

Encrypted Smartphone

Encrypts phone calls, video calls, messages,
voice messages, photos and documents

**This is how you
receive our service:**
swiss-protected-mobile.ch

**What do you get from us with prompt
delivery times?**

You receive a complete package with
a encrypted smartphone and the appropriate
data connection. No technical installation
is required.

With the “Bring Your Own Device” solution, you
receive all the services you need directly on
your own smartphone, including the necessary
data connection.

This is a service by:

Graphodata Sagl
Via Cantonale 15
6992 Vernate

www.swiss-protected-mobile.ch
info@swiss-protected-mobile.ch



swiss
protected mobile

We have a common problem!

The privacy of our phone calls and data traffic is under considerable pressure worldwide. There are several key players who intercept our communications:

State surveillance

This surveillance is legal, but subject to strict legal requirements. The collected data must be deleted after a specified period of time, and analysis is only permitted with judicial approval.

Hacker

Hackers illegally access our conversations and data in order to blackmail us or sell on the information they obtain. Industrial espionage is particularly popular.

International organizations and services

In addition, there are organizations and services around the world that have a great interest in our conversations and data. It often goes unnoticed that we are being tapped.

Well-known messenger services

Messenger services, which are used by almost everyone, pose a particular risk. Although they often claim that the communication is encrypted, the decryption codes are often known to authorities and other parties.

Conclusion

We are in an extremely precarious and potentially dangerous situation that requires an urgent new approach and stronger measures to protect our privacy.

We have the solution to the problem

Encryption as a solution

The solution to the increasing threat to communication security lies in the effective use of encryption. In addition, the entire communication cycle must be protected and its technical infrastructure housed in secure rooms in order to ensure comprehensive security.

Swiss Protected Mobile

As a trusted partner, Swiss Protected Mobile offers innovative solutions for selected customers. Our smartphones use their independent operating system and powerful end-to-end encryption to ensure maximum security.

Bunker for infrastructure

The entire technical infrastructure is located in a highly secure bunker in the Swiss Alps, which considerably strengthens the protection of sensitive data.

Conclusion

By combining state-of-the-art technology and Swiss security standards, Swiss Protected Mobile offers an optimal solution for secure and protected communication that works reliably worldwide.

Encrypted smartphone for “Top Secret”

Highest safety standard

Our encrypted smartphone has been specially developed for top-secret applications and meets the highest security requirements. The conventional Android operating system has been replaced by a proprietary, highly secure operating system that offers effective protection against external attacks and malware security.

No executable programs

All necessary services and applications are verified and checked by the proprietary operation system to eliminate potential vulnerabilities. The installation of additional programs, such as malware, is not possible, which ensures maximum device security.

Secure infrastructure

The smartphones are connected to a VPN at all times. The coordination servers are located in a high-security bunker in the Swiss Alps. This infrastructure ensures unparalleled physical and digital security while guaranteeing worldwide availability.

Encrypted communication

Communication takes place exclusively via our proprietary messenger app, which guarantees the highest security standards and effective end-to-end encryption thanks to AES-256 encryption. The app offers all the functionality of conventional messenger services, but with the decisive advantage of maximum security.

Conclusion

Our solution combines state-of-the-art technology, comprehensive security measures and Swiss precision to effectively protect top-secret communications.

BYOD solution as a supplement to the encrypted smartphone

The BYOD solution (Bring Your Own Device) complements the encrypted “Top Secret” smartphone and is classified in the “Confidential” category. It ensures secure transmission of messages, phone calls and video calls with the private smartphone.

Main differences

- » In contrast to the encrypted smartphone, the private smartphone remains unchanged with the BYOD solution so that the user can use all apps freely.
- » Responsibility for the security of the device lies with the user, including regular updates and compliance with security regulations. This is to ensure that no malware can be installed.

Areas of application

This solution is perfect for scenarios that require secure communication without having to purchase an encrypted smartphone – for example, when communicating and exchanging confidential documents between a lawyer and their client.

Conclusion

The BYOD solution offers flexible options for using your own smartphone while maintaining secure communication. It is a cost-effective alternative for certain use cases.