EIN—TEAM.org

Ein Team gegen digitale Gewalt

Digitale Ortung und Überwachung verhindern – mit diesen 5 Tipps

1. Richte deine Geräte *selbst* ein

Wer anderen das eigene neue Smartphone oder den eigenen neuen Laptop zum Einrichten anvertraut, hat selbst nicht die volle Hoheit über das Gerät. In Beratungsstellen erzählen Hilfesuchende häufig davon, dass ihr Smartphone von derselben Person geschenkt oder konfiguriert wurde, die jetzt Apps oder Systemfunktionen zur Überwachung ausnutzt.

2. Verwende starke Sperr-Codes statt Fingerabdruck oder Gesichtserkennung

Biometrische Entsperr-Methoden wie das Scannen des Fingerabdrucks oder des Gesichts lassen sich innerhalb von Sekunden gewaltsam erzwingen. Sicherer sind Passwörter oder Zahlenkombinationen, die schwer zu erraten sind.

3. Halte deine Passwörter immer geheim. *Immer!*

Wer die Passwörter zu seinen Diensten und Geräten geheim hält, ist vor Übergriffen sicher. Eine starke Bildschirmsperre ist der wichtigste Schutzmechanismus für ein Smartphone – selbst kommerzielle Spionage-Programme lassen sich nicht daran vorbei installieren, da sie physischen Zugriff auf das entsperrte Gerät erfordern.

4. Stelle deine Social-Media-Profile auf privat

Auch wenn es weniger Likes bringt: Persönliche Inhalte auf Instagram und Co. sollten nur Freund*innen lesen können. Wer unangenehme Personen bereits blockiert hat, geht damit sicher, dass sie nicht über neu angelegte Accounts mitlesen.

5. Entferne Metadaten aus deinen Fotos

Wer nicht möchte, dass die eigenen Fotos zum Beispiel den Standort verraten, kann solche Metadaten vor dem Versenden oder Hochladen entfernen. Dabei hilft die Android-App „Scrambled Exif“ und die iOS-App „Exif delete“.

KONTAKT

Inga Pöting

Projektleitung „ein Team gegen digitale Gewalt“

E-Mail: i.poeting@ituj.de
Tel.: +49152 125 062 27