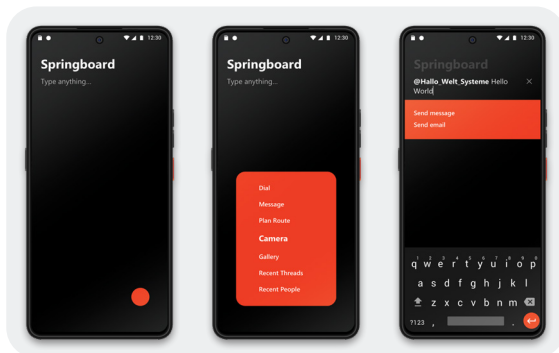


Das Volla Phone:

Ihre Freiheit durch Einfachheit und Sicherheit.

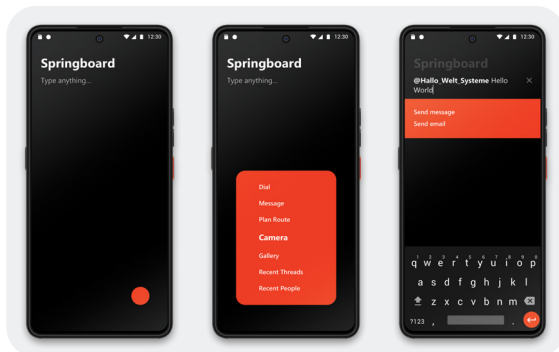
Das Smartphone aus Deutschland kombiniert ein einzigartiges Benutzererlebnis mit dem konsequenten Schutz der Privatsphäre. Entschieden Sie selbst, mit wem Sie welche Daten teilen und genießen Sie zu gleich den Komfort einer besonders einfachen Bedienung.



Android-kompatible Betriebssystem Volla OS.

Schnellmenü für Alltagsfunktionen mit einer einzigen Geste.

Intelligentes Textfeld als Sprungbrett für Ihre Kommunikation.



Intelligente Zusammenstellung wichtiger Kontakte, Mitteilungen und Nachrichten.

Jetzt informieren und online bestellen.

Schon in wenigen Tagen die neue Freiheit genießen.



hello.volla.online

Hallo Welt Systeme UG
hello@volla.online
Kölner Straße 102, 42897, Remscheid, DE

volla



**Mit dem Smartphone
sicher durch den Alltag**

Volla OS Sicherheit

Konsequenter Schutz der Privatsphäre



Volla Phone Plinius

Und für alle, die doppelte Sicherheit benötigen, bietet Volla auch extrem robuste Smartphones an, die sich perfekt für Sport- und Outdoor-Enthusiasten, Handwerker, medizinisches Personal, Rettungsdienste, Offshore Anwendungen und vieles mehr eignen.

12 Tipps für den Alltag.

Das Smartphone ist aus dem Alltag nicht mehr wegzudenken. Doch beim Umgang mit unseren mobilen Begleitern ist Sorgfalt geboten - schließlich befinden sich auf dem Smartphone viele vertrauliche Daten. Mit diesen zehn Tipps sind Sie sicher unterwegs.

- 01 Aktivieren Sie die PIN-Sperre:** Schützen Sie Ihr Smartphone vor unbefugtem Zugriff, indem Sie mit einer Zahlenkombination Ihren Bildschirm sperren. Die zusätzliche Verwendung eines Fingerabdrucks verhindert, dass in der Öffentlichkeit jemand Ihre PIN-Nummer sehen kann.
- 02 Halten Sie die Software stets aktuell:** Führen Sie regelmäßig Aktualisierungen des Betriebssystems und Ihrer Apps durch. Akzeptieren Sie angebotene Aktualisierungen.
- 03 Laden Sie Apps nur aus vertrauenswürdigen Quellen herunter, um Schadsoftware zu vermeiden:** Verwenden Sie die offiziellen App Stores von Apple und Google oder Alternativen wie F-Droid, Aurora sowie Webseiten der jeweiligen App-Hersteller.
- 04 Vermeiden Sie Apps, die ein Benutzerkonto erfordern.** Das gilt insbesondere dann, wenn es keinen offensichtlichen Grund oder Nutzen für ein Benutzerkonto gibt.
- 05 Prüfen Sie, ob und welche Tracker Apps verwenden,** die Ihre Nutzungsdaten und andere vertraulichen Informationen einsammeln und wägen Sie sorgfältig ab, ob Sie diese Apps verwenden wollen. Im Aurora und F-Droid App Store erhalten Sie jeweils Auskunft über verwendete Tracker.
- 06 Verwenden Sie möglichst keine umfassenden Cloud Dienste** wie die von Google oder Apple, die Zugriff auf alle Ihre Daten von Nachrichten bis Fotos haben.
- 07 Erteilen Sie Apps nur offensichtlich notwendigen Zugriffsrechte und prüfen Sie diese regelmäßig.** Achten Sie dabei auf besonders kritische Rechte wie Mikrophon, Kamera, Adressbuch und Standort.
- 08 Deaktivieren Sie Funkverbindungen und die Standortbestimmung,** wenn Sie diese nicht brauchen. Das gilt auch für Bluetooth, NFC oder die mobile Datenverbindung.
- 09 Vorsicht vor WLAN-Hotspots:** Die unverschlüsselte Kommunikation über öffentliche WLAN-Hotspots im Café, am Flughafen oder im Hotel. Hier sollten Sie unbedingt einen vertrauenswürdigen VPN Dienst verwenden. Deaktivieren Sie unterwegs zudem die WLAN-Funktion Ihres Smartphones, um Hacker Angriffe zu vermeiden.
- 10 Achten Sie auf eine verschlüsselte Kommunikation** für Text, Sprache und Videos. Viele Messenger und auch die Telefonie und Kurznachrichten sind nicht sicher oder sind sogar per Gesetz Teil der Vorratsdatenspeicherung. Verschlüsselte Kommunikation ermöglicht zum Beispiel die App Signal oder der E-Mail-Dienst StartMail.
- 11 Sichern Sie Daten vor Verlust.** Überspielen Sie beispielsweise Fotos regelmäßig auf Ihrem PC oder Mac oder einer Speicherkarte. Ihre Kontakte können Sie ebenfalls für eine Sicherheitskopie exportieren.
- 12 Verwenden Sie einen Anonymisierungsdienst für Internetverbindung:** Achten Sie bei der Wahl eines Virtuellen Privaten Netzwerkes (VPN), dass der Betreiber vertrauenswürdig ist. Vermieden Sie ausschließlich kostenfreie Dienste.

