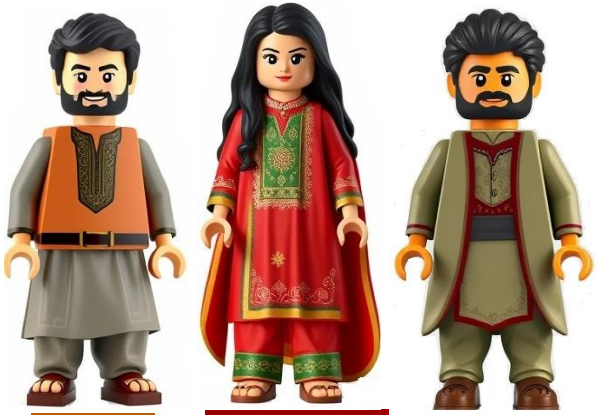
Threads of Trust: A Tale of Digital Security Risks in Pakistani Apps

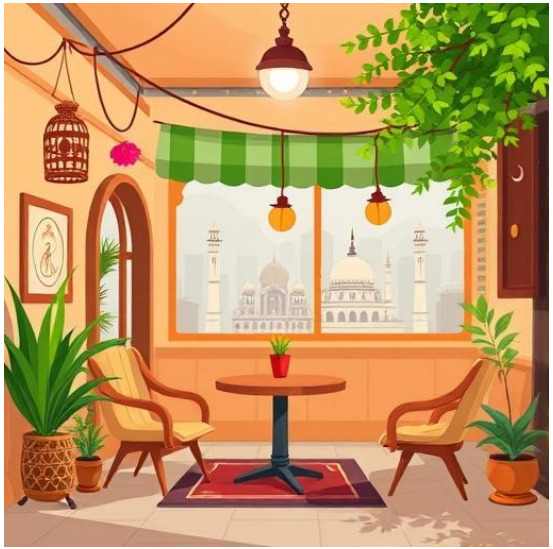
Disclaimer

This cartoon story is intended solely for educational purposes, focusing on security and privacy concerns related to Pakistani Android apps. It examines explicitly two key categories: government apps, including Pak Identity, Pakistan Citizen Portal, and Qeemat Punjab, and telecom apps, such as SIMOSA, My Zong, My Telenor, and UPTCL. Analyzing these apps is important because users are often encouraged to install and keep them on their devices for long periods. While the story references political events, the authors do not express political views. The three friends featured in the story are fictional characters and do not represent real individuals. Ali's experience, which involves researching Pakistani apps, is inspired by an actual researcher. That researcher is actively engaged in the ethical disclosure process with the app vendors. Additionally, authors have used AI technology to generate images and ensure 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

Now a security and privacy researcher, Ali enthusiastically explained his fascinating work on Pakistani apps.

4

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

6

That's troubling, Ali. 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 ID™

Pak Identity

Citizens Portal PAKISTAN

Pakistan Citizen Portal

Qeemat Punjab

Qeemat Punjab

5

Ayesha, who now works with at-risk groups like journalists, activists, and abuse victims to help them understand digital threats, replied.

Ayesha

7

Ayesha, during events like the February 8, 2024 elections (a), the local 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.

8

Ayesha

Ali

9

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

10

Amir, now a political scientist, had been listening intently and spoke up, his voice grave.

11

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 attack on Asad Ali Toor (b) and Absar Alum's (c) shooting suggest state actors are using location data to track individuals.

Amir

12

You're right, Amir. 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 also 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/

13

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?

14

Amir

SIMOSA

My Zong

My Telenor

UPTCL

15

I have received positive responses from the developers of the Pak Identity app, My Zong app, and My Telenor app, but I'm still waiting to hear back from the developers of the other apps. I am also concerned that some of these vulnerabilities are so deeply embedded that addressing them will require considerable effort from the app developers. Nevertheless, these issues must be addressed, as the potential consequences are too serious to ignore.

Ali

16

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

17

Yes, this makes me worry more about the victims of domestic abuse, as abusers can coerce victims' devices with or without their consent, with or without their knowledge, and secretly spy on them.

Ayesha

18

Ali, Ayesha, and Amir, once close friends, now started to realize the gravity of the situation. The urgency of digital security, political unrest, and human rights had never been clearer.

19

Amir, who had been listening closely to Ali and Ayesha, spoke up.

20

That's a valid point, Ayesha. I share your concerns about victims of domestic abuse, but I also worry about the potential misuse by corrupt state actors. While honest officials might justify surveillance capabilities in apps as a means to identify criminals, the situation becomes far more dangerous when corrupt individuals are involved. For instance, a dishonest local police officer could use these tools to spy on an ex-partner for harassment, or even plant fake evidence to frame an honest journalist. Worse yet, they could use this information to intimidate the friends and family of an at-risk individual.

Amir

21

You are right Amir. Corrupt state actors and private attackers can also exploit these vulnerabilities in Pakistani apps. I will share Ali's findings with my network of journalists so that they are aware of the potential risks.

22

Ali, is there anything users can do to protect themselves in the meantime, while the developers work on fixing these issues?

Ayesha

23

Well, users can avoid using government apps altogether, or refrain from using them in locations they consider sensitive. As for telecom apps, even if a user hasn't installed the app, if the device is confiscated, stolen, or otherwise compromised, an attacker could install the app on the user's phone and access sensitive personal information. In such cases, using a panic button that locks the device could help protect the user by preventing attackers from gaining access.

Ayesha

Amir

Ali

24

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.