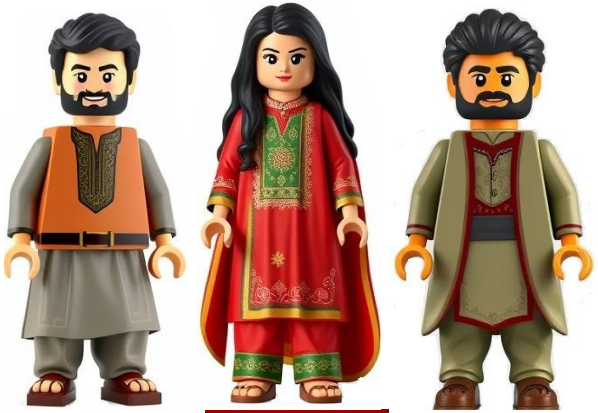
Threads of Trust: A Tale of Digital Security in Pakistani Apps

Disclaimer

This cartoon story is intended exclusively for educational purposes. It highlights the security and privacy concerns associated with Pakistani Android apps, specifically focusing on two key categories: government apps like Pak Identity, Pakistan Citizen Portal, and Qeemat Punjab, and telecom apps such as SIMOSA, My Zong, My Telenor, and UPTCL. Analyzing these apps is crucial, as users are often motivated to install and retain them on their devices for extended periods. While the story makes references to political events, the authors do not express any political opinions. The three friends depicted in the story are fictional characters and do not represent any real individuals. Ali's experience, which involves researching Pakistani apps, is inspired by a real researcher who has analyzed these apps and is actively engaged in the ethical disclosure process with the app vendors. Additionally, AI technology has been used to generate images, ensuring greater consistency throughout the text.

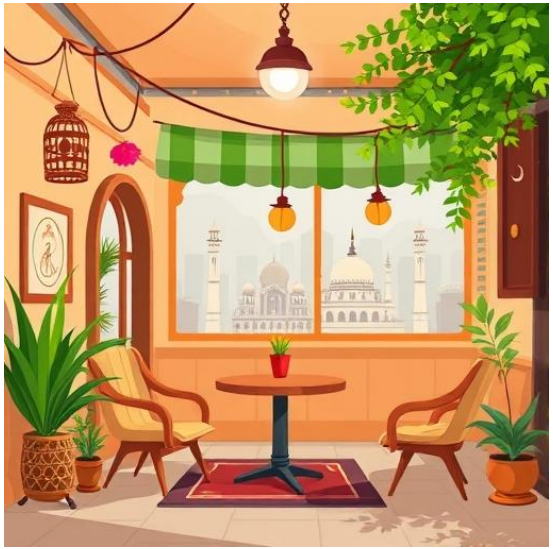


1

It had been years since Ali, Ayesha, and Amir, three friends from Pakistan, had last met. After their university days, their lives had taken different paths—higher education, careers, and new experiences. Yet, fate had a way of bringing them back together, and soon, a reunion was on the horizon.

2

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



3 Ali was the first to speak.

4 I've been studying security vulnerabilities in Pakistani Android apps, like Pak Identity, Pakistan Citizen Portal, and Qeemat Punjab. These apps collect vast amounts of personal data—location, names, phone numbers—and store it in plaintext, revealing shocking security flaws. Have you ever considered how exposed we are?

5 That's interesting, Ali. I work with at-risk groups like journalists, activists, and abuse victims, helping them understand digital threats. The more I learn, the more I realize their vulnerability. But if credentials are stored in plaintext, how does that put users at risk?

Ali

Pak Identity

Pakistan Citizen Portal

Qeemat Punjab

Ayesha

6

Ayesha, during events like the February 8, 2024 elections (a), the police made arbitrary arrests and seized phones. They could easily extract sensitive data, like names, phone numbers, and locations, to track and monitor individuals even after their release. That data could be used for spying and surveillance.

That's really disturbing.

7

Ayesha

Ali

8

But it doesn't stop there. State actors can not only exfiltrate data from these apps, but they can also intercept and manipulate communications between these apps and their servers. This creates another vulnerability. Attackers could tamper with data in transit—altering location coordinates or even planting fake documents to frame someone.

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

9

Amir, who had been listening intently, spoke up, his voice grave.

10

That's terrifying, especially with ongoing protests and government crackdowns. Even without concrete evidence, it's easy to imagine state actors exploiting these vulnerabilities and erasing traces. Incidents like Asad Ali Toor's (b) attack and Absar Alum's (c) shooting suggest state actors are using location data to track individuals.

Amir

11

You're right. State actors could exploit these vulnerabilities, but private attackers—like criminals or abusers—could also track movements, contacts, and extract call/SMS histories. This data could target individuals, as seen in the cases of Shahid Zehri (d) and Muhammad Zada Agra (e). Ali, have you looked into the telecom apps?

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

Yes, I actually found something troubling. The four major telecom apps—SIMOSA, My Zong, My Telenor, and UPTCL—don't require a password for login. They just use the mobile number and an OTP sent to the device for authentication. This means that if someone has access to the phone, they can easily log in to these apps and gain full access to the user's account.

Ali

That's a huge security flaw. Have you reported these risks to the app vendors yet?

13

Amir

SIMOSA

My Zong

My Telenor

UPTCL

15

I have. I received a positive response from the developers of Pak Identity, My Zong, and My Telenor, but I'm still waiting to hear back from the others. I'm also concerned that some of these vulnerabilities run so deep that addressing them could lead to political or social backlash. But these issues definitely need to be fixed. The potential consequences are too severe to ignore.

14

Ali

Ayesha

Amir

A moment of silence passed as the weight of their conversation sank in. Ali, Ayesha, and Amir, once close friends, now saw the power of combining their expertise. The urgency of digital security, political unrest, and human rights had never been clearer.

As the café's warmth faded, they began brainstorming—Ali on securing apps, Ayesha on protecting vulnerable groups, and Amir on providing political context. Their shared goal was to bridge technology, politics, and human rights for meaningful change.

What started as a reunion quickly became a partnership to address their country's most pressing issues. United by a common purpose, they were ready to make their country a safer, more just place for all.