EO SECURE PHONE

The EO Secure Phone serves for secure mobile communication and protection of personal data from third parties. Thanks to its key features, you will be protected from attack on both software and hardware.

EO Secure Phone uses the open-source Graphene OS operating system, which is designed with privacy and security in mind.

HARDWARE PERIPHERALS REMOVAL

For an additional fee, it is possible to remove hardware peripherals (microphone, front and rear camera, GPS ...) to prevent data collection from these peripherals in case of a successful attack on the device.

The main advantages of Graphene OS are:

- Each application runs in an isolated environment, so it does not have direct access to system resources or data from other applications
- Multiple user profiles can be used simultaneously
- Network access is restricted for certain applications
- Uses Storage Scopes, which divides the storage space into multiple parts, limiting data access by individual applications

FEATURES

- Google services work through a Sandbox, so your phone does not share personal data with third parties
- Trusted Execution Environment (TEE) secure core processor area, which ensures sensitive data is stored, processed and protected in an isolated and trusted environment
- An anonymized Wi-Fi connection (generating random MAC addresses for each connection
- Secure browse
- Rapid updates to protect against attacks that exploit newly discovered system vulnerabilities
- High battery life (2 to 3 days in normal operation, up to 10 days in restricted mode)
- Fully encrypted disk
- Isolated container

The design of the phone is identical to the Google Pixel 6a 5G. No one will know at first glance that it is a secure phone.

Package includes:

1. EO Secure Phone (Pixel 6a)
2. Mobile phone cover
3. Original USB-C cable
4. Key to open the SIM slot