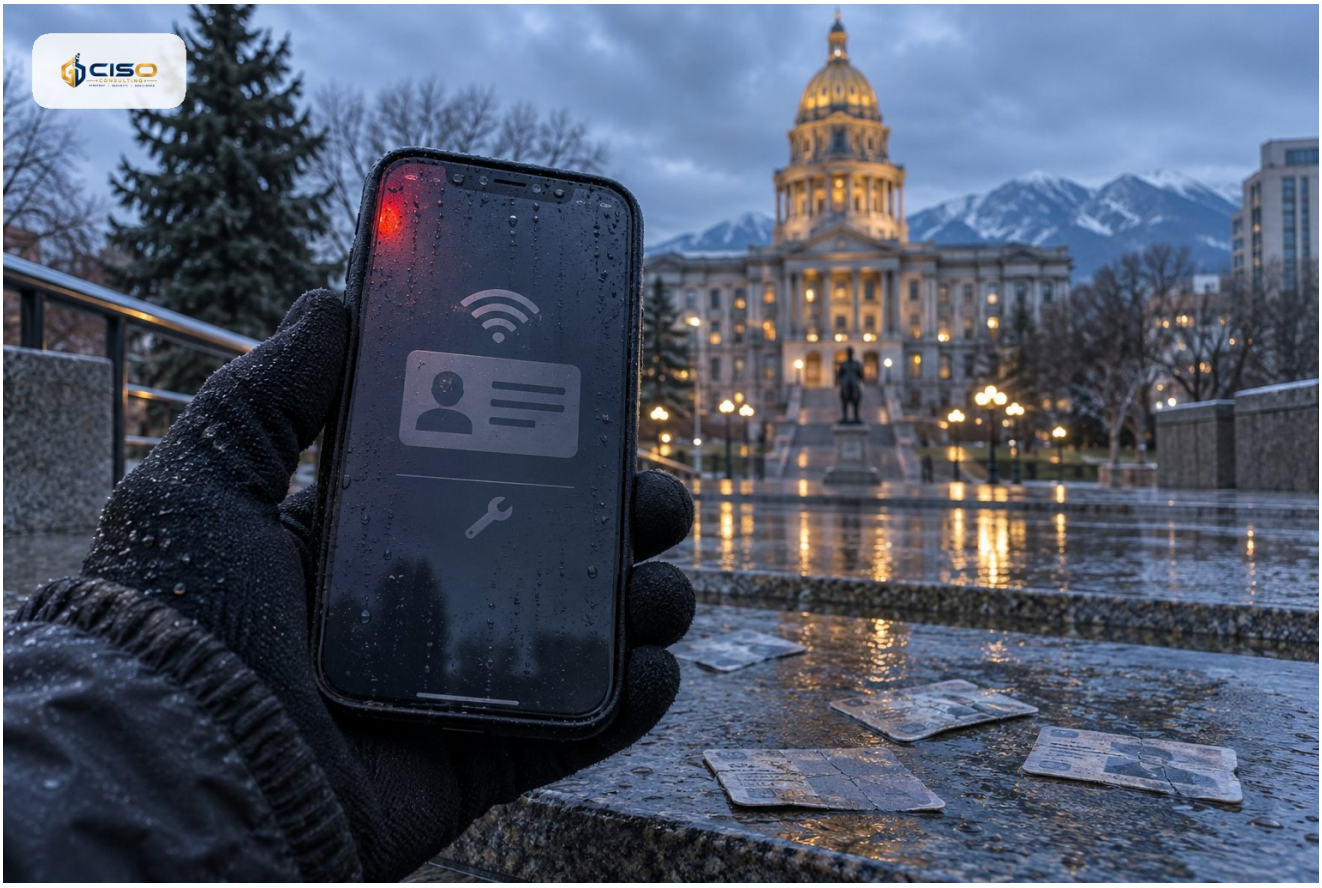
Colorado's myColorado app breach may affect about 100,000 people



Colorado's IT office says attackers accessed user-uploaded ID documents in the myColorado app. About 100,000 people may be affected; no payment data was accessed. The app remains offline.

- Unauthorized access hit the 'myCards and Documents' section of myColorado, which has about 2.1 million users.
- Exposed files include PDFs and photos of government IDs, vehicle registrations and insurance cards.
- About 100,000 people might be affected; the estimate may be refined as documents are matched to users.
- No payment information was accessed.
- Detection came from automated threat detection in the state's AWS environment; notifications are

> expected to begin on November 27.

The Colorado Governor's Office of Information Technology (OIT) has disclosed a data breach affecting documents that residents uploaded to myColorado, the state's official mobile app for digital identification, state services and document storage. The app has approximately 2.1 million users.

What happened

OIT took the application offline after identifying unauthorized access to platform data and started incident response and an investigation. It says the incident came to light when the attackers triggered automated threat detection systems deployed in its Amazon Web Services (AWS) environment.

The investigation found that the attackers accessed the 'myCards and Documents' section, which holds user-uploaded PDFs and photos of government IDs, vehicle registrations and insurance cards. About 100,000 individuals might be affected. No payment information was accessed.

Current status

Staff are matching the accessed documents to individual users, and OIT says it will refine the estimate as that work continues. The app remains offline with no restoration date announced. Direct notifications to affected people are expected to start on November 27. The state CIO said the priorities are user security, notifying those involved, and restoring the app with security enhancements.

Why it matters for Saudi institutions

The case shows how user-uploaded identity documents in a cloud-hosted service become a concentrated risk, and how automated detection can surface an intrusion. Organizations that collect copies of national IDs, vehicle or insurance documents should review how those files are stored, monitored and retained.

What to do now

1. Inventory where customer or employee ID document images are stored, including cloud storage, and who can access them.
2. Apply encryption, least-privilege access and retention limits to stored identity documents.
3. Confirm that cloud threat detection covers storage of uploaded documents and that alerts reach a staffed response process.
4. Test your incident response and PDPL breach-notification procedures, including how to identify affected individuals from accessed files.
5. Prepare a customer communication template and a plan for taking a service offline and restoring it safely.