„Sicher im Netz -

Wie schütze ich mich vor Staat, Großkonzernen und Stalkern?“

Andrea 'Princess' Wardzichowski
Chaos Computer Club Stuttgart e.V.

Vortrag zu den Frauenwochen Esslingen für
Frauen helfen Frauen Esslingen e.V.
https://www.cccs.de/
princess@cccs.de

Mein Vortrag beginnt mit meinem Nickname. Nur durch dessen (Mit-)Verwendung kann ich andeuten, daß ich privat unterwegs bin.

Coronabedingt findet dieser Vortrag online statt.

Über den CCCS / über mich

Über den CCCS:

Seit Sommer 2001 Treffen
Seit Oktober 2003/4 monatliche Vortragsreihe
Spaß am Gerät, aber auch Gefahren beim bedenkenlosen Einsatz von Technik

Über mich:

Seit November 1990 im Netz aktiv
(Mail, News, IRC, Relay Parties, CCC)
Heute: CCCS e.V. (Presse), Haecksen, querulantin.de, Herbstakademie der Alumni der dt. Studienstiftung, XPDays Germany 2019, Gastvorlesung HdM 2020

In vielen großen und inzwischen auch in vielen kleinen Städten gibt es sog. Chaostreffs, die im Sinne des CCC e.V. agieren, der 1986 in Hamburg gegründet wurde.

Ich selber bin auch schon sehr lange im Netz unterwegs und habe meine Homepage aufgebaut, damit man meine aktuellen Veröffentlichungen und Vorträge eher findet, als meine Jugendsünden aus Usenet-Zeiten.

Desweiteren pflege ich selber eine gewisse Paranoia und man findet hoffentlich nur wenige Bilder im Netz, dafür aber meine Veröffentlichungen, nicht jedoch Telefonnummern und meine Wohnadresse.

Man möchte weder, daß die eigenen „Fans“, noch die Menschen, die einen nicht mögen ungefragt vor der eigenen Haustür auftauchen.

Daher drehen sich die meisten meiner Vorträge um den **Datenschutz**, aber auch andere Themen sind spannend!

Agenda

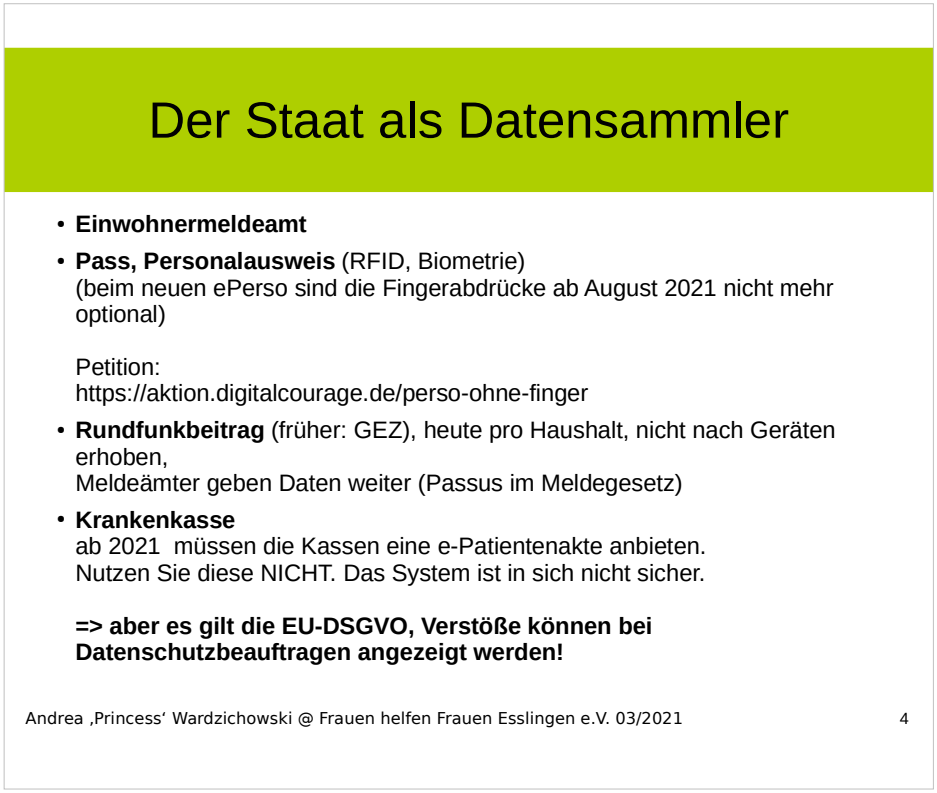
- Der Staat als Datensammler
- Wieviel müssen Großkonzerne wissen?
- Alternativen zu Großkonzernen
- Schutz gegen Stalker

In einem normalen Leben in Deutschland sammelt schon der Staat recht viele Daten, ist aber an die EU-DSGVO gebunden. Dennoch sollte man an allen Stellen mit der Preisgabe seiner Daten vorsichtig sein.

Großkonzerne wie google oder apple wissen allein durch unser Nutzungsverhalten des Smartphones sehr viel über uns. Es wird aufgezeigt, wie man das zumindest verminden kann.

Die gute Nachricht ist: es gibt viele Alternativen.

Nicht zuletzt kann auch vom eigenen (Ex-)Partner Gefahr ausgehen. Wie man sich hier schützen kann, wird ausführlich behandelt.



Wenn man in Deutschland lebt, kommt man nicht darum herum, einige seiner **Daten von Gesetzes wegen abzugeben**. Ich habe zu diesem Zweck auch einmal das Meldegesetz gelesen. Das Lesen von Gesetzestexten ist für Nichtjuristen zugegebenermaßen schmerzhaft, aber für eine CCCS Referentin gelegentlich notwendig ;-)
Die Einwohnermeldeämter geben auch Daten an Mammographie-Praxen weiter, dies ist vom Gesetzgeber so verfügt worden.

Zwischenfrage: muß man einen Ausweis mit sich tragen?
Nein! Man muß nur Perso oder Paß besitzen, der darf aber zuhause liegen. Aus praktischen Erwägungen ist es aber besser, ihn bei sich zu haben.

Der **Rundfunkbeitrag** wird nunmehr pro Haushalt erhoben, es gibt meines Wissens fast keine Möglichkeit, diesen nicht zu entrichten. Es gibt einen Vorteil des Systems: die „Klinkenputzer", die Nichtzahler zuhause aufgespürt haben, wurden von den Sendeanstalten entlassen. Hier gab es immer wieder abendfüllende Zwischenfälle am Rande der Legalität.

Inzwischen herrscht auch **Krankenkassenpflicht.** Die Krankenkasse hält besonders **intime und heikle Daten** vor. Daher muß man auch die Entwicklung der neuen **Krankenkassenkarte** sehr genau beobachten. Geht hier die Sicherheit flöten, ist der Zugriff und vielleicht auch die **Änderung von Gesundheitsdaten möglich!** Das Bild alleine auf der neuen eGK hilft übrigens gegen fast nichts, das war nur eine teure Aktion und wird den Mißbrauch nicht eindämmen. Als besonders gefährlich werden **Smartphone-Apps der Krankenkassen** erachtet. Das Smartphone ist kein sicheres Gerät.
e-Patientenakte: im Gegensatz zu einer Fehlbuchung bei der Bank ist es zu spät, wenn Ihre Gesundheitsdaten EINMAL öffentlich sind.

Datenschutzgesetz

- Bundesdatenschutzgesetz, seit Mai 2018: EU-DSGVO
- Landesdatenschutzgesetze
- Angepasste Datenschutzgesetze
- Zweckbindung bei der Datenerhebung
- Datensparsamkeit
- Datenschutzbeauftragter (Bundes-, Landes-, Firmen, KK, öffentliche Stellen, Schulen, Hochschulen...)

=> **Volkszählungsurteil**, Informationsfreiheitsgesetz, Transparenz bei der Verarbeitung von **personenbezogenen Daten**

Hier in der Bundesrepublik Deutschland gilt so gut wie überall eines der **Datenschutzgesetze**, die **personenbezogene Daten**, deren Speicherung und Verarbeitung, schützen. Seit Mai 2018 haben wir europaweit hohe Standards.

Grundsätze sind hierbei immer eine **Zweckbindung** bei der Erhebung von Daten (sie dürfen nicht anlaßlos erhoben werden), sowie die **Datensparsamkeit** (es dürfen nur die Daten erhoben werden, die für einen Zweck auch notwendig sind).

Jede Stelle, die personenbezogene Daten speichert, muß einmal im Jahr **kostenlos Auskunft** darüber geben, welche Daten sie gespeichert hat (auch die Schufa! Die verlangen ganz frech trotzdem Gebühren).

Allerdings nimmt nicht jede Stelle und nicht jede Firma es so genau mit dem Datenschutz: gelegentlich muß man einmal **nachfragen**, ob alles mit rechten Dingen zugeht, notfalls auch öfter als einmal. **Verstöße** können beim Landes- und Bundesdatenschutzbeauftragten gemeldet werden! (Habe dies auch schon gemacht!)

Firmen und öffentliche Stellen müssen zudem einen eigenen Datenschutzbeauftragen bestellen, der für Anfragen dieser Art zur Verfügung stehen muss!

Was aber ist mit Firmen, die ihren Hauptsitz und ihre **Server und Speicher nicht in Deutschland** stehen haben? Hier ist Vorsicht geboten!

Großkonzerne

- Google
- Apple
- Microsoft
- Social media
- Vertragspartner
- Versandhändler, u.a. Amazon

Google und Apple haben durch ihr Smartphonebetriebssystem bereits eine erhebliche Marktmacht.
Google bietet inzwischen soviele Dienste an, dass ganze Persönlichkeitsprofile entstehen können.

Microsoft hat mit Windows den Desktop-Markt fest im Griff, ebenso den Office-Markt. Hier gibt es aber brauchbare und auch zu MS-Office kompatible Lösungen.

Social Media „liefert" man sich idR. selbstständig und freiwillig aus.

Durchleuchten sie aber Ihre Vertragspartner. Mein Stromversorger wollte letztens mein Geburtsdatum wissen zur Authentifizierung. Dies ist aber ohnehin keine gute Idee, SO geheim ist ein Geburtsdatum meist nicht.

Geben Sie auch bei Versandhändlern nur soviel preis, wie eben nötig. Meist ist KEINE Telefonnummer nötig.

Amazon sammelt auch sehr viele Daten, hier kann man aber auch sehr viel abschalten und einschränken!

Was speichern Webseitenanbieter, Händler Großkonzerne und social media (1)?

Webseitenanbieter

- IP-Adresse
- Browserversion
- Von welcher Webseite kam der Klick
- Cookies sind weit verbreitet
- Leider auch: Tracker für gezielte Werbung

Händler:

- Adresse
- Zahldaten (Kontoverbindung, Kreditkarte, Paypal)

Die IP-Adresse ist eine Nummer, unter der Ihr Rechner im Netz erreichbar ist. IdR. wird diese von Ihrem Internetprovider jeden Tag dynamisch neu vergeben.

Ihre Identität wäre darüber nur festzustellen, wenn eine Straftat begangen wird und die Ermittler ZEITNAH (d.h. innerhalb von ca. 7 Tagen) beim Provider vorstellig werden und Namen und Adresse des Nutzers erfragen. Länger werden diese Daten aus Datenschutzgründen nicht gespeichert, da die Vorratsdatenspeicherung derzeit (zu Recht!) ausgesetzt ist.

Cookies sind kleine Dateien, die auf Ihrem Rechner gespeichert werden, damit der Webseitenanbieter Sie „wiedererkennen" kann, da er es über die IP-Adresse ja eben nicht kann. Cookies sind auch sinnvoll beim Einkauf, damit auch nach einer Verbindungsunterbrechung festgestellt werden kann, welches denn Ihr Warenkorb mit welchen Waren war.
Sinnvoll ist es aber dennoch, die Cookies mit dem Schließen des Browsers (einstellbar) zu löschen, um nicht zu viele Spuren zu hinternlassen.

Erwachsene hinterlassen auch bei Händlern ihre Adresse und natürlich Zahldaten, dies kommt bei Kindern eher weniger vor und diese sollten dahingehend sensibilisiert werden.

Was speichern Webseitenanbieter, Händler Großkonzerne und social media (2)?

Großkonzerne und social media

- Adressbuch
- Kontakte
- Aktivitäten
- GPS-Koordinaten
- Funkzelle (Smartphone)

Facebook & whatsapp: es fließen Daten, vor allem das Adressbuch. Whatsapp kam letzten Monat mit neuen, noch weitergehenden Datenschutzbestimmungen heraus. Viele Nutzer wollten dem dann nicht mehr zustimmen und sind zu signal oder threema abgewandert, selbst im total Nicht-technischen Bereich (Sportvereine, Elternvertreter, DLRG…).

Aktivitäten: facebook pinwand.
Auch: Businessplattformen wie xing oder linkedin sammeln Daten für „Empfehlungen".

Mobilfunkanbieter: ohne Funkzelle kann man natürlich keine Anrufe empfangen, aber GPS Koordinaten müssen nicht immer ansein, draußen auch nicht unbedingt WLAN, nur fallweise (Cafe, Bib…).

Alternativen zu Großkonzernen

Software	Alternative
Google als Suchmachschine	startpage.com, duckduckgo.com, qwant.com
Google maps	Openstreetmap osm.org, App osmand
Google play store	f-droid.org
Android Smartphone ohne google:	z.B. OnePlus
Gmail.com / Mailadresse	posteo.de, mailbox.org, web.de, GMX
Microsoft office	libreoffice nextcloud und onlyoffice
apple	--
whatsapp (gehört zu facebook)	signal, threema
Zoom, Microsoft Teams, Cisco Webex (Videokonferenzen)	Jitsi Meet BigBlueButton

Zu sehr vielen Anwendungen gibt es inzwischen GUTE Alternativen, auch um schulischen Software-Bereich.

Soziale Netzwerke, Vor- und Nachteile

- Zunächst: das Internet ist ein wunderbarer Raum zum **Kommunizieren** und zur **Wissensgewinnung**!
- „früher“: alle Freunde durchtelefonieren.
  Heute: alle per facebook oder whatsapp einladen
- Auch: **Sportvereine** haben keine „Telefonkette“ mehr. Aber hat auch **jedes Kind unbeschränkt Internetzugang**?
- Werden Menschen ohne Smartphone **abgehängt**?
- Bekommen Menschen ohne Internetzugang **weniger Rabatte**?
- Datenspuren (Äußerungen, Fotos)
- Daten liegen oft **im Ausland unter unklarer Rechtslage!**

Noch nie war es so leicht, **an Wissen zu gelangen**, wie heute. Früher endete mein Wissenshunger an dem Füllstand der Hamburger Öffentlichen Bücherhalle. Mehr als dort war für mich nicht zugänglich. Heute kann man auf unzählige Wissensdatenbanken zugreifen. Kernkompetenz ist zweifellos **„gut suchen“ können und die Bewertung von Quellen.**

Wenn man sich an **gewisse Regeln** hält, kann man viel Spaß haben und auch viele tolle Menschen kennenlernen. Die „Regeln“ sollten wie Verkehrsregeln begriffen werden. Diese hat man verinnerlicht und man begreift sie auch nicht als Last, sondern einfach als sinnvoll.

Wichtig: das Leben muß auch ohne Internet lebbar sein, ohne Nachteile! Nicht jeder will und kann am Internet teilnehmen. Manche Menschen haben nicht das Geld, einen Rechner und Internetzugang zu unterhalten. **Dafür gibt es hier in der Bibliothek Leihrechner!**

Schutz vor Datenmißbrauch

- Datensparsamkeit leben
- Telefonnummer bei Versandhändlern nicht angeben, wenn nicht nötig
- Geburtsdatum möglichst geheimhalten
- Einfache Adresssperre beim Einwohnermeldeamt
- Bei aktiver Teilnahme am Netz (Diskussionsforen, Leserbriefe) ein Pseudonym und eine andere Mailadresse verwenden

Mein Datenschutzgefühl und -gefüge zieht sich durch mein ganzes Leben und fängt damit an, Formulare nicht bis zuletzt auszufüllen. Dies ist online manchmal schwieriger als auf Papier, weil Webseiten zuweilen Dateneingaben erzwingen.

Es geht aber auch: Musterfrau, Musterstrasse, 0711234567890.

Mithilfe des Geburtsdatums werden Anfragen beim Einwohnermeldeamt und an anderen Stellen leichter.

Allerdings nutzen auch Arztpraxen dies am Telefon zur leichten Identifizierung (bei Namenskombinationen die einfacher sind als mein Name) und auch zum Abgleich, ob der Name richtig verstanden wurde am Telefon.

Die einfache Adresssperre beim Einwohnermeldeamt verhindert nicht in allen Fällen die Adressabfrage, aber z.B. dass man als Erstwähler von allen Parteien Post bekommt. Auch für die Rundfunkabgabe hilft sie leider nicht.

Überlegen Sie sich, ob sie alle Einlassungen im Netz unter Ihrem richtigen Namen tätigen. Ja, das führt auch zu unkontrolliertem hatespeech, aber es gilt trotzdem, Ihre Privatsphäre zu schützen. Politiker sind leider jetzt schon sehr ungeschützt.

Schutz gegen Stalker: Passworte

- Passwortsicherheit
- Passworte nie weitergeben
- Smartphone sichern (PIN mit 5 Stellen, Biometrie und „wischen“: besser als nichts, empfehle ich aber nicht)

Traditionelle Rollenklischees sorgen auch im Jahr 2021 immer noch dafür, dass die Männer Rechner und Smartphones einrichten und dann ggf. auch die Passworte kennen.

Erlangen Sie die Hoheit über Ihre Privatsphäre zurück, ändern Sie PIN und Passworte!

Passwortsicherheit

- Die Grundlage für jedwede Absicherung
- **Niemals ein Passwort an zwei Stellen** verwenden => es wird komplex. Lösung:
- **Passwortsafe**, z.B. keepassx
  Masterpasswort gut verwahren
- **Passwortsystem** mit Gedichten oder Liedern:
  FidEsdF,aLg.
  Ergänzt um 2 Zeichen pro Webseite/Versender
- Wo möglich: **2-Faktor-Authentifizierung**
  (wie bei PIN und TAN beim Banking)

Ein Masterpasswort sollte am besten aus einem ganzen Satz bestehen. Man spricht hier auch oft von einer Passphrase.

Sichere Passworte sollten heute mindestens 12 Stellen haben. Verwendet werden sollte Groß- und Kleinschreibung, Ziffern und die Zeichen . , $! (Punkt, Komma, Dollar, Ausrufezeichen).

Grundlage bildet ein Gedicht oder eine Liedzeile, wie oben werden die Anfangsbuchstaben genommen:
“Festgemauert in der Erden steht die Form, aus Lehm gebrannt.“
Zu dieser Grundlage, die persönlich ist und die man sich gut merken kann, ergänzt man vorne oder hinten 2 Zeichen für den jeweiligen Anbieter, also z.B. AZ für Amazon oder OT für den OTTO Versand usw.
Aus „ein“ könnte die Ziffer 1 werden, aus „to“, „too“, „two“ die Ziffer 2, aus der Silbe „eight“, „late“ die Ziffer 8, bzw. l8.

Viele Versandhändler bieten inzwischen auf eine 2-Faktor-Authentifizierung an, diese muss oft separat eingeschaltet bzw. angefordert werden und bietet mehr Sicherheit.

SingleSignOn

- Im beruflichen Kontext GOLD wert
- Im privaten: Tun Sie es nicht:
  - Mit facebook einloggen
  - Mit Google einloggen
  - Mit Apple einloggen
  - Mit Ebay einloggen
- Ungute Verbindung zwischen unterschiedlichen Unternehmen, Daten besser streng separieren!

Viele Plattformen bieten inzwischen an, sich gar keinen neues Konto (Login ist ja meist die Mailadresse) anzulegen, sondern sich mit einem bestehenden Konto wie facebook, google, apple, Ebay einzuloggen. Im beruflichen Rahmen ist dies angesagt, vor allem weil hier der Anbieter nur einer ist, nämlich die Firma/der Arbeitgeber. Im Privaten aber können wir von so einer Verbindung nur abraten, es entsteht eine ungute Verbindung von Firmen, die sonst nichts miteinander zu tun haben und wir wissen nicht, welche personenbezogenen Daten in den USA zusammengeführt werden, denn dort gilt die EU-DSGVO nicht!

Es gilt: separate Passworte verwenden!

Schutz gegen Stalker: Browser/surfen

- Passworte nicht im Browser abspeichern, allenfalls mit Masterpassword (firefox)
- Passworte aus dem Browser werfen: https://support.mozilla.org/de/kb/passworter-verwalten-speichern-loeschen-aendern
- Privates Browserfenster nutzen oder Historie regelmäßig löschen
- Cache und Cookies löschen

=> generell leider: Aktivitäten in social media vermeiden / herunterfahren,
vor allem keine Fotos hochladen, diese können GPS-Koordinaten enthalten!

Ohnehin gilt auch zuhause und gerade im Home-Office: bei Abwesenheit den Bildschirm sperren.

Passworte im Browser abzuspeichern ist zwar sehr bequem, aber nehmen Sie das auch ein wenig als Gedächtnistraining!

Sind die Passworte im Browser gespeichert, kann man sie aber auch wieder entfernen.

Wenn Sie das private Browserfenster benutzen, werden weder URLs (Adressen von Webseiten) noch Eingaben im Browser gespeichert, ihre Historie (z.B. Suche nach dem Frauenhaus) kann nicht zurückverfolgt werden. Auch nicht Ihre Route zur Beratungsstelle unter vvs.de.

Cache (Zwischenspeicher des Browsers) und Cookies sollten Sie regelmäßig löschen, auch aus technischen Gründen. Da verspult sich nach längerer Browsernutzung auch gern einmal etwas.

In Fotos befinden sich Metadaten, sog. EXIF-Daten. Sie enthalten sinnvolle Dinge wie Datum und Uhrzeit, aber bei eingeschaltetem GPS am Smartphone eben auch die Koordinaten des Aufenthaltsorts.

Schutz gegen Stalker: Smartphone

- (Mobil-)Telefonnummer ändern
- Sodann **threema statt whatsapp** benutzen:
  hier muss man weder Mailadresse noch Telefonnummer angeben
- Smartphone auf **Spyware** untersuchen:
  Schwierig! Suchen nicht auf dem Startbildschirm, sondern in den installierten Apps nach: familylink, pctattletale, mspy, autoforward, spybubble, ThetruthSpy, Mobipast, spyine, Highster Mobile, SpyPhone, Life360
- Ungetestet:
  Kaspersky Internet Security for Android
  kostenlos über den google playstore

Je nach Lage kann es nötig sein, die Mobilnummer zu ändern. Nach einer Umfrage vor einiger Zeit ist dies aber bei eigentlich allen Anbietern gegen eine Gebühr innerhalb weniger Tage möglich. Die neue Nummer nur sehr kontrolliert weitergeben, **vorher whatsapp deinstallieren!** Sonst hat die sofort jeder im Adressbuch gleich wieder.

In den installieren Apps (nicht auf dem Startbildschirm!) nach Applikationen suchen, die auf spyware hindeuten.

Die o.g. Auflistung von SpyApps habe ich durch Eingabe in die Suchmaschine erhalten:
Android App Cheating Spouse

Die Kaspersky App gibt es leider nur über den google playstore.

Bei **threema** erhält man eine eindeutige ID, die man an Kommunikationspartner weitergeben kann. Dies bedeutet, dass man nicht über die Telefonnummer oder Mailadresse ungewollt auffindbar ist. So kann man sich sehr gezielt nur bei wenigen Vertrauenswürdigen Menschen melden und ihnen die neue Nummer mitteilen.

Werkseinstellungen oder Beweise sichern?

- Werkseintellungen setzen tilgt jegliche Spyware
- Vorher aber: Bilder, Adressbuch, Chatverläufe sichern
- Nachteil: für Strafanzeigen und Prozesse sind alle Beweise weg
- Neues/gebrauchtes Smartphone besorgen neue SIM-Karte, neue Nummer

Ist die Lage sehr ernst und wird frau bereits verfolgt und überwacht, kann das Smartphone jederzeit auf Werkseinstellungen gesetzt werden, aber dann ist wirklich ALLES weg, was man nicht vorher sichert. Zudem bekommt der Stalker dies auch mit, was andere Folgen haben kann.

Zudem ist es manchmal wünschenswert, Beweise zu sichern.

Sich „mal eben" ein neues Smartphone zu kaufen, ist sicher für die betroffenen Frauen nicht drin. Wären sie finanziell gut gestellt, könnten sie eine andere Wohnung finden und einfach gehen, statt ins Frauenhaus zu müssen. Fragen sie im Bekanntenkreis herum, auch beim CCC in Ihrer Nähe, ob jemand ein gebrauchtes Smartphone überhat. Das alte kann dann in der Schublade weiterlaufen, das neue mit einer neuen SIM sichert die Kommunikation mit den vertrauenswürdigen Menschen.

Datenschutz in Corona-Zeiten

- Ich zahle weiter bar, es hat sich nicht gezeigt, dass das Virus über Zahlungsmittel übertragen wird
- Restaurants und Gaststätten:
  Die Verordnung ist sehr schwammig, es sollte reichen wenn EIN Gast pro Tisch Kontaktdaten hinterläßt, und zwar entweder Wohnadresse ODER Mailadresse ODER Telefonnummer.

Ich meide Kartenzahlung seit jeher, weil jeder Vorgang eine Datenspur hinterlässt. Hierbei ist unerheblich, ob es EC-Kartenzahlung ist, Geldkarte oder Kreditkarte. Zahlen per Smartphone kommt für mich ohnehin nicht in Frage, da ich nicht mein gesamtes Leben einem unsicheren Gerät anvertrauen möchte.

Lesetips

Steffen Heuer, Pernille Tranberg:
“Mich kriegt Ihr nicht“

Webseite / Verein / Petitionen / Broschüren:
https://www.digitalcourage.de/

In diesem Buch werden alle Tipps, die ich hier gebe und noch viel Mehr erklärt. Im Anhang sind genaue Schritte beschrieben, wie man alles umsetzt. Für Laien wären Screenshots noch hilfreicher, aber leider ändern sich die Programme zu oft für gedruckte Bücher.

Gut wäre, wir könnten all dies wieder auf Cryptoparties unterrichten.

Veranstaltungstips

Cryptoparty: können Corona-bedingt leider derzeit nicht stattfinden

Regelmäßige **Vorträge**: idR. 2. Donnerstag im Monat, Stadtbibliothek, 19:30, derzeit leider ebenfalls nicht.

Tips für diejenigen im Umfeld Stuttgart.

Für Ihren Wohnort: informieren Sie sich, in vielen großen und kleinen Städten gibt es Ableger des CCC mit spannenden Veranstaltungen!

Fragen / Diskussion

?

?

?