Threads of Trust: A Tale of Digital Security Risks in Pakistani Apps

Ali

Security and Privacy Researcher

Ayesha

At-risk Population Advocate

Amir

Political Scientist

Popular Pakistani Apps

Background

Pakistan is in the midst of a digital revolution that is transforming the way citizens interact with government and private services. Mobile apps—once used by only the few—are now an integral part of daily life for millions throughout the country. These apps make essential services more accessible and efficient by streamlining tasks, such as updating national identity documents and managing telecom accounts.

Unfortunately, however, many of these apps are riddled with security vulnerabilities and hidden backdoors that can easily expose personal information. Within the country's surveillance-based software development ecosystem, opportunities for exploitation abound—making apps highly susceptible to targeted attacks that put users at risk

Ali

Ayesha

Amir

1

On a chilly winter afternoon, Ali, Ayesha, and Amir the three friends gathered at their favorite café—, a cozy, warm spot they had frequented together during their undergraduate years. The moment they laid eyes on each other, the joy filled the air—hugs, smiles, and laughter flowed freely as they reminisced about their past. The time years apart seemed to vanish, and the bond they shared was as strong as ever.

2

After catching up on family and shared friends, Ali sat back from the table. He couldn’t wait any longer. He needed to tell Ayesha and Amir about his recent research breakthrough.

3

Guys! I've been studying security vulnerabilities in Pakistani Android apps and made a shocking discovery. Many of these apps collect vast amounts of personal data—like location, names, and phone numbers—and store it in plaintext. Security flaws like these leave us incredibly exposed!

4

At the mention of this news, Ayesha leaned forward. She had spent the past several years working with at-risk groups like journalists, activists, and abuse victims of abuse and knew just how serious digital threats could be.

5

Tell us more, Ali. How does storing credentials in plaintext, put users at risk?

Ali

Pak Identity

Pakistan Citizen Portal

Qeemat Punjab

Government Apps

Ayesha

6

Local police can make arbitrary arrests and seize phones, like what happened during the February 8, 2024 elections (a). In cases like these, authorities can easily extract sensitive data—including names, phone numbers, and locations—if it is stored in plaintext on a device. That data could be used for spying and surveillance.

7

Yikes! That's really disturbing.

Ali

8

It is! But it doesn't stop there. State actors can also use these vulnerabilities to intercept and manipulate communications between apps and servers. Attackers could exploit this to alter location coordinates or even plant fake evidence to frame someone.

Ayesha

(a) Political Unrest post Feb 08, 2024 elections.
https://www.nytimes.com/2024/08/01/world/asia/pakistan-protests-politics.html

9

Having studied the politics of Pakistan for years, Amir could hold back no longer.

10

That's terrifying, Ali, especially with the ongoing protests and government crackdowns. It's easy to imagine state actors exploiting these vulnerabilities and erasing any evidence. Incidents like the attack on Asad Ali Toor (b) or the shooting of Absar Alum (c) suggest some state actors are using location data to track individuals for nefarious purposes.

Amir

11

And that means private attackers—like criminals or abusers—could also track movements, contacts, and extract call/SMS histories if they were to steal or confiscate a phone. Just think of the cases of Shahid Zehri (d) and Muhammad Zada Agra (e)!

Ayesha

(b) Asad Ali Toor. https://www.aljazeera.com/news/2021/5/26/pakistani-journalist-assaulted-in-latest-press-freedom-attack

(c) Absar Alam. https://www.nytimes.com/2021/04/20/world/asia/pakistan-journalist-military.html

(d) Shahid Zehri. https://cpj.org/data/people/shahid-zehri/

(e) Muhammad Zada Agra. https://cpj.org/data/people/muhammad-zada-agra/

12

Exactly. And unfortunately I found troubling issues with telecom apps, too. None of the four major telecom apps require a password for login. They just use the mobile number and an OTP sent to the device for authentication. If someone has access to the phone, they could easily log in to these apps and gain full access to a user's account!

13

Wow—that's a huge security flaw. Have you reported these risks to the app vendors?

Ali

SIMOSA

My Zong

My Telenor

UPTCL

Telecom Apps

Amir

14

I did, and I received positive responses from the developers of the Pak Identity, My Zong, and My Telenor apps. Nothing yet from the developers of the others—but hopefully they will respond, too. I'm concerned some of these vulnerabilities are so deeply embedded that fixing them will require considerable effort. But they must be addressed! Millions of Pakistanis rely on these apps, and many of them are at-risk users.

Ali

15

A moment of silence passed as the weight of their conversation sank in. Then Ayesha spoke up.

16

Like victims of domestic abuse! From my experience, I know abusers can coerce access to victims' devices with or without their knowledge or consent.. These vulnerabilities make it easier for them to secretly spy on their victims.

Ayesha

17

The urgency of this unique intersection of digital security, political unrest, and human rights was clear to all three friends. Amir spoke up.

19

So many bad actors could exploit these vulnerabilities. I will share this news with my network of journalists so they are aware of the potential risks. In the meantime, Ali, is there anything users can do to protect themselves?

18

Based on my studies, I also worry about the potential for misuse by corrupt state actors. Honest officials might justify surveillance capabilities in apps as a means to identify criminals, but the situation changes when corrupt motives are involved. A dishonest local police officer could easily use these loopholes to spy on an ex-partner for harassment, or even plant fake evidence to frame an innocent journalist. The friends and family of an at-risk individual could be targeted and intimidated, too!

Amir

20

Ali nodded eagerly. As a digital security researcher, he was always excited to make his findings actionable for everyday people.

Ali

Ayesha

21 I'm glad you asked! The bottom line is, anyone who considers themselves at-risk or vulnerable should be careful anytime they use these seven apps.

Ali

24 Several things! In fact, I actually created a set of tips explaining what to do with government apps and telecom apps. Here—please share them with your network and family members. Together we can bridge technology, politics, and human rights to create meaningful change in Pakistan!

22 That makes a lot of sense.

Ayesha

23 Yes—but what does "being careful" mean in this case?

Amir

Government Apps

Keep these security tips in mind when using the Pak Identity, Pakistan Citizen Portal, and Qeemat Punjab apps:

1. As a proactive safety measure, only use these apps when necessary and be sure to uninstall them afterwards.

2. Be careful whenever using a VPN, and remember these apps transmit location data.

3. Regularly update your passwords to safeguard your accounts and minimize the risk of compromise (keeping in mind these apps cannot detect login activity from unknown devices or places).

Telecom Apps

Keep these security tips in mind when using the SIMOSA, My Zong, My Telenor, and UPTCL apps:

1. Because these apps do not require a user-specified password, you should use the "panic button" if your phone is stolen or confiscated. Doing this will lock your phone and prevent an attacker from installing a telecom app on the device to obtain call logs, SMS logs, and other sensitive information.

2. Be cautious if you receive an OTP (One-Time Password) on your phone that you did not request. This could be a sign of unauthorized access to your account, and you should take immediate action to secure it.

DISCLAIMER: This cartoon story—intended solely for educational purposes—focuses on security and privacy concerns related to Pakistani Android apps. In doing so it examines two key categories: government apps (including Pak Identity, Pakistan Citizen Portal, and Qeemat Punjab), and telecom apps (including SIMOSA, My Zong, My Telenor, and UPTCL). Understanding potential vulnerabilities related to these apps is important because users are often encouraged to install and keep them on their devices for long periods of time. Recommendations offered at the end of the story will not provide 100% security and privacy, but they likely will enhance security and privacy if followed by at-risk users. While the story itself references political events, the authors do not express political views. Notably, the three featured friends are fictional characters and do not represent real individuals. Ali's experience researching Pakistani apps, however, is inspired by an actual researcher. That researcher has actively engaged in an ethical disclosure process with the app vendors. Finally, authors have used AI technology to generate images and ensure greater consistency throughout the text.