MARIA
Der Protest letzte Woche war ein riesiger Erfolg!
Schaut euch nur dieses Video von all diesen Menschen an, die für unsere Sache kämpfen.

ALEX
Stellt euch nur vor, wie viele es noch sein werden, wenn wir deine genialen Aufnahmen in den sozialen Medien teilen.

SARAH
Moment mal, Alex. Wir können dieses Video nicht einfach online stellen.

MARIA
Was? Wieso nicht?

SARAH
Weil man darauf zu viele identifizierbare Merkmale erkennen kann. Zum Beispiel Gesichter oder Tattoos, das könnte diejenigen belasten, die uns an dem Tag unterstützt haben.

SARAH
Und was ist außerdem mit den Metadaten* deines Videos? Sie zeigen das Datum und die Uhrzeit der Aufnahme an. Sogar deine genauen GPS-Koordinaten, falls das aktiviert ist. Willst du wirklich all diese Informationen einfach so weitergeben?

TEXTBOX
*Externe Daten, die Details zu einer Datei liefern. Sie werden zusammen mit ihr gespeichert und weitergegeben. Die meisten Geräte erstellen sie automatisch.

SARAH
Erinnerst du dich, was Daniel passiert ist? Er wurde auf einer Aufnahme von unserer letzten Protestaktion erkannt und verhaftet.

MARIA
Ich habe gehört, dass seine Eltern auch eine Menge bedrohlicher Nachrichten bekommen haben. Ich will auf keinen Fall, dass meinen so etwas passiert.

ALEX
Solche Dinge sind unvermeidlich. Glaubt ihr, ich bekomme keine Drohungen oder fiesen Kommentare?

Der Punkt ist: Ich kann damit umgehen. WEIL ich weiß, wie viele andere meine Ideale teilen. Ich bin es ihnen schuldig, mich nicht einschüchtern zu lassen!

SARAH
Wir sind es ihnen aber auch schuldig, niemanden in Gefahr zu bringen.

ALEX
Newsflash: Aktivismus ist hier gefährlich! Was sollen wir also tun? Einfach schweigen und still sein?

Denkst du nicht, dass das genau IHR Ziel ist?

SARAH
Niemand hier sagt das. Ich sage nur, dass wir vorsichtig sein müssen.

Alex, ich fange an zu glauben, dass dich die Online-Belästigungen mehr mitnehmen, als du zugibst.

ALEX
Und was ist mit dir? Du bist immer die Erste, die unsere Ideen aus Sicherheitsgründen ablehnt, seit das mit Daniel passiert ist.

Glaubst du, ich merke nicht, wie du jedes Mal schaust, wenn du dein Handy checkst? Ihre Einschüchterung funktioniert! Sie haben dir Angst gemacht!

SARAH
Du weißt genau so gut wie ich, wie schnell sich Online-Aktivitäten heutzutage auf die reale Welt auswirken.

ALEX
Aber das sollte uns nicht davon abhalten, die harte Arbeit unserer Freund*innen zu würdigen!

ALEX
Also Maria hat es mit den Metadaten ziemlich vermasselt. Ich zeig ihr jetzt, wie man sie löscht.

MARIA
Woah!

ALEX
Ich muss vorsichtiger sein, wenn ich Fotos und Videos mache, damit niemand einfach so identifiziert werden kann.

ALEX
Maria, es tut mir leid. Ich bin so ein Idiot. Du warst da draußen großartig, ich wollte nur…
MARIA
Schon gut, Ich glaube, wir sind alle angespannter, als wir dachten.

SARAH
Wir sollten uns alle beruhigen. Ich kenne ein tolles Café. Lasst uns mal für einen Moment abschalten.

Wir können später immer noch überlegen wie wir das Video bearbeiten können, um Gesichter unkenntlich zu machen und die ursprünglichen Metadaten zu entfernen.
MARIA
Klingt gut. Ich deaktiviere nur schnell den GPS-Zugriff meiner Kamera.

NACHRICHT
„Du kleine SCH*****, pass lieber auf, wo du hingehst.“

MARIA (DENKT)
Durchatmen, Maria. Ruhig bleiben. Es ist nur eine weitere Nachricht.
TEXTBOX
Das Internet ist unberechenbar und vergisst nie. Sei achtsam mit dem, was du hochlädst.

MARIA (DENKT)
Und doch… Körperliche Gewalt… Digitale Gewalt… So weit sind sie nicht voneinander entfernt, oder?
TEXTBOX:
Wenn einmal etwas ins Internet gestellt wurde, ist es schwierig, es vollständig zu löschen, da Kopien häufig auf verschiedenen Servern gelagert werden und von anderen unendlich geöffnet und geteilt werden können.

STÄRKUNG DEINER DIGITALEN FESTUNG

TEXTBOX
Einige Tage nach dem Protest…
MARIA
Hey Sarah. Ja, ich bin gerade nach Hause gekommen.

Waaaas?!

Ich habe noch nichts gepostet. Ich war den ganzen Tag über nicht online

MARIA
Eigentlich wollte ich mich gerade einloggen, um…
PC
ZUGRIFF VERWEIGERT. Ihr Benutzername oder Passwort sind falsch.

Hä?

MARIAS ACCOUNT
“Ohne Witz, der Protest war echt lahm. Kannst halt nix kaputtmachen mit nur ein paar dutzend Verlierern.“
MARIA
Nein! Ich wurde gehackt?! Das kann doch nicht wahr sein!
SARAHS STIMME DURCH DAS TELEFON
Ich bin auf dem Weg.

SARAH
Also stimmt es. Ich fand deine plötzliche Meinungsänderung heute Morgen seltsam, also habe ich alle gewarnt, keine Nachrichten von dir zu öffnen – falls sie Schadsoftware enthalten, die weitere Accounts kapern könnte.
MARIA
Uff, ich hätte euch alle in Schwierigkeiten bringen können. Was mache jetzt nur?

SARAH
Erstmal: Keine Panik! Die meisten Webseiten haben einen Support, den du in solchen Fällen kontaktieren kannst.

Gib ihnen so viele Details wie möglich – deinen Benutzernamen, die ursprünglich mit dem Account verknüpfte E-Mail-Adresse und das Datum, an dem du dich zuletzt eingeloggt hast.

MARIA
Die Wahrheit ist… Es geht nicht nur um diesen Account. Ich benutze für alles dasselbe Passwort. Man braucht heutzutage für so viele Dinge einen Account, und ich kann mir all diese Buchstaben und Zahlen einfach nicht merken…
SARAH
Nun, in diesem Fall… würde ich sagen, wir ändern das jetzt sofort.

SARAH

Das Internet ist ein unglaubliches Werkzeug, aber um sicher unterwegs zu sein, ist es wichtig, seine persönlichen Daten vor den falschen Leuten zu schützen. Bei Passwörtern gibt es ein paar Dinge zu beachten. Viele gezielte Hacks nutzen Bots, die Passwörter durch reines Ausprobieren erraten. Diese Bots sind automatisierte Programme, die hunderte von Passwörtern pro Minute testen, bis sie das richtige finden.

TEXTBOX

Bot: Erledigt digitale Fleißarbeit für seine Menschen – auch für die Kriminellen.

SARAH

Die gute Nachricht ist: Je länger das Passwort ist, desto mehr Versuche werden benötigt. Das bedeutet, dass die Länge das wichtigste Sicherheitsmerkmal eines Passworts ist.

ERSTER BOT

8 Zeichen? Gib mir eine Woche. Nein, einen Tag.

ZWEITER BOT

10? Ich hoffe wirklich, dass sie ihr Passwort nicht in den nächsten sechs Monaten ändern.

DRITTER BOT

15 Zeichen – Geschätzte Zeit bis zum Erfolg: Tatsächlich mehrere Jahrhunderte.

SARAH

Außerdem sollte das Passwort nicht leicht zu erraten sein.

MARIA

Klar. Keine Sachen wie „PASSWORT“ oder „123456“.

SARAH

Ja, aber weißt du, dass „FUSSBALL“ auch eines der häufigsten Passwörter ist? Es ist am besten, überhaupt keine klaren Begriffe zu verwenden. Eine Mischung aus Buchstaben, Zahlen und Sonderzeichen ist viel sicherer. Auch dein Name oder dein Geburtsdatum sind problematisch. Alles, was sich leicht herausfinden lässt, kann ausgenutzt werden.

MARIA

Also dürfen Passwörter nicht kurz sein, nicht persönlich und sie müssen alle unterschiedlich sein… Wie soll ich mir die bloß merken?

Sollte ich sie irgendwo in meiner Notizen-App verstecken? Oder auf einen Klebezettel unter meinen Schreibtisch schreiben?

SARAH

Schlechte Idee. Notizen können gefunden werden, und Standard-Textprogramme sind leicht zu knacken.

Ein sicherer Passwort-Manager ist viel sicherer als ein Dokument auf deinem Gerät. Manche generieren und speichern sogar sichere Passwörter für dich.

MARIA

Das klingt wirklich hilfreich, aber… steckt dann nicht alles an einem einzigen Ort? Hacker wüssten doch sofort, wo sie suchen müssen! Und was, wenn mein Gerät gestohlen wird oder der Passwort-Manager gehackt wird?

SARAH

Wenn Du wirklich sicher sein willst, kannst Du eine Offline-Variante nutzen. Außerdem kannst Du 2-Faktor-Authentifizierung [2FA] aktivieren und mit einer externen App nutzen. Einen zweiten Faktor zu haben, ist immer eine gute Sache, aber eine externe App zu nutzen, macht es sogar noch sicherer. Aber aktuell sind Passwort-Manager sehr sicher. Sie speichern deine Passwörter nicht einfach, sondern verschlüsseln sie mit einem Master-Passwort als Schlüssel. Der Manager selbst kann dein Master-Passwort nicht lesen – er führt nur Berechnungen damit durch. Das Ergebnis stimmt nur, wenn das richtige Passwort eingegeben wird.

NORMALE WEBSITE:

Glückwunsch, du stehst auf meiner Liste!

PASSWORT-MANAGER

Benutzername… Passwort… Lass mich das mal ausrechnen…

SARAH

Jemand, der Zugriff auf deinen Passwort-Manager will, müsste dein Master-Passwort knacken…

MARIA

...und die Bots, die das tun, haben bei langen, komplexen Passwörtern keine Chance – nicht vor dem nächsten Jahrhundert! Das ist genial!

Also brauche ich ein Master-Passwort – und das muss richtig gut sein!

SARAH

Jemand, der Zugriff auf deinen Passwort-Manager will, müsste dein Master-Passwort knacken…

MARIA

...und die Bots, die das tun, haben bei langen, komplexen Passwörtern keine Chance – nicht vor dem nächsten Jahrhundert! Das ist genial!

Also brauche ich ein Master-Passwort – und das muss richtig gut sein!

SARAH

Es könnte eine Zeile aus deinem Lieblingslied sein, ein Zitat oder einfach ein Satz, der zufällige Elemente kombiniert. Zum Beispiel „Ich esse gerne Reis mit Bohnen zum Mittag“, abgekürzt „IegRmbzm“.

Zu kurz. Also fügen wir noch Zahlen hinzu – zum Beispiel das Erscheinungsdatum eines Films, den du magst, „28SEP2004“ für den 28. September 2004. Und als Verbindung ein Sonderzeichen: „IegRmbzm&28SEP2004“.

MARIA

Ja, ich denke, mir fällt da was ein.

SARAH

Aber denk dran: Selbst das sicherste Passwort schützt deine Daten nicht, wenn es gestohlen wird.

Die meisten Straftaten, die wir als „Hacking“ bezeichnen, nutzen eigentlich menschliche Fehler aus.

Betrüger versuchen, dich dazu zu bringen, ihnen deine Zugangsdaten selbst zu geben.

ORANGER FISCH
Vorsicht! IHR ACCOUNT WIRD DEAKTIVIERT WENN SIE IHN NICHT UPDATEN!
PINKER FISCH:
„HALLO MAMA, DAS IST MEINE NEUE NUMMER“
ROTER FISCH:
„VERDÄCHTIGE AKTIVITÄT AUF IHREM ACCOUNT ENTDECKT! KLICKEN SIE AUF DIESEN SICHEREN LINK UM SICH ZU VERIFIZIEREN.
GELBER FISCH: „SIE KOMMEN FÜR EINE STEUERRÜCKERSTATTUNG IN FRAGE. KLICKEN SIE HIER UM IHR STEUERRÜCKERSTATTUNGSFORMULAR ANZUFORDERN.“
BLAUER FISCH:
„RECHNUNG FÄLLIG, LETZTE WARNUNG!“
SARAH
Die häufigste Methode nennt sich „Phishing“ – dabei geben sich Hacker als Personen, Websites oder Dienste aus, denen du normalerweise vertraust.
MARIA
Deshalb hast du Alex gewarnt, keine Nachrichten von meinem gehackten Account zu öffnen

SARAH
Sei immer vorsichtig mit Dateien, die du bekommst oder herunterlädst. Und gib deine Login-Daten niemals auf einer Website ein, die dir als Link geschickt wurde. Öffne lieber selbst einen neuen Tab und suche die richtige Seite oder nutze die offizielle App.

Jetzt, wo du deine Passwörter sicher verwaltest, gibt es noch eine Sache: Ich habe gesehen, dass du dein aktuelles Konto schon genutzt hast, bevor du dich für unsere Sache engagiert hast. Es ist sicherer, verschiedene Konten für verschiedene Zwecke zu haben.
MARIA
Stimmt… Vorher habe ich mir nie Gedanken gemacht, was ich poste. Diese Abschlussfotos auf meinem alten Account bedeuten mir viel, aber wenn die falschen Leute sie sehen…
MARIA
Moment mal…

SARAH
Es ist Zeit, sich auszuloggen. Mach dir das zur Gewohnheit.

MARIA
Alles erledigt! Danke, Sarah!

MARIA
Du hättest mir wirklich kein neues Handy kaufen müssen, nur wegen des einen Risses im Display, Alex.

ALEX
Das war das Mindeste, was ich tun konnte. Außerdem weiß ich, wo man die besten Angebote bekommt.

POLIZIST
Halt! Wir führen Inspektionen von Kommunikationsgeräten durch. Ich muss einen Blick auf Ihre Handys werfen, bitte.

MARIA
Mein altes Handy hatte einen kleinen Unfall. Tut mir leid.

Klick!

POLIZIST
Ich nehme an, dein Handy hatte keinen Unfall?

ALEX
Natürlich nicht. Mann…

POLIZIST
Ich sehe, du bist aus all deinen sozialen Netzwerken ausgeloggt.
ALEX
Ja. Ist das nicht die beste Methode, um sich vor Hacks zu schützen?

POLIZIST
Melde dich hier an.

ALEX
Hier, bitte.
POLIZIST
Hm. Danke für die Kooperation.

MARIA

Puh, meine Nerven. Gut, dass ich mein altes Handy nicht dabeihatte.

ALEX

Hey, immerhin haben sie die Handys diesmal nicht konfisziert.

MARIA

Aber mal ehrlich: Du bist der engagierteste Aktivist, den ich kenne. Wie hat den nichts auf deinem Handy misstrauisch gemacht?

ALEX

Du wolltest dein Handy jetzt einrichten, oder? Ich zeig dir ein paar Tricks.

ALEX-CAPTION-OBEN

Aktiviere die Geräteverschlüsselung und wähle "PIN-Code". Nutze keine biometrischen Merkmale.

ALEX-CAPTION-UNTEN

So kannst du dein Handy nicht mit Gesicht oder Fingerabdruck entsperren – aber ebenso wenig jemand anderes.

ALEX-CAPTION-OBEN

Manche Apps erlauben es, Icons und Namen zu ändern. Apps mit... einem gewissen Ruf bekommen ein kleines Makeover.

ALEX

Benutze in Messenger-Apps keine echten Namen – nicht mal deinen eigenen. Niemand ist unter seinem echten Namen in meinen Kontakten. Sarah ist zum Beispiel Charlie Martinez.

MARIA

Wirklich? Und wer ist "Todd Bonzales"?

MARIA
Dieser Kontakt... Das war Daniel, oder? Bevor er verhaftet wurde.
ALEX
Ja... "Todd Bonzales" ist eine Anspielung auf ein Videospiel, das wir zusammen gespielt haben. Du weißt, wie sehr ich es hasse, dass wir all das tun müssen... Aber irgendwann musst du entscheiden, was du auf deinem Handy behältst – und was du löschst.

MARIA
Also musstest du alles löschen, was zeigte, dass ihr euch nahestandet? Fotos, Nachrichten, alles?
ALEX
Sie sind mir noch nicht auf den Fersen, also stehen die Chancen gut, dass er sein Handy rechtzeitig ausgeschaltet hat und sich jetzt weigert zu reden. Er schützt die Leute, die dadurch identifiziert werden könnten.

Wenn ich verhaftet werde, weil sie Bilder von uns auf MEINEM Handy finden, dann würde ich damit sein Schweigen verraten

ALEX
Sie haben Daniels Namen in den Kontakten eines anderen Protestierenden gefunden. Auf einem alten Handy ohne Verschlüsselung. So haben sie ihn erwischt.

ALEX
Also, ich halte Leute gerne auf dem Laufenden. Sorry, das wurde jetzt ein bisschen schwer. Falls du noch Fragen zu deinem Handy hast, sag einfach Bescheid.
MARIA
Oh... Also… Ich habe überlegt…

MARIA
Vielleicht behalte ich mein altes Handy. Eines nur für den Aktivismus, mit möglichst wenig sensiblen Daten darauf... Kannst du mir auch damit helfen?
ALEX
Klingt nach einem Plan.

WEGE BAHNEN BEI INTERNET-SHUTDOWNS

MARIA
Und ihr seid sicher, dass das Absicht ist? Die Behörden schalten absichtlich das Internet ab? Vielleicht ist es einfach nur eine normale Störung?
SARAH
Nein, Maria. Das ist eine bewusste Maßnahme.

Unsere letzten Proteste waren sehr erfolgreich und die Wahlen stehen kurz bevor.

MARIA
Aber was ist mit all den Leuten, die das Internet für die Arbeit brauchen? Oder wenn es einen Notfall gibt?
ALEX
Leider ist das ein Preis, den manche Menschen an der Macht bereit sind zu zahlen.

ALEX
Sie behaupten immer, es sei aus guten Gründen, etwa zur „Terrorismusbekämpfung“. Aber Statistiken zeigen, dass das für solche Zwecke kaum wirksam ist.

Die Wahrheit ist, dass es genutzt wird, um Proteste zu unterbinden und kritische Stimmen zum Schweigen zu bringen. Diesmal ist es nur eine teilweise Abschaltung. Ich kann das Internet noch über mein VPN erreichen.
MARIA
VPN?

ALEX
Ein VPN ist ein „Virtuelles Privates Netzwerk“. Es stellt eine sichere Verbindung zu einem Server in einem anderen Land her. Dadurch kann dein Standort verschleiert werden, sodass man eine teilweise und lokal begrenzte Internetsperre umgehen kann.

Ich glaube, ich habe eins auf deinem Handy installiert, als wir es eingerichtet haben.

SARAH
Ja, aber sei vorsichtig damit. Es gibt Gerüchte, dass VPNs bald verboten werden könnten, also könnte diese App irgendwann zum Problem werden.
ALEX
Na toll, was für ein Pech.

MARIA
Die meisten Menschen wissen über diese Dinge ohnehin nichts. Das Internet ist noch relativ neu.

Wenn du meinen Eltern sagst, es ginge um „öffentliche Sicherheit“, würden sie wahrscheinlich einer Abschaltung zustimmen. Sie verstehen nicht, was wir verlieren.

SARAH
Wir versuchen immer, die Menschen über ihre Rechte und die digitale Landschaft aufzuklären, aber es ist schwer, die richtigen Informationen zu verbreiten. Wir dürfen nicht aufgeben.

SARAH
Heute Nachmittag treffen wir uns mit einer anderen aktivistischen Gruppe, um gegen die Abschaltung zu protestieren. 15:30 auf der Hauptstraße, das war unsere Absprache im Fall einer Abschaltung. Ich wollte es dir früher sagen, aber dann war das Internet schon weg.

MARIA
Aber ihr hättet mich doch anrufen oder eine SMS schicken können, oder? Es sind doch nur die Online-Messenger betroffen.

SARAH
Zu riskant. Telefonanrufe sind nicht Ende-zu-Ende verschlüsselt wie die meisten App-Anrufe. Wenn sichere Kommunikation nicht verfügbar ist, ist es am besten, persönlich zu sprechen.

SARAH
Wir müssen auf alles vorbereitet sein. Sobald das Internet abgeschaltet wird, wird es schwieriger, Beweise für Menschenrechtsverletzungen zu sammeln.

ALEX
Stimmt. Soll ich Maria schnell Bluetooth-Kommunikation erklären?

SARAH

Ihr solltet beide eine App haben, die über Bluetooth Nachrichten sendet. Bluetooth hat zwar eine geringe Reichweite, aber Handys können sich gegenseitig nutzen, um Informationen weiterzugeben. Je mehr Leute es nutzen, desto weiter verbreiten sich Nachrichten in diesem dezentralen Mesh-Netzwerk.

Die Nachrichten könnten codiert sein, damit sie nicht sofort als Protestaufruf erkennbar sind. In unserem Fall könnten wir "Pizza essen gehen" als Code für eine Versammlung nutzen.

MARIA

Das ist eine Lösung, denke ich...

ALEX

Die beste Lösung wäre, diese verdammten Abschaltungen von vornherein zu verhindern. Aber oft ist es schwer nachzuvollziehen, wie sie umgesetzt werden, und die Telekommunikationsunternehmen geben dem Druck der Behörden nach.

SARAH:
Es gab Versuche, rechtliche Schritte einzuleiten, aber das Internet ist in den meisten Verfassungen einfach nicht berücksichtigt, sodass es schwer ist, eine solide rechtliche Grundlage dafür zu finden.

MARIA:
Und was ist mit der internationalen Gemeinschaft? Die müssen doch wissen, dass das falsch ist!
SARAH:
Im Moment werden Internet-Shutdowns zwar missbilligt, aber es gibt keine Sanktionen auf internationaler Ebene.

ALEX:
Es gibt internationale Aktivist*innengruppen, die diese Art von Abschaltungen dokumentieren, um zu zeigen, wie groß das Problem wirklich ist. Ich habe diesen Fall bereits bei der #KeepItOn-Initiative von Access Now gemeldet.

ALEX:
Hey, warum schreibst du ihnen nicht einfach deine Meinung?
MARIA:
Ich?
SARAH:
Gar keine schlechte Idee. Jede Stimme zählt, und viele Organisationen hören gerne direkt von Aktivist*innen aus aller Welt.

MARIA:
Aber ich fühle mich doch noch so neu in all dem. Ich hätte seit dem letzten Protest fast eine Menge Fehler gemacht...
ALEX:
Unterschätz dich nicht. Du hörst gut zu, lernst schnell und erkennst, was wichtig ist. Und wenn ich mir deine Kameraarbeit so anschaue, hast du vielleicht sogar das Herz einer Journalistin.

MARIA:
Okay... Ich gebe mein Bestes.

MARIA
Guten Tag,

ich schreibe Ihnen, um auf den aktuellen Internet-Shutdown in meinem Heimatland aufmerksam zu machen und eine Diskussion darüber anzustoßen.

Internet-Shutdowns greifen direkt in die Fähigkeit der Menschen ein, ihre Grundrechte auszuüben.

Ihr Recht zu sprechen.

Ihr Recht, Protest zu organisieren.

Ihr Recht, sich zu informieren und weiterzubilden.

Jeder dieser Punkte wäre für sich genommen schon problematisch, aber ich glaube, dass die Verletzungen durch Internet-Shutdowns noch viel tiefer gehen.

Menschen haben ein grundlegendes Bedürfnis nach Kommunikation und danach, verstanden zu werden. Interaktion liegt in unserer Natur.

So sehr, dass der Entzug jeglicher menschlicher Interaktion als grausame und unverhältnismäßige Bestrafung gilt.

Deshalb sage ich, dass Internet-Shutdowns nicht nur im Zusammenhang mit eingeschränkten Menschenrechten betrachtet werden sollten, sondern auch als eine Verletzung der menschlichen Natur an sich.

Ich fordere die internationale Gemeinschaft auf, dieses Problem ernst zu nehmen und Sanktionen gegen Regierungen zu verhängen, die Telekommunikation unterbrechen und nicht anderweitig zur Rechenschaft gezogen werden können.

Mit freundlichen Grüßen
Maria.

Dieser Comic basiert auf Erkenntnissen, die aus über 90 Interviews mit Aktivist*innen in semi-autoritären Staaten und Ländern, die einen demokratischen Rückschritt erleben, gesammelt wurden. Wir sind den Aktivist*innen, die ihre Erfahrungen geteilt, die durch Technologie ermöglichte Gewalt, der sie ausgesetzt sind, beleuchtet und die Strategien, die sie genutzt haben, um ihre Privatsphäre und Sicherheit zu schützen, diskutiert haben, immens dankbar. Obwohl dieser Comic allgemeine Empfehlungen gibt, muss betont werden, dass die Aktivist*innen selbst die wahren Expert*innen für ihre eigenen Situationen sind. Jeder Kontext ist einzigartig, und was an einem Ort funktioniert, ist an einem anderen vielleicht nicht geeignet. Risiken entwickeln sich schnell, und Gesetze – wie solche, die auf Tools wie VPNs abzielen – können sich ohne Vorwarnung ändern. Informiert zu bleiben, persönliche Bedrohungsanalysen durchzuführen und Sicherheitspraktiken an lokale Kontexte anzupassen, sind Schritte, die dabei helfen können, wirksame Bewältigungsmechanismen zu entwickeln. Es ist auch wichtig, Sicherheit ganzheitlich zu betrachten und zu erkennen, dass die digitale und die physische Welt tief miteinander verbunden sind. Online-Sicherheitsmaßnahmen sind nur ein Teil eines breiteren Ansatzes, um sicher zu bleiben. Organisationen wie Access Now und Front Line Defenders bieten wertvolle Ressourcen zur Analyse von Bedrohungen und zur Verbesserung der digitalen Sicherheit.
Während wir uns auf eine Zukunft ohne Unterdrückung freuen, bleiben wir inspiriert von denen, die unermüdlich auf eine gerechtere und gleichberechtigtere Welt hinarbeiten.

Unterzeichnet: Laura Guntrum, Technische Universität Darmstadt
Redaktionelle Unterstützung: Julian Lawrence, Teesside University

Dieser Comic wurde vom Bundesministerium für Bildung und Forschung (BMBF) im Rahmen von TraCe, dem Regionalen Forschungszentrum für Transformationen politischer Gewalt (01UG2203E), und vom Hessischen Ministerium für Wissenschaft und Kunst im Rahmen seiner gemeinsamen Unterstützung für das Nationale Forschungszentrum für Angewandte Cybersicherheit ATHENE gefördert.

Verstehe die lokale Situation:
· Es könnte hilfreich sein, Einblicke in den spezifischen lokalen Kontext zu sammeln.
· Überprüfe, wer deine Aktivitäten überwachen könnte und bewerte potenzielle Bedrohungsakteur*innen.
· Untersuche rechtliche Einschränkungen bezüglich Tools wie VPNs oder verschlüsselten Messaging-Apps.
· Verstehe mögliche Konsequenzen, wie Strafen oder Beschlagnahmungen während Inspektionen.

Halte Software aktuell:
· Erwäge, regelmäßig alle deine Software, insbesondere Sicherheitsupdates, zu aktualisieren, um das Ausnutzungsrisiko gering zu halten.

Separate Konten und Geräte:
· Es könnte sinnvoll sein, separate Konten – und wenn möglich separate Geräte – für die Aktivismusarbeit zu nutzen, um das Risiko einer Kreuzbelastung mit persönlichen Aktivitäten zu minimieren.

Begrenze deine digitale Spur:
· Sei vorsichtig damit, deine wahre Identität mit Aktivist*innen-Konten zu verknüpfen. Überlege, Pseudonyme zu verwenden und vermeide echte Namen/Fotos, besonders in Messaging-Apps, in denen Fremde auf dein Profil zugreifen können.
· Denke zweimal nach, bevor du Fotos, Videos oder Beiträge hochlädst, die unbeabsichtigt deinen Standort, Aktivitäten oder Verbindungen preisgeben könnten.
· Wenn du ein sensibles Foto senden möchtest, überlege, die „nur einmal ansehen“-Funktion zu verwenden, die in einigen Apps verfügbar ist. Dies stellt sicher, dass der*die Empfänger*in das Bild nur einmal ansehen kann und verhindert, dass er einen Screenshot macht.
· Überprüfe deine sozialen Medien und sei vorsichtig, wen du hinzufügst oder wem du folgst.

Reinige deine Geräte regelmäßig:
· Du könntest erwägen, regelmäßig sensible Nachrichten, Dateien oder andere digitale Beweise zu entfernen.
· Vergiss nicht, deine Kontakte zu überprüfen und diejenigen zu entfernen, die deine Sicherheit oder ihre eigene gefährden könnten.

Setze grundlegende Sicherheitsmaßnahmen um:
· Überlege, für jedes Konto einzigartige, starke Passwörter zu erstellen und einen vertrauenswürdigen Passwort-Manager zu verwenden.
· Du könntest die Zwei-Faktor-Authentifizierung (2FA) für alle Konten aktivieren, app-spezifische PINs festlegen und automatische App-Sperrfunktionen nutzen.
· Denke sorgfältig darüber nach, ob du dich mit öffentlichen Wi-Fi-Netzwerken verbinden möchtest.

Sichere Kommunikation:
· Überlege, Ende-zu-Ende-verschlüsselte Messaging-Plattformen (auch für Anrufe!) zu verwenden und Selbstlöschnachrichten zu aktivieren, um Risiken zu minimieren, falls dein Gerät kompromittiert wird.
· Sei dir bewusst, dass bestimmte Apps in deiner Region Verdacht erregen oder kriminalisiert werden könnten.

Begrenze App-Berechtigungen und Zugriffsrechte:
· Du könntest die App-Berechtigungen überprüfen und auf wesentliche Funktionen beschränken.
· Vermeide unnötige Apps, insbesondere solche, die übermäßigen Zugriff auf deine Daten anfordern.

Stelle sichere Backups und Wiederherstellungspläne auf:
· Du könntest kritische Daten sicher mit Verschlüsselung sichern, um sie vor Geräteverlust oder Beschlagnahmung zu schützen.
· Hab einen Wiederherstellungsplan parat, falls ein Konto kompromittiert wird.

Bereite dich auf Geräteinspektionen vor:
· Überlege, einen Plan zu haben, um sensible Informationen im Falle unerwarteter Geräteprüfungen schnell zu löschen oder zu verbergen.
· Sieh dir Apps oder Einstellungen an, die es dir ermöglichen, sensible Daten und Browser-Verlauf schnell zu verschlüsseln, zu verbergen oder zu löschen.

Bleibe wachsam bei Phishing-Angriffen:
· Sei vorsichtig bei Links, Anhängen und Nachrichten von unbekannten Quellen.
· Es ist hilfreich, regelmäßig dein Bewusstsein für Phishing-Taktiken zu schärfen und die Authentizität von Absendern zu überprüfen, bevor du auf Links klickst oder Informationen bereitstellst.

Indem du diese Schritte befolgst, kannst du proaktive Maßnahmen ergreifen, um deine Identität, deine Daten und deine Aktivismusbemühungen in risikobehafteten Umfeldern zu schützen.

Für detaillierte Schulungen und technische Unterstützung sind die folgenden Webseiten hilfreich: Front Line Defender: https://securityinabox.org/en/ Helpline Access Now: https://www.accessnow.org/resources/

Sicherheit steht an erster Stelle – online und offline

Maria, Alex, Sarah und Daniel sind vier Freund*innen, die sich leidenschaftlich für Menschenrechtsaktivismus in einem Land einsetzen, das mit zunehmendem Autoritarismus zu kämpfen hat. Ihre Bemühungen, ihre Botschaft in den sozialen Medien zu organisieren und zu verstärken, stoßen auf unaufhörliche Herausforderungen: Internetabschaltungen, gehackte Konten, direkte Bedrohungen und ständige Überwachungstaktiken, die darauf abzielen, abweichende Meinungen zum Schweigen zu bringen und Angst zu schüren. Daniels Verhaftung wegen seiner Teilnahme an den Protesten ist eine klare Erinnerung an die Gefahren, denen sie alle ausgesetzt sind. Begleite Maria, während sie mehr über digitale Sicherheit lernt und was dies für Aktivist*innen in vier kurzen Comic-Geschichten bedeutet.