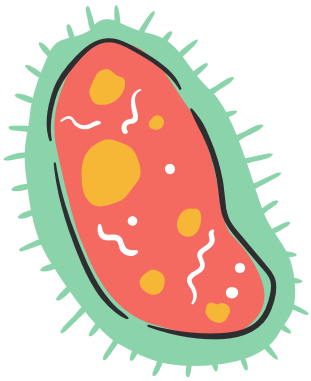
DigitalRightsFoundation "KNOW YOUR RIGHTS"

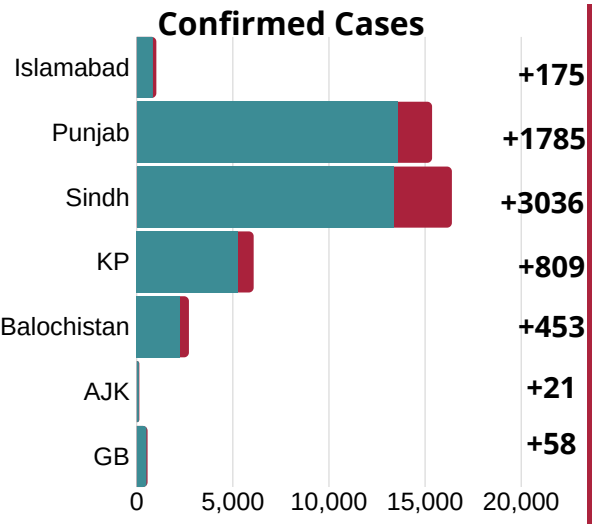
Pakistan Coronavirus CivActs Campaign

Issue #29

18.5.2020

Situations like the coronavirus pandemic can quickly become a catalyst for social conflict due to misinformation, rumors and fake news, as we've seen in the past. Every day we continue to see more false information shared throughout communities, confusing citizens and leaving them unsure as to who can answer their questions.





The Pakistan Coronavirus CivicActs Campaign (CCC) captures rumors and perceptions among communities to eliminate information gaps between the government, media, humanitarian agencies and citizens. By providing the public with facts, these coronavirus bulletins aim to create a better understanding of needs regarding coronavirus and to debunk rumors before they can do more harm.

Protect Yourself!

Follow these steps to help prevent the spread of coronavirus.

- **Wash your hands frequently with soap and water for at least 20 seconds. Use hand sanitizer (with at least 60% alcohol) if soap and water aren't available.**
- **Cover your nose and mouth (with your elbow or a tissue) when sneezing.**
- **Avoid crowded places and practice social distancing. If you think you have been exposed to someone with coronavirus, quarantine yourself for a minimum of 14 days and monitor any symptoms.**
- **Do not stockpile supplies.**

accountabilitylab PAKISTAN

Digital Safety during COVID-19

Conversation with an Expert

To learn about the impact of COVID-19 on digital safety, we spoke to Muhammad Arslan Athar, a Digital Security Trainer at the Digital Rights Foundation. The Digital Rights Foundation is an organization working to make the internet safer and more accessible.

Arslan explained that during the pandemic, DRF has seen a spike in reports related to phishing, not just through email, but also related to the Ehsaas Program and JazzCash apps. This is where DRF's work to spread awareness around digital security becomes more important. When DRF receives phishing complaints through their helpline, they work to address the issues as quickly as possible. Additionally, they create and distribute awareness materials, such as infographics, to reach a larger audience.

On being asked about advice for parents looking to protect their kids from cyber harassment, Arslan said the best way to do so is by having an open conversation with your kids. This will build trust and support them in better preparing for such incidents, and reporting it if it occurs.

From an information security perspective, Arslan mentioned that DRF is concerned about the health and tracking data being collected by the government during this period, and how it will be used and disposed of after the pandemic. To learn about the data operating procedures, DRF is conducting mini advocacy campaigns, and believes in constant messaging to ensure data security.

As the world shifts to virtual classrooms, e-commerce, virtual office meetings, and more, Arslan sees digital security becoming a major concern. While the situation concerning the coronavirus is an emergency, he stressed that it is still important for the Pakistani government to establish boundaries and limitations for its activities, and be transparent, especially if it intends to track the movements of its citizens and save their health information on a mobile application. DRF would welcome the release of SOPs regarding how the data available on the app is being kept and processed.

Data relating to an individual's health is extremely personal, and is information that affects not only the individual, but those immediately around them. Having access to sensitive information about the locations of confirmed cases on a mobile application can be dangerous, as it puts families of victims at risk, as well as exposing their location and data regarding their health. The stigmatisation of those who have tested positive for coronavirus has only made matters in this regard worse.

Which scams have been the most common during this time?

According to the Digital Rights Foundation (DRF), there has been an increase in cyber attacks, specifically individuals reaching out to people via email to ask for money. These individuals claim to have personal information or photos of the people they are targeting, which they will presumably release if the money they are asking for is not paid within a specified timeframe.

If you suspect someone is trying to scam you, contact DRF's cyber harassment helpline at 0800-39393. DRF representatives can help make sure that your accounts have not been compromised.

Digital Safety during COVID-19

What are some different types of online harassment?

Online harassment means using digital platforms like email, social media, applications and websites to attack and elicit the emotions of fear, anxiety and depression in the intended target. There are many forms of online harassment that we should be aware of. Some of these include:

Phishing: This form of online harassment is when a harasser creates fake email or social media accounts and portrays themselves as someone else or as a legitimate institution in order to trick people into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. Anyone can be a victim of phishing at any time but the best way to avoid such interactions is to avoid adding unknown accounts to your social media, or even replying to suspicious emails.

Trolling: is when a harasser uses provocative, harassing statements or irrelevant topics to cause outrage in the intended target. Although it may be difficult to tell if someone is trolling or just arguing, the result can cause negative effects on the psychological well-being of the victim, through illnesses such as depression.

Flaming: One of the most common forms of online harassment is flaming. Flaming is the act of starting intense arguments including racism and any hatred designed to hurt someone's feelings. The option of appearing anonymous on social media is one reason why flaming is rampant in computer mediated communication. Anonymity allows users to become immune to any sanctions imposed in a regular social setting. Flaming can be avoided by responding to all questions politely with strong facts and evidence to back them up, or by not responding at all.

What steps can be taken to protect against cyber harassment?

While many sites and social networks are working to keep their users safe and to ensure that all reports of cyber-bullying and abuse are dealt with effectively, users also have a responsibility to make sure we are using them in a safe, respectful and appropriate manner. Some steps they can follow include:

- If someone makes you feel uncomfortable, embarrassed, or afraid online, tell someone immediately. Hesitating can cause danger.
- Never set up a social networking site in someone else's name or upload false information about them. You are not allowed to upload a picture or video of anyone without their permission.
- Don't click on ads while browsing through the internet, or reply to emails that you received from an anonymous source as these are among the ways hackers steal your information and hack into your accounts.
- Anything you post on the Internet stays there and can come back and cause problems for you later on. If you're happy for the world to see the photo or comment, hit send. If you're not, don't upload it.
- Parental controls should be used on any device being used by children to help keep the children away from explicit content and accidentally stumbling into something dangerous. Use age-appropriate settings to filter, monitor and block activities.

What is an infodemic?

An infodemic is an excessive amount of information about a problem, which makes it difficult to identify a solution. Earlier this year, Director General of the World Health Organization, Mr. Tedros Adhanom Ghebreyesus used the word "infodemic" to refer to fake news that spreads faster and more easily than the virus. This includes the spread of misinformation, disinformation, and rumors, which can create confusion and distrust among the public, and hinder an effective public health response.

accountabilitylab PAKISTAN

Digital Safety during COVID-19

How should I report cyber harassment on social media platforms?

Most social media platforms have a reporting system in place for taking action against cyber bullying. Some of these include:

Facebook adheres to a set of community standards as it does not tolerate any act of harassment or abuse. You can report bullying to Facebook using the Report links which appear on the page, a 'drop-down arrow' should appear giving you a menu option to report the image, post or comment.

Twitter, known for emphasizing real-time information, is also working towards reducing online abuse. The platform allows you to report any unwanted replies, abuse, or threats from someone through this link.

YouTube does not support the upload of any videos with hate content, graphic violence or inappropriate scenes. In case you want to report abusive, bullying or threatening comments on YouTube, you can report them here and they will investigate.

Instagram is becoming the fastest growing social network, attracting many hackers and abusers. Instagram's advice to someone facing harassment is to block and unfollow the person who is being abusive. If it continues, you can report it here.

Snapchat has recently seen a rise in its daily users as people are turning to the app to stay connected with others. If a person is bullying or harassing you, or you receive an inappropriate image, report it through Snapchat's online form.

As a messaging service, harassment can happen in many ways via WhatsApp. You can block and delete a contact who may be bullying you. You can find out more by emailing WhatsApp at this address support@whatsapp.com.

Who can I contact to report cyber crime or cyber harassment?

If you are a victim or know someone who is a victim of cyber harassment or cyber crime, cases can be reported on the following helpline numbers:

1. Digital Rights Foundation Toll-free number: 0800-39393 (Monday to Friday from 9:00 a.m. to 5:00 p.m.).
2. FIA National Response Center for Cyber Crimes Helpline: 9911
3. The Citizens-Police Liaison Committee Call: 021-35662222
4. Madadgaar National Helpline: 1098
5. Federal Investigation Agency's National Response Centre for Cyber Crime has an online complaint form that can be filled out here.

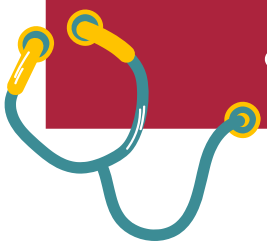
What are some ways that social networks are protecting users against misinformation?

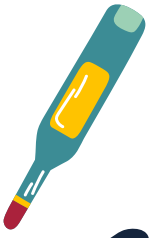
A team of WHO "mythbusters" are working with companies like Facebook, Twitter, TikTok, YouTube, and more, to counter the spread of misinformation. According to news reports, these companies are filtering out false medical advice, hoaxes, and other false information that could risk public health. Facebook and Twitter even went as far as to remove a post by a head of State because it falsely stated that a certain drug was working everywhere against the coronavirus. Find out more about how the following social networks are fighting misinformation: Facebook, Instagram, Twitter, TikTok.

What do I do if I think I have coronavirus?

Do you have any symptoms?

- Fever
- Shortness of breath
- Dry cough
- Tiredness





If so, contact your doctor or the coronavirus helpline at 1166.

Where can I get tested?

Karachi

Aga Khan University Hospital
Stadium Road, Karachi

Civil Hospital
DOW University Campus
Mission Road, Karachi

Dow Medical Hospital
Ojha Campus
Suparco Road, Karachi

Indus Hospital
Opposite Darussalam Society, Korangi Crossing, Karachi

Lahore

Punjab AIDS Lab
PACP Complex
6 - Birdwood Road, Lahore

Shaukat Khanum Memorial Hospital
7A Block R-3 M.A. Johar Town, Lahore

Islamabad

National Institute of Health
Park Road
Chak Shahzad, Islamabad

Rawalpindi

Armed Forces Institute of Pathology
Range Road
CMH Complex, Rawalpindi

Multan

Nishtar Hospital
Nishtar Road,
Justice Hamid Colony, Multan

For more cities visit the
COVID-19 Health Advisory Platform

Coronavirus CivActs Campaign is brought to you by **Accountability Lab Pakistan** in collaboration with **Digital Rights Foundation**

DRF
DigitalRightsFoundation
"KNOW YOUR RIGHTS"

accountabilitylab
PAKISTAN