HACKSHIELD MOBILE FAQ

- **If the government of the United States of America could not prevent a cyber-attack and Breach of information, how can your company claim to prevent such attacks?**

None of the software or the organization is hack-proof. Every software and organization has a bug on its own. So, the organizations host bug bounty and responsible disclosure programs. Coming to our product we try to minimize the attack surface and prevent from most common and advanced attacks. For most dangerous threats like 'Zero Day'. We can't assure full protection but we can assure you to patch and mitigate the attack surface as soon as possible with the help of our team.

- **Does the feature require administration rights?**

Yes, For Anti-theft (Device Shield) it required administration rights. (Android)

- **This product slow down the phone or not?**

Depends on devices how much memory the user is giving for the HackShield.(Android)

- **How much Ram it requires to run the application.**

To run Application Minimum 2GB ram required. (Android)

- **Any app installed on my phones without permission, how can I use the app?**

That application user not able used because those applications are hidden in the users phone.

- **Mobile software users are able to use their computer or not?**

No, But can access or sync data of Password Module through a web panel and from Geo Location can control User's device.

- **In google play store show the error if something went wrong?**

That time from setting go to application manager selected their google play store in that click on the storage and click on clear data then try to download from the google play store.

- **How sustainable your product and its quality?**

This product is certified and we are giving them 100% sustainable products.

- **Why so many permissions and what are they for...?**
    1. **Prevent phone from sleeping-** HackShield takes the required permission stating "Prevent phone from sleeping" because it has a feature of Device-Shield wherein it requires the permission in case of Phone Theft.
    2. **View Wi-Fi connections-** HackShield takes the required permission stating "Viewing Wi-Fi connections" because through the Device Connected feature of HackShield lets you know the IP Address that is connected to the Wi-Fi
    3. **Receive data from internet-** HackShield takes the required permission stating "Receive data from internet" because through the login and signup the user's data does gets stored in the Backend so that HackShield knows if the user is new or existing.
    4. **Disable your screen lock-** HackShield takes the required permission stating that" Disable your screen lock" because with HackShield's feature rightly known as Total Unlock it prevents intruder from accessing the user's device.

5. **Google play billing service-** HackShield takes the required permission stating “Google play billing service” for the payment process when required to purchase the HackShield Anti Spying Solution.
6. **Connect and disconnect from Wi-Fi-** HackShield take the required permission stating as “Connect and Disconnect from Wi-Fi” because HackShield does want to check the Wi-Fi Status in on or off for the Wi-Fi security.
7. **Have full network access-** HackShield takes the required permission stating as “Have Full network access” because HackShield has a range of features in Network Shield which are Wi-Fi Security, Connected Devices, VPN and Speed Test which requires full network access.
8. **This app can appear on top of other apps-** HackShield takes the required permission stating as “This app can appear on top of other apps” because if there are real time threat to the device then HackShield will appear on the top of other apps to alert the user.
9. **Run at start-up-** HackShield takes the required permission stating that “Run at Start-up” because when the intruder tries to switch off the users device, HackShield with its Highlighted feature “Device Shield “ automatically works when restarted the device as when restarting the device all other application’s service get stopped.
10. **Access Do Not Disturb-** HackShield takes the required permission stating “Access Do Not Disturb” for sending the notification in silent mode.
11. **Read badge notifications-** HackShield takes the required permission stating “Read badge Notifications” because HackShield wants the user to know the total counts of notifications pending to read from the users end.
12. **View network connections-** HackShield takes the required permission stating “View Network Connections” because with HackShield Network Shield, it checks how many devices are connected to the respective network.
13. **Use fingerprint hardware-** HackShield takes the required permission for “using the fingerprint hardware” because with HackShield Privacy Shield it gives an extra layer of security to access the Privacy Shield Feature.
14. **Control vibration-** HackShield takes the required permission stating as “Control Vibration” because with HackShield feature rightly known as Proximity Sensors, when an intruder tries to turn the users device into silent mode HackShield can control the vibration and play the hooting alarm through which the user gets alert.
15. **Change network connectivity-** HackShield takes the required permission stating that “Change Network Connectivity” because with HackShield Network Shield’s feature rightly known as VPN the user can connect the device to the best performance server.
16. **Play install Referrer API-** HackShield takes the required permission stating that “Play install referrer API” because if the user is satisfied with the HackShield application then the User can give a feedback to the HackShield application by giving stars which will be displayed in the Play store.
17. **Change your audio settings-** HackShield takes the required permission stating that “Change your audio settings” because with HackShield’s Feature rightly known as Proximity sensors it creates a hooting alarm in case of phone theft and if the intruder tries to turn down the volume to silent the hooting the volume won't be turned down.

- **Does permission 3 indicate the user of the app is signing up to a cloud account...?**

1- What Data is stored?

Name, Email ID only stored.

2- Where and how it is stored?

IT is stored on our secured servers with encryption mechanism. It is used for identification of the application user.

3- Who has the access to it?

No employee or any 3rd party has access to this database. As it is only used for identification purpose programmatically.

- **Can you explain more about "Device Shield" and "Privacy Shield" features a bit more...?**

Privacy shield consist of password manager, Vault using which you can store password, photos, videos, all your file and document file in encrypted way. Whereas device shield is designed to take care of your physical device using which user can identify the intruder, trying to access your device in your absence.

- **Why the amount charge me if your given 30 days free trial?**

As users selected the subscription plan for 1 month that the reason they have charged for the 1-month charges. Here instead for 1 month if a user selects a 1-year subscription then they are getting a 1-month free trial along with a 1-year subscription.