Digitale Sicherheit

Wir haben im Moment leider keine Ressourcen um das Wiki auf aktuellem Stand zu halten. Informationen sind deswegen mit Vorsicht zu genießen. Falls du beim Wiki weiterarbeiten willst, melde dich doch bitte bei uns.

Hier findest du:

- Informationen zur Nutzung von digitalen Kommunikationsmitteln, Umgang mit Daten, deinem Computer und deinem Handy.
- Programmempfehlungen für Handy und Computer.
- Hintergründe und Erklärungen zu Informationstechnologie und Programmen.

Sicherheitspläne - Get going!

Dein persönlicher Sicherheitsplan
Du weisst eh, dass du das mal angehen solltest aber schiebst es immer wieder vor dir her? Du setzt dich neu mit dem Thema auseinander? Wir machen mal nen Vorschlag wie du deine Digitale Sicherheit möglichst sicher und solidarisch gestalten kannst.
Gruppensicherheit
Solidarität ist unsere stärkste Waffe! Also müssen wir einen gemeinsamen Umgang zu digitaler Sicherheit entwickeln. Eure Sicherheit ist nur so stark wie das schwächste beschlagnahmte Telefon.

Anleitungen - Get your Shit together!

Smartphone Sicherheit

Sichere Kommunikation

Aufbewahrung von Daten & Verschlüsselung

Sicheres Surfen & Anonymität

Passwortsicherheit

Digitales Zusammenarbeiten

Verpixeln und (Meta)-Daten löschen

Social Media

Systemli-Kollektiv: Wir möchten auf *Systemli* aufmerksam machen! *Systemli* ist ein linkes Tech-Kollektiv und bietet ihre wichtigen Services für Aktivist*innen unentgeltlich an – du kannst dir aber durchaus überlegen dem Kollektiv Geld zukommen zu lassen für ihren Aufwand.
Sie haben auch ein sehr empfehlenswertes Wiki zu digitaler Sicherheit.

Warum wir uns alle mit digitaler Sicherheit auseinandersetzen sollen

Dieses Wiki soll euch einen Überblick bieten, welche Sicherheitsrisiken im Umgang mit digitalen Kommunikationskanälen, Speicherung von Daten und Nutzung von Informationstechnologien verbunden sind. Wir möchten euch dabei unterstützen, Maßnahmen zur digitalen Selbstverteidigung zu ergreifen, damit ihr euch vor unerwünschten Zugriffen auf eure Daten und eure Kommunikation schützen könnt. In diesem Wiki findet ihr Hintergrundtexte, konkrete Anleitungen und Handlungsempfehlungen zum Umgang mit digitaler Sicherheit im politischen Alltag und in der politischen Praxis.

Und warum das alles?
Die Nutzung von Informationstechnologien prägt unseren Alltag: Wir lesen auf dem Mobiltelefon Emails, Whatsapp- und Signal-Nachrichten. Wir telefonieren mit Freund:innen über Skype, nehmen an Gruppenkonferenzen über Jitsi, Mumble und Microsoft Teams teil. Das Telefon ist gleichzeitig Digitalkamera, Fotoalbum und Kalender. Am Computer liegen Texte und Fotos. Der Internetbrowser (Firefox, Chrome oder Opera) merkt sich die Adressen von aufgerufenen Internetseiten. Google kopiert automatisch alle Kontakte und speichert Dokumente in der Google Cloud, also auf den Computern von Google, ab. In der Schublade liegen eine handvoll USB-Sticks und eine externe Festplatte für Backups liegt auch am Tisch. Daneben liegt das alte Mobiltelefon, dessen Bildschirm gebrochen ist. Diese Beispiele zeigen, wo überall deine Daten herumliegen. Sie können möglicherweise in falsche Hände geraten. Nehmen wir das Handy mit dem kaputten Bildschirm als Beispiel: Obwohl das Handy „kaputt“ ist, kann der Datenspeicher im Handy natürlich immer noch gelesen werden. Wenn du das Protokoll eines Treffens öffnen willst und dieses wird im Zuge dessen von deinem Computer zu Google hochgeladen, dann bedeutete das, dass Google Zugriff auf dieses Plenums-Protokoll hat. Die Beispiele, in denen digitale Sicherheit eine Rolle spielt, sind unzählig. In diesem Text gehen wir kurz auf drei Aspekte ein, warum Datensicherheit in unserer politischen Praxis und unserem politschem Alltag wichtig ist. Weiters wollen wir Überlegungen zu unserem politischen Zugang zu dem Thema mit euch teilen.

Warum ist Datensicherheit und Kommunikationssicherheit wichtig?

Datenschutz
Viele nehmen den Schutz ihrer Daten nicht ernst: Wer hat nicht schon die Aussagen gehört: „Ich habe ja nichts zu verbergen„. Wir sagen, diese Aussage ist falsch, denn: Alle Menschen haben etwas zu verbergen, die Frage ist nur, in welchen Situationen und vor wem. Außerdem betrifft der unsichere Umgang mit den „eigenen“ Daten meist nicht nur einen selbst, sondern auch andere Personen: Bei

einer Messenger-Konversation habe ich auch immer ein Gegenüber, auf Fotos bin oft nicht nur ich selbst abgebildet, das Plenumsprotokoll meiner Politgruppe betrifft alle involvierten Aktivist:innen. Dein Umgang mit deinen Daten betrifft nicht nur dich selbst, sondern auch alle Menschen mit denen du zu tun hast. Beispielsweise verrät dein Facebook-Profil nicht nur etwas über dich, sondern auch über deine Freund:innen. Das Facebook-Profil von Politgruppen hat auch schon dazu beigetragen, dass Personen, die es geliked haben, von der Polizei wegen (angeblicher) Straftaten ausgeforscht wurden. Das sollte uns allen bewusst sein. Staaten sind bestrebt, die Kontrolle von Internetkommunikation immer weiter auszubauen, wie etwa bei der Vorratsdatenspeicherung oder bei aktuellen Versuchen Ende-zu-Ende-Verschlüsselung gesetzlich zu erschweren oder zu verbieten. Wir verstehen das als massive Eingriffe in die persönliche Freiheit und obwohl manche Maßnahmen als Schutz angepriesen werden, bedeutet es eine Normierung von Verhalten in der Gesellschaft: Im Endeffekt läuft es darauf hinaus, dass alle zu jedem Zeitpunkt verdächtig sind, bis sich ihre Unschuld herausgestellt hat.

Überwachungsgesellschaft

In der Schule, mit der Familie und am Arbeitsplatz bekommt das Thema Überwachung/Repression durch technische Entwicklungen neue Dimensionen: Ich kann meinen Job verlieren, wenn ich online poste, dass mir die Arbeit keinen Spaß macht. Am Arbeitsplatz hält Digitalisierung Einzug und damit auch neue Kontrollmechanismen. Sieht mein Arbeitgeber, welche Webseiten ich während der Arbeitszeit aufgerufen habe? Oder wird überprüft, ob ich tatsächlich vorm Bildschirm sitze? Eltern kontrollieren die Aktivitäten ihrer Kinder mit Überwachungsapps – “zu ihrem Schutz, falls was passiert”. So ist es für Eltern jederzeit möglich, nachzuschauen, wo sich das Kind gerade aufhält. Der Begriff „digitale Gewalt“ wurde vor kurzem von feministischen Initiativen eingeführt, um das Phänomen zu beschreiben, dass durch die Digitalisierung unseres Lebens auch Gewaltbeziehungen betroffen sind.Täter verwenden neue Technologien, um Kontrolle über Betroffene auszuüben und sie zu schickanieren. Dies kann beispielsweise über das Bloßstellen auf Sozialen Medien, wenn Fotos der Betroffenen geposted werden, durch die Übernahme von Profilen, wenn dem Täter das Passwort bekannt war oder durch ständige Kontaktaufnahme oder Kontrolle über Überwachungsapps geschehen. Unternehmen erstellen Profile von uns, um uns angepasste Werbung zu schicken. Die technischen Entwicklungen betreffen alle unsere Lebensbereiche. Unangepasstes Verhalten kann unmittelbar über verschiedene Plattformen der Öffentlichkeit zugänglich gemacht werden und Personen bloßstellen. Um mit diesen Situationen selbstbestimmt umgehen zu können, müssen wir lernen, wie wir sicher mit unseren Handys, Computern und diversen Internetdiensten umgehen können.

Staatliche Repression

Bei Repression durch den Staat und seine Behörden ist der Fantasie der Beamt:innen selten Grenzen gesetzt: Die leeren Bierflaschen werden zu vermeintlichen Wurfgeschossen, das Plakat vom linken Straßenfest wird als Zugehörigkeit einer vermeintlich kriminellen Vereinigung ausgelegt. Diese Fantasien gefährden uns und unsere Freund:innen, politischen Mitstreiter:innen oder auch komplett unbeteiligte Personen, an die wir gar nicht denken. Neben der Verfolgung von konkreten Vorwürfen geht es den Beamt:innen nämlich auch sehr oft darum, möglichst viel Informationen über politische Zusammenhänge zu sammeln: Über unsere Gruppen, Netzwerke, Zusammenhänge, Aktionen, Freundschaften, undundund. Informationen über persönliche Beziehungen werden in polizeilichen Einvernahmen genutzt, um die vernommene Person zu verunsichern. Schaffen es Beamt:innen ein Handy in unverschlüsseltem Zustand wegzunehmen, ist das für sie eine reine Goldgrube. Bewegungsprofile können erstellt werden und schnell bist du verdächtig, weil du auf bestimmten Demonstrationen warst. Wenn ich mich in antikapitalistische, antirassistische, antifaschistische, feministische und andere emanzipatorische Kämpfe einbringe, sollte ich mich daher grundlegend mit digitaler Sicherheit auseinandersetzen.

Unser politischer Zugang zum Thema digitale Sicherheit

Gemeinsam besprechen und handeln
Du bist nicht allein – im doppelten Sinne: Es braucht unter Umständen nur ein unsicheres Gerät in den falschen Händen, um die Kommunikation und Inhalte einer ganzen Gruppe offen einzusehen. Unser eigenes Verhalten wirkt sich also auch auf andere aus, daher bedenke: Es geht nicht nur um deine eigene Sicherheit! Du bist aber auch nicht allein, dich darum zu kümmern, dass mit deiner digitalen Sicherheit alles passt! Es ist die Verantwortung einer politischen Gruppe praktikable Sicherheitskonzepte zu überlegen und einen niederschwelligen Zugang zum Thema Sicherheit allgemein zu gewähren. Und natürlich auch konkret Hilfe und Erklärungen anzubieten! Das beste Programm ist nur so sinnvoll, wie es auch von allen gut verwendet werden kann. Gemeinsam auszuprobieren und nach Lösungen zu suchen kann auch lustvoll und inklusiv sein. Und vor allem braucht sich echt niemand schlecht fühlen, etwas nicht zu wissen!

Selbstermächtigung
Bei vielen löst das Thema digitale Sicherheit, Handy und Computer verschlüsseln und Kommunikationssicherheit große Widerstände aus oder sie sind verunsichert, ob sie sich überhaupt zutrauen. Das Einrichten von sicheren Lösungen für Computer, etc und sich bewusst darüber werden, was sicher ist und was ein Problem darstellt, ist oft gar nicht so schwer, wie es scheint. Wichtig ist auch, die Berührungsängste zu dem Thema zu verlieren. Wir wollen mit diesem Wiki einen leichten und unbeschwerten Zugang schaffen, sich mit dem Thema digitaler Sicherheit zu beschäftigen sowie euch bei der Umsetzung von Lösungen für euch selbst und politische Gruppen unterstützen. Eine Auseinandersetzug mit diesem Thema bedeutet, sich selbst zu ermächtigen.

Werden wir unbequem
Wir verstehen, dass es durchaus bequem ist, sich von Google-Maps durch die Welt leiten zu lassen: Der Umstand, dass mit den Grundeinstellungen von Google dein Bewegungsablauf auch gleich online gespeichert wird, ist jedoch gruselig. Auch der Aufwand sichere Passwörter zu verwenden, diese auswendig zu lernen oder sicher zu verwalten, scheitert oft an der Bequemlichkeit. Aber wieder gruselig: Es dauert mit Hilfe von entsprechender Software nur wenige Minuten ein kurzes Passwort zu knacken. Unsere Bequemlichkeit steht uns oft dort im Weg, wo digitale Sicherheit eine Rolle spielen sollte. Dies sollten wir ändern und praktikable Lösungen dafür finden, Sicherheitsstandards in unseren Alltag zu integrieren. Technische Möglichkeiten verändern sich laufend, daher reicht es auch nicht aus, einmal die Festplatte zu verschlüsseln oder einen sicheren Messenger zu installieren, denn was heute als sicher gilt, kann in naher Zukunft schon wieder unsicher sein. Digitale Sicherheit bedeutet für uns daher auch, dass wir uns kontinuierlich damit auseinandersetzen.