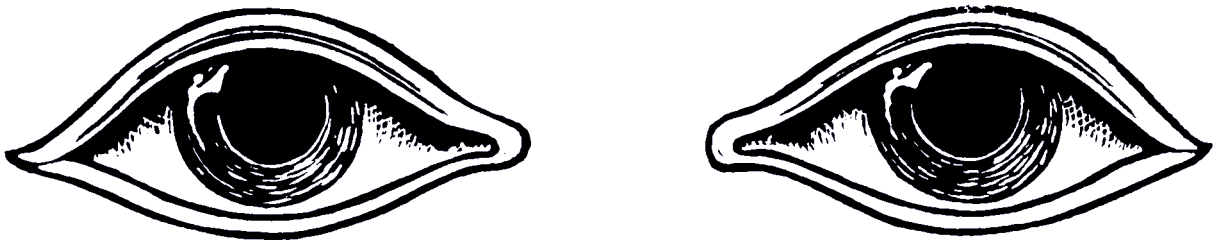


OCTOBER REBELLION PHONE LOCKDOWN

DU HAST VOR, DEIN HANDY MIT ZU EINER AKTION ZU NEHMEN?

Bevor du das tust, solltet du sicherstellen, dass es geschützt ist ...

Die wenigsten Handys speichern nur die Daten ihres Besitzers: Die meisten enthalten viele Kontakte, Fotos und Videos von anderen Menschen - den Menschen in unserem Leben. Selbst wenn du wenig Bedenken hast, deine Daten zu verlieren, empfinden andere das möglicherweise nicht so. Und die könnten Schaden nehmen - besonders dann, wenn dein Handy nicht ausreichend gegen Datendiebstahl geschützt ist. Falls du ein XR-Koordinator bist, hast du wahrscheinlich sogar eine lange Kontaktliste, die von einem Gegner verwendet werden kann, um deiner Gruppe zu schaden. Account Logins können ebenfalls missbraucht werden. Es ist wichtig dir das bewusst zu machen, vor allem dann, wenn du planst zivilen Ungehorsam zu betreiben.

GEDANKENÜBUNG: GIB DEIN HANDY AUF

Such dir einen ruhigen Ort und leg dein Handy mit dem Bildschirm nach unten vor dir auf den Tisch. Nimm deine Hände weg und sieh es dir an. Stell dir sich vor, du würdest dir das Handy von einem Polizisten abnehmen lassen, der es dann in eine Plastiktüte packt. Stell dir vor, du würdest dein Handy nie wieder sehen. Experten auf der Polizeistation würden es durchforsten, um Bilder und Videos (wenn es sich um ein Smartphone handelt), Kontakte und SMS Nachrichten zu kopieren. Sie würden den Browser öffnen, um sich bei deinen sozialen Netzwerken, Medien- und XR-Plattformkonten anzumelden. Vielleicht finden sie deine MicroSD-Karte und nehmen diese auch heraus.

Denke nicht nur darüber nach, *was* sich auf deinem Handy befindet, sondern auch *wer* sich darauf befindet und mit welchen Konten (und Informationen) es sich verbinden kann. Überleg dir, wie all dies andere Rebellen in Mitleidenschaft ziehen könnte - nicht nur bei dieser Aktion, sondern auch in Zukunft, und selbst dann wenn sie nicht mehr Teil unserer Bewegung sind.

Kurz gesagt, **wir sperren unser Handy nicht nur für uns selber, sondern auch für andere und um unsere Gruppe zu schützen**. Der Schutz der Privatsphäre und der Anonymität ist in einer Zeit, in der solche Grundrechte von Unternehmen und Regierungen in großem Umfang missachtet werden, um uns zu kontrollieren, zu entmachten und zu verurteilen, auch für unsere regenerative Kultur von großer Bedeutung.

ZEIG MITGEFÜHL, WENN ES UM DATEN GEHT

- Fotos, Videos und Audioaufnahmen von Rebellen, insbesondere bei XR-Gruppentreffen
- XR-Konto-Anmeldedaten (Mattermost, Base, E-Mail, Pads usw.)
- Kontaktlisten

Stell dir selbst die Frage

„Muss ich mein Handy auf diese Aktion mitnehmen?“

ÄLTERE HANDYS ("DUMBPHONES")

Sogenannte „Dumphones" sind besonders schwer zu sichern, weil Inhalte nicht intern verschlüsseln werden können. Die begrenzte Speicher- und Anwendungskapazität von Dumbphones sorgt allerdings in der Regel dafür, dass weniger verloren geht als bei einem modernen Gerät.

WICHTIG: Das Extrahieren von Kontakten und anderen Informationen von Dumbphones ist trivial. Stelle sicher, dass du möglichst viele Kontakte - sowohl von dem Gerät als auch von der SIM-Karte - löschst und nur Kontakte behältst, die du für die Aktion benötigst.

SMARTPHONES
SICHERN VON IPHONES MIT VERSCHLÜSSELUNG

Bei den meisten modernen Apple-Handys (iOS) ist der Inhalt des Handys bereits verschlüsselt. Dies hält natürlich niemanden, der Zugriff auf dein Gerät hat, davon ab, deine Daten zu lesen. Deshalb muss die Datenverschlüsselung durch einen Sperrcode gesichert sein.

WICHTIG: Wenn du einen rein numerischen Sperrcode wählst, bekommst du zum Entsperren einen numerischen Tastenblock. Das ist zwar einfacher, als Buchstaben und Symbole auf einer kleinen virtuellen Tastatur einzugeben. Es wird trotzdem empfohlen, einen alphanumerischen Sperrcode mit mehr als 6 Zeichen zu wählen, weil er schwieriger to knacken ist.

iOS4 bis iOS7

1. Gehe zu 'Code' in den Einstellungen (oder iTouch & Passcode).
2. Folge den Anweisungen, um ein Passwort zu erstellen.

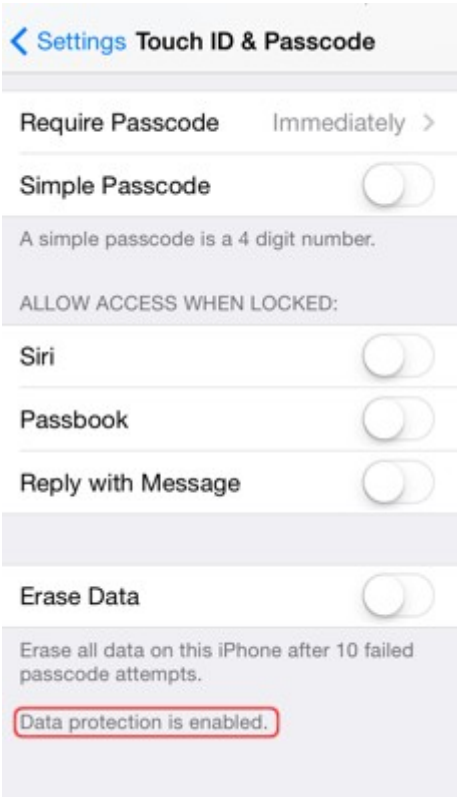
iOS8 oder neuer

In manchen iOS Versionen musst du 'Einfacher Code' in den Allgemeinen Einstellungen deaktivieren, um einen Code zu erstellen, der mehr als vier-stellig ist. Seit der Veröffentlichung von iOS 9 verwendet Apple standardmäßig einen 6-stelligen Passcode.

Um dein Passwort zu erstellen, wähl "Code-Optionen" und "Eigener alphanumerischer Code". Wenn du ein vorhandenes Passwort ändern möchtest, wähl "Code deaktivieren" und dann "Code-Optionen". Du solltest auch die Option "Code anfordern" auf " Sofort " stellen, damit dein Gerät nicht entsperrt bleibt, wenn du es nicht verwendest.

Scroll nach dem Festlegen eines Passcodes auf der Seite mit den Passcode-Einstellungen nach unten. Es sollte eine Meldung angezeigt werden, die besagt, dass Datenschutz aktiviert ist. Das bedeutet, dass die

Verschlüsselung des Geräts jetzt an deinen Passcode gebunden ist und dass die meisten Daten auf deinem Handy diesen Code zum Entsperren benötigen.



Apple-Backups: eine Warnung

Backups von Apple-Gerätebesitzern sind in der Regel entweder auf der Apple iCloud oder in iTunes gespeichert.

WICHTIG: Wenn du auf der iCloud speicherst, solltest du davon ausgehen, dass die Strafverfolgung auf alle Daten zugreifen kann. Obwohl Apple sagt, dass die Daten verschlüsselt sind, verfügen es über die Codes zur Entschlüsselung und ist im Falle einer strafrechtlichen Untersuchung zur Unterstützung der Gerichtsbarkeit verpflichtet. Aus diesem Grund sollte diese Option ganz vermieden werden.

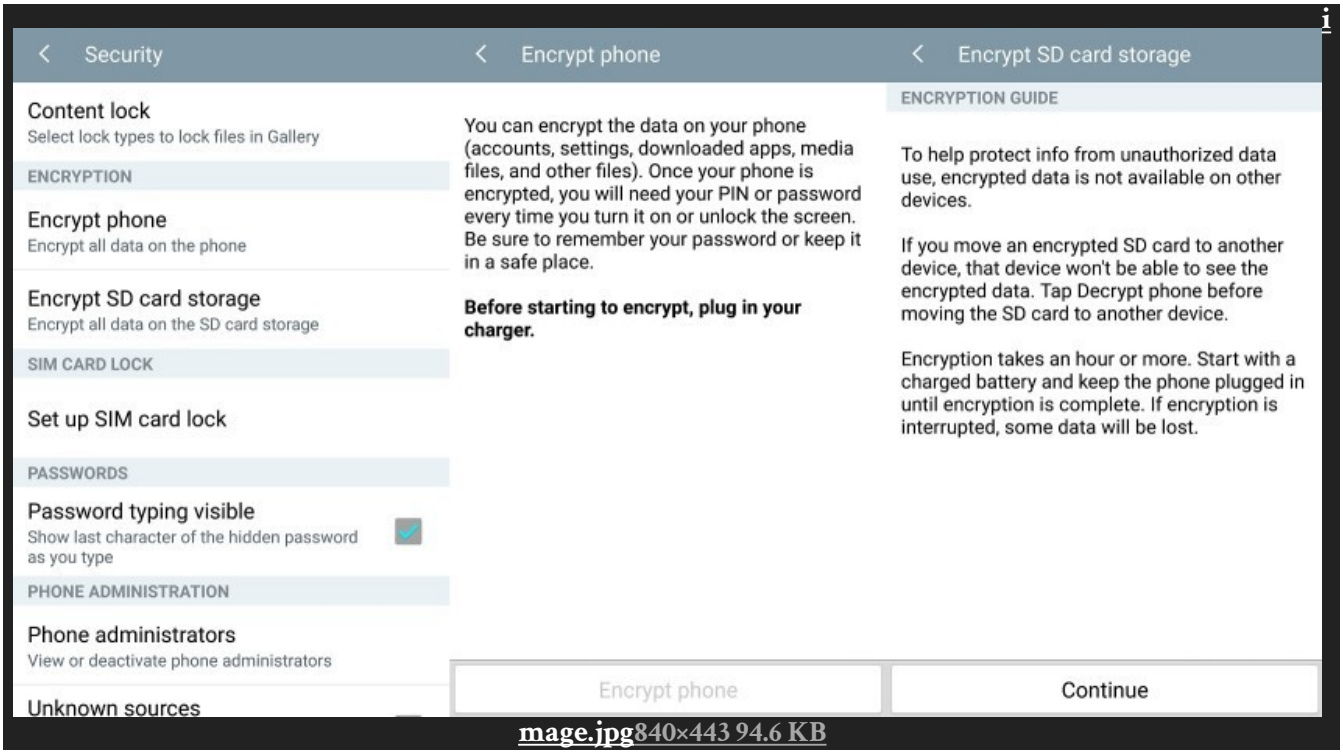
Wenn du in iTunes speicherst, ist es wichtig zu wissen, dass das iTunes-Sicherungssystem die Daten nicht standardmäßig verschlüsselt. Deshalb solltest du die Option 'IPhone-Backup verschlüsseln' wählen, so dass alle Daten, die du auf deinem Computer speicherst verschlüsselt werden. Merk dir dein gewähltes Passwort und wähle die Option einer vollständigen Verschlüsselung auf deinem Laptop.

ANDROID-HANDYS MIT VERSCHLÜSSELUNG SICHERN

Die Verschlüsselungstechnik ist auf allen Android-Geräten sehr ähnlich, aber die Methoden zur Aktivierung haben sich im Laufe der Jahre etwas geändert. Bei den meisten Geräten ist die Verschlüsselung heutzutage standardmäßig aktiviert, insbesondere bei Geräten, auf denen neuere Versionen von Android ausgeführt werden. Beispielsweise ist für jedes Pixel-Smartphone, das Nexus 6P, das Nexus 5X, das Nexus 6 und das Nexus 9 die Verschlüsselung standardmäßig aktiviert. Wenn nicht, macht Android dies zu einem sehr einfachen Vorgang.

Android 5.0 und höher

Bei Android-Handys und -Tablets mit Android 5.0 Lollipop oder neuer kannst du in den Einstellungen direkt zum Menü „Sicherheit“ navigieren. Die Anfahrt kann je nach Hersteller geringfügig abweichen.



mage.jpg840×443 94.6 KB

Hier sollte eine Option zum Verschlüsseln des Smartphones angezeigt werden. Während des Ladevorgangs wirst du aufgefordert, dein Smartphone an das Stromnetz anzuschließen, um sicherzustellen, dass es sich nicht ausschaltet und Fehler verursacht. Wenn du es noch nicht getan hast, wirst du aufgefordert, eine PIN oder ein Kennwort für den Sperrbildschirm festzulegen. Die musst du von jetzt an jedesmal eingeben, wenn du dein Smartphone einschaltest oder den Bildschirm entsperrst, um auf deine neu verschlüsselten Dateien zugreifen zu können.

Android 4.4 und älter

Wenn du ein Mobiltelefon mit Android 4.4 KitKat oder älter verwendest, musst Sie eine PIN oder ein Kennwort einrichten, bevor du den Verschlüsselungsvorgang startest. Zum Glück ist das einfach genug. Gehen zu Einstellungen> Sicherheit> Displaysperre. Hier kannst du entweder ein Muster, eine numerische PIN oder ein alphanumerisches Passwort für deinen Sperrbildschirm auswählen. Dies ist das gleiche Passwort, das zur Entschlüsselung verwendet wird. Merk es dir.

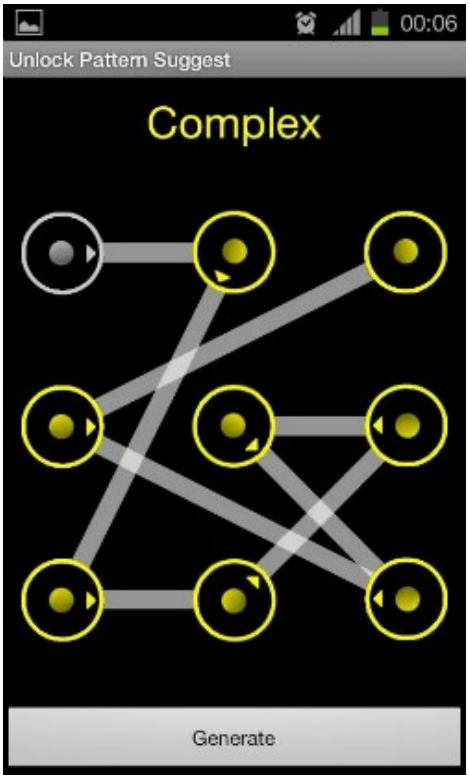
Sobald dies erledigt ist, kannst du zum Menü Sicherheit zurückkehren und auf “Smartphone verschlüsseln" oder "Tablet verschlüsseln” oder ähnliches klicken. Du solltest dein Smartphone an das Stromnetz anschließen und die Warnmeldungen lesen, und wirst mit ziemlicher Sicherheit deine Angaben bestätigen und PIN oder Passwort ein letztes Mal eingeben müssen, bevor der Verschlüsselungsvorgang beginnt.

Das Verschlüsseln deines Smartphones kann eine Stunde oder länger dauern, je nachdem, wie leistungsfähig dein Gerät ist und wie viele Daten du gespeichert hast. Sobald der Vorgang abgeschlossen ist, kannst du deine PIN eingeben und dein neu verschlüsseltes Gerät verwenden.

Zurück im Menü Sicherheit findest du wahrscheinlich auch eine Option zum Verschlüsseln von Dateien auf deiner microSD-Karte. Dies ist ein empfohlener Schritt, mit dem du alle deine Daten schützen kannst. Bitte beachte, dass bei Auswahl dieser Option die microSD-Karte in keinem anderen Gerät (wie einem Laptop oder einer Kamera) verwendet werden kann.

Mustersperre für Android-Handys

Ein ausreichend sicheres Kennwort kann schwer zu merken sein, und daher verwenden Benutzer in der Regel weniger sichere, kürzere Kennwörter. Bei allen Android-Geräten besteht jedoch die Möglichkeit, eine Mustersperre zum Entsperren des Smartphones zu verwenden. Dies ist eine hervorragende Option, weil komplexe Gesten oft leichter zu merken sind als Passwörter. Stelle sicher, dass das Muster aus mindestens 6 Linien besteht, und verwende ein 4x4-Gitter (oder ein dichteres Gitter). Ein 3x3-Gitter kann auch passend sein, vorausgesetzt, es ist ausreichend komplex. Hier ein Beispiel:



ANDROID-BACKUPS: EINE WARNUNG

Android-Geräte werden auf verschiedene Arten mit Remote-Backups synchronisiert. Alle sollten deaktiviert werden, um die Sicherung statt dessen auf einem lokalen Gerät (z. B. einem Laptop) durchzuführen, das selbst über eine vollständige Festplattenverschlüsselung verfügen sollte. Ein Abschnitt zur Laptop-Sicherheit wird in Kürze verfügbar sein. Bevor du eine Aktion durchführst, sollten Funktionen wie „SideSync“ von Samsung deaktiviert werden.

WICHTIG: Bist du ein App-Entwickler? Deaktiviere das USB-Debugging. Entwickler und Geeks verwenden häufig spezielle Funktionen, um ihr Smartphone mit Code zu manipulieren. Wenn beispielsweise das USB-Debugging aktiviert ist, besteht die reale Gefahr, dass ein Angreifer mit physischem Zugriff auf dein Gerät mithilfe der Adb-Tools von Android auf Inhalte zugreifen kann. Stell sicher, dass das USB-Debugging auf deinem Smartphone deaktiviert ist, bevor du eine Aktion durchführst!

MICROSD-KARTEN

MicroSD-Karten können einfach von einem Telefon entnommen, die Inhalte analysiert und kopiert werden. Geh unbedingt den gesamten Inhalt der Karte durch, bevor du eine Aktion ausführst. Geh davon aus dass alle Daten auf der Karte anfällig sind.

WICHTIG: Auch wenn dein Telefon verschlüsselt ist, ist dies bei deiner MicroSD wahrscheinlich nicht der Fall. Auf einigen Handys ist es möglich, Daten auf einer MicroSD-Karte zu verschlüsseln. Vergewissere dich bevor du eine Aktion ausführst, dass sich keine sensiblen Daten auf deiner MicroSD-Karte befinden, es sei denn sie sind verschlüsselt.

SICHER KOMMUNIZIEREN VOR UND WÄHREND AKTIONEN

Zwei Arten von Netzwerken

Heutzutage werden zwei Hauptnetze für die Sprach- und Textkommunikation mit anderen Personen über ein Handy verwendet: SMS und Sprachanrufe über ein herkömmliches Mobilfunknetz (GSM, CDMA) oder die Kommunikation über das Internet mithilfe von Apps und einem mobilen Datentarif (3G / 4G) oder eine lokale WiFi-Verbindung.

Wenn wir an einer Aktion teilnehmen, haben wir nur sehr selten den Luxus einer WLAN-Verbindung. Daher verwenden wir in der Regel die SIM-Karte in unserem Gerät, um eine Verbindung zu einem Mobilfunknetz herzustellen (zum Anrufen oder zum Senden von SMS), oder wir verwenden eine Datentarif mit einer App (wie Signal, Wire, Telegram oder WhatsApp).

SIM-Karten ähneln Kfz-Kennzeichen: Sie sind über den Vertrag mit deinem Mobilfunkanbieter an deine Identität gebunden, häufig auch an dein Bankkonto. Dies kann eine sehr schnelle Art sein, dich zu identifizieren. Überleg dir, eine anonyme Wegwerf-SIM-Karte in deinem Handy zu verwenden. Eine Wegwerf-SIM-Karte ist eine SIM-Karte, die bar und ohne Ausweisübergabe gekauft werden kann. Dies macht es für Überwachungsdienste und Dienstanbieter deutlich schwerer, Anrufe und SMS Nachrichten von deinem Gerät mit dir in Verbindung zu bringen. SIM-Karten können in vielen Ländern mit Bargeld und ohne Ausweis gekauft werden, aber nicht in allen. LycaMobile ist ein Beispiel für einen Betreiber in Deutschland, der solche SIM-Karten in Geschäften verkauft. Hilf deinen Kontakten, Wegwerf-SIMs zu verwenden, und schütze wo möglich deine SIM mit einem Passcode.

WICHTIG: Vermeide es, XR-bezogene Anrufe zu tätigen oder SMS-Nachrichten über ein Mobilfunknetz zu senden, sofern dies nicht unbedingt erforderlich ist. Gib niemals belastende und identifizierende Details über dein Handy weiter.

SICHER TELEFONIEREN MIT ENDE-ZU-ENDE-VERSCHLÜSSELUNG (E2EE)

Ende-zu-Ende-Verschlüsselung (englisch end-to-end encription: E2EE) is eine Art Datenschutz, bei der

die Daten für andere als die an beiden Enden kommunizierenden Personen nicht lesbar sind. Niemand auf dem Weg kann auf diese Daten zugreifen. Es gibt verschiedene Apps, mit denen du beim Telefonieren und Versenden von Kurzmitteilungen E2EE nutzen kannst. Bei allen diesen Apps ist es erforderlich, dass der beabsichtigte Empfänger deiner SMS oder deines Anrufs die App installiert hat und dass du ihn zu deinem App Adressbuch hinzugefügt hast.

WICHTIG: WhatsApp und Telegramm haben beide schwerwiegende Sicherheitsprobleme. Wir empfehlen nur Signal oder Wire für verschlüsselte Anrufe und SMS während unserer Aktionen oder bei deren Planung zu verwenden.

SIGNAL (OPENWHISPERSYSTEMS)

Signal hat in der Informationssicherheitsszene einen hervorragenden Ruf und wird immer mehr verwendet. Die Popularität basiert zum Teil auf der Kontakterkennung mit Hilfe von Handynummern. Du kannst einfach die Nummer eines Freundes eingeben und ihn zu Signal einladen. Du kannst auch über die Suchfunktion eine Freundin finden, die Signal bereits mit ihrer Nummer verwendet.

Signal verfügt über Gruppenchat-, Sprach- und Videoanruffunktionen und wird in XR-Filialen häufig verwendet, um geschäftskritische Kommunikationen zu sichern.

Das System der Verwendung von Handynummern ist allerdings für Aktivisten nicht ohne Risiken. Wenn dein Smartphone kompromittiert und / oder unzureichend gesichert ist, kann ein Gegner leicht herausfinden, mit wem du über Signal kommuniziert hast.

WICHTIG: Wenn du Signal verwenden möchtest, verwende eine Wegwerf-SIM-Karte (eine SIM-Karte, die du mit Bargeld und ohne Ausweisübergabe gekauft hast), sofern dies möglich ist. Außerdem solltest du die Signal Mustersperr-Funktion verwenden um den Zugriff auf die App und deine Kontakliste zu schützen.

Hier kannst du Signal für iOS und Android herunterladen. Beachte, dass es auch eine Desktop-Version der Software gibt.

WICHTIG: Installiere Signal nur dann auf deinem Laptop, wenn er ausreichend gesichert ist, weil alle deine Signal -Kontaktlisten und -Nachrichten auf deinem Laptop zugänglich sind.

WIRE

Im Gegensatz zu Signal ist Wire nicht auf eine SIM-Karte angewiesen. Wire bietet Chat, Sprach- und Videoanrufe sowie File Sharing. Eine besonders einzigartige Funktion ist die Unterstützung mehrerer Konten.

Was gegen Wire spricht, ist, dass es deutlich weniger verwendet wird als Signal. Das liegt zum Teil daran, dass eine stabile Version der Signal App bereits viel früher existiert hat. Ein weiterer Nachteil ist, dass man bei Wire kein Passwort und keine Mustersperre einrichten kann, um den Inhalt vor einem Angreifer zu schützen, der bereits Zugriff auf das Gerät hat.

Wire läuft unter iOS 10.0 oder Android 5.0 oder neuer. Wenn du ein älteres Gerät hast und kein Upgrade durchführen kannst, empfiehlt es sich Signal zu verwenden.

Beachte, dass es auch eine Desktop-Version von Wire gibt.

WICHTIG: Installiere Wire nur dann auf deinem Laptop, wenn er ausreichend gesichert ist, da alle deine Wire-Kontaktlisten und -Nachrichten auf deinem Laptop zugänglich sind.

Du kannst Wire hier herunterladen.

BRIAR

Briar ist das neuste im Bereich der Smartphone Anti-Überwachung, mit dem vielleicht einzigartigsten Angebot. Im Gegensatz zu allen anderen E2EE-verschlüsselten Messaging-Lösungen ist Briar nicht auf die herkömmliche Netzwerkinfrastruktur angewiesen. Es wurde für Aktivisten entwickelt und geht von Bedingungen aus, unter denen staatliche Behörden in der Nähe einer Aktion oder eines Protests Mobilfunk- oder WiFi-Netzwerke deaktiviert und / oder blockiert hat, wie es in der Türkei, in China, den USA und der Ukraine schon oft passiert ist, um nur einige zu nennen.

Dazu nutzt Briar die BlueTooth-Funktionalität die auf fast jedem Smartphone existiert, um Nachrichten in einem Mesh-Netzwerk von Gerät zu Gerät zu übertragen. Dies ist ein wesentlicher Vorteil bei koordinierten Bemühungen der Autoritäten, die Kommunikationsinfrastruktur für eine dauerhafte Aktion zu deaktivieren, sofern die Polizei nicht physischen Zugang zu allen Teilnehmern hat und ihre Geräte einfach beschlagnahmen kann.

Wenn der Zugang zum Internet verfügbar ist, nutzt Briar das anonymisierende Tor-Netzwerk und fügt damit eine zusätzliche Sicherungsebene hinzu, die bewirkt dass es nicht mehr nachweisbar ist, dass ein Gerät die Quelle einer Transaktion zu einem anderen Gerät war.

Du kannst Briar hier herunterladen.

SICHERER SMARTPHONE-LOGIN-SCHUTZ

Eine gute Übung um „an Sicherheit zu denken“, ist sich unser Handy in den Händen eines Gegners vorzustellen, der uns, unsere Gruppe oder Mitglieder unserer Gruppe belasten möchte.

REGELN FÜR ALLE SMARTPHONES

1. VERWENDE NIRGENDWO ANDERS DENSELBEN CODE WIE AUF DEINEM HANDY

Wenn du bei deiner Bank dasselbe Login verwendest, das du zum Entsperren deines Handys nutzt, und einem Ermittler im Zusammenhang mit einem Haftbefehl Zugang zu allen Daten deines Bankkontos gewährt wird (sehr häufig), kann dein Smartphone von der Polizei entsperrt werden. Aus diesem Grund ist es immer eine gute Idee, eine neues Passwort zu verwenden, vorausgesetzt, du möchtest ein Passwort und keine Mustersperre (Android) einrichten.

2. VERWENDE KEIN BIOMETRISCHES LOGIN (FINGERABDRUCK ODER GESICHTSERKENNUNG)

Wenn du verhaftet wirst, musst du davon ausgehen, dass sich die Polizei Zugang zu deinem Körper verschaffen kann, um sich bei deinem Gerät anzumelden. Es ist bereits vorgekommen, dass in Frankreich festgenommenen Rebellen von Polizeibeamten festgehalten und ihre Handys entsperrt wurden, sowohl über Gesichtserkennung als auch Fingerabdruck. Diese Anmeldemethoden sollten von Aktivisten vermieden werden.

3. PASSWÖRTER NIEMALS UNVERSCHLÜSSELT ODER IN DER CLOUD SPEICHERN, SONDERN NUR VERSCHLÜSSELT AUF DEINER FESTPLATTE

Es ist vorteilhaft, ein Backup für Passwörter auf einem Handy oder Computer zu haben, aber sehr nachteilig, wenn ein Gegner Zugriff darauf hat. Verwende keine Dienste wie LastPass oder iPassword, da sie deine Passwörter im Netz speichern. LastPass wurde bereits gehackt und gefährdet unzählige vertrauensvolle Nutzer. Obwohl iPassword nach eigenen Angaben nicht in der Lage ist, deine Passwörter zu entschlüsseln, musst du dem Unternehmen vertrauen. Du legst deine Sicherheit in die Hände von Menschen, denen du noch nie begegnet bist, in die Hände einer Firma in einem Land, das unter seiner eigenen Gerichtsbarkeit zur Zusammenarbeit mit Strafverfolgung und Ermittlern des Bundes verpflichtet ist.

Verwende unbedingt einen Offline-Passwort-Manager wie KeePass oder KeePassXC, der Passwörter verschlüsselt und auf deinem Gerät (wie einem Laptop) unter deiner Kontrolle speichert.

Es ist im Prinzip kein Problem, Passwörter auf einem SmartPhone oder Laptop zu speichern, aber nur, wenn du eine sichere Methode verwendest.

CHECKLISTE FÜR ORTS/LANDESGRUPPEN VOR FESTNAHMEN

1. PLATFORM-ADMINS UND SYSADMINS SOLLTEN NICHT ZU AKTIONEN GEHEN

Dies mag für Administratoren sehr enttäuschend sein. Sie sind aber als besonders wertvolle Ziele zu betrachten, und wenn sie der Polizei bekannt sind, können sie extremer Nötigung und / oder Inhaftierung ausgesetzt sein. **Insbesondere Sysadmins sollten keine Aktionen durchführen.** Außerdem ist ein Administrator im Gefängnis für seine Gruppe nicht verfügbar, was für deren Operation katastrophal sein kann. Sysadmins und Plattform-Admins sollten die ganze Zeit online sein, um bei Plattformsperrungen zu helfen (siehe unten).

2. NOMINIERT SPERR-KONTAKTE

Jede Orts-/Landesgruppe sollte einen oder mehrere Passwort Sperr-Kontaktpersonen benennen, deren anonymisierte Kontaktdaten auf jedem Handy verfügbar sind, das für eine Aktion verwendet wird. Es ist Aufgabe der Rebellen sicherzustellen, dass Plattform-Administratoren und Sysadmins über Sperr-Kontakte sofort über Verhaftungen informiert werden, sodass alle Anmeldesitzungen widerrufen und die Passwörter geändert werden. Die Sperr-Kontakte sollten während der gesamten Aktion an einem sicheren Ort mit guter Bandbreite / Verbindung sein. Sie müssen die ganze Zeit erreichbar sein.

Es ist Aufgabe der Gruppen, ihr eigenes Protokoll für die Kontosperrung zu definieren.

3. DESIGNIERTE SMARTPHONE TRÄGER

Besprecht in euren XR-Gruppen die Möglichkeit, Smartphone-Träger zu bestimmen, um Aktionen zu dokumentieren, zu koordinieren, zu streamen und in sozialen Medien usw. zu veröffentlichen so dass andere an der Aktion beteiligte Rebellen ihre Handys nicht mitzubringen brauchen. Dies hilft das Risiko zu mindern, dass Daten in die falschen Hände gelangen.

4. STUDIERT DIE RECHTSLAGE

Alle Orts/Landesgruppen sollten ein Rechtsteam einsetzen, das zum Zeitpunkt der Festnahme speziell an den Rechten der Rebellen arbeitet. Rebellen können nur dann sicher festgenommen werden, wenn sie ihre Rechte kennen. Ein Rebell, der nicht weiß, dass es illegal ist, physisch gezwungen oder gedrängt zu werden, die Anmeldedaten an sein Telefon weiterzugeben, wird dies wahrscheinlich tun. Ein Teil der gegenseitigen Fürsorge besteht darin, sicherzustellen, dass wir alle auf einer Seite sind un zuversichtlich sein können, dass wir unsere Rechte kennen, und nicht durch Lügen dazu gebracht werden, die Sicherheit unserer Mit-Rebellen zu gefährden.

WICHTIG: Es ist sehr wichtig, dass ihr euch für euren Zuständigkeitsbereich darüber informiert, ob es gegen das Gesetz ist, ein Passwort zum Zeitpunkt der Festnahme den Strafverfolgungsbehörden vorzuenthalten. Wenn dies der Fall ist, ist es wichtig, dass alle Rebellen dies wissen und dass alle Geräte mit vertraulichen Informationen nicht zu einer Aktion mitgenommen werden, egal ob verschlüsselt oder nicht. Das Zurückhalten von Informationen von

Strafverfolgungsbehörden - „Behinderung von Rechtsverfahren“ - ist im Allgemeinen eine Straftat, die weitaus schwerwiegender ist als das Sperren einer Straße und die in manchen Rechtsräumen mit mehreren Jahren Gefängnis bestraft werden kann

CHECKLISTE FÜR REBELLEN VOR VERHAFTUNGEN

1. Wenn du nicht viel Zeit hast, versuche nicht, jemanden anzurufen, auch nicht deinen Sperr-Kontakt.

Was "viel Zeit" ausmacht, ist natürlich subjektiv, aber solange du ausreichend Zeit hast, zögere nicht, diesen Anruf zu tätigen. Wenn nicht, beende den Vorgang und fahre mit Schritt 2 fort.

2. DRÜCK DIE EIN/AUS-TASTE AUF DEINEM HANDY UND STELL SICHER, DASS ES AUSGESCHALTET IST, BEVOR DU ES ÜBERGIBST

Wenn du Grund zur Annahme hast, dass dein Smartphone möglicherweise in die Hände von Strafverfolgungsbehörden oder Ermittlern gelangt, halte den Ein- / Ausschalter gedrückt und schalten es aus. **Nur wenn ein verschlüsseltes Telefon ausgeschaltet ist, sind die Daten geschützt.**

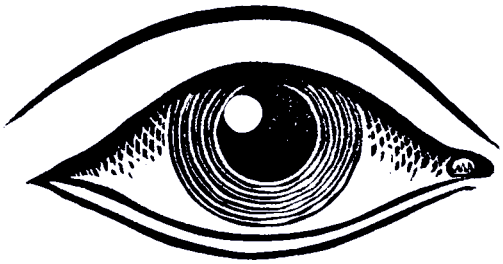
3. DENK AN DEINE RECHTE

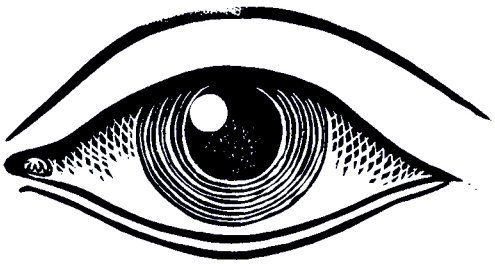
Mach dir deine Rechte bewusst, auch wenn dies schwer ist, während du gerade weggetragen/-gezogen wirst. Sage deine Rechte zu dir selbst, bevor du ein Wort zur Polizei sagst.

WICHTIG: Wenn dir die Polizei dein Handy zurückgibt und es nicht verschlüsselt ist, solltest du es als kompromittiert und somit vollständig übergeben betrachten. Malware-Implantate werden immer häufiger in Handys von Aktivisten eingesetzt. Sie erlauben es Ermittlern dich ausspionieren, dein Mikrofon zu aktivieren oder Daten von deinem Telefon zu kopieren.

DU LÄSST DEIN HANDY ZUHAUSE?

Du hast dich entschieden, dein Handy zu Hause zu lassen? Hervorragend! Damit verhinderst du nicht nur, es an die Polizei zu verlieren, sondern verringerst auch das Risiko, dass all deine Konten und Kontakte für diejenigen offengelegt werden, die sie möglicherweise gegen dich und / oder andere Rebellen verwenden würden. Bitte verschlüssle dein Gerät trotzdem. Nachträgliche Festnahmen sind Realität. Durch das Verschlüsseln eines Smartphones ist der Inhalt für andere Personen quasi unerreichbar – solange das Telefon zuerst ausgeschaltet wurde.





NACHWORT

Dieser Leitfaden befindet sich noch im Entwurf. Er ist ausschließlich dazu gedacht, Rebellen an vorderster Front bei (und im Vorfeld von) Aktionen zu schützen.

Die Routenverschlüsselung mit einem VPN, die Anti-Tracking- und XSS-Minderung, die Erkennung von Stingray- und Rogue-Zelltürmen, Anonymitäts-Apps wie Orfox, benutzerdefinierte ROMs wie LineageOS mit MicroG für ein De-Google-Setup, EXIF-Bereinigung usw. werden nicht berücksichtigt Dieses Dokument richtet sich an Nicht-Geeks und wird in der globalen Datenbank in der Kategorie Betriebssicherheit weiter behandelt.

Wenn du Vorschläge zu Verbesserungen oder Ergänzungen hast, schreib bitte an support@organise.earth.