#HeyFriend, do you think someone is spying on you?

Are you worried about someone having physical or remote access to your devices? If you would like to know about preventative methods and ways to identify if this is happening on your phone, this is the right place for you.

Red flags to look out for in your interactions with people around you:

- Are your posts being monitored and shared with people (family, colleagues, peers) without your consent?
- Someone revealing surprising knowledge of what you're up to — when you have not shared that information with them.
- Encouraging you to leave your devices unattended, especially when things between you are going south.
- Wanting to know where you are and who you are speaking to at all times.
- Insistence on having access to your devices.

Technical signs that something is not quite right:

- Your device has **applications you don't recognise.**
- Some applications have **excessive permissions** granted to them. Why does your calculator app need access to your microphone?
- You see **unusual security notifications**. Your system security notifications may often alert you to suspicious behaviour.
- There are **unknown devices** connected to your accounts. Check them regularly!
- All of a sudden, **your battery** starts overheating or draining quickly.

If you're doing dangerous or sensitive work, stay alert! Pay attention to:

- Data usage: Check unknown apps and excessive data consumption. For example, your alarm may show excessive data usage — something like this should definitely be looked into.
- Repeated authorisations for Wi-Fi access, to receive SMS, or access to your accounts.
- All your applications: Check them thoroughly. What can they do? What features do they have access to?
- Requests for sensitive permissions, such as administrator privileges on your device.

Tip: You can also check who has administrator privileges in settings under security and linked accounts. If you find an unfamiliar account linked to your device something is amiss!

- Security notifications are important — keep your eye out for them, because they may help you detect something unusual. This is also why invasive applications will try to block them.
- On Android, check the setting ‘Google Play Protect’. If this was disabled without your knowledge, it’s a red flag.
- Have an understanding of what is “normal” for your phone — battery levels, permissions for applications, administrative privileges on Android, etc.

Tip: Permissions to install other apps, camera, microphone, SMS, and calls are always the most sensitive points.

- If an application is requesting accessibility services. This is important because accessibility allows an app to perform actions that a casual user would not ordinarily have access to, such as tracking keystrokes. The bottom line being: Is it requesting a function it does not need?

Tip: If you see extensive authorisations granted but are unfamiliar with the app, treat it with caution and investigate it further.

For more information, scan this code: