Sicher mit Smartphone

Tipps für den Schutz von Handy und Privatsphäre

Dies sind Informationen, die den Schutz von persönlichen Daten bei der Nutzung eines Smartphones betreffen. Auf die eigene Privatsphäre und Sicherheit zu achten, ist keine Frage von akuten Gewaltsituationen. Aber auch gerade bei Gewalt in Beziehungen oder während und nach Trennungen ist es wichtig, persönliche Daten und somit sich selbst zu schützen.

1. Handy mit Passwort schützen

Die meisten Handys können mit einer PIN oder einer Tastenkombination vor unbefugten Zugriffen geschützt werden. Die Einrichtung erfolgt meist in den Einstellungen unter dem Stichwort Sperrbildschirm. Solch ein Passwort erschwert es Anderen das Telefon zu benutzen, Nachrichtenverläufe zu lesen oder schädliche Software zu installieren. Auch wenn es gestohlen wird, ist die Hürde an persönliche Informationen zu kommen höher.

2. Sichere Passwörter und PINs benutzen

Verwendete Passwörter und Tastenkombinationen sollten nicht leicht zu erraten sein (zum Beispiel der eigene Geburtstag). Für den Schutz des Smartphones können meist auch PINs verwendet werden, die länger als 4 Ziffern sind. In konkreten Bedrohungssituationen ist es sinnvoll, die bestehenden Passwörter zu ändern. Es sollten immer verschiedene Passwörter für verschiedene Accounts benutzt werden.

3. Privatsphäre und Sicherheitseinstellungen prüfen

Die Sicherheitseinstellungen des Smartphones erlauben eine grundlegende Kontrolle darüber, welche Anwendungen, die auf dem Handy installiert sind, Zugriff auf bestimmte Daten und Funktionen haben. Die Einstellungen können im Smartphone-Menü meist unter „Einstellungen“ oder „Settings“ vorgenommen werden. Mit den richtigen Sicherheitseinstellungen können die eigenen Daten, wie Bilder, Kontakte, Standorte, Gesprächsverläufe etc. geschützt werden.

4. Bluetooth-Funktion deaktivieren

Bluetooth wird benutzt, um Verbindungen zu anderen Geräten herzustellen, zum Beispiel zur Freisprechanlage im Auto. Über Bluetooth können sich aber auch andere Personen relativ einfach Zugang zu Informationen verschaffen oder Telefongespräche abfangen. Wenn die Bluetooth-Funktion nicht benutzt wird, sollte sie immer deaktiviert sein.

5. „Standort mitteilen“ vermeiden

Viele Smartphones können GPS (Global Positioning System; deutsch: Globales Positionsbestimmungssystem) nutzen, um den eigenen Standort zu bestimmten. Durch diese technische Möglichkeit können Apps und andere Anwendungen Informationen über Aufenthaltsorte und Bewegungen sammeln und Anderen mitteilen. Es wird empfohlen die Funktion „Standort mitteilen“ grundsätzlich auszuschalten. Unter „Einstellungen“ oder „Settings“ kann eingestellt werden, welche Anwendungen und Apps Zugriff auf die GPS-Funktion haben sollen. Manche Smartphones und Apps bieten keine spezifische Einstellung an und es gibt Apps, die nur funktionieren, wenn die Funktion „Standort mitteilen“ aktiviert ist. Beim Herunterladen neuer Apps sollte dementsprechend darauf geachtet werden, welche Funktionen voreingestellt sind.

6. Automatische Log-Ins prüfen

Um schnellen Zugriff auf Online-Konten zu haben, wie zum Beispiel den E-Mail Posteingang, sind bestimmte Anwendungen oft so voreingestellt, dass das Smartphone immer mit dem jeweiligen Account (Konto) verbunden ist. Dadurch wird das mühsame Einloggen vor jedem Nutzen der Anwendung vermieden. Dies bedeutet aber auch, dass das Telefon immer die Verbindung zu sensiblen Daten herstellen kann und diese auch von anderen Personen eingesehen werden können, wenn sie das Telefon (unbefugt) benutzen. Sich aus bestimmten Accounts auszuloggen, kann ein Sicherheitsfaktor sein. Je nach Smartphone und Anwendung kann es sein, dass das Ausloggen aus manchen Accounts, zum Beispiel aus E-Mail-Programmen, nicht möglich ist. Die Entscheidung, ob die Anwendung dann deinstalliert werden sollte, kann von der individuellen Einschätzung und Gefährdung abhängig sein.

7. Überprüfen der eigenen Apps

Es ist wichtig den Überblick darüber zu haben, welche Apps auf dem Handy installiert sind. Apps, die unbekannt sind und nicht selbst heruntergeladen wurden, sollten gelöscht werden. Erscheint die App unbekannt, kann es sein, dass sie einfach schon vor einer Weile heruntergeladen wurde und nicht mehr benutzt wird. Es gibt aber auch Apps, die dazu da sind Smartphone-Aktivitäten wie Gespräche und Suchanfragen zu überwachen und Informationen weiterzuleiten an die Person, die die App auf dem Handy installiert hat. Es gibt viele solcher Spionage-Apps, die nicht auf dem Smartphone angezeigt werden und trotzdem Informationen und Daten weiterleiten. Sie können häufig nur von Fachleuten entdeckt und gelöscht werden. Manchmal ist selbst das Löschen nicht möglich. Bekannte Apps sind zum Beispiel: FlexiSPY, mSpy und Spybubble.

8. Online-Accounts in Verbindung zum Smartphone sichern

Zusätzlich zum Smartphone und dessen Einstellungen müssen auch die Online-Accounts, die mit dem Smartphone verknüpft sind, ausreichend gesichert sein. Dazu kann gehören: der Online-Account beim Mobilfunkanbieter, Google Play/Apple AppStore, iCloud, E-Mail-Zugang und Accounts in sozialen Netzwerken. Auch hier sollten die Sicherheitseinstellungen und die Vergabe von Passwörtern überprüft und, wenn möglich, weitere Maßnahmen zum Schutz der Daten vorgenommen werden. Bei verschiedenen Konten oder dem Mobilfunkanbieter kann zum Beispiel eine sogenannte „Zwei-Faktor-Authentifizierung“ eingerichtet werden. Hier erfolgt die Anmeldung bzw. das Einloggen dann über zwei unabhängige Wege, zum Beispiel über ein Passwort und eine zugesandte SMS-PIN.

Generell sollten Online-Aktivitäten auf verschiedene Geräte verteilt werden. Nicht alle vorhandenen Accounts sollten auch mit dem Handy benutzt werden.

9. Keine sensiblen Daten auf dem Smartphone speichern

Je weniger sensible Daten, wie Passwörter, persönliche Informationen, Zugangsdaten oder Fotos auf dem Smartphone gespeichert werden, umso geringer ist die Chance, dass diese Daten von einer anderen Person verwendet werden.

10. Sich Unterstützung holen

Bei Problemen mit den Handyeinstellungen und bei Fragen zu Sicherheit und Privatsphäre können Fachmenschen weiterhelfen. Es ist am sichersten, sich dabei von professionellen Personen unterstützen zu lassen. Freund_innen und Bekannte aus dem privaten Umfeld können das Wissen über die Sicherheitseinstellungen des Handys auch noch nach längerer Zeit missbrauchen oder weitergeben. In manchen Fällen können Beraterinnen aus den Fachberatungsstellen Expert_innen empfehlen. Medienprojekte oder Organisationen, die sich mit Datenschutz befassen, können auch Informationen zu Sicherheitseinstellungen geben.

bff: aktiv gegen digitale Gewalt

bff: Bundesverband Frauenberatungsstellen und Frauennotrufe
Frauen gegen Gewalt e.V.

info@bv-bff.de
www.frauen-gegen-gewalt.de

@bff_gegenGewalt

Unterstützung bei Gewalt finden Sie in einer Beratungsstelle in Ihrer Nähe:

Das bundesweite Hilfetelefon Gewalt gegen Frauen bietet telefonische Erstberatung für Betroffene. Kostenlos, vertraulich und rund um die Uhr.

HILFE TELEFON
GEWALT GEGEN FRAUEN
08000 116 016

Gefördert vom

Bundesministerium für Familie, Senioren, Frauen und Jugend