Patriarchale Gewalt im digitalen Raum

AG Link, Kritische Jurist*innen & weitere,
01.06.2023

Wer wir sind

- AG Link
- Kritische Jurist*innen Leipzig
- Erster Workshop zu diesem Thema

Fahrplan

- Einleitung (ca. 30 Minuten)
- Interaktiver Teil (ca. 90 Minuten)
- Rechtlicher Input (ca. 20 Minuten)
- Outro (ca. 10 Minuten)

Geschlechtsspezifische digitale Gewalt

- Jede Form geschlechtsspezifischer Gewalt, die durch technische Hilfsmittel ausgeübt wird oder im digitalen Raum stattfindet (bff 2019).
- Fortsetzung von “analoger Gewalt”
- Nimmt zu

Aspekte des Digitalen

- Unkontrollierbares Weiterleiten & Kopieren, Anonymität
- Kontaktaufnahme standortunabhängig & kostenlos möglich
- Fehlende Sensibilisierung, Victim Blaming
- Rückzug aus digitalen Raum oft keine Option
- Herausfordernd für Beratungsstellen

Hate Speech

- Betrifft vor allem öffentliche Personen, die sich für polarisierende politische Themen einsetzen
- Gefährdung steigt durch Zugehörigkeit zu marginalisierter Gruppe
- FLINTA im Kontext ihrer Geschlechtsidentität

Digitale Gewalt im Nahfeld

- In und nach gewaltvollen Paarbeziehungen
- Mit Ablehung von gewünschter Beziehung

- Kaum Informationen zu digitaler Gewalt gegen Queere Menschen → wenn, dann zu **Hate Speech**
- Bedeutung von Social Media zur Vernetzung
- Ungewolltes Outing
- Ziel: Rückzug der Person aus der Öffentlichkeit

Wer ist betroffen?

- „Analoge Gewalt”
  - Betroffene sind meist Frauen, Ausübende meist Männer
  - EU-weit 18% der Frauen von Stalking betroffen
- Digitale Gewalt
  - Studie Wiener Frauenberatungsstellen:
    - Queere Frauen überdurchschnittlich oft beschimpft und erhielten ungefragt sexuell anzügliches Material
    - Frauen mit Migrationsgeschichte doppelt so häufig beschimpft
  - Jüngere Menschen häufiger betroffen
  - Datenlage schlecht

Formen digitaler Gewalt

- **Hate Speech**
- **Doxing**

  Veröffentlichen privater Information
- **Identitätsdiebstahl /-missbrauch**

  durch Fake-Accounts oder hacken von Accounts
- **(Cyber-)Stalking**

  Nachstellen mit technischen Hilfsmitteln
- **Diffamierung**

  Falschzitate, Verbreiten von Gerüchten

- **Bedrohung & Aufruf zur Gewalt**

  “Sextortion”: Erpressung durch intime Bilder

- **Non-Consensual Pornography** (“Revenge-Porn”)

- **Belästigung** (auch cyber harassment)

  ungefragtes senden von pornographischem Material / Nachrichten

- **Cyber-Grooming**

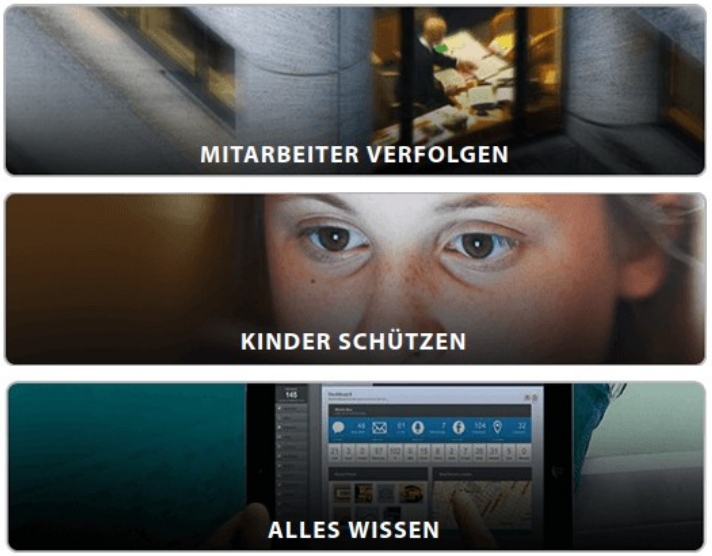
  Zielperson zu einem Treffen locken um Übergriffe zu ermöglichen

- **Deepfakes**

  durch KI erzeugte pornographische Aufnahmen

- Spy-Apps:
  - Standortdaten
  - Blockieren von Websites, Apps, Geräten (“Kindersperre”)
  - Screen mitlesen (→ Zugang zu Passwörtern)
  - Aufzeichnen von Audio & Video
  - Nachrichten lesen & schreiben
  - Nachrichten senden,

    Gerät zum klingeln / vibrieren bringen
- Frei verfügbar
- Auf Geräten kaum auffindbar



Werbung eines Anbieters

Auswirkungen digitaler Gewalt

- Verunsicherung, Scham, Ohnmacht, Angst
- Stören von Beziehungen zu Freund*innen und Familie
- Rückzug aus Onlineleben
- Psychische Krankheiten: Depression, Angsstörung, Schlafstörung, …

Pause

Workshop-Teil

Was Euch jetzt erwartet….

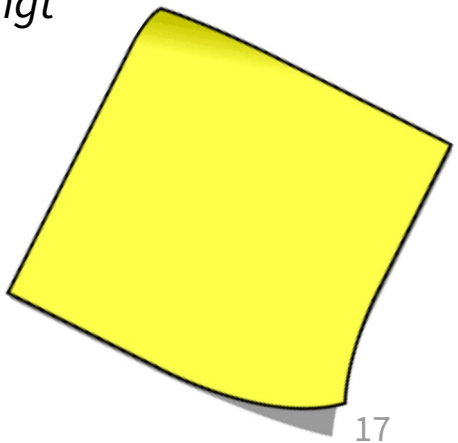
- Unser digitaler Alltag: *Wo fallen überall Daten an?*
- *Formen digitaler Gewalt unter der Lupe: Was passiert genau?*
- *Maßnahmen – Was können wir tun, um unsere Daten zu schützen?*

Nachbar*innenplausch (10 Min)

Welche Geräte und Anwendungen (z.B. Apps) sind Teil unseres digitalen Alltags?

Welche Informationen bzw. Daten fallen dabei an?

- *z.B. Infos, die die Anwendung von ihren Nutzer*innen verlangt (Benutzer*innenname, Passwort, E-Mail)*
- *Daten, die Nutzer*innen selbst teilen (z.B. Fotos…)*

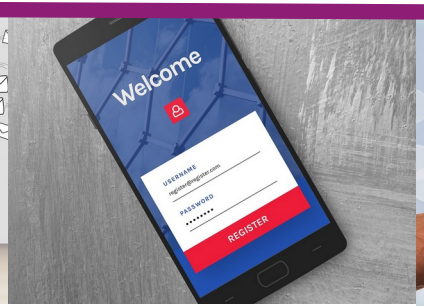


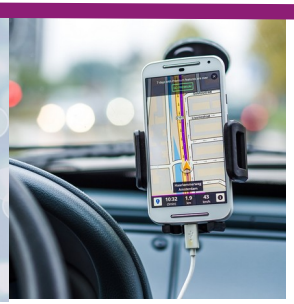
Beispiel:

Online-Warenhaus Account – Name, Anschrift, Geburtsdatum, Zahlungsinformationen, Telefonnummer, letzte Bestellungen + Adressen

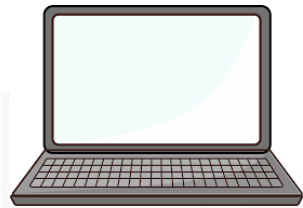
Welche Geräte und Anwendungen (z.B. Apps) sind Teil unseres digitalen Alltags?

Welche Daten fallen dabei an?



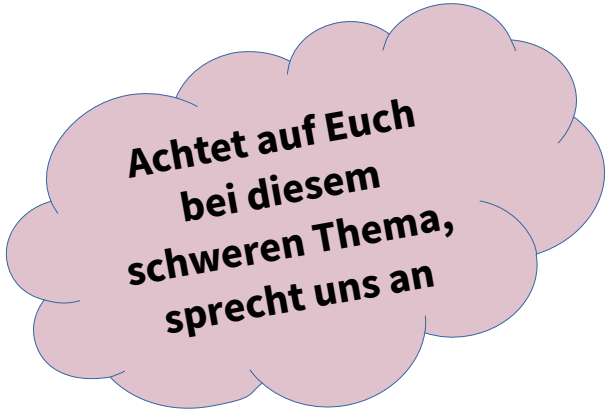





Formen digitaler Gewalt unter der Datenlupe:

Stille Diskussion (10 Min)

Welche Geräte, Anwendungen & Daten können bzw. werden bei den verschieden Formen digitaler Gewalt missbraucht?



Beispiel:

Cyberstalking – mit Passwort auf E-Mail Konto zugreifen, mitlesen

Pause

Willkommen zurück!

… was wir bisher gemacht haben

Maßnahmen – Prävention und Intervention

- Murmelgruppen (10min)
- Einigt euch auf **einige** der besprochenen Szenarien digitaler Gewalt und besprecht Maßnahmen, die davor (*Prävention*) oder auch in der Situation (*Intervention*) helfen könnten.
- Schreibt eure Ergebnisse gerne auf die Karten.
- **Beispiel:**
  - Szenario: Cyberstalking – mit Passwort auf E-Mail Postfach zugreifen, mitlesen
  - Mögliche Maßnahmen:
    - Schaden sichten/ Inventur → Was weiß Angreifer nun? Welche Folgen? (*intervenierend*)
    - Passwort regelmäßig ändern (*präventiv & intervenierend*)
    - E-Mail Kontakte informieren (*intervenierend*)
    - sicheres Passwort (*präventiv*)
    - 2-Faktor-Authentifizierung (*präventiv*)
    - keine Passwörter teilen (*präventiv*)

Was tun?

Überblick über eigene digitale & technische Nutzung (--> Handout)

(Privatsphäre-)Einstellungen von Geräten, Apps & Accounts

Datensicherheit + Datensparsamkeit

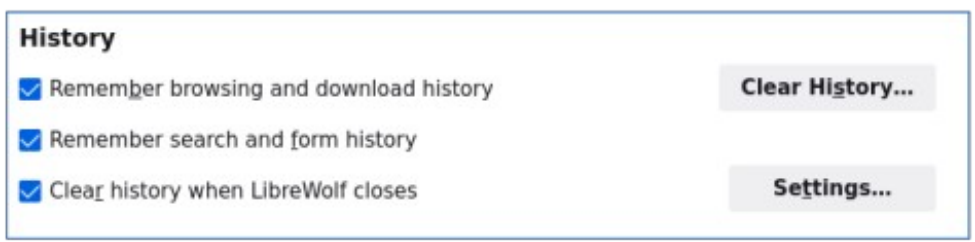
up-to-date bleiben

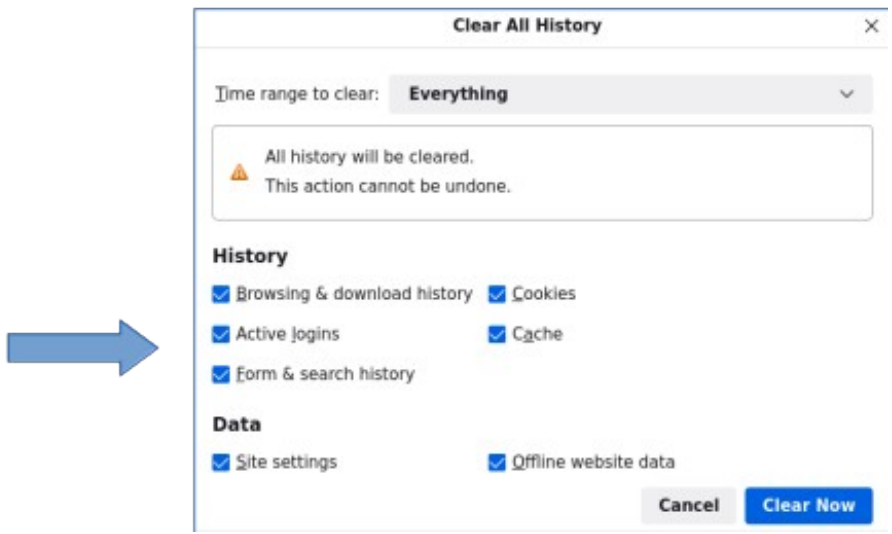
Medienkompetenz & digitale Selbstbestimmung stärken (individuelle Ebene)

öffentliche Debatte verfolgen & sich einmischen (gesellschafts-politische Ebene)

Was tun? - Browser

- Browserverlauf & gespeicherte Logins verraten sehr viel
- Phishing! (besonders bei E-Mail)
- Ausloggen (Amazon, Instagram, Banking, etc.)
- Regelmäßig Browserdaten löschen (Cookies, Zahlungsdaten, Logins, …)

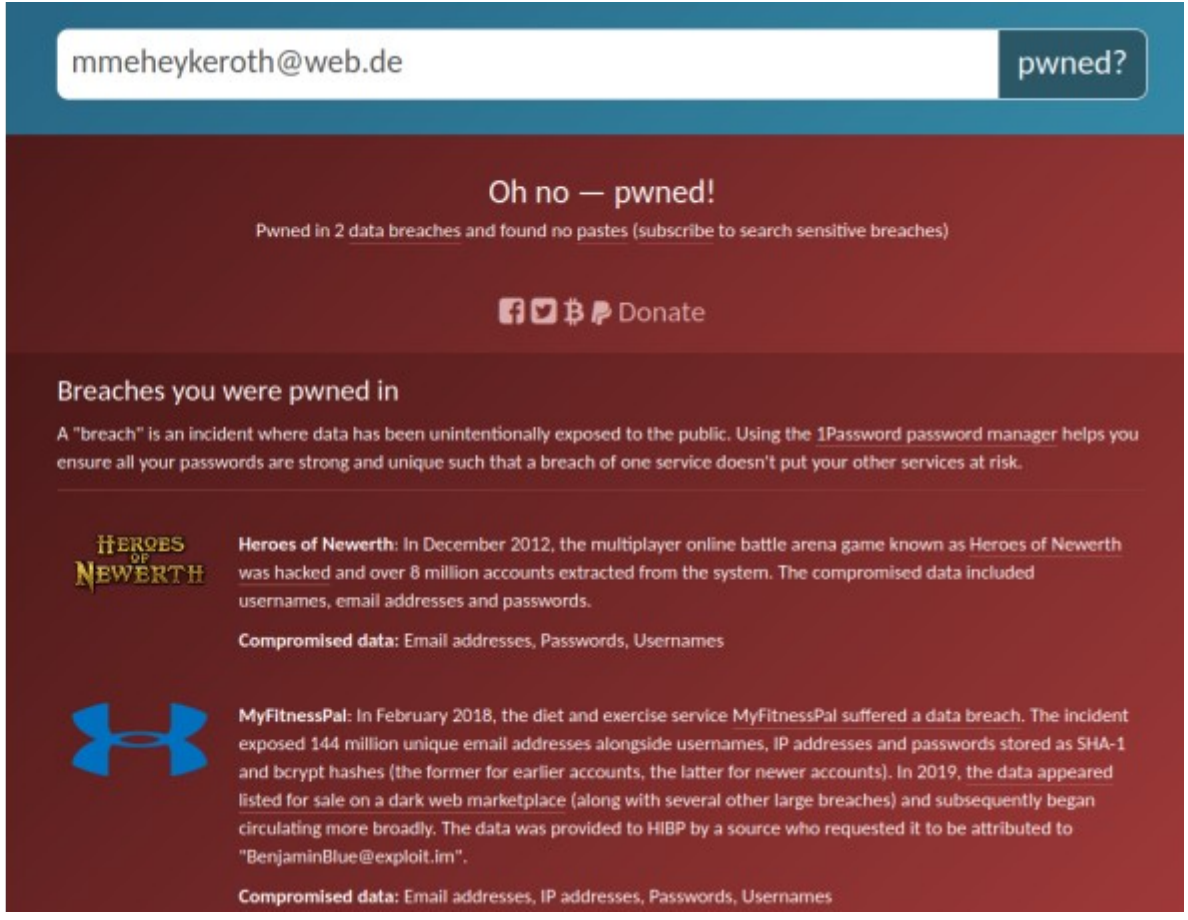




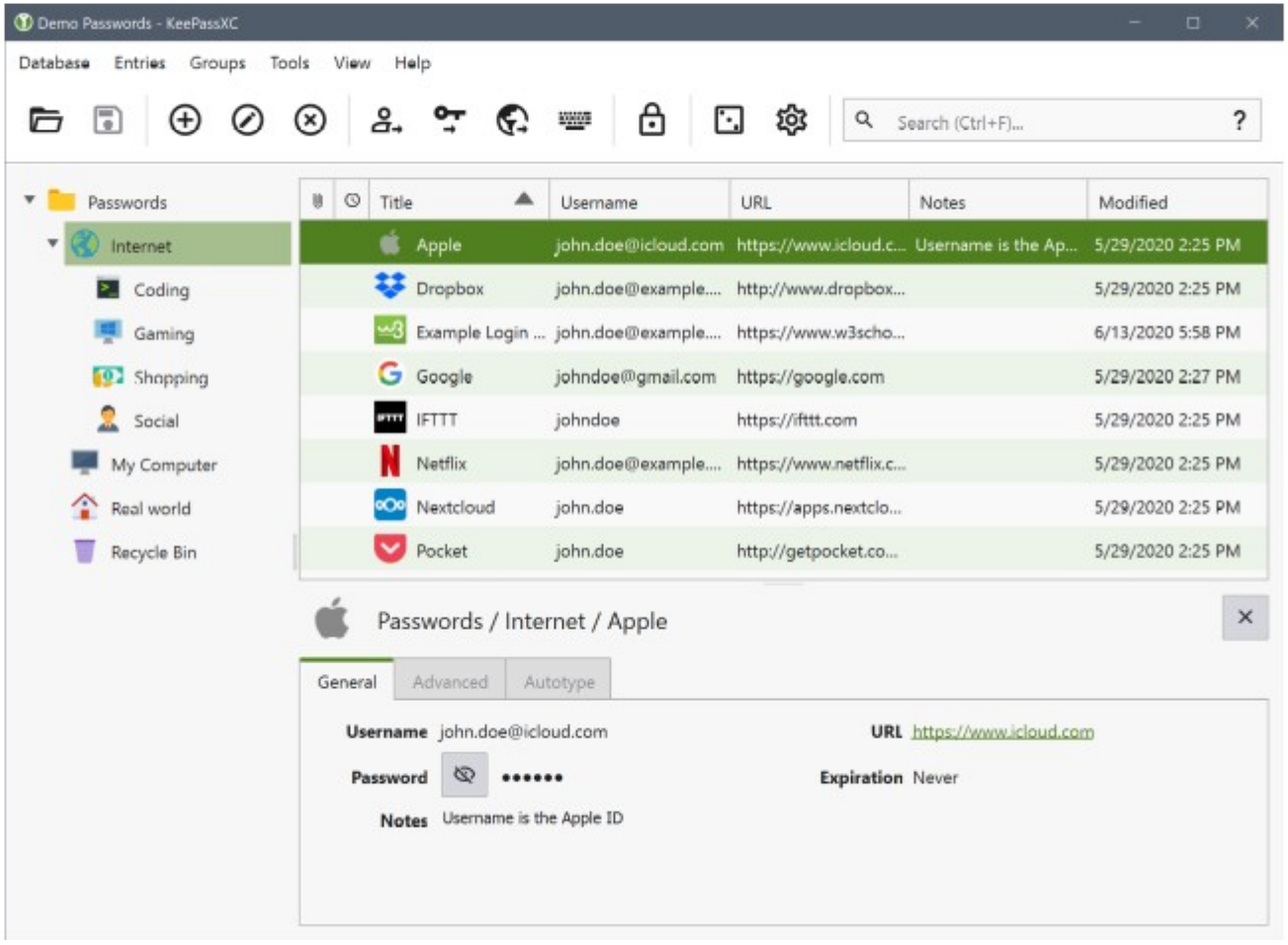
Was tun? - sichere Passwörter

- Empfehlung für Passwort:
  - ca. 12 oder mehr Zeichen
  - echte Wörter vermeiden: “Tisch123”
  - Viele Sonderzeichen (“, !,ß, ?, Ö, +), Zahlen
  - PINs vermeiden (Handy auch besser Passwort als PIN)
- Passwörter nur einmal verwenden
- Passwörter ändern (z.B. W-LAN Passwort nach Trennung)
- Passwort-Reset Optionen sichern (E-Mail Zugang, Handy-Zugang)

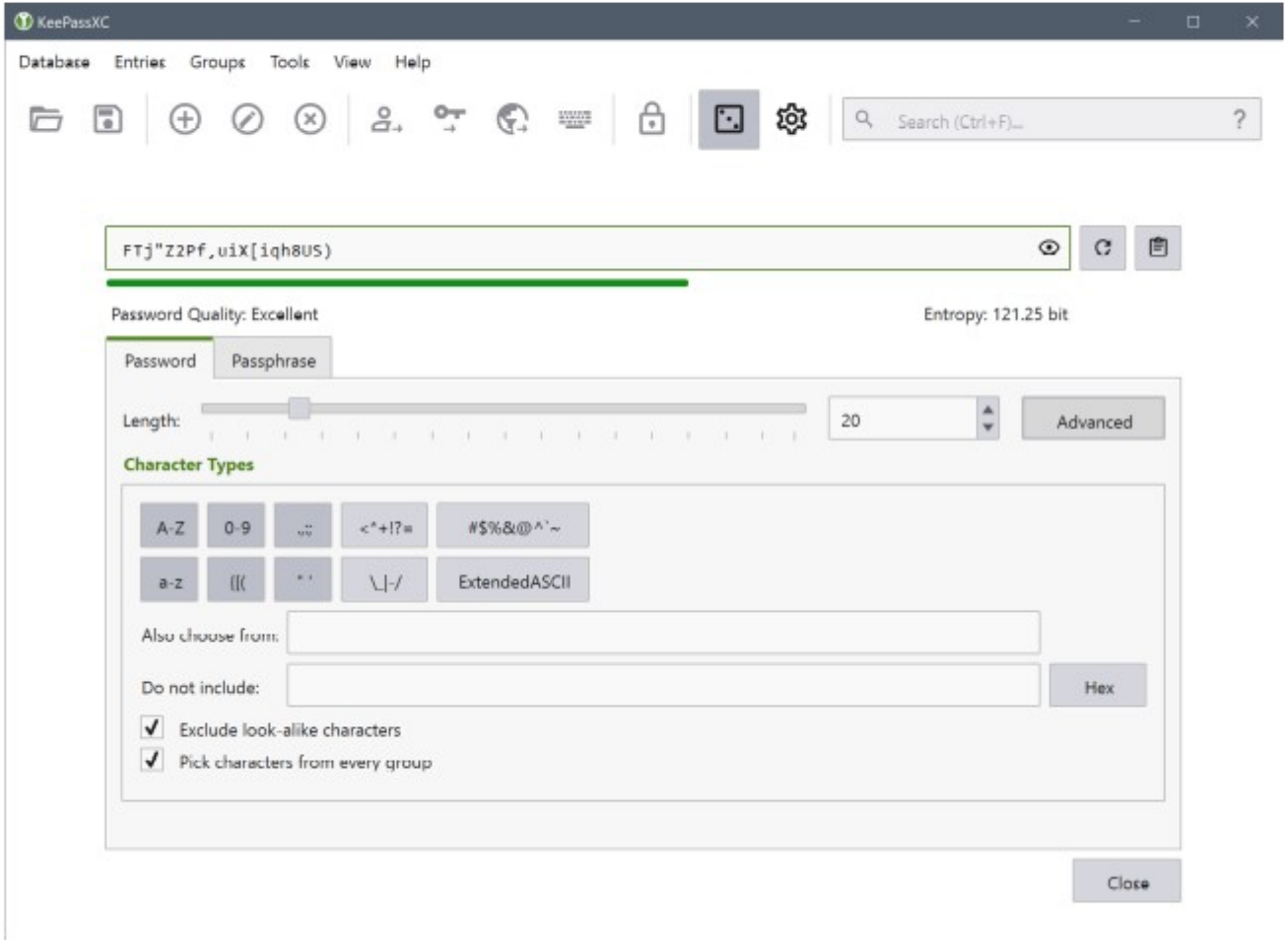
- Sich mal in Datenleaks selbst suchen
- https://haveibeenpwned.com/



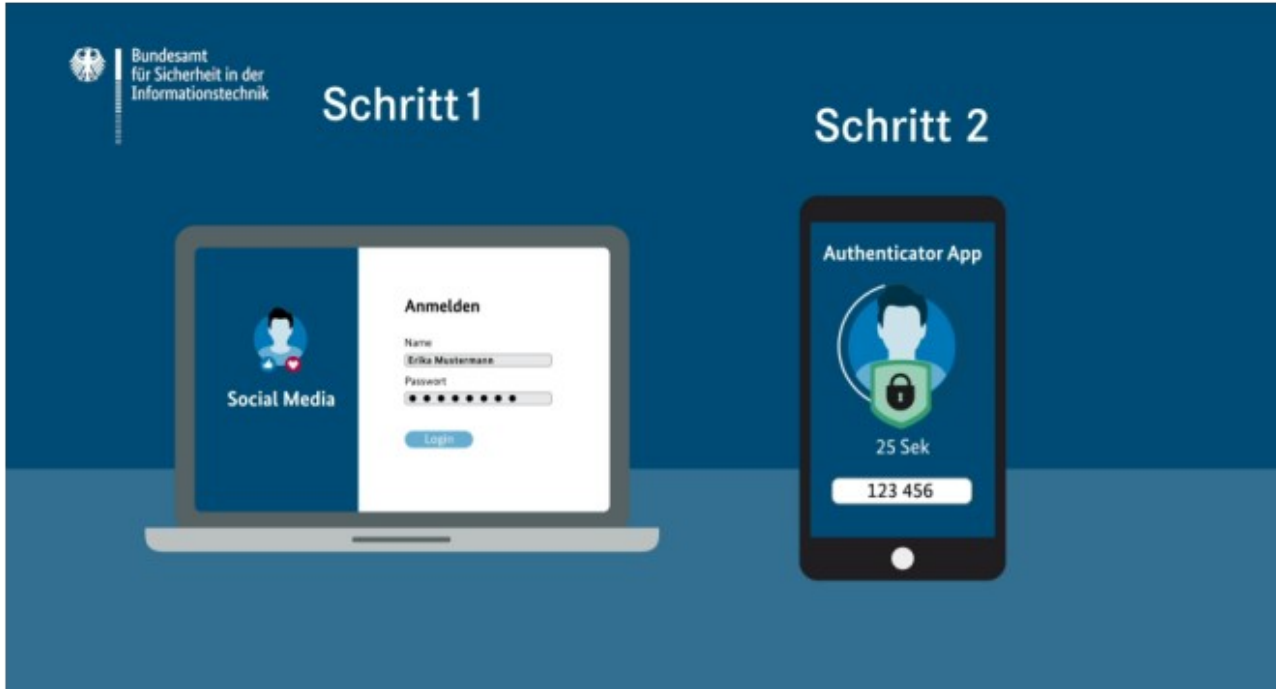
- Passwort-Manager verwenden (KeepassXC)



- Passwort-Manager verwenden (KeepassXC)



- 2-Faktor-Authentifizierung verwenden
- App-Empfehlung:
  - PC: **KeePassXC**
  - Android: **FreeOTP**
  - IOS: **Tofu/ FreeOTP**



Was tun? - Social Media

- Welche Daten sollen von mir veröffentlich werden? Kann was gegen mich verwendet werden? Wer kann das sehen?
- Privatsphäre Einstellungen überprüfen (z.B. privates Konto auf Instagram, Stories nur für enge Freunde)
- Plattform kontaktieren, Personen blocken, Chats melden (kann auch andere Person übernehmen)
- Stalking-Tagebuch führen/ rechtssichere Screenshots anfertigen
- Phishing aufpassen
- Fallspezifisch → Beratung!
  - z.B. Dickpics → Online Formular für Erstellung Anzeige (https://dickstinction.com/)

Was tun? - Cloud

- Wer hat Zugang zu meiner Cloud?
- Daten verschlüsseln (z.B. “Cryptomator”)
- Sicheres Passwort + 2-Faktor-Authentifizierung
- Geteilte Ordner → restlichen Zugang beschränken
- Welche lokalen Daten werden automatisch synchronisiert?

Was tun? - Verschlüsseln

- **Idee**: Daten nicht im Klartext speichern, sondern so, dass diese nicht gelesen werden können
- **Ansatz**: Daten werden mit einem Geheimnis (Schlüssel) so unkenntlich gemacht. Nur wer den Schlüssel kennt, kann die Ausgangform wiederherstellen.
- “Hallo Welt”  U2FsdGVkX18PnDvp/NfUIIvRaGnySMUdoSmbqbB3ZDc
  - Dauer Entschlüsselung ohne Wissen des Passworts = $3{,}3*10^{56}$ Jahre
  - vgl. Alter des Universums: $13{,}8*10^{9}$ (bzw. 13.8 Mrd. Jahre) Jahre

Was tun? - Verschlüsseln

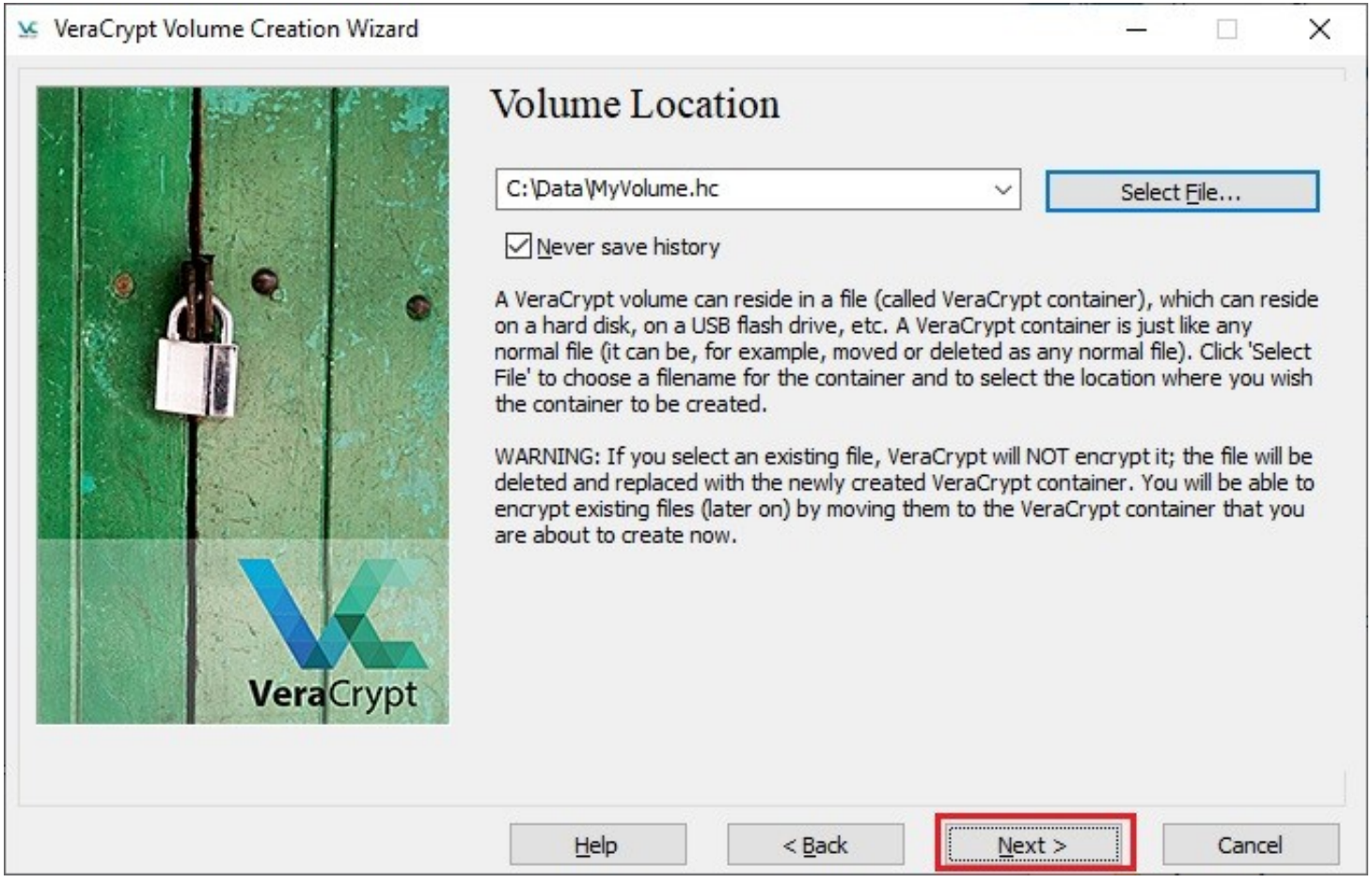
- Standardmäßig **nicht verschlüsselt** sind:
  - Windows Betriebssysteme
  - Linux Betriebssysteme
  - Ältere MacOS Betriebssysteme
  - Externe Festplatten/ USB-Sticks
  - Cloud Speicher
- Standardmäßig **verschlüsselt** sind:
  - Android, iOS, spezielle Speichermedien (Self-Encrypting Drives)

Was tun? - Verschlüsseln

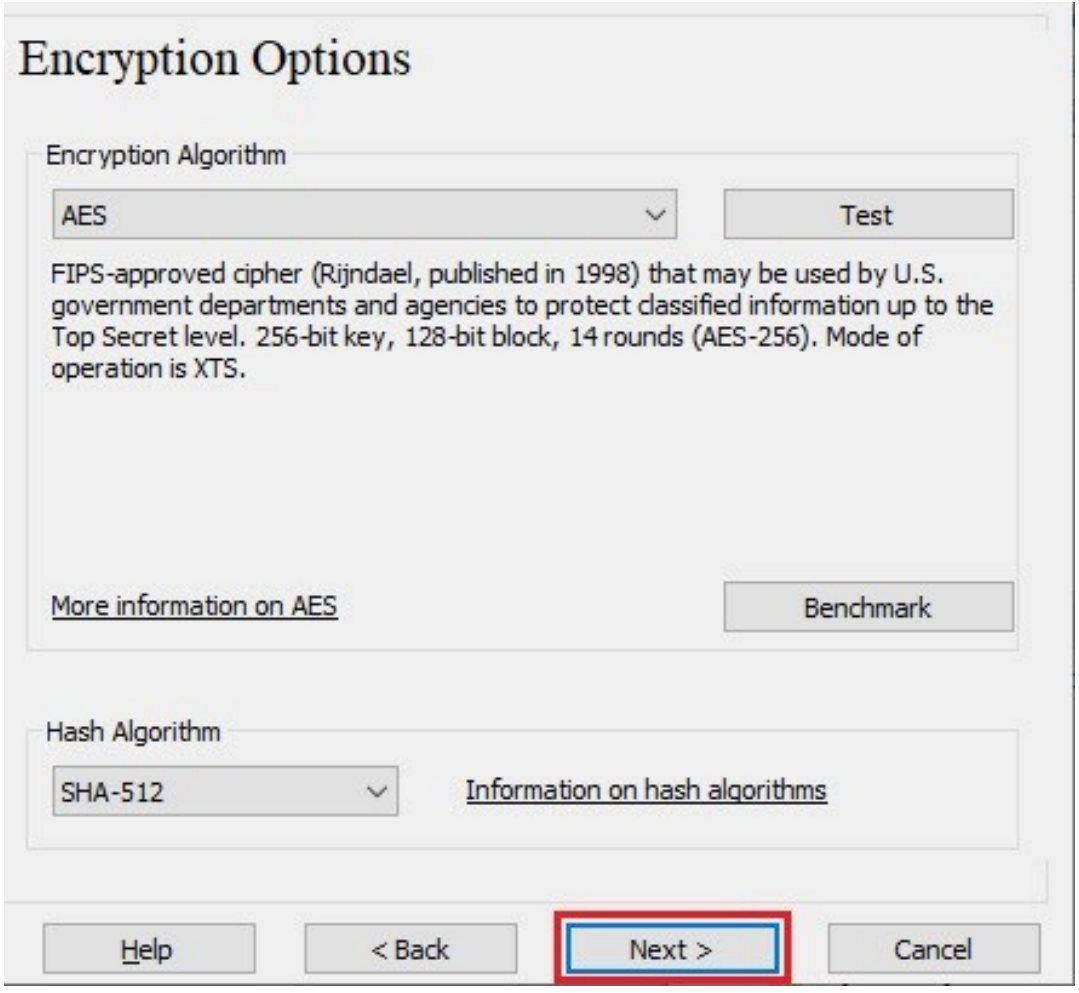
- *Unsere Empfehlung*
- Verschlüsselungs-Programm:
  - für eigenen Rechner/ Festplatten/ USB-Sticks:
    - **VeraCrypt**: verschlüsselt Festplatte oder “Daten-Safe”

  - Für Cloud-Speicher:
    - **Cryptomator**: Daten auf eigenem Rechner verschlüsseln, dann synchronisierung der Daten in Cloud

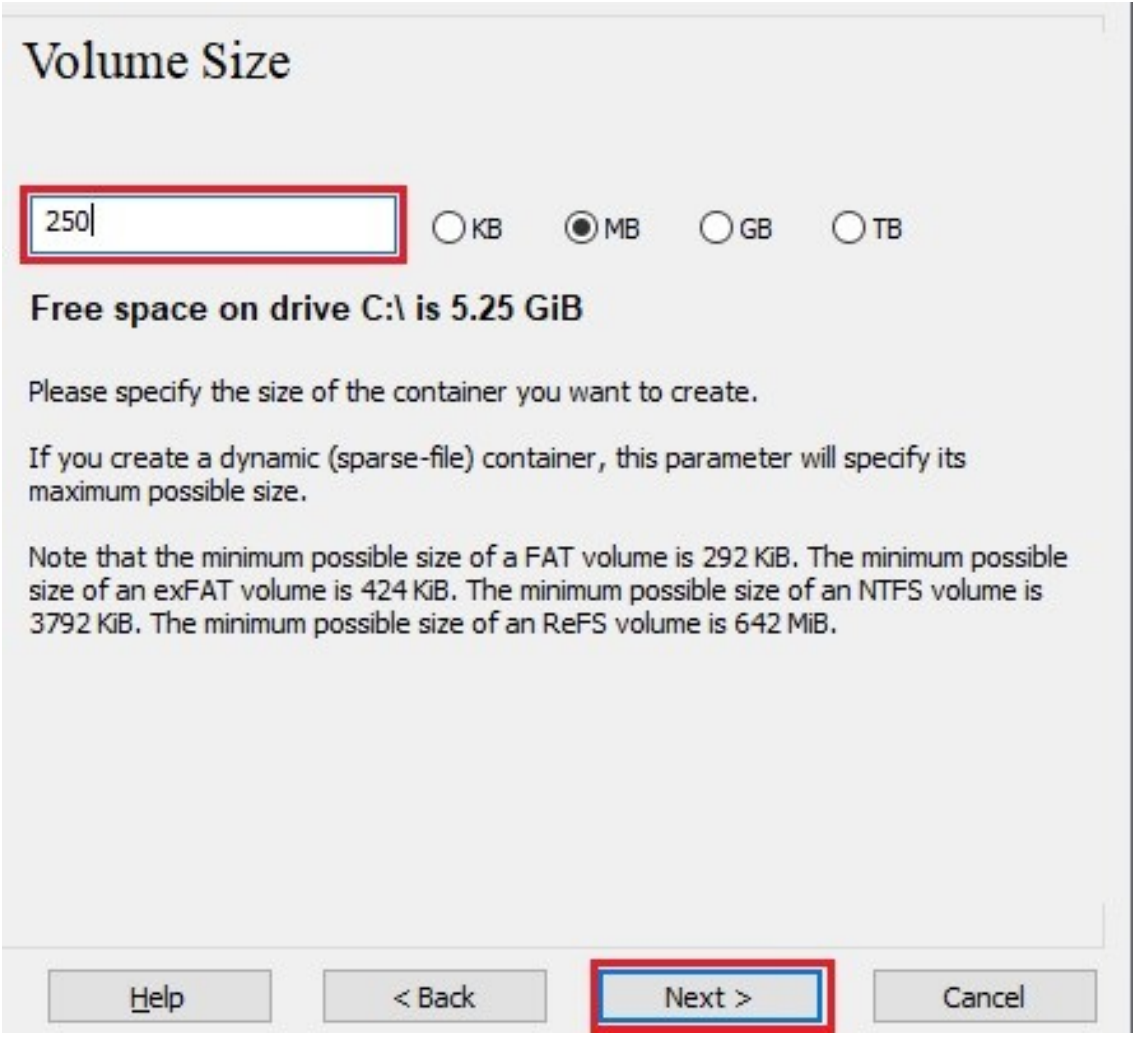
Verschlüsselung – **Schritt 1**



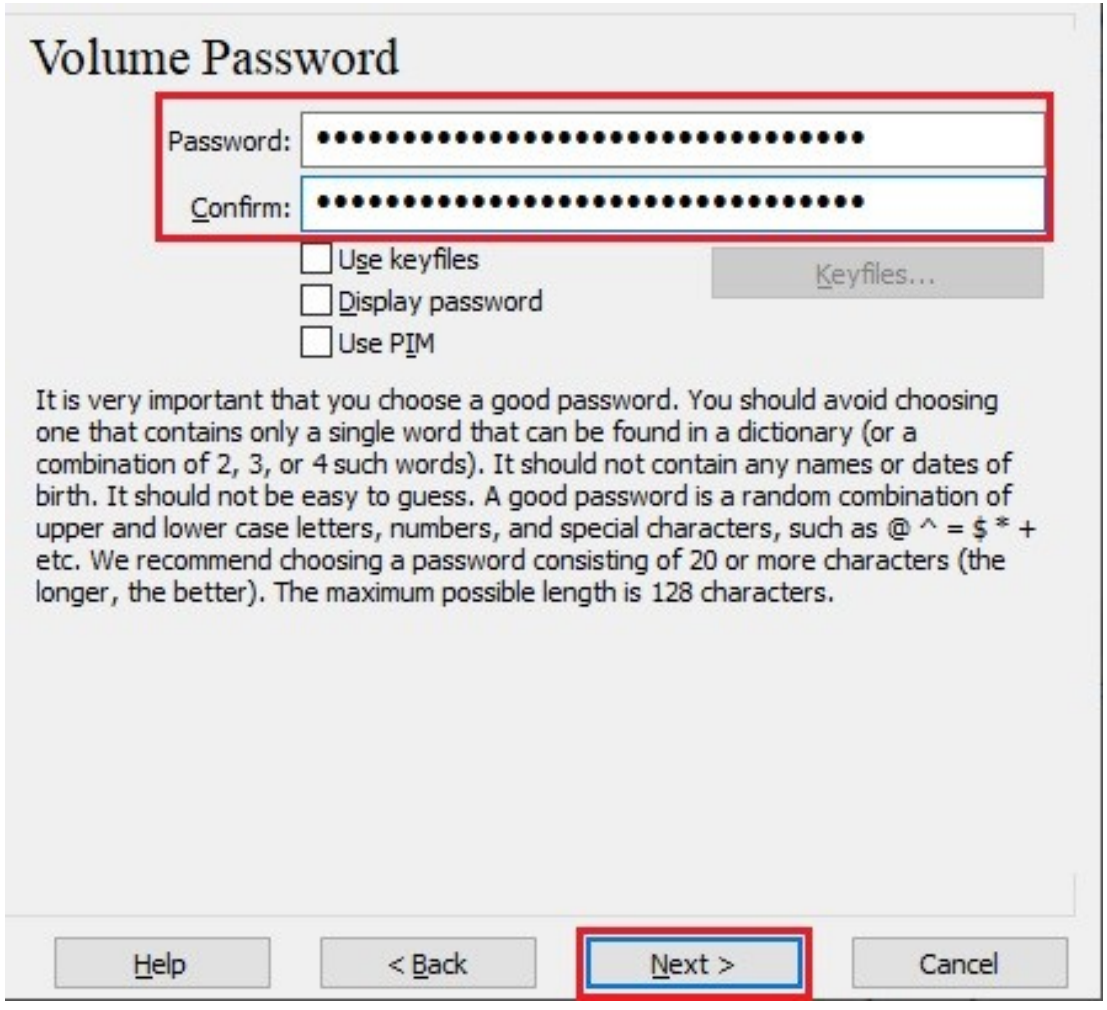
Verschlüsselung – **Schritt 2**



Verschlüsselung – **Schritt 3**



Verschlüsselung – **Schritt 4**




Volume Created
The VeraCrypt volume has been created and is ready for use. If you wish to create another VeraCrypt volume, click Next. Otherwise, click Exit.
Help
< Back
Next >
Exit

Beispiel “neue” technologische Entwicklungen

Insbesondere smart home Geräte (Stichwort: Internet der Dinge) können patriarchale digitale Gewalt verstärken

Was tun? - AirTag Stalking

- Apples *AirTags* erlauben Stalking durch Echtzeit-Abfrage des Standortes

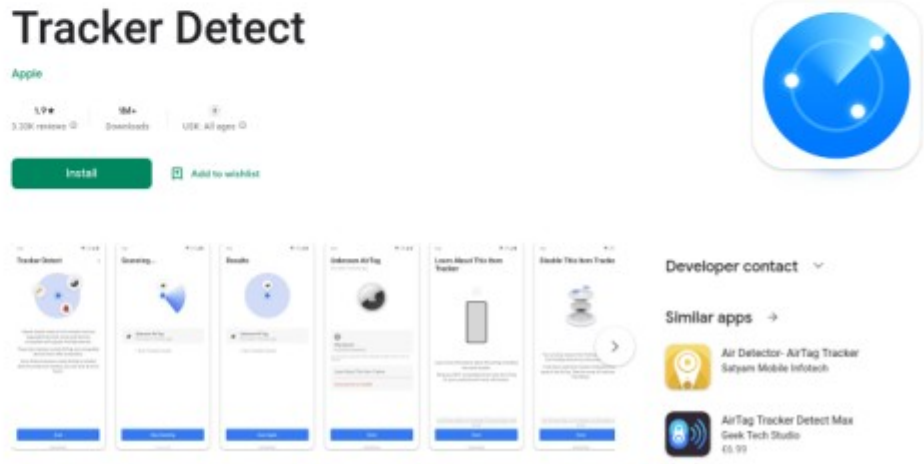
AirTags Are A Growing Headache For Apple Amid Disturbing Reports Of Tracking

Women around the country say they've gotten notifications that the relatively cheap location-tracking devices are following them.

By Sara Boboltz

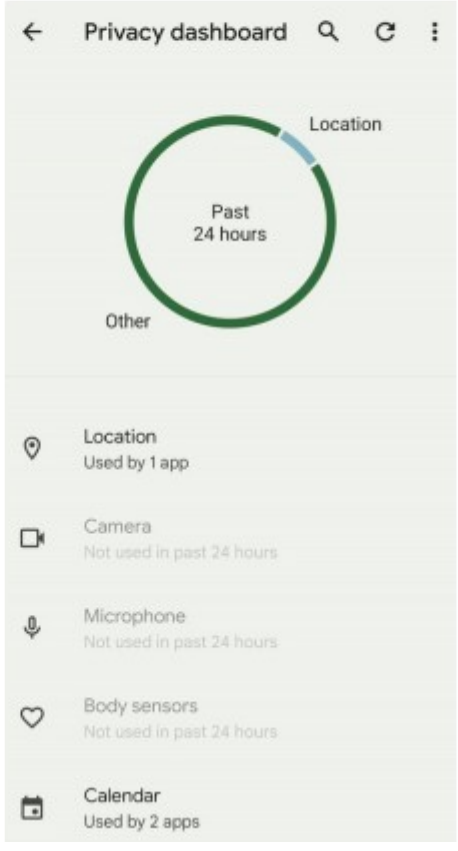
Feb 12, 2022, 03:56 PM EST

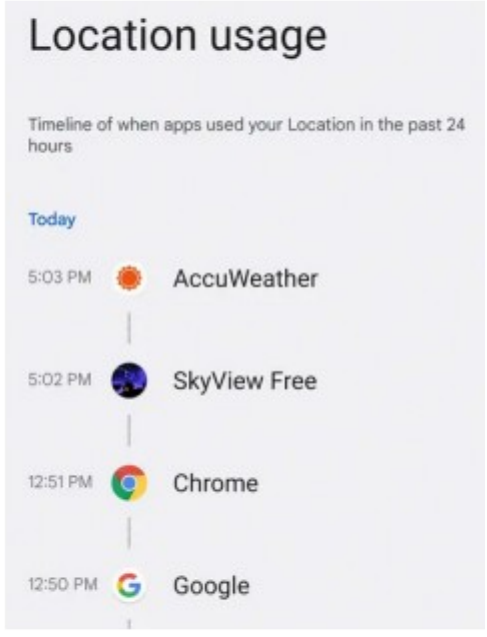
- neuere iOS Versionen warnen automatisch (ab iOS 14.5)
- Android: **Tracker Detect**



Was tun? - Stalking Apps erkennen

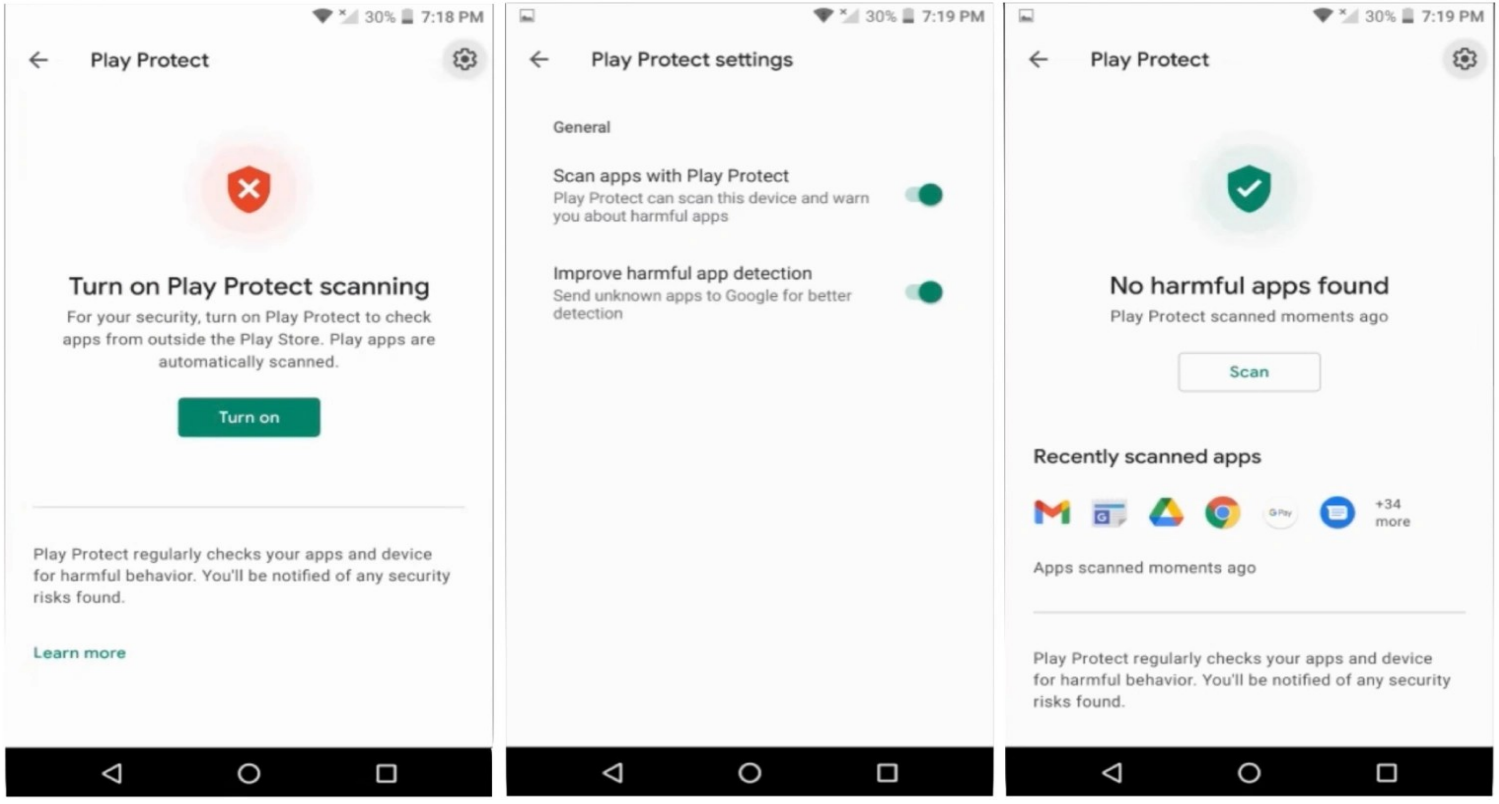
- Gibt viele Stalking Apps
- Überwache was deine Apps an Daten sammeln
- Android 12 & iOS 15: **Privacy Dashboard**
- Im Zweifel Handy zurücksetzen & Passwort ändern





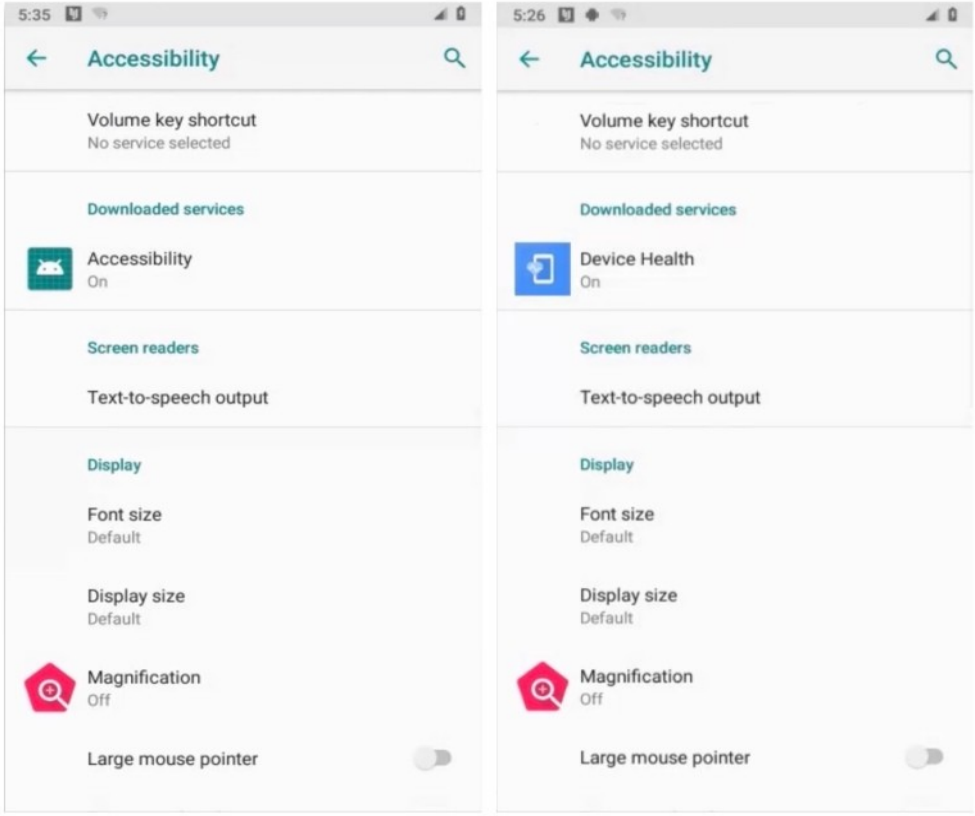
Was tun? Stalking Apps erkennen

1) Google Play Protect aktivieren



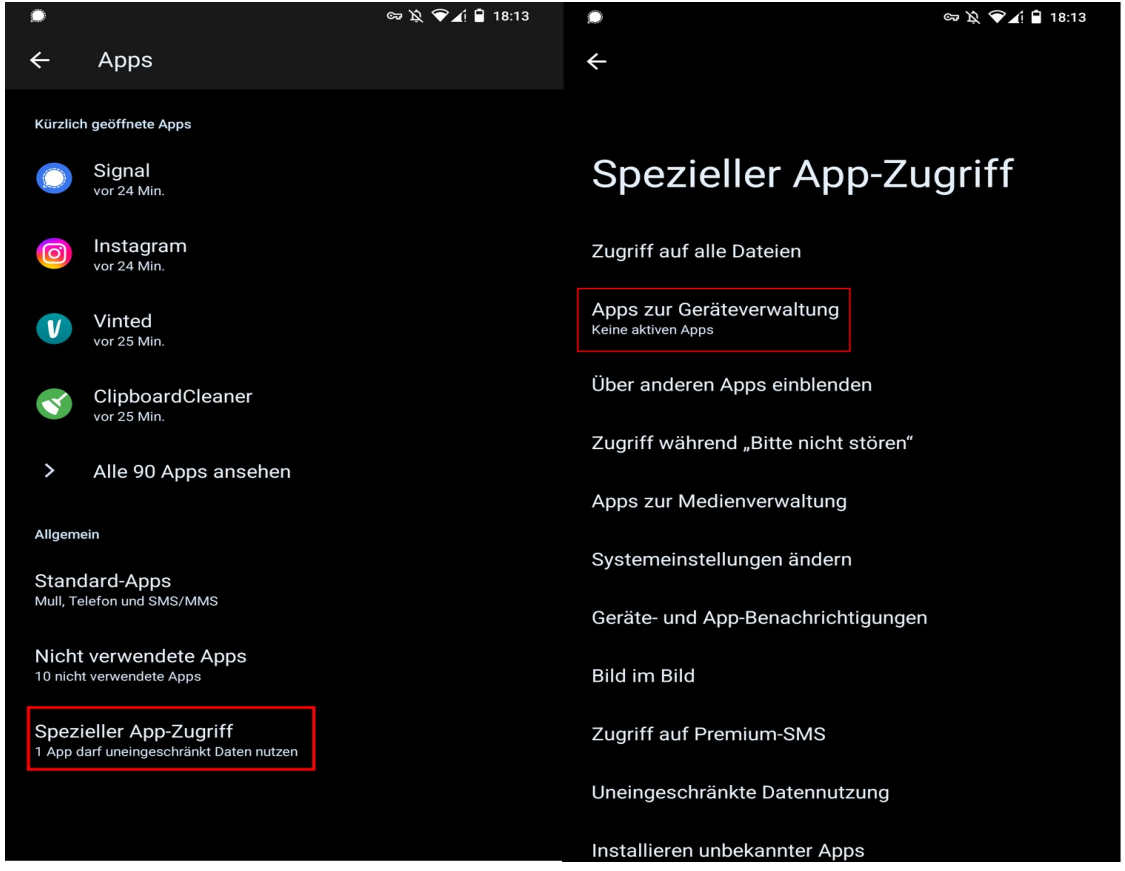
Was tun? Stalking Apps erkennen

2) Bedienungshilfen Einstellungen überprüfen



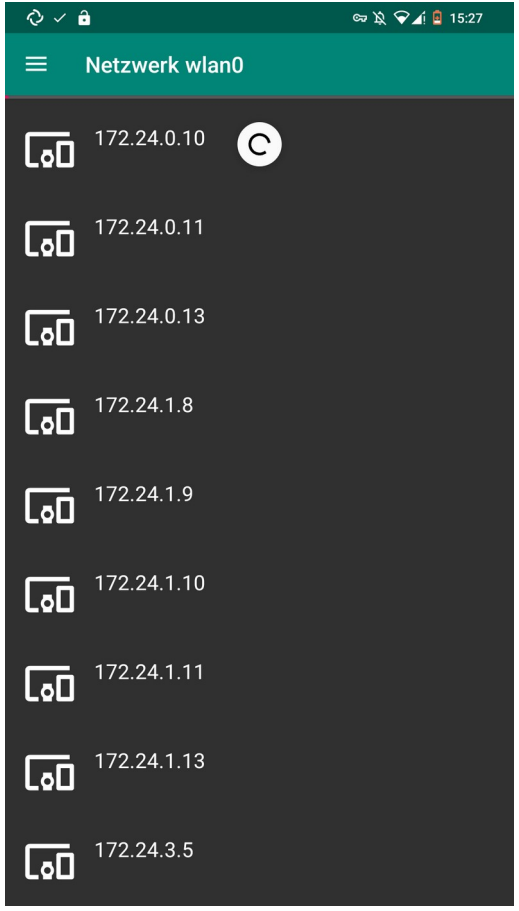
Was tun? Stalking Apps erkennen

3) Admin Apps & Apps mit speziellen Berechtigungen finden



Was tun? - SmartHome & versteckte Kameras

- Inventur! Welche Geräte? Was können die? (Stecker, Lampen, Thermostate, Thermometer, Kameras, Türschloss, Waschmaschine, ...)
- Wer hat Geräte eingerichtet?
- Gibt es Geräte, von denen ich nichts weiß
  - Scanne lokale Geräte (z.B. Android – “Ning”, iOS – “Vernet”)
  - Nutze Handy-Kamera, um Kameras zu finden (mehr Infos)



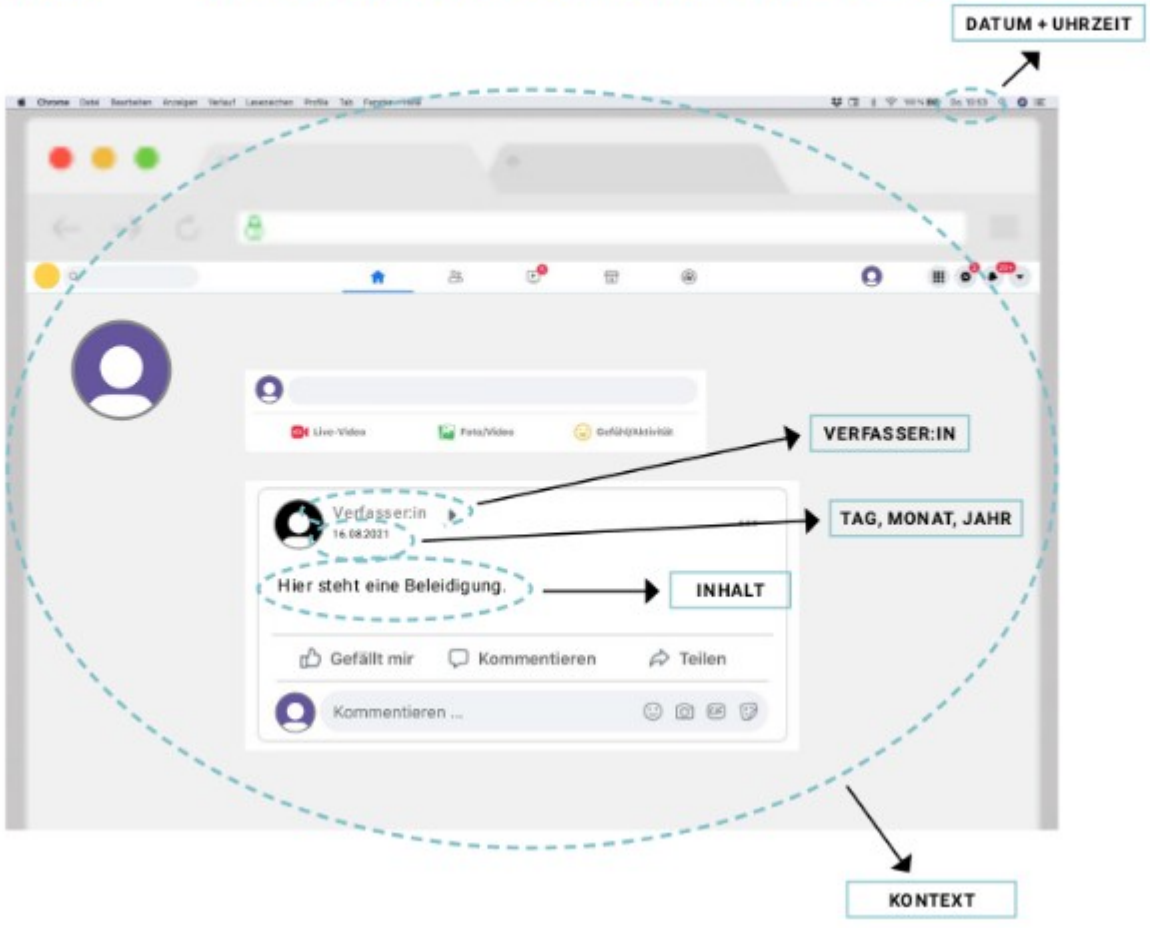
Was tun? - Sensible Bilder verschicken

- *Es gibt keine Garantie auf Sicherheit → überlege genau was & warum du etwas machst*
- Nutze nur Ende-Zu-Ende-Verschlüsselte Messenger (z.B. Signal – hat View-Once-Funktion, **KEIN** Snapchat, Facebook, etc.)
- Kein Gesicht/ Tattoos/ auffälliger Hintergrund
- GPS deaktivieren
- Cloud-Synchronisierung deaktivieren
- Verändere Bild o. füge Wasserzeichen mit Namen der Person ein
  - Erleichtert Identifikation falls Bild veröffentlicht wird
  - Hemmt Person am weiterleiten
  - **ABER:** Wasserzeichen können entfernt werden

Was tun? - Rechtssichere Screenshots

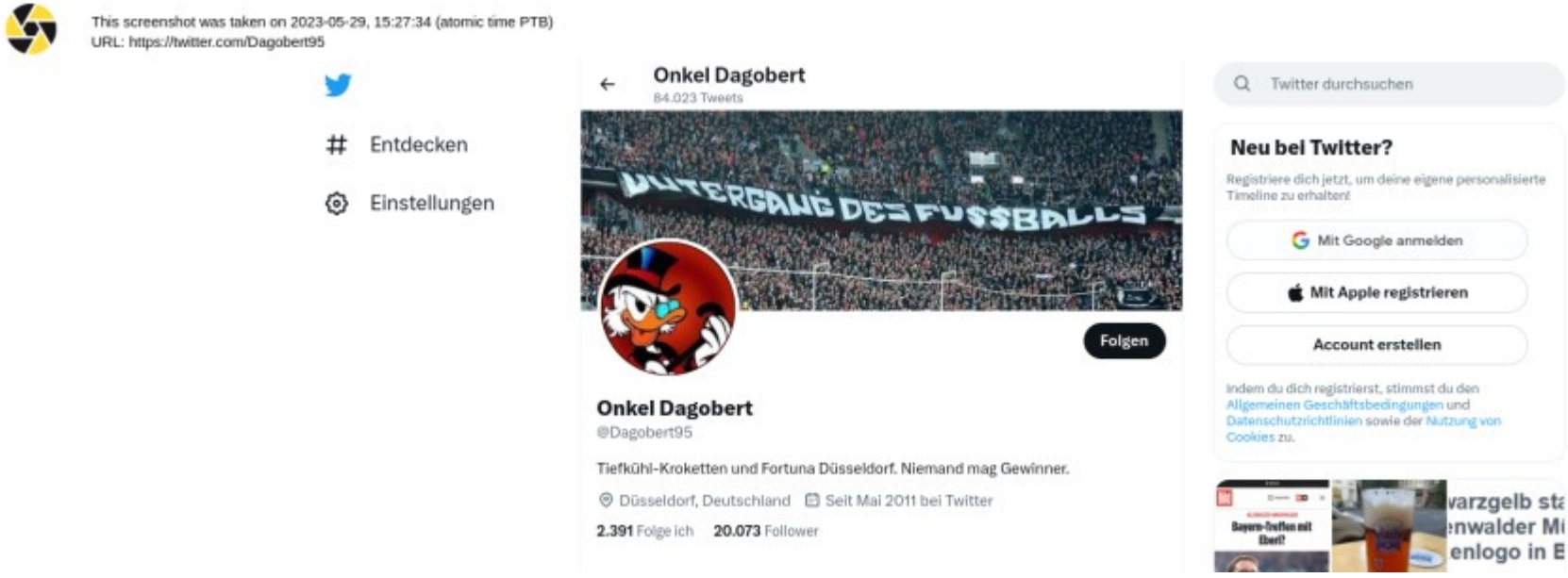
- Auf Screenshot sichtbar:
  - URL
  - Datum & Uhrzeit
  - Verfasser der Nachricht (bei z.B. Twitter)
  - Kontext muss ersichtlich sein (an wen richtet sich Kommentar oder Nachricht)
  - Auch Screenshot des Profils der Person
  - Keine persönlichen Information sichtbar (andere offene Tabs, etc.)
- Evtl. Weitere Infos/ Handlungen von Vorteil → hängt aber von Service ab (YouTube, Twitter, Facebook, …)
  - Handout: Rechtssichere Screenshots als Beweismittel bei Gewalt im Netz

Was tun? - Rechtssichere Screenshots



Was tun? - Rechtssichere Screenshots

- Browser Plug-in (Chrome):
  - Atomshot (Dokumentiert Datum & URL für jeden Screenshot)



Was tun? - Rechtssichere Screenshots

- App: **No-Stalk**
- Erleichtert Dokumentation von Stalking-Vorfällen
- Verschlüsselter Upload von Fotos, Videos, Audio
- Dokumentiert: Wo, Wer, Wann, Was zu jedem Upload
- Materialien können über Website gesammelt & chronologisch runtergeladen werden

Fragen?

Rechtliche Einordnung

Vorab:

- Wertung “rechtlich relevant” ≠ automatisch richtig
- Rechtlicher Weg kann für Betroffene schwer sein, ist nicht für alle der richtige Weg/ der gewünschte

Grundlagen

- Allgemeines Persönlichkeitsrecht aus Art. 2 Abs. 1 GG i.V.m. Art. 1 Abs. 1 GG jeder Person

  → Schutz der Intimssphäre, Privatssphäre, Sozialsphäre

  → Recht auf informationelle Selbstbestimmung, Recht am gesprochenen Wort

- Recht am eigenen Bild aus KUG (Kunsturhebergesetz)

“Rechtlich Relevant”

- Verletzung des Allgemeinen Persönlichkeitsrechtes
- Verletzung des Kunsturhebergesetzes (nicht konsensuales Verbreiten von Fotos) - § 33 KUG
- Strafbare Handlungen in dem Zusammenhang (nicht abschließende Liste):

  → Gefährdenes Verbreiten personenbezogener Daten - § 126 a StGB

  → Ausspähen, Abfangen von Daten, Verbreitung, Vorbereitung dieses Handelns - §§ 202a, 202b, 202c, 202d StGB

  → Bedrohung, Beleidigung, Verleumdung - §§ 241, 185, 186, 187 StGB

  → Unaufgefordertes Versenden pornographischer Inhalte - § 184 Nr. 6 StGB

  → Stalking - § 238 StGB

Rechtliche Handlungsoptionen

	Außergerichtlich	Gerichtlich
Gegen den*die Täter*in	Abmahnung, Strafbewehrte Unterlassungserklärung	Strafrechtlich Zivilrechtlich Gewaltschutz
Gegen Plattformanbieter*innen	Beschwerde mit Ziel der Inhaltsentfernung	Zivilrechtlich

Rechtliche Handlungsoptionen

Zivilrechtlich **Bürger*in gegenüber Bürger*in**	**Strafrechtlich** **Staat gegenüber Bürger*in**
Klage auf Schadensersatz, Unterlassen, (Folgen-)Beseitigung	Anzeige, Anstoß der Strafverfolgung
Einstweilige Sicherungsverfügung, Gewaltschutz	Nebenklage

Außergerichtlich	Zivilrechtlich	Strafrechtlich
*Betroffene*r* Mahnungserklärung (= Schreiben) *Täter*in* **Ergebnis:** Eventuell folgt Täter*in Aufforderung	*Betroffene*r* → Kontakt mit Anwält*in Klageeinreichung am Zivilgericht Wird Täter*in („Beklagte*r) zugestellt *Täter*in* Gerichtsverhandlung mit Betroffene*r und Täter*in Gerichtsurteil nach Ablauf der Verhandlungen **Ergebnis:** Anspruch ja oder nein	*Betroffene*r* → Strafanzeige Staatsanwaltschaft wird tätigt Bringt Anklage vor Gericht (Strafrechtskammer) *Täter*in* Verhandlung Gerichtsurteil **Ergebnis:** Strafbarkeit von Täter*in ja oder nein – Geld-/ Freiheitsstrafe/ Auflagen

Beispiel: Spionagesoftware

	Außergerichtlich	Zivilrechtlich	Strafrechtlich
Gegen Täter*in	Mahnung, nicht mehr Daten abzufangen; Unterlassungs-erklärung vorlegen	Anspruch Software zu deinstallieren, Daten zu löschen, Schadensersatz wie Schmerzensgeld (Sicherungsverfügung: ggf Geräte, auf denen Daten sind, sichern)	Strafbar = Ausspähen, Abfangen von Daten sowie die Verbreitung nach §§ 202a, 202b, 202d StGB
Gegen Plattform-betreiber*in	Gepostete Inhalte melden	Schadensersatz, wenn Prüfpflichten nicht nach gegangen	

Beispiel: “Dickpics”/ Cyber Harassment

	Außergerichtlich	Zivilrechtlich	Strafrechtlich
Gegen Täter*in	Mahnung, Strafbewehrte Unterlassungs-erklärung	Unterlassen (Person muss Verhalten stoppen), Folgenbeseitigung (Löschen von Kommentaren/Bildern), Schmerzensgeld	Beleidigung nach § 185 StGB Strafbar nach § 184 Nr. 6 StGB (https://dickstinction.com/)
Gegen Plattform-betreiber*in	Inhalt melden	Schadensersatz bei Verletzung der Prüfpflicht	

Zivilrechtlicher vs. strafrechtlicher Prozess

- Bürger*in klagt gegen Bürger*in
- Verfahrensgestaltung selbst in der Hand

- **Probleme:**

  → Last Beweise selbst zu erbringen

  → nicht abschätzbare Verfahrensdauer

  → ggf selbst zu tragende Kosten

- Staat (Vertreten durch Staatsanwaltschaft) klagt gg. Bürger*in
- Amtsermittlungsgrundsatz (Staatsanwaltschaft erbringt Beweise)

- **Probleme:**

  → Verfahrensgestaltung nicht in der Hand der Betroffenen → nur Möglichkeit der Nebenklage

  → Kontakt mit Polizei und Staatsanwaltschaft

Prozessführung

- Beweissicherung

  - rechtssicher → siehe hateaid.org:

  - ggf URL speichern

  - Die NO STALK App des WEISSEN RINGS

- Zeug*innen

  - zur Unterstützung

  + Hilfe bei Erstellung von Beweisen

- Rechtliche und psychosoziale Beratung

- Prozesskostenhilfe

WEISSER RING
Wir helfen Kriminalitätsopfern.

Die NO STALK App

Die Stalking Tagebuch-App des WEISSEN RINGS

Dokumentieren Sie einfach alle Stalking-Vorfälle per Foto-, Video- sowie Sprachaufnahmen chronologisch und lückenlos mit Ihrem Smartphone (Betriebssystem: mindestens iOS 11 oder Android 4.4). Ihre Aufnahmen zählen bei der Polizei bzw. vor dem zuständigen Gericht als vollwertige Beweise! Die NO STALK App des WEISSEN RINGS unterstützt Sie dabei, aktiv und selbstbestimmt gegen Stalking vorzugehen.

NO STALK App –
Ab sofort in Ihren APP Stores verfügbar!

Laden im App Store
JETZT BEI Google Play

Betroffenen-/Opferrechte im Strafverfahren

- Möglichkeit der psychosozialen Prozessbegleitung
- Möglichkeit der Anwesenheit einer Vertrauensperson
- Adressdatenschutz
- Aufzeichnung von Vernehmungen
- Position der Nebenklage

Outro

Ausblick

- Relevanz digitaler Gewalt nicht genügend anerkannt

  → Justiz, Politik, Plattformbetreiber*innen, Entwickler*innen

- Fehlende Sensibilisierung
- Digitale Gewalt im Nahfeld bei IT Sicherheit nicht mitgedacht

Forderungen

- Öffentlichkeitsarbeit & Prävention
- Forschung und Monitoring

  → Ausmaß abschätzen

  → besseres Verständnis
- Expertise von Beratungsstellen auf- & ausbauen
- Digitale Gewalt im Nahfeld bei Digitalisierungsstrategien mitdenken
- Spy-Apps verbieten

Wie Betroffene im Umfeld unterstützen?

Abhängig von den Bedürfnissen der Betroffenen...

- vorsortieren von Nachrichten & Kommentaren anbieten (bei Hate Speech)
- Beweissicherung und Dokumentation unterstützen
- Öffentliches solidarisieren (Counterspeech)
- gemeinsam Beratungssangebote suchen

Anlaufstellen für Betroffene

- Hateaid.org, auch mit Anleitungen zu Vorgehen
- frauen-gegen-gewalt.de
- Hilfetelefon "Gewalt gegen Frauen": 116 016

Vielen Dank!

Feedback ? → ag-link@riseup.net

ag-link.xyz/events

Weiterführendes Material

Weiterführendes Material (Links)

- Broschüre Cyberstalking entgegen treten
- Checkliste Digitale Trennung
- Leitfaden zum Umgang mit digitaler Gewalt
- Geschlechtsspezifische Gewalt in Zeiten der Digitalisierung