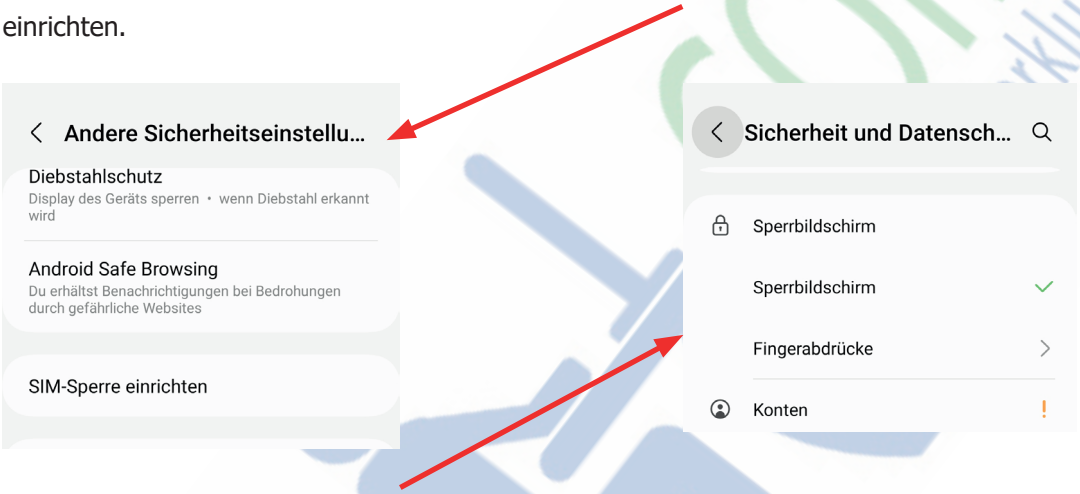
SMARTPHONE SICHER MACHEN
das sollte man beachten

Egal ob Hackerangriffe, Schadsoftware oder Phishing. Cyberkriminelle versuchen es auf vielen Wegen, an Ihre Daten zu kommen. Kontodaten, Adressen und unzählige Kontakte, Identitätsnachweise per Führerschein oder Ausweis – all das sollte gut geschützt sein.
(Je nach Android-Version kann die im Folgenden verwendete Menüfolge variieren.)

SIM- und Displaysperre einrichten

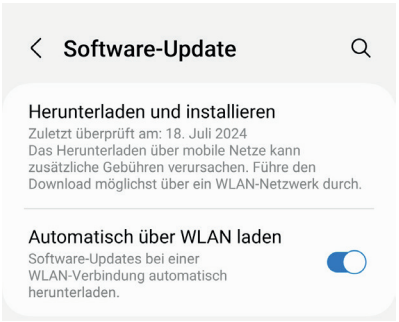
Ohne Sperre öffnet man Angreifern die Tür zu all Ihren Daten. Die SIM-Karte ist standardmäßig mit einer PIN geschützt. Wenn nicht, aktiviert oder ändert man diese unter *Einstellungen -> Sicherheit und Datenschutz -> Andere Sicherheitseinstellungen -> SIM-Sperre* einrichten.



Außerdem sollte man eine Display-Sperre einrichten. Dann kann nur auf das Handy zugreifen, wer Code, Passwort oder das passende Muster kennt. Die meisten aktuellen Smartphones haben auch einen Fingerabdruck-Sensor oder Gesichtserkennung, die man ebenfalls zur Absicherung verwenden können. Die Sperre stellt man in den Einstellungen unter *Sicherheit und Datenschutz -> Sperrbildschirm* ein.

Updates sofort installieren

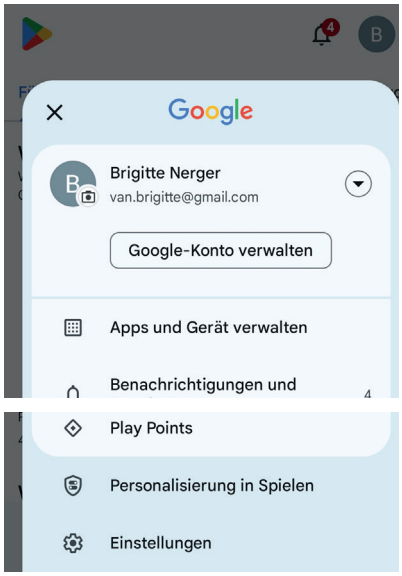
Betriebssystem als auch alle Programme müssen immer aktuell sein, und Updates müssen umgehend installiert werden. Die Entwickler liefern mit Aktualisierungen nicht nur neue Funktionen, sondern auch Sicherheitslücken. Unter *Software-Update* kann man einstellen, dass das Update automatisch heruntergeladen wird. Man bekommt eine Nachricht wenn es eine neue Android-Version gibt.

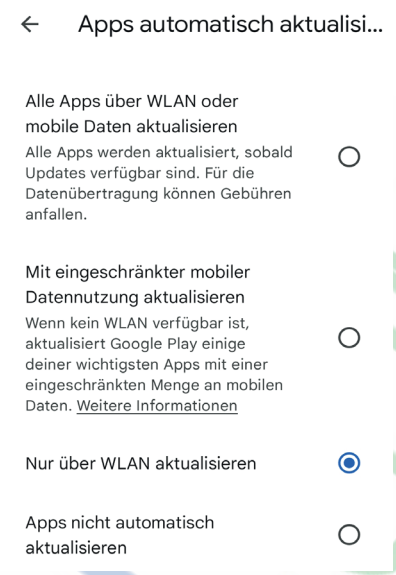


FLOCOM-Info SMARTPHONE SICHER MACHEN

Apps sollten auch regelmäßig auf den neuesten Stand gebracht werden – Einstellungen dazu erfolgen im Play Store.

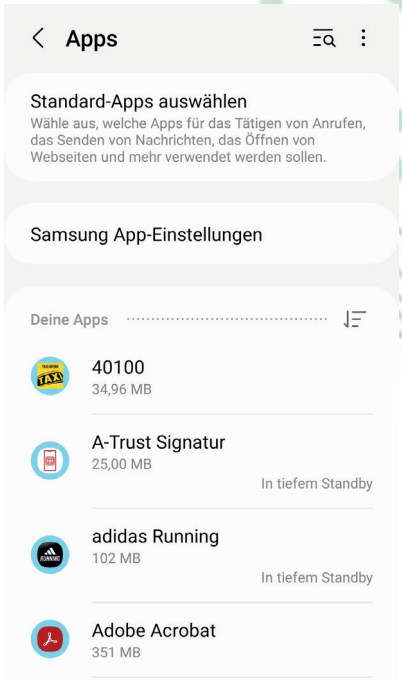
Play Store öffnen und rechts oben auf den Kreis klicken. Im folgenden Menü wählt man *Einstellungen* -> *Netzwerkeinstellungen* – hier kann man einstellen, ob und wie die Updates heruntergeladen werden sollen.

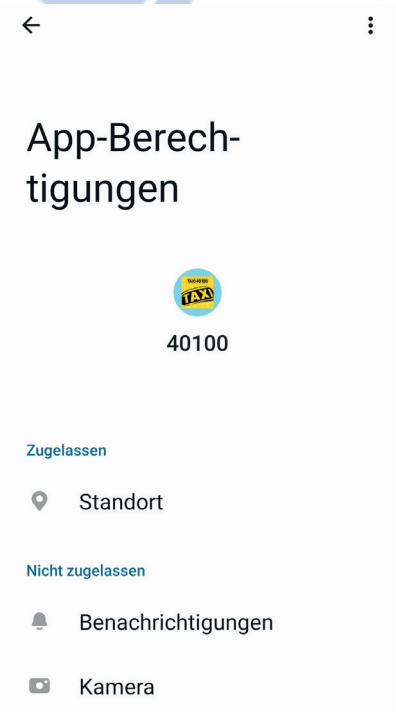




Auf Berechtigungen achten

Bei jeder App, die man installiert hat, sollte man überprüfen welche Berechtigungen man einräumen will. Eine Taschenlampen-Funktion benötigt zum Beispiel keinen Internet-Zugriff. Unter *Einstellungen* -> *Apps* findet man die Liste der installierten Apps. Durch öffnen einer App erhält man eine Menge Infos, unter anderem die Berechtigungen die diese App hat.



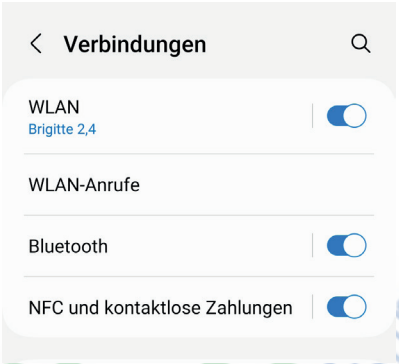


Achtung im offenen WLAN

Im offenen WLAN im Café oder am Flughafen surft man kostenlos. Aber Vorsicht: Mit relativ einfachen Mitteln können andere das Smartphone ausspionieren und mitlesen. Man sollte deshalb dort nie Online-Banking machen.

Verbindungen deaktivieren

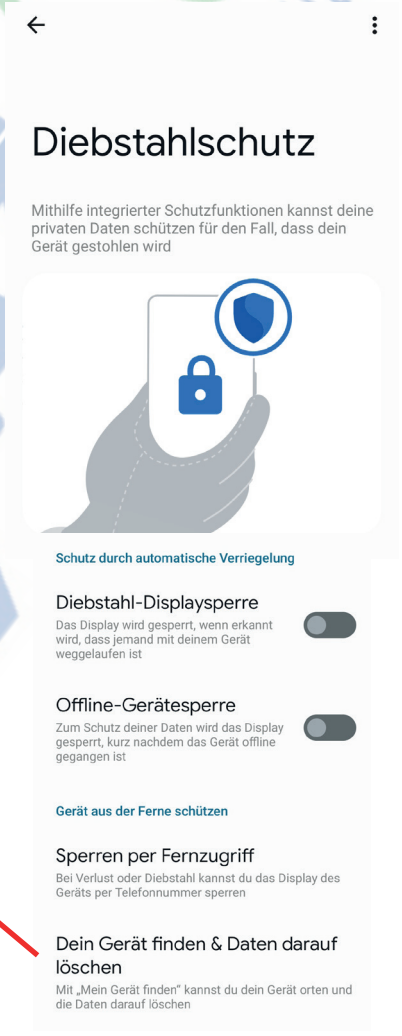
Man sollte alle Netzwerk-Funktionen deaktivieren, die man nicht ständig benützt. Dazu gehören auch Bluetooth und NFC. Diese Funktionen schaltet man in den *Einstellungen* -> *Verbindungen* ab. Schieben Sie jeweils den virtuellen Regler auf die Aus-Position.

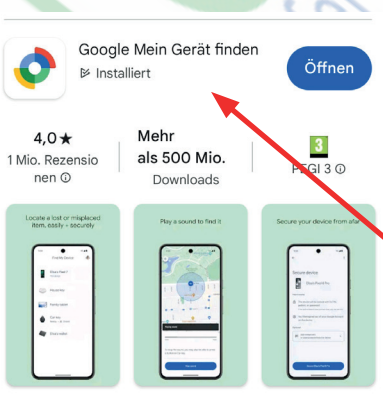


Diebstahlschutz aktivieren

Unter *Einstellungen* -> *Sicherheit und Datenschutz* -> *Andere Sicherheitseinstellungen* -> *Diebstahlschutz* gibt es mehrere Einstellungen für den Fall wenn das Smartphone verloren hat oder es gestohlen wurde.

Mit der App *Mein Gerät finden* kann man das Smartphone orten, falls es verloren geht – auch wenn es offline ist. Zudem lassen sich dann aus der Ferne alle Daten löschen.

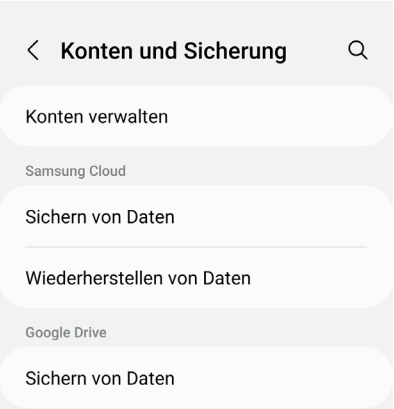




Verlorene Android-Geräte finden, klingeln lassen, sperren und Daten löschen

Regelmäßige Backups

Wenn das Smartphone den Geist aufgibt, sind alle Daten weg – außer, man sichert sie regelmäßig. Ein Backup der Fotos klappt am einfachsten mit Cloud-Diensten wie Google Drive oder OneDrive, die diese automatisch speichern. Die Einstellungen und Daten von Apps, WLAN-Passwörter oder den Anrufverlauf sichert Google. Aktiviert wird das über *Einstellungen* -> *Konten und Sicherung* und *Sichern von Daten*.



IMPRESSUM:
Eine Information vom Floridsdorfer Computerklub FLOCOM @ Brigitte Nerger
www.flocom.at | vorstand@flocom.at