Smartphone, halt's Maul!

✔ Eine Checkliste für deine mobile Sicherheit

Du willst Sicherheit für dein Smartphone ohne technisches Gelaber und abgehobene nerdige Vorträge?

Du willst sichergehen, dass dein Telefon dich nicht ausspioniert oder verrärt wo du bist?

Dieses Buch sagt dir schnell und einfach was du tun solltest, wenn du dich in außergewöhnlichen Situationen befindest oder dein Smartphone einfach nur sicherer machen willst.

Das Geheimnis: Ich verrate dir zuerst was du tun solltest und spare mir nerdige Details für danach. Wenn du willst kannst du alle Aufgaben hinterfragen oder die technischen Details verstehen. Aber du musst es nicht.

Bist du vielleicht von Stalking betroffen oder auf der Flucht? Dann solltest du dein Smartphone vorbereiten. Einfache Checklisten leiten dich durch deine Bedrohungslage.

Neugierig? Dann blätter jetzt weiter.

Aufgaben nach Themen und Bedrohungen

Nicht alle Tipps und Empfehlungen in diesem Buch werden für dich relevant sein. Welche Maßnahmen wirklich wichtig sind entscheidet deine aktuelle Lebenssituation. So müssen Menschen, die zum Beispiel von Stalking betroffen sind andere Maßnahmen ergreifen als Menschen die aus einem anderen Land fliehen. Die nachfolgende Liste ermöglicht dir einen schnellen Einstig in besondere Bedrohungsszenarien und Themen. Trifft ein Szenario auf dich zu oder interessiert dich ein Thema ganz besonders? Dann ließ direkt dort weiter!

Alle Aufgaben

Hier findest du eine komplette Liste aller Aufgaben.

Wichtige Basics

Diese Aufgaben sind ein guter Anfang, wenn du etwas für deine mobile Sicherheit tun möchtest. Viele andere Aufgaben bauen auf ihnen auf. Diese Sicherheitsmaßnahmen für Mobiltelefone sind somit eine solide Grundlage, um deine Privatsphäre zu wahren und persönliche Daten zu schützen.

Checkliste zum Abhaken

Gefahren durch direkte Zugriffe

Gefahren durch direkte Zugriffe entstehen immer dann, wenn Menschen dein Gerät selbst in den Händen halten können. Also zum Beispiel bei Hausdurchsuchungen, Beschlagnahmungen und Sicherstellungen durch die Polizei. Ungewollte physische Zugriffe von Menschen auf dein Smartphone sind problematisch, da sie sensible persönliche Daten wie Nachrichten, Fotos, Passwörter und Bankdaten enthalten. Unbefugter Zugriff kann zu Identitätsdiebstahl, Datenmissbrauch oder finanziellen Schäden führen. Darüber hinaus speichern Smartphones oft Zugangsdaten zu sozialen Netzwerken, E-Mails und anderen wichtigen Konten, wodurch Fremde nicht nur private Informationen einsehen, sondern auch Manipulationen oder Angriffe durchführen könnten.

Checkliste zum Abhaken

Gefahren im Mobilfunknetz

Im Mobilfunknetz lauern viele Gefahren, denen du dich normalerweise nur schwer entziehen kannst. Diese Aufgaben sollen dich ermutigen es trotzdem zu versuchen. Hier ist nicht nur dein Mobilgerät direkt betroffen sondern auch deine Daten und deine Kommunikation, die zwischen einer vielzahl von Stellen ausgetauscht werden. Es ist wichtig, sich über die Gefahren von z.B. Ortung oder Datenweitergabe im Mobilfunknetz im Klaren zu sein. Diese Daten können von Dritten, wie Unternehmen oder Behörden, zur Überwachung, Profilbildung oder Verfolgung verwendet werden. Zudem können Datenlecks oder missbräuchliche Zugriffe durch Cyberkriminelle gravierende Folgen haben.

Checkliste zum Abhaken

Gefahren im Internet

Ein umsichtiges Verhalten im digitalen Raum ist entscheidend, um die eigene Privatsphäre und Sicherheit zu schützen. Durch Achtsamkeit im Umgang mit persönlichen Daten und gezielten Schutzmaßnahmen, wie der Nutzung von Passkeys, Zwei-Faktor-Authentifizierung und verschlüsselten Cloud-Speichern, minimierst du das Risiko von Datenmissbrauch und Cyberangriffen. Das proaktive Löschen nicht genutzter Accounts und das regelmäßige Überprüfen auf Datenlecks sind ebenso wichtig, um die Kontrolle über sensible Informationen zu behalten. Datenschutzfreundliche Technologien wie TOR und alternative Frontends sowie die Verschlüsselung von E-Mails bieten zusätzliche Schutzebenen.

Checkliste zum Abhaken

Journalismus, Regimekritik und Exil

In einigen Ländern ist es für Journalist*innen und Regimekritiker*innen besonders wichtig, ihre Smartphone-Sicherheit zu bedenken, da sie oft sensible Informationen verwalten, die sie oder ihre Quellen gefährden könnten. Autoritäre Regime nutzen gezielte Überwachungsmaßnahmen, um Journalist*innen auszuspionieren, ihre Kommunikation abzuhören oder ihre Kontakte nachzuverfolgen. Smartphones sind dabei ein leichtes Ziel, da sie ständig mit dem Internet und dem Mobilfunknetz verbunden sind und oft Standortdaten oder unverschlüsselte Informationen preisgeben. Ein mangelnder Schutz kann dazu führen, dass vertrauliche Recherchen kompromittiert werden oder Journalist*innen selbst Verhaftungen, Einschüchterungen oder sogar körperlicher Gefahr ausgesetzt sind. Daher ist es essenziell, Verschlüsselung, Anonymisierungstools und sichere Kommunikationsmethoden zu nutzen.

Checkliste zum Abhaken

Politischer Aktivismus

Es ist wichtig, dass Personen, die politischen Aktivismus betreiben, sich Gedanken um ihre Smartphonesicherheit machen. Smartphones speichern und übertragen sensible Daten, darunter Nachrichten, Kontakte und Standorte, die von Behörden oder unerwünschten Akteuren überwacht oder abgegriffen werden können. Ein bewusster Umgang mit Sicherheitsmaßnahmen wie Verschlüsselung, sichere Kommunikationsapps und regelmäßige Software-Updates schützt Aktivist*innen vor Überwachung, Verfolgung und potenzieller Repression. Zudem hilft es, die Vertraulichkeit und Integrität ihrer Netzwerke und Aktionen zu wahren.

Checkliste zum Abhaken

Migration, Flucht und Asyl

Für Asylsuchende und geflüchtete Menschen ist Smartphone-Sicherheit von großer Bedeutung, da ihre Geräte oft die einzige Möglichkeit sind, mit Angehörigen, Anwält*innen oder Unterstützungsnetzwerken in Verbindung zu bleiben. Gleichzeitig enthalten Smartphones sensible Informationen wie Aufenthaltsorte, Fluchtrouten, Identitätsdokumente oder persönliche Nachrichten, die bei unzureichendem Schutz in falsche Hände geraten könnten. Regierungen oder kriminelle Organisationen könnten diese Daten missbrauchen, um Rückverfolgung, Überwachung oder Druck auszuüben. Ein sicheres Smartphone hilft, die eigene Privatsphäre zu schützen, die Kommunikation vertraulich zu halten und sich vor möglichen Gefahren wie Abschiebung zu schützen.

Checkliste zum Abhaken

Hausdurchsuchungen und Beschlagnahmungen

Für Menschen, die ein erhöhtes Risiko für Hausdurchsuchungen oder Beschlagnahmungen haben, ist Smartphone-Sicherheit besonders wichtig, da ihre Geräte eine Fülle sensibler Informationen speichern. Diese Informationen, wie Kontakte, Nachrichten, Fotos und Standortdaten, könnten bei einer Beschlagnahmung eingesehen oder verwendet werden, um Netzwerke offenzulegen oder strafrechtliche Ermittlungen zu unterstützen. Durch Verschlüsselung, sichere Passwörter und das regelmäßige Löschen kritischer Daten kann der Zugriff auf private Informationen erschwert werden. Zudem helfen die Maßnahmen dabei, im Falle einer Beschlagnahmung die Privatsphäre und Sicherheit ihrer persönlichen oder beruflichen Netzwerke zu schützen.

Checkliste zum Abhaken

Stalking und Frauenhäuser

Menschen, die in Frauenhäuser fliehen müssen oder die von Stalking betroffen sind erleben häufig sogenannte Advanced Persistend Threads (APTs). Das bedeutet, dass sie über einen langen Zeitraum immer wieder auf vielfältige Weise und mit viel Energie Angriffen ausgesetzt sind. Oft kommen die Täter*innen aus dem nahen oder ehemaligen Umfeld.

Checkliste zum Abhaken

Verhaltens-basierte Risiken

Verhaltensbasierte Risiken entstehen durch unüberlegtes oder unreflektiertes Verhalten von Personen. Dazu gehören unvorsichtige Online-Aktivitäten wie das Verwenden schwacher Passwörter, das Klicken auf unsichere Links, das Teilen sensibler Informationen auf unsicheren Plattformen oder das Nicht-Aktualisieren von Software. Diese Verhaltensweisen erhöhen das Risiko für Cyberangriffe, Datenmissbrauch oder Identitätsdiebstahl, da sie es Angreifern leichter machen, Schwachstellen auszunutzen. Verhaltensbasierte Risiken lassen sich durch bewusstes und sicherheitsorientiertes Handeln minimieren.

Checkliste zum Abhaken

Betrug und Abzocke

Es ist wichtig, sich vor Betrug und Abzocke zu schützen, da Betrüger zunehmend raffinierte Methoden verwenden, um persönliche Daten zu stehlen oder finanziellen Schaden zu verursachen. Schutzmaßnahmen wie das Verwenden starker Passwörter, das Vermeiden verdächtiger Links und das regelmäßige Aktualisieren von Apps können helfen, Angriffe wie Phishing, Malware oder betrügerische Apps zu verhindern. Durch proaktive Sicherheitsvorkehrungen schützt du nicht nur deine persönlichen Informationen, sondern minimierst auch das Risiko finanzieller Verluste und Identitätsdiebstahls.

Checkliste zum Abhaken

Apps und Betriebssystem

Es ist wichtig, sich um die Aktualität und die Einstellungen von Apps und Betriebssystemen auf dem Mobiltelefon zu kümmern, da regelmäßige Updates Sicherheitslücken schließen und Schutz vor neuen Bedrohungen bieten. Veraltete Software kann anfällig für Sicherheitsrisiken wie Malware oder Exploits sein, die von Angreifern ausgenutzt werden können. Zudem sorgen korrekte Einstellungen dafür, dass Apps nur die notwendigen Berechtigungen erhalten und persönliche Daten nicht unnötig exponiert werden. Durch eine regelmäßige Überprüfung und Aktualisierung der Software sowie durch sorgfältige Verwaltung der App-Berechtigungen bleibt das Gerät sicher und die Privatsphäre geschützt.

Checkliste zum Abhaken

Eher einfach

Diese Sicherheitsmaßnahmen werden als besonders einfach eingestuft und bieten auch technisch nicht so versierten Menschen einen schnellen Einstieg in die Materie.

Checkliste zum Abhaken

Eher komplizierter

Diese Aufgaben sind etwas komplizierter oder setzen ein gewissen Grundwissen voraus. Du wirst dich eventuell etwas genauer mit technischen Details beschäftigen müssen, für die Aufgaben länger brauchen oder Hilfe von Expert*innen in Anspruch nehmen müssen.

Checkliste zum Abhaken

Ist eher teurer

Diese Aufgaben kosten in der Regel etwas mehr Geld, da sie teurere oder separate Geräte voraussetzen oder spezielles Werzeug oder Tools empfehlen.

Checkliste zum Abhaken

1. Allgemeine Tipps

Du interessierst dich für deine Sicherheit

Sehr gut! Offenbar ist dir deine Sicherheit wichtig. Sonst würdest du das hier nicht lesen. Deine ersten Punkte sind dir sicher.

Du teilst diese Liste mit anderen

Wenn wir es schaffen die Sicherheit aller Menschen zu erhöhen werden sich staatliche Überwachungsmaßnahmen weniger lohnen. Das kommt auch deiner Sicherheit zugute. Teile diese Liste daher in deinen Kanälen oder drucke den Flyer aus.

Du prüfst diese Liste von Zeit zu Zeit

Genauso, wie sich die Technologie und diese Liste ständig wandelt wird sich dein Leben, deine Gewohnheiten und deine Geräte in Zukunft ändern. Nimm dir daher einmal im Jahr Zeit und prüfe diese Liste.

Du hast schon mal an einer Cryptoparty teilgenommen

Cryptoparties sind Events auf denen du lernst deine Geräte und deine Kommunikation zu schützen.

Wenn du dich für Cryptoparties interessierst und Gleichgesinnte treffen möchtest kannst du dich zum Beispiel auf der Seite cryptoparty.in über

bevorstehende Events informieren. Oder du befolgst den Guide unten und veranstaltest gleich selbst eine.

Du kennst deine wichtigsten Kontakte und Logins auswendig

Du kennst die wichtigsten Nummern und Namen deiner Freund*innen, deiner Familie und deinen Bekannten auswendig. Du kannst dich außerdem in deine wichtigsten Accounts wie z.B. E-Mail auswendig einloggen. Solltest du dein Telefon oder sämtliche Geräte verlieren, hast du so eine Möglichkeit deine Kontakte wiederherzustellen.

Entferne vor sensiblen Besprechungen den Akku aus deinem Telefon

Entferne den Akku aus deinem Gerät oder lagere es etwas entfernt, um vertrauliche Besprechungen zu schützen.

Bedenke, dass andere Personen nicht wissen können wie gut du dich selbst mit deinem Telefon auskennst. Es ist daher immer ein Zeichen des gegenseitigen Vertrauens Telefone aus sensiblen Gesprächen heraus zu halten. Grundsätzlich sollte gelten: Vertraue Personen eher als ihren Geräten.

2. Gefahren durch direkte Zugriffe

Du verwendest kein Dumbphone

Nicht smarte Tasten-Geräte werden oft leichtfertig als "sicher" eingestuft. Diese lassen sich aber oft nicht verschlüsseln und bieten keine sichere Kommunikation.

Bei Beschlagnahmungen oder Diebstahl können Kontakte, SMS und Anruflisten ausgelesen werden. Darüber hinaus sind Dumbphones ohne weitere Schutzmaßnahmen genauso anfällig für Angriffe im Mobilfunknetz. Dumbphones lassen sich nicht verschlüsseln, du kannst keine Apps wie Passwortmanager darauf installieren, du kannst deine Bilder nicht von Metadaten bereinigen und kannst keine sicheren Messenger nutzen. Auf der einen Seite haben diese Telefone also Nachteile. Auf der anderen Seite muss aber auch festgehalten werden, dass nicht smarte Geräte einige Gefahren komplett ausschließen. Zum Beispiel ist hier die Gefahr durch Infektionen mit Malware sehr viel geringer. Verschlüsselung und sichere Kommunikation erscheint aber angesichts inflationärer Beschlagnahmungen und Überwachung so wichtig, dass ein smartes Gerät unbedingt zu bevorzugen ist.

Du hast deine Simkartennummer entfernt

Auf der Rückseite deiner Simkarte befindet sich eine unscheinbare Nummer. Zerkratze sie, damit du im Falle einer Beschlagnahmung nicht über sie und deinen Provider identifiziert werden kannst.

Sei dabei bitte vorsichtig und achte darauf den Chip nicht zu zerstören. Kratze also nicht zu tief!

Du hast eine Displaysperre eingerichtet

Der Display deines Gerätes schaltet sich nach einer Weile automatisch ab. Um diesen wieder zu entsperren nutzt du komplexe Muster oder alphanumerische Passworte.

Deine Smartphones sind verschlüsselt

Verschlüssel deine Smartphones mit einem starken alphanumerischen Passwort das mindestens 20 Zeichen lang ist. Dies verhindert das Auslesen von Daten sehr effektiv.

Eine starke Verschlüsselung ist wichtig. Eine Bildschirmsperre ist nicht ausreichend. Software wie Cellebrite kann über die USB-Schnittstelle die meisten Bildschirmsperren einfach umgehen. Alle deine Daten, Kontakte, Anruflisten, Standortdaten, Login-Daten und vieles mehr können dann durch automatisierte Software wie Cellebrite Pathfinder via USB gesammelt und aufbereitet dargestellt werden. Dein Verschlüsselungspasswort sollte besonders stark sein. Nutze ein sehr komplexes Muster oder ein alphanumerisches Passwort zur Verschlüsselung.

Du kannst deine Geräte schnell abschalten

Eine Verschlüsselung ist nur effektiv, wenn das Telefon ausgeschaltet ist. Übe daher wie du dein Telefon in Stresssituationen schnell abschalten kannst.

Auch wenn dein Telefon verschlüsselt ist kann Software wie Cellebrite via USB darauf zugreifen. Solange dein Telefon eingeschaltet ist, ist die Verschlüsselung wirkungslos. Erst wenn es abgeschaltet ist, ist Verschlüsselung wirklich effektiv. Schalte dein Telefon unbedingt ab, bevor du es in fremde Hände gibst! Wenn du auf Nummer sicher gehen willst kannst du auch einen Killswitch an deinem Telefon anbringen. So lässt sich der Akku in Gefahrensituationen schnell entfernen. Damit verschwindet dann der Schlüssel vom Speicher deines Geräts.

Du verwendest eine Blickschutzfolie

Du kannst eine spezielle Folie auf deinen Display kleben, die verhindert, dass umstehende Personen oder Kameras mitlesen können. Diese Folien gibt es für viele Modelle.

Deine Simkarte ist mit einer Pin geschützt

Du solltest den Pin-Schutz deiner Simkarte niemals deaktivieren. Bei deaktiviertem Pin können Behörden oder andere Personen die Karte selbst nutzen, um sich beispielsweise Zugriff auf Messenger zu verschaffen.

Hinweis für anonyme Simkarten: Wenn du anonyme Simkarten verwendest kannst du die Pin-Sperre oft nicht aktivieren, da du die zur Karte gehörige Pin / PUK oft nicht kennst. Du erhältst diese Karten oft mit deaktiviertem Pin. Du solltest in diesem Fall darauf achten, dass alle deine Messenger mit einem zweiten Faktor (z.B. Pin) abgesichert sind und dass du die Karte nicht selbst für eine Zwei-Faktor-Authentifizierung nutzt.

Du verzichtest auf Speicherkarten

Nicht auf allen Geräten lassen sich Speicherkarten zuverlässig verschlüsseln. Zudem lassen sich Daten wiederherstellen, die bei einer früheren Nutzung mit anderen Geräten darauf gespeichert wurden. Nutze Speicherkarten daher nur, wenn du weißt was darauf gespeichert wird und wenn du diese vorher überschrieben hast.

Einige ältere Android-Geräte erzeugen auch eine Signatur über verwendete Apps auf deiner Speicherkarte indem sie dort für verwendete Apps eigene Ordner anlegen. Dadurch können Rückschlüsse auf deine verwendeten Apps gezogen werden. Achtung! Das Überschreiben von Flash-Speichern ist oft nicht zu 100% möglich. Es können trotzdem Daten zurück bleiben.

Verzichte auf biometrische Freischaltung

Du solltest nie deinen Fingerabdruck oder dein Gesicht nutzen, um dein Telefon freizuschalten. Behörden mit Zugriff auf Fingerabdrücke oder Bildmaterial können das Gerät sonst entsperren. Nutze daher komplexe Muster oder alphanumerische Passworte.

Fingerabdrücke und Gesichtserkennung sind keine sicheren Methoden, um das eigene Gerät zu entsperren. Sie sind wie Passwörter, die du niemals ändern kannst. Durch Datenlecks oder Malware könnten diese sensiblen Informationen abhanden kommen und dir so zum Nachteil werden. Zudem darf auch die Polizei deine Fingerabdrücke nutzen, um dein Gerät zu entsperren. In Deutschland und den USA gab es dazu bereits Gerichtsurteile. Wenn du ein iPhone hast kannst du durch das betätigen einer speziellen Tastenkombination Face ID und Fingerabdruck temporär sperren. Für Android ist auf einigen Geräten der Lockdown-Mode verfügbar mit dem du diese Funktionen im Notfall schnell abschalten kannst.

Du hast die Entwickler*innen-Features deaktiviert

Deaktiviere unbedingt USB-Debugging, wenn du dich damit auskennst. Normalerweise ist diese Funktion auf allen Geräten standardmäßig deaktiviert und muss von dir bewusst aktiviert werden.

Du verwendest nur dein eigenes Ladekabel

Verwende nur Netzteile und Kabel zum laden, denen du vertraust. Markiere Kabel und Netzteil, um ein Austauschen zu verhindern.

Wenn möglich nutze ein USB-Kabel ohne Datenfunktion zum Laden. Manipulierte Kabel oder USB-Dosen in Hotels, Bussen oder Bahnen könnten Daten auslesen oder unerwünschte Software installieren. Wenn du dir nicht sicher bist kannst du dein Telefon für den Ladevorgang einfach abschalten. So kann nichts installiert oder ausgelesen werden und es wird trotzdem geladen.

Dein Betriebssystem verfügt über verified Boot

Verified Boot verhindert Manipulationen an deinem Betriebssystem. Du solltest dich vergewissern, dass dein Gerät damit abgesichert ist. Wenn du selbst ein eigenes System installiert hast, solltest du verified Boot aktivieren.

Ob dein Gerät verified Boot unterstützt oder nicht erfährst du bei der herstellenden Firma.

Du hast dein Gerät versiegelt

Eine Versiegelung kann dir helfen nach einer Rückgabe deines Gerätes festzustellen, ob Hardware manipuliert wurde. Gib z.B einen Tropfen speziellen Siegellack oder Nagellack auf die Nahtstellen deines Geräts. So kannst du feststellen, ob es geöffnet wurde.

Du hast die eindeutigen Nummern deines Gerätes notiert

In den Einstellungen deines Telefons findest du eindeutige, unveränderliche Hardwarenummern wie Seriennummer, Wi-Fi-Mac-Adresse, Bluetooth-Mac-Adresse und IMEI. Notiere diese Nummern. So kannst du dir jederzeit sicher sein, dass dein Gerät nicht heimlich ausgetauscht wurde.

Du fertigst regelmäßig Backups an

Erstelle von deinen wichtigsten Daten regelmäßig Backups. Dein Backup muss nicht perfekt sein. Ein schlechtes Backup ist besser als kein Backup!

Du solltest bei deinem Backup auch an wichtige Apps wie 2-Faktor-Apps oder Passwortmanager denken. Die Einstellungen lassen sich daraus meist leicht exportieren. Nutze wenn möglich quelloffene Backup-Software wie "oandbackup" oder "Neo Backup". Diese benötigen allerdings Root-Rechte. Eine einfache regelmäßige Kopie deiner wichtigsten Daten auf einen USB-

Stick ist aber auch ein guter Anfang! Denke daran, dass "No Backup, No Mercy" eine arrogante Haltung ist. Nicht alle Menschen haben das Wissen und die technischen Möglichkeiten für Backups. Helft euch gegenseitig!

Deine Backups sind verschlüsselt

Wenn du die Möglichkeit hast solltest du deine Backups unbedingt verschlüsseln, um diese vor ungewollten Zugriffen zu schützen.

Die Android-App Neo Backup unterstützt Verschlüsselung von Haus aus. Du kannst aber auch verschlüsselte Zip-Archive von Hand erstellen oder gleich ganze USB-Sticks verschlüsseln. Unter Linux, MacOS und einigen Windows-Versionen geht das ganz einfach über eine grafische Oberfläche. Du kannst aber auch eine Verschlüsselungssoftware für deine Sticks wie VeraCrypt einsetzen, die auf den meisten Betriebssystemen funktioniert. Wenn du dich tiefer mit der Materie befassen möchtest und die Kommandozeile nicht scheust kannst du dir professionelle Software wie Restic (Linux) oder duplicity (Linux) ansehen. Dafür musst du dein Gerät dann mit einem Computer verbinden.

Deine Backups sind dezentral gelagert

Du solltest deine Backups unbedingt dezentral und auch außerhalb deiner Wohnung speichern, damit du bei Diebstahl oder Beschlagnahmung schnell darauf zugreifen kannst.

Verschaffe dir einen Überblick über die Wichtigkeit deiner jeweiligen Daten und lagere sie entsprechend. Lagere z.B. unwichtigere Kopien deiner Musik- oder Bildersammlung weiter entfernt bei Freund*innen. Kritische Backups von Zugangsdaten oder wichtige Dokumenten solltest du eher redundant und auch in deiner Nähe lagern. Generell solltest du eine Kopie deiner Backups auch außerhalb deiner Wohnung aufbewahren.

Du übst die Wiederherstellung deiner Backups

Die Wiederherstellung deiner Daten ist das Wichtigste an einem Backup. Übe diese Situation. So kannst du sehen, ob dein Backup intakt ist. Stelle sicher, dass du dein Backup ohne Zugriff auf Passwortmanager und Zwei-Faktor-Apps wiederherstellen kannst.

Du lagerst nicht genutzte Geräte nicht in deiner Wohnung

Im Falle einer Hausdurchsuchung oder eines Einbruchs werden oft alle Geräte entwendet. Bereite dich darauf vor indem du nicht genutzte Geräte bei deinen Freund*innen lagerst. So hast du schnell Ersatz.

Du entsperrst dein Smartphone nicht auf Verlangen

Bei Beschlagnahmungen auf richterliche Anordnung oder bei Sicherstellungen eines Smartphones fragt die Polizei oft nach Pins und Passworten. Sage nichts. Entsperre nichts. Kontaktiere Anwält*innen.

Du hast dein Telefon einmal überschrieben

Du hast das Telefon gebraucht gekauft? Dann solltest du einmal den kompletten Speicher überschreiben, um zu vermeiden, dass ungewollte Daten auf deinem Gerät gefunden werden.

Gebrauchte Telefone könnten illegale Daten enthalten haben, die wiederhergestellt und ausgewertet werden könnten. Um zu vermeiden, dass dir das zum Verhängnis wird solltest du das Telefon einmal komplett überschreiben. Wenn du die Möglichkeit hast generiere dir große Zufallsdateien und kopiere diese auf dein Telefon, bis es voll ist. Andernfalls kannst du dir auch große Testdaten aus dem Internet herunterladen und damit

den Speicher deines Telefons überschreiben. Achtung! Das Überschreiben von Flash-Speichern ist oft nicht zu 100% möglich. Es können trotzdem Daten zurück bleiben. Bei moderneren Android-Geräten und iPhones ist das wegen des verschlüsselten Dateisystems für gewöhnlich nicht notwendig. Achte aber in diesem Fall darauf, dass das Telefon ordnungsgemäß auf Werkseinstellungen zurückgesetzt wurde. Solltest du dir nicht sicher sein, kannst du es trotzdem überschreiben.

Deaktiviere nicht genutzte Schnittstellen

Du solltest Positionierung, Wi-Fi, Bluetooth oder NFC nur aktivieren, wenn du es wirklich benötigst

Über Wi-Fi kannst du in bestimmten Fällen wiedererkannt werden. Im extremsten Fall kann sogar deine Wohnadresse ermittelt werden. Einige Geräte verraten die eindeutige Hardwarenummer deiner Wi-Fi-Schnittstelle sowie die Liste deiner bekannten Wi-Fi-Netze. Auf Websites wie wigle.net kannst du einfach nach den physischen Standorten der Wi-Fi-Netze suchen. Google und Apple nutzen ihre Marktmacht, um die Standorte von benachbarten Wi-Fis durch ihre Geräte in ihren eigenen Datenbanken zu speichern. Betreibst du ein eigenes W-Lan? Google, Apple und sämtliche Geheimdienste kennen dadurch seine Koordinaten. Aber auch Bluetooth und andere Schnittstellen bergen Gefahren. Bluetooth ist zum Beispiel Anfällig für Bluesnarfing (Öffnung eigentlich geschlossener Ports durch Befehle von Außen), Bluejacking (Zusendung unerwünschter Nachrichten), Bluebugging (Ausnutzen einer Backdoor), Bluesmacking (Denial of Service) oder Car Whispering (Abhören der Freisprecheinrichtung).

Verzichte wenn möglich auf Bluetooth-Geräte wie Earbuds

Wenn du dir sicher sein möchtest, dass du nicht über Bluetooth abgehört wirst, solltest du eine Kabelverbindung für deine Kopfhörer nutzen.

Bluetooth-Geräte wie Earbuds können möglicherweise beim Austausch ihrer geheimen Schlüssel belauscht werden. Angreifer*innen in Reichweite könnten so unbemerkt mithören.

Nicht genutzte Kameras sind abgedeckt

Du solltest nicht genutze Kameras einfach mit Stickern abdecken. Zum Beispiel, wenn du die Selfie-Kamera nicht oder nur kaum nutzt.

Wenn du in Deutschland wohnst kannst du dir beim Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) kostenlos wiederablösbare Spezialaufkleber für deine Smartphone-Kameras bestellen. Aber auch normale Sticker erledigen diese Aufgabe. Achte darauf, dass du nicht den unscheinbaren Helligkeitssensor überklebst! Dies führt dazu dass einige Smartphones den Display abschalten, da diese sich in einer Hosentasche wähnen. Wenn du Probleme mit Stalking hast oder von Ex-Partner*innen verfolgt wirst solltest du deine Kameras zur Sicherheit komplett abkleben.

3. Gefahren im Mobilfunknetz

Du nutzt datensparsame Telefon-Tarife

Eine Flatrate erzeugt in der Regel weniger Daten als ein Tarif mit minutengenauer Abrechnung oder Einzelverbindungsnachweisen. Denn diese müssen erfasst und gespeichert werden. Flatrates erzeugen weniger Daten. Prepaid-Tarife erzeugen in der Regel nicht mal Rechnungsdaten und sind daher sehr datensparsam.

Du hast der Vermarktung deiner Bewegungsdaten widersprochen

Viele Netzbetreiber*innen verkaufen eure Bewegungsdaten an diverse Werbefirmen weiter. Ihr könnt dieser Weitergabe widersprechen.

Frag bei den Provider*innen nach wie lange die Daten in den verschiedenen Tarifen gespeichert werden und mit wem sie geteilt werden. Es gibt auch extra datenschutzfreundliche Provider*innen wie z.B. "Wetell" in Deutschland. Trotzdem schützen diese nicht vor den zahlreichen Überwachungsmöglichkeiten im Mobilfunknetz! Anonyme Simkarten sind daher immer zu bevorzugen.

Du hast deine mobile Datenverbindung nicht durchgehend aktiviert

Deaktiviere mobile Daten, wenn du diese nicht brauchst. Eine aktivierte mobile Internetverbindung hinterlässt eine durchgehende Aufzeichnung deiner genutzten Funkzellen in den Verkehrsdaten deines Providers.

Wenn du gerade weder telefonierst, keine SMS schreibst bzw. empfängst und die mobilen Daten nicht nutzt, ist dein Telefon im sogenannten "idle state". Es entsteht dann keine Historie über deine Funkzellen-Position bei deinem Provider. Dem Funknetzwerk ist nur die letzte sogenannte Location Area bekannt. Dies ist ein Verbund aus einer Vielzahl von Funktürmen, die keinen verlässliche Aussage über deinen genauen Standort liefert. Will dich eine Behörde oder eine Angreifer*in dann finden, sind diese oft auf stille SMS (silent pings) angewiesen. Erst dadurch wird dein Telefon wieder mit einer konkreten Funkzelle verbunden.

Du nimmst dein Handy nicht mit zur Demo

Du solltest dein Telefon nicht mit zur Demo nehmen oder es einige Zeit vorher in den Flugmodus schalten und es auch nach der Demo noch einige Zeit im Flugmodus belassen.

Das gilt auch dann, wenn du anonyme Simkarten nutzt. Durch die gezielte Verfolgung (zum Beipiel auf dem Heimweg) einzelner Personen mit sogenannten IMSI-Catchern lässt sich eine Telefonnummer einer Person zuordnen. Egal, ob die Simkarte anonym ist oder nicht.

Du verzichtest auf Apps wie "SnoopSnitch"

Apps, die potentiell IMSI-Catcher oder Stille SMS detektieren können werden dir in den allermeisten Fällen nichts bringen. Du solltest auf diese Apps

verzichten und stattdessen lernen warum sie nicht viel bringen und was die Alternative ist.

Zunächst einmal ist an Apps wie "SnoopSnitch" generell nichts verkehrt. Wir können froh sein, dass es Menschen gibt, die sich mit dieser Materie befassen und solche Apps bauen. Trotzdem musst du verstehen, dass derartige Apps in den allermeisten Fällen völlig wirkungslos sind. SnoopSnitch zum Beispiel funktioniert nur in 2G und 3G Netzen, wenn dein Telefon Root hat und wenn auf dem Mainboard deines Gerätes ein ganz spezieller Chip verbaut ist. Du musst verstehen, dass die Kommunikation mit dem Mobilfunknetz für dein Betriebssystem eine völlig intransparente Blackbox ist. Dein Betriebssystem und deine Apps sind nicht in der Lage die Kommunikation mit einem Funkturm (Basisstation) im Detail zu steuern oder zu überwachen. Das bedeutet das Funknetzwerk kann mit dem Chip auf deinem Gerät kommunizieren ohne, dass dieses etwas davon mitbekommt. Schuld daran ist proprietäre, kommerzielle Hardware, die nicht quelloffen ist. So kommt es auch, dass du durch Stille SMS (Stealth Ping) grob geortet werden kannst. Der Funkchip in deinem Telefon registriert das zwar, meldet das aber nicht an dein Betriebssystem weiter. Nur einige wenige Chips haben Schnittstellen, die dem Betriebssystem eine Beobachtung erlauben. Nur dafür gibt es SnoopSnitch. Die einzig sinnvolle Verteidigung ist eine anonyme Simkarte.

Du verwendest anonyme Simkarten

Anonyme Simkarten erschweren staatlichen Akteuren und anderen Angreifer*innen die Auswahl ihrer Ziele erheblich. Ob stille SMS, IMSI-Catcher, Bestandsdatenauskunft, Verkehrsdatenauskunft, Funkzellenauswertungen, Quellen-TKÜ, Staatstrojaner oder Standortüberwachung. Eine anonyme Simkarte ist oft die einzig sinnvolle Verteidigung gegen derartige Überwachung.

Das Thema der Mobilfunküberwachung ist komplex und kann in diesem Rahmen nicht komplett behandelt werden. Wichtig zu verstehen ist aber, dass Security-Apps gegen derartige Überwachung nichts ausrichten können, weil z.B. Daten betroffen sind, die ohnehin bei deinem Provider liegen und nicht auf deinem Telefon. Oder weil die Apps selbst keinen Zugriff auf den proprietären Funkchip deines Telefons haben und so z.B. stille SMS nicht sehen können. Oder weil sich der Angriff im Funknetzwerk zwischen Netzanbieter*innen abspielt. Oder weil deine Mobilfunkanbieter*in deine Daten einfach weiter

verkauft. Hier auf Apps oder Verhaltensänderungen zu setzen bringt also nichts. Die einzige Verteidigung sind anonyme Simkarten. Bedenke auch, dass in Deutschland über 100 staatliche Stellen die Personen zu Telefonnummern und andersherum ohne Gerichtsbeschluss abfragen können.

Du nutzt dein Smartphone exklusiv für eine Simkarte

Nutze deine anonyme Simkarte nur in einem bestimmten Telefon. Verwende nie das gleiche Telefon für eine andere Simkarte. Denn die eindeutige Nummer der Sim und die eindeutige Nummer deines Telefons werden immer zusammen in den Verkehrsdaten des Providers gespeichert.

Du verwendest oft andere Simkarten und ein Proxy-Telefon

Um die Sicherheit weiter zu erhöhen kannst du oft deine anonymen Simkarten wechseln. Bei jedem Wechsel solltest du auch das dafür verwendete Telefon wechseln.

Da in den Verkehrsdaten deiner Netzanbieter*in immer die IMSI zusammen mit der IMEI auftaucht solltest du beim Wechsel deiner Simkarte auch dein Telefon wechseln. Wie du dir sicher vorstellen kannst ist es aufwändig und auch teuer das Telefon von Zeit zu Zeit zu wechseln. Du müsstest ja ständig deine Apps neu einrichten und viel Geld für ein neues Telefon ausgeben. Um die Kosten gering zu halten kannst du mit Proxy-Telefonen arbeiten. Und das geht so: Du hast ein teureres Gerät für deine reguläre Nutzung auf dem all deine Apps installiert sind. In diesem Telefon befindet sich keine Simkarte. Es ist also für das Mobilfunknetzwerk unsichtbar. Internet bekommst du über ein günstiges Zweitgerät, in welches eine Simkarte eingelegt ist. Dieses Telefon braucht nicht viel Leistung. Dieses kann dir aber einen Wi-Fi Hotspot und damit Internet bereitstellen. Außerdem kannst du damit ganz normal telefonieren, wenn du willst. Dieses Telefon lässt sich mit samt der eingelegten Simkarte schnell austauschen. Einziger Nachteil: Du hast immer zwei Smartphones dabei.

Deaktiviere deine Simkarte wenn du dich mit einer Gruppe bewegst

Wenn du mit Freund*innen, Bekannten, Familie oder Genoss*innen unterwegs bist solltest du deine anonyme Simkarte nicht verweden.

Du solltest nicht damit telefonieren, keine SMS schreiben und deine mobile Internetverbindung nicht nutzen. Entferne sie sicherheitshalber aus deinem Telefon. Bewegst du dich über einen längeren Zeitraum mit anderen Personen gemeinsam durch identische Funkzellen ist theoretisch eingrenzbar wer du sein könntest oder wer dein Familien- bzw. Freund*innenkreis ist. Gleiches gilt für eine mögliche zweite Simkarte, die auf deinen Namen registriert ist. Z.B. wenn du ein zweites nicht anonymes Telefon dabei hast. Bewegt sich diese Simkarte zusammen mit der anonymen Simkarte durch ein Gebiet ist anhand der gleichen Funkzellenwechsel bekannt wem die anonyme Karte gehört. Die Funkzellenwechsel werden möglicherweise in den Verkehrsdaten deines Providers geloggt. Lass dir von Bekannten einen Wi-Fi Hotspot bereitstellen, wenn du unterwegs bist und verwende diesen mit einem VPN oder TOR. Wenn du mit einer größeren Gruppe unterwegs bist sollte nur eine einzige Person einen Hotspot erstellen. Alle anderen sollten ihre Simkarten für diese Zeit entfernen.

Du gibst deine Telefonnummer nicht weiter

Wer deine Telefonnummer kennt kann dich leicht angreifen. Halte deine Nummer wenn möglich geheim. Um trotzdem erreichbar zu sein kannst du auf Messenger mit Anruffunktion ausweichen, die keine Nummer benötigen oder bei denen sich die Nummer verbergen lässt.

Auf Seiten wie cell-track.com oder phone-location.info kann zum Beispiel einfach herausgefunden werden, ob sich ein Gerät im Ausland befindet oder nicht oder ob ein Gerät gerade eingeschaltet ist. Alles was du brauchst ist die Telefonnummer. Du kannst nichts dagegen tun als deine Nummer geheim zu halten. Staatliche Akteure haben zudem weitere Möglichkeiten wie z.B. die Infektion des Gerätes mit einem Zero-Click-Exploit (Staatstrojaner). Nur eine

anonyme Simkarte und das Geheimhalten deiner Nummer schützen dich effektiv vor staatlichen Übergriffen.

Du telefonierst nicht mit deiner anonymen Karte

Nutze deine anonyme Simkarte/Telefon nicht für reguläre Telefonate oder SMS. In den Verkehrsdaten ist ersichtlich wer die Zielkontakte sind, wenn diese nicht auch eine anonyme Karte haben. Dadurch ist evtl. eingrenzbar wer du bist. Nutze die Karte wenn möglich nur mit anderen anonymen Karten oder weiche auf Internet-Messenger für Nachrichten und Telefonate aus.

Du hast Simkarten und Telefone anonym bezogen

Du solltest Simkarten und Telefone nie direkt an deine Adresse bestellen oder von deinen Konten bezahlen. Um keine Spuren zu hinterlassen kannst du Freund*innen bitten diese für dich zu bestellen oder abzuholen. Zahle in bar.

Du beziehst dein Guthaben anonym

Du solltest auch das Guthaben für deine Simkarte anonym oder über Mittelspersonen beziehen. Verwende daher Simkarten für die du Guthaben bar an Kassen kaufen kannst oder bitte Freund*innen dir den Guthaben-Code zu senden.

Du unterdrückst deine Rufnummer, wenn du telefonierst

Du kannst deine Rufnummer unterdrücken, wenn du telefonierst. So kann die angerufene Person deine eigene Nummer nicht sehen. Das kannst du für bestimmte Personen oder für alle Anrufe einstellen.

Besonders wenn du von Stalking betroffen bist solltest du deine Nummer unterdrücken. Denn deine Nummer kann auf vielfältige Weise genutzt werden um dich anzugreifen. Sei dir auch im Klaren darüber, dass das Unterdrücken der Rufnummer lediglich dazu führt, dass diese auf dem Telefon der Gegenstelle nicht angezeigt wird. In den Anrufprotokollen (Verkehrsdaten) der beteiligten Provider*innen wird deine Nummer dennoch gespeichert. Für Behörden ist dein Anruf also trotz unterdrückter Rufnummer nachvollziehbar. Nutze anonyme Simkarten, wenn du auf wirkliche Anonymität angewiesen bist.

Du wählst Notrufnummern wie 110 und 112 mit bedacht

Seit 2019 wird in Deutschland und vielen anderen Ländern Advanced Mobile Location (AML) eingesetzt und schrittweise ausgebaut, um Personen in Notsituationen zu orten. Wenn du das nicht möchtest solltest du dich darauf vorbereiten.

Vor AML standen den Rettungsleitstellen lediglich extrem ungenaue Funkzellendaten zur Verfügung (wenn überhaupt), um Personen in Notsituationen orten zu können. AML dagegen ist fest in moderne Telefone und deren Betriebssysteme integriert: Wird eine Notrufnummer gewählt aktiviert das Telefon selbstständig GPS und Wi-Fi, um die eigene Position bestimmen zu können. Diese wird dann via Internet oder SMS automatisch an die Leitstelle übertragen. Diese extrem genaue Ortung wird nur durch das Wählen der Notrufnummern aktiviert und ist nicht von außen ohne dein aktives Handeln nutzbar. Du kannst in den meisten Fällen nichts dagegen tun, dass du beim Wählen dieser Nummern automatisch geortet wirst. Leider werden so aber auch anonyme Meldungen erschwert. Du solltest daher immer abwägen, ob die Wahl von Notrufnummern durch dein eigenes Telefon wirklich notwendig ist. Auf Wikipedia findest du eine Liste mit allen Ländern in denen es AML gibt. AML ist auf Android Teil der Play-Services und kann über die Notfalleinstellungen deaktiviert werden.

Du hast eine Sperre für Drittanbieter*innen eingerichtet

Mit einer Drittanbieter*innensperre kannst du verhindern, dass Apps, Websites oder Betrüger*innen Kosten für Abos oder sonstige Käufe über deine Telefonrechnung abbuchen können.

Wenn du eine solche Sperre einrichten möchtest kannst du dich online oder telefonisch an deinen Provider wenden.

Du nennst nicht sofort deinen Namen, wenn du ans Telefon gehst

Du solltest nicht deinen Namen nutzen, um ein Gespräch anzunehmen. Nutze stattdessen allgemeine Floskeln wie 'Hallo'.

4. Apps und Betriebssystem

Du verwendest ein freies Betriebssystem

Freie Android-basierte Betriebssysteme wie grapheneOS, CalyxOS oder DivestOS können dir helfen deine Privatsphäre zu schützen und sind nicht an Google, Apple oder Microsoft gebunden.

Wenn du dir unsicher bist welches System du installieren solltest so lautet die klare Empfehlung derzeit grapheneOS auf einem der kompatiblen Telefone zu installieren. Mehr Informationen findest du in den Links.

Du hast dein Telefon von Bloatware befreit

Hersteller*innen von Smartphones erhalten von Google oder Apple Millionen bis Milliarden dafür, dass ihre Software fest auf deinem Telefonen platziert wird. Du solltest diese Apps unbedingt entfernen.

Derartige Beträge lohnen sich natürlich nur wenn das einen Nutzen hat: Die vorinstallierte Software sammelt Daten und verwertet eure Gewohnheiten. Ihr solltet Bloatware daher entfernen (Manchmal ist das ohne Root-Berechtigungen nicht möglich) oder gleich ein custom Betriebssystem wie GrapheneOS installieren.

Du hast deine Werbe-ID deaktiviert oder gelöscht

Du solltest unbedingt deine „mobile advertising ID“ (MAID) löschen, öfters ändern (Android) oder deinen Apps das Tracking verbieten (iOS), wenn du

nicht möchtest, dass die Daten aus verschiedenen Apps durch sogenannte Datenbroker wieder zusammengeführt und verkauft werden.

Wenn du iOS oder Android verwendest überträgt dein Betriebssystem im Hintergrund eine Werbe-ID an deine Apps. Diese ID können an die Datensätze einzelner Apps gehangen werden. Wenn die Anbieter*in deiner Apps diese Daten dann verkauft können Broker diese mit anderen Datensätzen von dir zusammenführen. Dadurch entstehen regelrechte Halden aus deinen persönlichen Daten und Interessen, die online gehandelt werden.

Sind deine Apps und dein System aktuell?

Halte Apps und dein Betriebssystem aktuell. Malware und Staatstrojaner nutzen oft Schwachstellen in der Software aus. Aktuelle Apps und ein aktuelles Betriebssystem sind daher wichtig.

Nutze einen Passwortmanager

Deine Sicherheit wird enorm erhöht, wenn du für alle Services im Internet ein anderes komplexes Passwort verwendest. Diese solltest du in einem Passwortmanager wie KeepassXC oder Bitwarden speichern.

Denke daran, dass dein Passwortmanager ein besonders sicheres Passwort braucht. Denke auch daran eine regelmäßige Sicherungskopie deiner Passwortdatenbank zu erstellen. Wenn du Probleme hast dir starke Passworte auszudenken kannst du das Diceware-Verfahren nutzen. Unten findest du einen Link mit einer Anleitung. Alles was du brauchst ist ein Spiel-Würfel.

Du installierst Apps nur aus vertrauenswürdigen Quellen

Nutze nur offizielle App-Stores oder F-Droid, um deine Apps zu beziehen. Wenn du dich auskennst kannst du Apps auch direkt von den Websites der Hersteller*innen laden. Überlege immer, ob du eine App überhaupt brauchst.

Infizierte Apps haben viele Möglihkeiten dich anzugreifen. Sie können zum Beispiel Passworte stehlen.

Du prüfst Zugriffsrechte sorgfältig

Deine Taschenlampen-App will auf den Speicher zugreifen? Keine gute Idee! Frage dich immer wozu eine App Berechtigungen benötigt und gib diese nur schrittweise oder bei Bedarf frei.

Du nutzt alternative App-Stores

Über F-Droid oder Aurora Store kannst du die meisten Apps auch ohne Anmeldung in Google bzw. ohne Google-Services beziehen.

Du verzichtest auf Google-Play-Dienste und Apple-Services

Google-Play-Services bzw. Apple-Services stellen zentrale Infrastrukturen für einige Apps bereit. Zum Beispiel werden darüber Push-Nachrichten versendet. Staatliche Stellen nutzen diese Tatsache, um damit iPhone- bzw. Android-Geräte zu überwachen.

Du kannst dich davor schützen indem du Apps verwendest, die ohne Google bzw- Apple Services auskommen. Verzichte auch auf Alternativen wie microG, wenn du ein eigenes Betriebssystem installiert hast. Installiere zum Beispiel Apps aus F-Droid, die ohne diese Services auskommen. Messenger wie Telegram, Signal und Matrix bieten eigene Alternativen für zentralisierte Pushnachrichten an.

Du nutzt datenschutzfreundliche Webbrowser

Nutze Browser, wie DuckDuckGo-Browser, die keine Daten über dich sammeln und gleichzeitig deine Privatsphäre aktiv schützen.

Du verzichtest auf Root-Rechte

Root-Rechte ermöglichen dir viele einzigartige Apps. Diese Rechte gelten dann aber eventuell auch für schadhafte Apps, weswegen du auf Root generell verzichten solltest.

Wenn du nicht weißt was Root ist, hast du es vermutlich nicht. Root muss bei den meisten Geräten aufwändig aktiviert werden. Leider benötigen auch einige Apps, die deine Sicherheit potentiell erhöhen können oft Root-Rechte. Zu nennen wären da zum Beispiel Backup-Anwendungen wie "Neo Backup" aber auch Apps wie "SnoopSnitch", die versuchen IMSI-Catcher oder Stille SMS zu erkennen. Du solltest immer genau abwägen, ob du wirklich Superuser-Rechte auf deinem Gerät benötigst. In den allermeisten Fällen gibt es dafür keine gute Begründung. Apps wie z.B. "SnoopSnitch" funktionieren sowieso nur in wirklich wenigen Software- und Hardwarekonstellationen. Deswegen Root einzurichten steht in keinem Verhältnis.

Du nutzt sichere Messenger

Du solltest unbedingt quelloffene, verschlüsselte Messenger wie Briar, Signal, Threema, Element oder SimpleX nutzen. Verzichte auf unsichere kommerzielle Messenger wie WhatsApp und Co.

Wenn du dir unsicher bist welche Messenger gut sind oder wenn du Argumente brauchst, um Familie und Freud*innen zu überzeugen, solltest du dir unbedingt die Messenger-Matrix von Kuketz ansehen. Dort kannst du die einzelnen Messenger bequem nach Funktionen und Sicherheitsaspekten vergleichen.

Aktiviere die zweistufige Bestätigung in deinen Messengern

Die zweistufige Bestätigung (Zwei-Faktor-Authentisierung) verhindert, dass deine Simkarte oder Kopien davon genutzt werden können, um an deine Nachrichten zu kommen.

In einigen Messengern funktioniert das über Mails. In anderen kannst du eine zusätzliche Pin vergeben. Wenn du deine Telefonnummer verlierst oder andere

Menschen bzw. Behörden an deine Simkarte oder eine Kopie davon gelangen (Sim-Swapping), können sie sich mit der Telefonnummer anmelden und deine Nachrichten lesen bzw. in deinem Namen schreiben.

Du gibst deine Apple-ID nicht weiter und deaktivierst iMessage

Du solltest iMessage nicht nutzen und deine Apple-ID geheim halten. iMessage wurde in den vergangenen Jahren immer wieder Ziel sogenannter Zero-Click-Angriffe.

Durch speziell präparierte Nachrichten für iMessage konnten in der Vergangenheit immer wieder Staatstrojaner auf iPhones installiert wedern. Du solltest diese Software daher meiden.

Du hast auf deinem iPhone den Lockdown-Mode aktiviert

Der Lockdown-Mode (Blockierungsmodus) kann auf dem iPhone benutzt werden, um Infektionen mit Malware vorzubeugen. Hierbei werden einige Features stark eingeschränkt, um das System besonders zu schützen.

Für Android ist ein ähnliches Feature nicht verfügbar.

Du startest dein Telefon oft neu

Du solltest dein Telefon öfter neu starten. Zum Beispiel jeden Morgen oder vor kritischen Gesprächen. Einige Staatstrojaner überleben Neustarts nicht, da diese oft nicht persistent sind. Obwohl später Neuinfektionen möglich sind, kann dir diese Strategie private Zeitfenster verschaffen.

Du hast dein Gerät auf Werkseinstellungen zurückgesetzt

Du solltest dein Telefon auf Werkseinstellungen zurücksetzen, wenn du ihm nicht mehr traust. Diese Methode ist effektiv gegen handelsübliche Spionage-Apps aus dem App-Store, die sich womöglich auf deinem Gerät verstecken könnten.

Diese Methode entfernt in der Regel ungewollte Spionage- oder Stalking-Apps von deinem Telefon. Diese Apps wurden eventuell von Menschen aus deinem nahen Umfeld installiert, als sie direkten Zugriff auf dein Gerät hatten. Bitte sei dir bewusst darüber, dass diese Apps nicht vergelichbar sind mit professionellen Staatstrojanern, die auch nach einem ZUrücksetzen des Telefons möglicheriweise aus der Ferne wieder installiert werden können. Trotzdem ist diese Möglichkeit ein guter Anfang, um aus toxischen Beziehungen zu entkommen oder um Stalking vorzubeugen. Bitte sichere deine wichtigsten Daten vor dem Zurücksetzen.

5. Gefahren im Internet

Du bist vorsichtig beim Scannen von QR-Codes

Achte beim Scannen von QR-Codes auf die Echtheit der Zielseite und prüfe genau wohin der Code dich leitet. Sei skeptisch, wenn du nach dem Scannen persönliche Daten oder Bankinformationen eintippen sollst.

Immer wieder werden QR-Codes zum Beispiel an Ladesäulen oder Automaten überklebt. Sie werden aber manchmal auch mit Briefen versendet. So werden Menschen dazu gebracht persönliche Informationen auf Fake-Seiten einzugeben oder bösartige Apps zu installieren. Prüfe daher das Ziel genau. Sei skeptisch bei aufgeklebten Codes. QR-Codes sollten so gestaltet sein, dass sie fälschungssicher sind. Zum Beispiel sollten diese hinter einer Glasscheibe angebracht sein, um ein Austauschen zu verhindern.

Du trägst deine Bankkarte nicht direkt bei deinem Smartphone

Du solltest deine Bankkarte nicht direkt neben deinem Smartphone tragen oder lagern. Malware könnte die Daten über NFC auslesen und verschicken. Nutze alternativ RFID-Schutzhüllen für deine Karten und deaktiviere NFC.

Malware kann die NFC-Schnittstelle deines Smartphones nutzen, um Daten von Bankkarten auszulesen. Du kannst dich schützen indem du die Karten nicht direkt neben deinem Smartphone aufbewarst. Online kannst du auch spezielle RFID-Schutzhüllen bestellen, die dich schützen können.

Du gehst achtsam mit deinen persönlichen Daten um

Du solltest dir genau überlegen welche persönlichen Informationen du im Internet teilst. Bist du z.B. leicht über Suchmaschinen zu finden? Wenn ja solltest du versuchen diese Daten zu entfernen.

Spezialisierte Agenturen und Datenbroker sammeln öffentliche Informationen und Informationen aus Datenleaks über dich und verkaufen diese z.B. an Geheimdienste weiter. Unternehmen wie PimEyes, die auf Gesichtserkennung ausgerichtet sind, nutzen deine persönlichen Bilder, um ihre KIs zu trainieren. So werden die biometrischen Merkmale deines Gesichts erfasst und du kannst in Bruchteilen von Sekunden auf anderen Bildern identifiziert werden. Versuche dich selbst im Internet zu finden, identifiziere die Services und versuche deine persönlichen Daten von dort zu entfernen. Nutze zum Beispiel Google Alerts, um dich automatisch via E-Mail informieren zu lassen sobald dein Name oder andere persönliche Daten im Internet auftauchen. Du kannst manchmal auch DMCA-Takedown-Anfragen nutzen, um deine Daten von US-Websites löschen zu lassen.

Nutze alternative Frontends

Alternative Frontends für Webservices wie YouTube, Twitter, TikTok und andere Websites können dir helfen deine Daten zu schützen.

Anstelle von Youtube kannst du zum Beispiel eine der zahlreichen Invidious-Instanzen wie yewtu.be nutzen. So kannst du Werbung vermeiden und gleichzeitig deine Privatsphäre schüzen. Du kannst auch LibRedirect für FireFox installieren. Dieses Plugin leitet dich beim Surfen im Internet automatisch auf ein alternatives Frontend um.

Du nutzt Passkeys

Passkeys können in manchen Anwendungen und Apps Passwörter ersetzen und machen diese komplett überflüssig. Sie können nicht wie Passwörter durch Pishing oder Datenleaks entwendet werden. Nutze sie, wenn sie angeboten werden!

Du solltest PassKeys nicht an eine biometrische Entsperrung binden. Denke außerdem daran deine Passkeys zu sichern für den Fall, dass du dein Gerät verlieren solltest.

Du sicherst deine Accounts mit Zwei-Faktor-Authentifizierung

Viele Dienste und Plattformen im Internet bieten eine Absicherung der Logins mit einem zweiten Faktor an. Nutze diese Möglichkeit wann immer es geht.

Bedenke dabei bitte auch, dass es möglich sein muss ein Backup von deinem zweiten Faktor zu erzeugen. Eine Handynummer ist kein wirklich guter zweiter Faktor. Erstens kannst du deine Nummer potentiell verlieren. Es kann aber auch sein, dass andere Menschen oder Behörden Zugriff auf deine Nummer erlangen können. Im Falle eins Verlustes deiner Simkarte kommst du erst mal nicht an deine Accounts. Solltest du einen Hardware-Token als zweiten Faktor nutzen, stelle bitte sicher, dass es für Notfälle noch einen zweiten gibt! Solltest du Softwarelösungen wie Time-Based-One-Time-Passwords nutzen, fertige bitte Backups in deinen OTP-Apps an!

Dein zweiter Faktor liegt auf einem separaten Gerät

Deine Zwei-Faktor-App ist auf einem separaten Gerät installiert. So kann dein zweiter Faktor bei einer Kompromittierung deines Geräts nicht zum Einloggen in deine Accounts genutzt werden.

Du verwendest einen Werbeblocker

Gezielte Werbekampagnen (Microtargeting) werden unter anderem von Geheimdiensten genutzt, um einzelne Geräte passgenau mit Malware zu infizieren.

Aber nicht nur Geheimdienste nutzen Werbung, um Menschen zu verfolgen. Datenbroker verkaufen aggregierte Daten über dich weiter und legen Profile von dir an.

Du nutzt verschiedene Pseudonyme und Mailadressen

Du kannst deine Sicherheit verbessern, indem du auf allen Plattformen einen anderen Namen und andere Mailadressen bzw. Mobilnummern für die Registrierung verwendest. So können deine Accounts durch Datenlecks nicht zusammengeführt werden.

Du nutzt deine Pseudonyme nicht zur gleichen Zeit

Arbeite zeitversetzt wenn du in verschiedenen Kanälen oder Gruppen mit verschiedenen Pseudonymen die gleiche Nachricht teilen willst. Sonst ist ersichtlich dass eine Person hinter den diversen Pseudonymen steckt.

Du nutzt TOR oder den TOR-Browser

Deine Internetzugangsprovider können sehen welche Websites du besuchst und welche Apps du nutzt. TOR (The Onion Router) kann dir helfen deine Anonymität im Internet stark zu verbessern. Nutze Websites über den Tor-Browser und leite Apps mit der Orbot-App über das Tor-Netzwerk um.

Du nutzt datenschutzfreundliche Suchmaschinen

Google, Apple und andere Hersteller*innen geben Daten ohne zu zögern an Ermittlungsbehörden weiter. Verwende daher alternative Suchmaschinen wir duckduckgo.com oder stract.com

Du nutzt Cloud-Speicher nur verschlüsselt

Viele Cloud-Anbieter*innen arbeiten vollumfänglich mit Ermittlungsbehörden zusammen und werden nicht zögern deine Daten auszuliefern. Lege dort nur verschlüsselte Daten ab.

Generell solltest du überlegen, ob du die entsprechenden Cloud-Dienste überhaupt brauchst. Du kannst zum Beispiel Apps wie "OpenKeychain" verwenden, um Dateien vor dem Upload in eine Cloud zu verschlüsseln. Für den Fall, dass du ein Apple-Gerät mit deiner iCloud nutzt aktiviere dort den erweiterten Datenschutz.

Du nutzt VPNs mit Bedacht

Bedenke, dass du VPN-Anbieter*innen vertrauen musst. Du bezahlt sie, also kennen Sie deine Identität. Viele VPN-Dienste arbeiten vollumfänglich mit Ermittlungsbehörden zusammen. Wenn du kannst, nutze stattdessen das TOR-Netzwerk.

Du löschst Metadaten aus deinen Bildern

Dein Smartphone heftet Metadaten wie Koordinaten, Kameratyp, Auflösung, Smartphone-Modell oder Betriebssystem unsichtbar an deine Bilder. Bei einigen Kamera-Apps lässt sich das teilweise oder ganz deaktivieren.

Wird dein Telefon entwendet können diese Daten Aufschluss über deine Herkunft geben. Nutze Apps wie "Imagepipe" um deine Bilder zu bereinigen bevor du diese ins Internet lädst. Imagepipe kannst du über den F-Droid auf deinem Android-Smartphone installieren.

Du ließt dir Datenschutzerklärungen durch

Nimmst du dir Zeit Datenschutzerklärungen von neuen Apps und Services bei denen du dich registrierst zu lesen? Interessiert es dich mit wem deine Daten geteilt werden und was damit passiert?

Du verschlüsselst deine E-Mails

Nutzt du E-Mails? Dann solltest du unbedingt über Verschlüsselung wie GPG/OpenPGP nachdenken.

Hast du gewusst, dass zum Beispiel in Deutschland viele E-Mail-Provider als Telekommunikationsdienst gelten? Damit dürfen Behörden deine Bestandsdaten und E-Mails anfordern. Aber auch ohne behördliche Überwachung sind E-Mails vielen Gefahren ausgesetzt. Eine E-Mail passiert beim Weg in ein Postfach viele Knotenpunkte und kann an zahlreichen Stellen mitgelesen werden.

Lösche nicht genutzte Accounts

Es ist wichtig nicht mehr benötigte Accounts zu löschen. Nimm dir einmal im Jahr Zeit dafür. Egal, ob du diese für eine Website oder eine App benötigt hast. Wenn du sie länger nicht mehr genutzt hast, solltest du sie schließen. Das minimiert das Risiko von Datenlecks.

Du prüfst, ob du von Datenlecks betroffen bist

Täglich leaken persönliche Daten aus Websites, Portalen und Onlineshops. Betroffne werden dabei selten informiert. Die Daten werden verkauft, gehandelt oder sind oft auch völlig frei zugänglich.

Auf der Website haveibeenpwned.com kannst du schnell und unkompliziert feststellen, ob deine Mailadresse in Datenlecks auftaucht. Du kannst dir dort auch einen Account zulegen, und dich bei neuen Funden automatisch benachrichtigen lassen.