How Does Groww Keep My Data Safe?

At Groww, we highly value your data and privacy. We follow some prudent practices at both the application and infra layers to ensure that we can work in tandem to keep your data safe.

1. We provide three factors of authentication whenever you login from a new device. They are:
    a. Something you know - Users can either login via Google or via your email.
    b. Something you own - Whenever a user logs in from a new device, we send an OTP to their registered mobile number to register the device on our end.
    c. Something you are - Users who enable biometric authentication on their Groww app, can use that to log into the app post onboarding.
2. We intimate users every time they login with a new device and provide them an option to logout or contact us in case of any suspicion.
3. Users can also view all their active devices and logout from any device they had previously logged in from.
4. Groww works in highly regulated industry with multiple regulators. We have an internal compliance and security team that ensures we are compliant with all regulatory guidelines. Audits are conducted on the same from time to time.
5. We ensure that we keep our technology at par with the industry standard. Also, as a common sense practice, any new technology is only integrated upon a go ahead from the security team.
6. We conduct periodic internal and external audits over both our infrastructure and application.
7. Groww is ISO 27001 compliant and we ~~conduct~~ undergo InfoSec (information security) audits by authorized external auditors based on the regulatory requirements.
8. Select employees are granted access to customer and payment related data. Only the necessary details needed to resolve the query of the customer are given to the employees.
9. At the database layer, the customer and payment data is encrypted as per industry standard and stored within the Indian Jurisdiction.
10. We conduct a mandatory InfoSec training when any new employee is onboarded and, again, on a periodic basis, and assessments are conducted on the same. This ensures that every employee is aware of the InfoSec practices and repercussions on breaching it.
11. We have proper access controls in place for employees which helps keep our application safe.
12. We have network and application level protection to prevent against external attacks like DDoS, SQL injection XSS, etc.
13. We follow SSO (single sign-on) VPN based login, for safe multi-application access using same set of secure credentials, at the organisation and application level to avoid any password related risks.

14. We have an in depth authentication strategy implemented at the infrastructure level, i.e. various layers of firewalls which ensure multi-layer protection.
15. We have alerting mechanisms set over all our internal systems and processes which helps us monitor any anomalous behaviour in our application.
16. Third party vendors undergo rigorous Infosec screening by our security team before they are onboarded.

At Groww, we have a dedicated GRC and cybersecurity team that is always on top of any new vulnerabilities that may have caused havoc in the industry.