Esc-It

esc-it logo

esc-it (gesprochen escape it oder escape IT) ist ein Kollektiv welches Inhalte für IT-Sicherheitstrainings für Aktivist*innen erstellt. Zielgruppe sind Aktivist*innen und Trainer*innen im Kontext des politischen Aktivismus.

Warum es uns gibt

In der linken Szene in Deutschland gibt es ein Bedürfnis sich vor der zunehmenden staatlichen Überwachung und digitalen Formen der Repression zu schützen. Dies führt teilweise zu Unsicherheit und Paranoia aber auch zu Resignation. Aufklärung und Bildung kann dem entgegenwirken und Menschen ermächtigen selbstbestimmt und informiert zu entscheiden, wie Sie mit digitaler Überwachung umgehen wollen.

Da es nur wenige Gruppen gibt welche IT-Sicherheitstraining mit spezieller Ausrichtung auf Aktivist*innen anbieten hat sich esc-it gegründet. Bei der Suche nach Material ist aufgefallen, dass es für Trainings zu IT-Sicherheit nur wenig öffentlich zugängliches Material gibt, welches auf politisch aktive Menschen und den deutschsprachigen Raum ausgerichtet ist. Die Materialien die es gibt sind teilweise auf spezielle Problemstellungen fokussiert und lassen sich daher nicht in ein zusammenhängendes Konzept eingliedern, sind nicht didaktisch aufbereitet, veraltet oder auf andere Regionen / Gesetzgebung ausgerichtet.

Deshalb haben wir begonnen eigene Materialien zu erstellen. Hiermit wollen wir nicht den Eindruck erwecken, dass alle anderen Materialien nicht zu gebrauchen sind. Wir haben uns lediglich Gedanken gemacht was uns für die Materialien wichtig ist und versuchen dies hier umzusetzen.

Menschen abholen

Wir möchten Menschen dort abholen, wo sie sind und sie dabei Unterstützen für sich passende Schutzmaßnahmen umzusetzen. Dem in der Technik- und Datenschutzszene so verbreitete Muster, andere Menschen für Ihren Technikkonsum zu verurteilen und für die eigenen Verhaltensweisen zu missionieren wollen wir nicht folgen. Kommunikation auf Augenhöhe ist uns wichtig.

Konkret heißt das beispielsweise, dass wir Aktivist*innen gerne auch dabei helfen ihre Computer mit Windows oder macOS abzusichern und nicht etwa grundsätzlich versuchen, sie davon zu überzeugen Linux zu verwenden. Aus Sicht des Datenschutzes mag Linux zu bevorzugen sein, aber nicht unbedingt aus Sicht der Sicherheit. Klar ist auch, dass Menschen das Betriebssystem am

besten sicher verwenden können, mit dem sie sich auskennen. Der Umstieg auf Linux ist damit für viele eine zusätzliche Hürde und senkt damit die Wahrscheinlichkeit, dass diese Veränderung angenommen wird. Und wenn es nicht angenommen wird, hilft es am Ende auch nicht.

Zudem ist es einfach scheiß tech bro Verhalten.

Selbstverständlich heißt das nicht, dass wir zu sicherheitsrelevanten Themen keine entsprechenden Empfehlungen aussprechen. Beispielsweise ist ein Ende-zu-Ende verschlüsselter Messenger einem vorzuziehen, der nicht Ende-zu-Ende Verschlüsselt ist. Das Ziel einer solchen Empfehlung ist jedoch zu informieren, sodass eine selbstbestimmte Entscheidung getroffen werden kann.

Fokus auf Selbstermächtigung

Unser Anspruch ist es, Aktivist*innen so zu bilden, dass sie selbstständig entscheiden können in welcher Situation sie sich wie vor digitaler Überwachung schützen wollen. Deshalb priorisieren wir ein grundsätzliches Verständnis über konkrete Handlungsempfehlungen.

Dafür gibt es mehrere Gründe. Es beginnt damit, dass wir für passende Empfehlungen wissen müssten was ihr macht. Das wollen wir allerdings gar nicht wissen. Zudem können sich Verhältnisse ändern, und damit auch Empfehlungen. Eine konkrete Software mag heute noch zu empfehlen sein, vielleicht wird sie aber bald grundsätzlich verändert, verkauft oder sie wird schlicht von neue staatliche Überwachungsmöglichkeiten eingeholt.

Ihr selbst könnt am besten Einschätzen, welche Gegenmaßnahmen die richtigen für euch sind. Daher sehen wir die Methode der Bedrohungsmodellierung als Grundlage an. Um diese Anwenden zu können müsst ihr jedoch auch wissen welche Bedrohungen und Gegenmaßnahmen es gibt. Daher versuchen wir diese aufzulisten und zu erklären.

Realistisches Bedrohungsbild

Zudem müsst ihr für die Bedrohungsmodellierung wissen, wie wahrscheinlich das Eintreten einer Bedrohung ist. Dies ist für staatliche Überwachungsmaßnahmen nicht genau zu beziffern. Dennoch versuchen wir beispielsweise durch Statistiken und Fallbeispiele eine faktenbasierte Einschätzung zu ermöglichen.

Didaktisch aufbereitet

Unser Ziel ist es Wissen zu vermitteln. Daher bemühen wir uns Inhalte so aufzubereiten, dass sie auch für Laien möglichst verständlich sind. Fremd- und Fachwörter versuchen wir zu vermeiden oder sie verständlich zu erklären.

Wir möchten Themen nicht nur sachlich erklären, sondern auch didaktisch aufbereiten. Beispielsweise durch Grafiken, Präsentationen oder interaktive Elemente wie Aufgaben oder Spiele.

Alle Materialien sollen sich zu einem ganzheitlichen Konzept zusammenfügen.

Aktuell und geprüft

Auch wir wissen natürlich nicht alles. Um Fehler in unserem Material zu vermeiden, gehen alle Inhalte vor der Veröffentlichung durch einen Review-Prozess. Für die Veröffentlichung muss mindestens eine zweite Person zustimmen.

Dennoch können Fehler passieren. Falls euch etwas auffällt, freuen wir uns über Hinweise. Am besten erstellst du hierfür einen Issue in unserem git-Repository oder schreibst uns eine Mail.

Damit das Material inhaltlich korrekt bleibt, haben wir auch den Anspruch es aktuell zu halten. Wie gut das funktionieren wird muss sich noch herausstellen.

Offene Lizenz

Alle Materialien, welche wir selbst erstellen, stehen unter einer freien Lizenz. Wenn wir externe Inhalte verwenden, versuchen wir auch hierbei möglichst Inhalte unter freien Lizenzen zu verwenden.

Damit wollen wir sicherstellen, dass Alle unser Material verwenden und verändern können. Das hilft auch dabei das Material aktuell zu halten, denn falls wir das nicht mehr tun könnte das so von anderen übernommen werden.

IT-Sicherheit als Form von Anti-Repression und Solidarität

Wir möchten vermitteln, dass IT-Sicherheit in politischen Kontexten meistens nicht nur dich selbst betrifft. Auch andere kann es betreffen, wenn du mit Informationen nicht verantwortungsvoll umgehst.

Entsprechend betreffen die Entscheidungen die du hierzu triffst nicht nur dich. Daher solltest du dir überlegen, ob du Betroffene in diese Entscheidungen einbeziehst. Beispielsweise bietet es sich für Gruppen an, sich gemeinsam Gedanken über ein standardisiertes Sicherheitslevel und Maßnahmen zu machen.

Mit IT-Sicherheit schützt du dich und andere. Daher ist es Bestandteil von Anti-Repression.

Version #2
Erstellt: 14 Januar 2025 18:53:13 von ESC-IT Migration Bot
Zuletzt aktualisiert: 11 Februar 2025 13:17:48 von ESC-IT Migration Bot