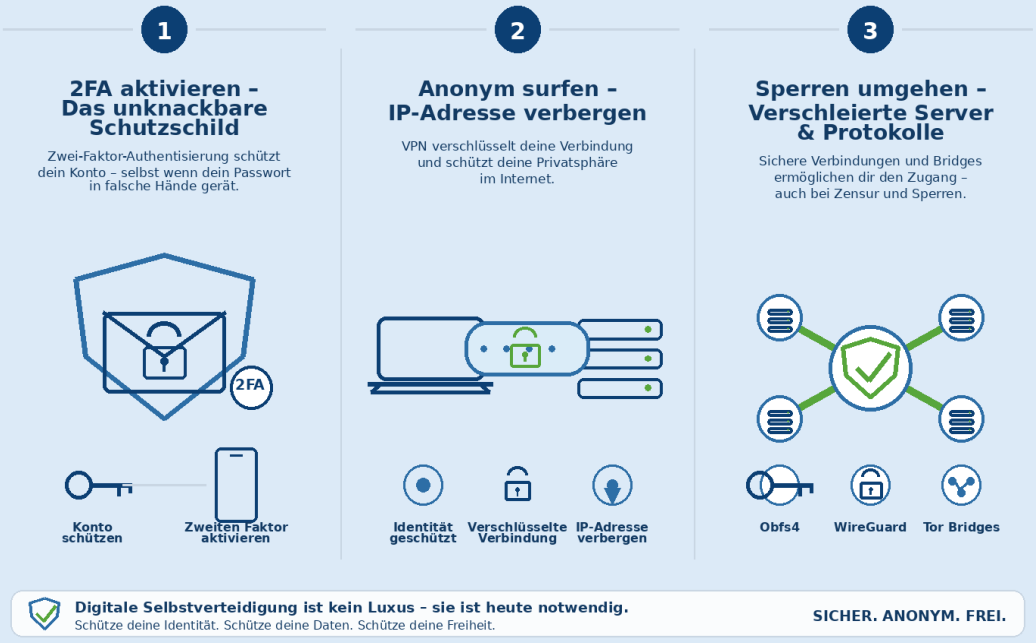
MICHAEL B. BARNES
BÜRGERANLIEGEN • STELLUNGNAHMEN • KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

2026-08-08

Digitale Selbstverteidigung: Leitfaden zum Schutz Ihrer Privatsphäre im Internet



Inhalt

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Wenn „Kinderschutz“ als Trojanisches Pferd für die totale Internet-Kontrolle missbraucht wird

📖 KAPITEL 1: VORWORT

Wer schützt uns vor der Politik?

1.1 Der Generalverdacht im digitalen Raum

Wir müssen den Tatsachen ins Auge sehen: Es sind die Regierenden selbst, die den rechtschaffenen Bürgern das Leben im Internet durch immer neue Regulierungen und digitale Hürden systematisch unmöglich machen. Während die herrschende Politik unter dem Deckmantel des Schutzes eine lückenlose digitale Kontrolle hochzieht, zeigt sich ein unerträgliches und brandgefährliches Paradoxon im echten Leben.

1.2 Die journalistische Kernrecherche von Dominik Kettner

Um die immense Tragweite und Brisanz der folgenden Enthüllungen zu verstehen, müssen wir zuerst einen Blick darauf werfen, wer die Fakten ans Licht gebracht hat. Die journalistische Kernrecherche zu den Hintergründen der neuen EU-Altersverifikations-App stammt von Dominik Kettner, dem Gründer und Geschäftsführer des führenden Fachunternehmens *Kettner Edelmetalle*.

Kettner ist kein Unbekannter: Als ausgewiesener Finanz- und Wirtschaftsexperte landete er mit seinem aufrüttelnden Werk *„Der digitale Euro – Die größte Enteignung der Geschichte“* auf Platz 1 der SPIEGEL-Bestsellerliste. Seine tiefe Skepsis gegenüber der zunehmenden Digitalisierung und dem Abbau von Bürgerrechten kommt nicht von ungefähr. Durch seine tägliche Arbeit mit physischen Sachwerten und Vermögenssicherung analysiert er seit Jahren die schleichenden Pläne der Zentralbanken und Regierungen zur Bargeldabschaffung und lückenlosen Bürgerüberwachung. Für seine tiefgründigen Analysen holt er regelmäßig hochkarätige Insider, Juristen und Ökonomen in sein Studio, um politische Nebelkerzen sachlich und rechtssicher zu demontieren. Was er in seinen Publikationen voraussagte, wird heute Schritt für Schritt bittere Realität.

1.3 Die unzensierten Fakten zur EU-Altersverifikation

Viele Bürger spüren es bereits im Alltag: Der Login bei Instagram, TikTok oder Facebook hakt, Konten sperren sich scheinbar grundlos. Während die Nutzer noch ratlos vor ihren Bildschirmen sitzen, tritt EU-Kommissionspräsidentin Ursula von der Leyen vor die Kameras und verkündet eine Nachricht, die tiefer blicken lässt als jedes gelekte Geheimdokument der Welt.
Ihre offizielle Botschaft lautet:
„Unsere europäische App zur Altersverifikation ist technisch bereit und steht den Bürgern bald zur Verfügung. Diese App wird es den Nutzern ermöglichen, ihr Alter beim Zugriff auf Online-Plattformen nachzuweisen – genau wie Geschäfte nach einem Altersnachweis fragen, wenn Menschen alkoholische Getränke kaufen.“ [1, 2]
Von der Leyen zieht in ihrer Rede selbst den direkten, entlarvenden Vergleich zur jüngsten Vergangenheit. Sie erinnert stolz daran, wie die Kommission während der Pandemie in einer Rekordzeit von nur drei Monaten die Covid-App entwickelte. Damals hieß es, das Scannen des Zertifikats sei ein „temporäres Notfallinstrument“. 78 Länder auf vier Kontinenten nutzten das System. Den offiziellen Beweis und die gesamte Erklärung zu dieser folgenschweren Technologie können Sie direkt im Presseportal der Europäischen Kommission nachlesen: europa.eu.

1.4 Die Corona-App als psychologische Blaupause

Und genau diesen „Erfolg“ überträgt die EU nun eins zu eins auf die Internet-Verifikation. Als Bestsellerautor Dominik Kettner diese Passage in seiner journalistischen Recherche einspielt und analysiert, wird das perfide Spiel aus Brüssel sofort offengelegt. Kettner kommentiert fassungslos:
„Ich hatte Gänsehaut, als ich hörte, was hier gerade vorbereitet wird. Denselben Prinzipien der Covid-Zeit, demselben Modell.“
Die Enthüllungen von Dominik Kettner zeigen schonungslos, dass im Untergrund ein gigantischer, koordinierter Kontroll-Apparat hochgezogen wird. Die Behauptung, dass diese App dem Jugendschutz dient, bricht bei genauer Betrachtung der technologischen Fakten sofort in sich zusammen.

1.5 Der Bau der staatlichen Überwachungsinfrastruktur

Kettner legt offen, wer im Hintergrund die Fäden zieht und massiv an der Entrechtung der Bürger verdient. Die amtierende Politik hat den Bau dieser Infrastruktur klammheimlich an dieselben Großkonzerne übergeben, die bereits bei der Corona-Infrastruktur hunderte Millionen an Steuergeldern eingestrichen haben.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

SAP und die Deutsche Telekom bauen im Auftrag der Brüsseler Eliten ein zentralisiertes Netzwerk auf.
Die Telekom und der Software-Riese SAP – die damals bereits über 214 Millionen Euro Steuergelder für die Corona-Warn-App kassierten – haben auch jetzt wieder den Auftrag erhalten, das System zu bauen. Mit dem Geld der Steuerzahler wird hier ein digitales Gefängnis hochgezogen. Die Millionenbeträge und Verträge für diese Überwachungsinfrastruktur können Sie offiziell in den Berichten des Bundesrechnungshofes einsehen: bundesrechnungshof.de.

1.6 Die Zwangsverknüpfung mit der Digital ID

Kettner warnt in seinen Analysen eindringlich vor den wahren Konsequenzen: Das System ist so aufgebaut, dass die Alters-App nahtlos mit der staatlich kontrollierten, digitalen Identität (Digital ID) verknüpft wird. Den unumstößlichen Beweis hierfür liefert das offizielle EU-Amtsblatt auf EUR-Lex, welches die gesetzliche Zusammenführung von Altersnachweisen und der europaweiten eIDAS-Identitätsinfrastruktur schwarz auf weiß dokumentiert: eur-lex.europa.eu.
Es ist die totale Schikane und digitale Erpressung: Entweder Sie geben Ihre intimste Privatsphäre an der staatlichen Schleuse ab, oder Sie fliegen komplett aus dem Internet. Kettner verknüpft dieses System mit den schleichenden Plänen zur Bargeldabschaffung und der Einführung des digitalen Euros. Das Ziel dieser elitären Gruppen im politischen Sumpf ist die absolute, unumstößliche Kontrolle über das Denken, das Schreiben und die Finanzen jedes einzelnen Bürgers.
Damit kommt die unerträgliche Wahrheit im Untergrund ans Licht: Die Corona-App dient den Mächtigen heute als exakte technologische und psychologische Blaupause für eine dauerhafte, niemals endende Kontrolle des gesamten Internetzugangs. Es hat im Kern überhaupt nichts mit dem Schutz von Kindern zu tun! Der Kinderschutz wird von Brüssel nur als moralischer Vorwand missbraucht, um jede Gegenrede im Keim zu ersticken. Wer künftig das Netz nutzen will, muss sich über diese Infrastruktur digital vor dem Staat ausweisen.

1.7 Das ewige Muster der Mächtigen: Moral, Infrastruktur, Zwang

Wie Bestsellerautor Dominik Kettner lückenlos offenlegt, folgt der Weg in die totale digitale Kontrolle immer derselben dreistufigen Strategie:

1. **Die moralische Erpressung:** Am Anfang steht immer eine moralische Begründung, die so emotional aufgeladen ist, dass sie unangreifbar wirkt. Diesmal missbraucht man das Schutzbedürfnis unserer Kinder. Wer es wagt, die Überwachungsinfrastruktur kritisch zu hinterfragen, wird sofort gesellschaftlich mundtot gemacht und als „Gegner des Kinderschutzes“ gebrandmarkt.
2. **Die schrittweise Gewöhnung:** Die App wird als „innovative, nutzerfreundliche Lösung“ auf dem Silbertablett serviert. Sechs Länder haben das System bereits im Hintergrund getestet.
3. **Der flächendeckende Zwang:** Aus dem vermeintlich freiwilligen Werkzeug wird schleichend ein Standard, aus dem Standard eine absolute Voraussetzung. Am Ende betrifft es nicht mehr nur die Jugend, sondern jeden einzelnen Bürger, der sich im Internet bewegen möchte.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

1.8 Das unerträgliche Paradoxon und der Kontrollverlust auf den Straßen

Betrachtet man diese Entwicklung aus der Vogelperspektive, stößt man auf eine unerträgliche und brandgefährliche Doppelmoral der herrschenden Politik, die die Bürger fassungslos zurücklässt: Während die Regierenden Abermillionen Fremde unkontrolliert ins Land lassen, wird der rechtschaffene, einheimische Bürger im digitalen Raum wie ein Schwerverbrecher unter Generalverdacht gestellt. Seit Beginn der Flüchtlingsbewegung unter der Merkel-Regierung sind bis heute über 4 Millionen Schutzsuchende nach Deutschland zugewandert. Allein im Jahr 2025 wurden 168.543 Asylanträge registriert, wobei der Anteil von im Inland geborenen Kleinstkindern unter den Antragstellern bei 15,6 Prozent lag.
Die bittere Realität, die vor der Regierungsbank verschwiegen wird, ist der vollständige Kontrollverlust auf unseren Straßen. Während die Politik die Grenzen offen ließ und die reale Sicherheit im Land kollabieren ließ, wodurch unzählige Menschen und insbesondere wehrlose Kinder im echten Leben Opfer von Gewalt wurden, dreht der Staat die Schuld um. Die Zahlen des Bundeskriminalamtes belegen dieses vollständige Versagen der Regierenden auf dramatische Weise. Während die Politik wegschaut, zeigt die offizielle Polizeiliche Kriminalstatistik des BKA, dass im Bereich der Gewaltkriminalität nichtdeutsche Tatverdächtige mit rund 43 Prozent massiv überrepräsentiert sind. Die polizeilichen Daten zeigen schwarz auf weiß: Die Kriminalitätsbelastung ist bei dieser Gruppe etwa viermal höher als bei der deutschen Bevölkerung. Besonders verwerflich ist, dass im Zuge dieser Entwicklung erwiesenermaßen immer mehr unschuldige Kinder im realen Leben zu Schaden kommen, was sich auch im kontinuierlichen Anstieg tatverdächtiger Kinder in den Kriminalstatistiken widerspiegelt.
Hier wird ein Schuh daraus: Die reale und akute Bedrohung für Leib und Leben geht von dem durch die Politik verursachten Kontrollverlust aus. Anstatt jedoch genau hier anzusetzen, die Grenzen rigoros zu sichern und das eigene Volk vor dieser Gewalt zu schützen, erlassen die Mächtigen lieber Gesetze zur digitalen Totalüberwachung. Sie stellen den rechtschaffenen Bürger unter Generalverdacht, während auf unseren Straßen das Chaos regiert. Das ist die absolute Bankrotterklärung einer Regierung, die die Augen vor den echten Opfern verschließt und stattdessen die Privatsphäre der eigenen Bevölkerung vernichtet.

1.9 Die Verantwortlichen im politischen Sumpf

Dieses historische Versagen und die aktuellen Zustände in unserem Land haben wir einzig und allein den etablierten Altparteien der amtierenden Politik zu verdanken. Weder die AfD noch das BSW tragen hierfür die Schuld, da sie sich nicht in der Regierungsverantwortung befinden. Das ständige, ermüdende Framing in den Medien gegenüber alternativen politischen Kräften dient nur als Ablenkungsmanöver, um von den echten, drastischen Problemen im Land abzulenken. Es gibt einflussreiche Gruppen in diesem politischen Sumpf, die diese Zustände und den Verlust unserer Privatsphäre ganz bewusst so wollen.

1.10 Ein global koordinierter Plan: Der Rotherham-Missbrauchsskandal

Dass es sich hierbei um keinen Brüsseler Alleingang, sondern um einen global koordinierten Plan elitärer Netzwerke handelt, beweist ein direkter Blick nach London und Australien. Fast zeitgleich preschte die australische Regierung mit Netzsperren voran. Und noch am selben Tag postete der britische Premierminister Keir Starmer auf der Plattform X, dass er „alles tun wird, was benötigt wird, um Kinder im Internet sicher zu machen“.

MBB
MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Hinter dieser weltweiten, zeitgleichen Kampagne im Namen des Kinderschutzes steckt jedoch bittere Heuchelei. Die historischen Fakten der britischen Justiz zeichnen ein völlig anderes Bild von den wahren Absichten dieser Akteure. Während Keir Starmers Amtszeit als Leiter der britischen Staatsanwaltschaft von 2008 bis 2013 ereignete sich der tiefgreifende Missbrauchsskandal von Rotherham, bei dem mindestens 1.400 Kinder rituell und systematisch missbraucht wurden. Die Strafverfolgungsbehörden unter seiner Führung versagten damals auf ganzer Linie, stuften die Hauptzeugin als unglaubwürdig ein und stellten die Ermittlungen einfach ein. Echte Opfer, echte Täter, greifbare Akten – und keine Strafverfolgung. Die unzensierten, offiziellen Untersuchungsberichte zu diesem historischen Behördenversagen sind direkt im Regierungsportal des UK Government Home-Office für jeden unabhängig nachprüfbar dokumentiert: www.gov.uk.
Wenn genau diese elitären Kreise, die beim realen Schutz weggeschaut haben, nun zeitgleich eine lückenlose Internet-Überwachung fordern, ist das an Verlogenheit nicht zu übertreffen. Es geht ihnen nicht um den Schutz der Schwachen. Es geht um die lückenlose Kontrolle darüber, wer wann welche Seite im Internet aufruft, liest und denkt.

1.11 Ihre Verteidigungslinie: Warum Abwarten keine Option mehr ist

Wenn die größte Gefahr für unsere Freiheit von staatlichen Gesetzen, Schikanen und digitalen Identitäts-Zwängen der Mächtigen ausgeht, dürfen wir nicht länger passiv bleiben. Echte Sicherheit im Netz gibt es von der herrschenden Politik nicht geschenkt – wir müssen sie uns selbst von den Entscheidungsträgern zurückholen. Digitale Selbstverteidigung ist heute kein Hobby mehr für IT-Spezialisten, sondern Bürgerpflicht für jeden, der frei bleiben will.
Wer wegschaut, wird kontrolliert. Wer handelt, bleibt frei!

KAPITEL 2: DAS E-MAIL-POSTFACH

Der Generalschlüssel zu Ihrem Leben

2.1 Die reale Gefahr im Alltag

Das eigene E-Mail-Postfach ist der absolute Mittelpunkt unseres gesamten digitalen Daseins. Ob Online-Banking, Amazon, soziale Netzwerke wie Facebook und X oder staatliche Zugänge: Fast jede Registrierung im Internet läuft über Ihre E-Mail-Adresse.
Das macht Ihr Postfach zum begehrtesten Ziel für Kriminelle. Wenn Hacker Zugriff auf Ihre E-Mails erlangen, können sie bei all Ihren anderen Konten einfach auf „Passwort vergessen“ klicken. Sie erhalten den Bestätigungslink direkt in Ihr geknacktes Postfach und übernehmen im Handumdrehen Ihr gesamtes Leben.

2.2 Die Datenskandale der großen Provider

Viele Menschen wiegen sich in Sicherheit, weil sie seit Jahrzehnten bei großen Traditionsanbietern sind. Doch die Realität sieht anders aus: Erst kürzlich wurde wieder über massive Datenlecks berichtet, bei denen sensible Kundendaten im Darknet gelandet sind.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Regelmäßig tauchen Berichte über gestohlene Passwörter auf, die zeigen, wie massiv Nutzerdaten durch Schadsoftware im Alltag abgegriffen werden.
Während der Staat den unbescholtenen Bürger mit der Chatkontrolle bis ins intimste Detail ausspionieren will, schaut er bei den echten Datenkraken und den Sicherheitslücken der Großkonzerne weg.

2.3 So überprüfen Sie den Sicherheitsstatus Ihrer Konten

Wer auf Nummer sicher gehen will, lässt seine Konten von Zeit zu Zeit überprüfen. Professionelle Sicherheitssoftware meldet unbefugte Datenabflüsse sofort.
Die offizielle Webseite von Kaspersky zur Überprüfung finden Sie hier: kaspersky.de. Ob Ihre eigene E-Mail-Adresse bereits in kriminellen Datenbanken im Netz kursiert, lässt sich zudem über den kostenlosen *Identity Leak Checker* des Hasso-Plattner-Instituts sekundenschnell überprüfen. Die direkte Prüfseite lautet: hpi.de.
Hinweis: Den vollständigen und ausführlichen Leitfaden zu diesem Thema finden Sie in unserem Dokument Nummer 84 unter www.klartext-info.online.

2.4 Die goldene Regel gegen Phishing: Der Blick in die App

Hacker versuchen täglich, über gefälschte Rechnungen oder dringende Zahlungsaufforderungen per Mail an Ihre Daten zu kommen. Doch ein geschulter Blick entlarvt diese Betrüger: Die Formatierung ist fehlerhaft oder weicht vom Original ab. Die wichtigste Praxis-Regel lautet hier: Ignorieren und niemals Links in solchen E-Mails öffnen! Wenn ein Anbieter, eine Bank oder eine Plattform wirklich etwas Wichtiges von Ihnen will, hinterlässt er diese Nachricht grundsätzlich direkt in Ihrem persönlichen Account oder in der offiziellen Smartphone-App – und nicht im ungeschützten Postfach. Gehen Sie im Zweifelsfall immer manuell über die offizielle Webseite oder die App des Anbieters, um den Status zu prüfen. Rechnungen von echten Bestellungen erkennen Sie daran, dass sie fehlerfrei geschrieben sind und Sie korrekt mit Ihrem vollständigen Namen ansprechen.

2.5 Digitale Selbstverteidigung mit Sinn und Verstand

Der beste Schutz vor Cyber-Kriminellen ist ein gesundes Misstrauen. Wenn Sie eine Nachricht oder einen Absender – insbesondere aus dem Ausland – nicht zweifelsfrei einordnen können, lassen Sie im Zweifelsfall einfach die Finger davon. Wer als Anfänger kopflos agiert, verliert. Wer mit Sinn und Verstand vorgeht, bleibt sicher.
Die absolute Basislinie für ein unknackbares System besteht aus zwei simplen, aber hochwirksamen Schutzmauern: Zufällig generierte, starke Passwörter, die man sich niemals im Kopf merken kann, sowie die Aktivierung der Zwei-Faktor-Authentisierung (2FA). Das Bundesamt für Sicherheit in der Informationstechnik betont in seinen Leitfäden, dass diese Kombination die wichtigste Hürde gegen Identitätsdiebstahl ist. Offizielle Informationen erhalten Sie unter: bund.de.

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Hinweis: Den vollständigen und ausführlichen Leitfaden zu diesem Thema findest du in unserem Dokument Nummer 84 unter www.klartext-info.online.

🔒 KAPITEL 3: DIE ZWEI-FAKTOR-AUTHENTISIERUNG

Das unknackbare Schutzschild

3.1 Die Sicherheitslücke herkömmlicher Passwörter

Bisher schützten die meisten Menschen ihre Konten nur mit einem einfachen Passwort. Wenn dieses Passwort jedoch bei einem Datenskandal gestohlen wird, ist das Konto sofort offen.

Die Zwei-Faktor-Authentisierung (2FA) schließt diese gefährliche Sicherheitslücke komplett. Sie funktioniert wie ein Tresor mit zwei verschiedenen Schlössern: Um dich anzumelden, brauchst du nicht mehr nur dein Passwort, sondern zusätzlich einen zweiten, kurzzeitigen Bestätigungscode. Diesen bekommst du direkt auf dein eigenes Smartphone geschickt.

3.2 Warum Hacker hier absolut chancenlos sind

Selbst wenn ein hochprofessioneller Hacker dein Passwort erbeutet hat, kann er sich ohne diesen zweiten Code von deinem Smartphone nicht einloggen. Er steht unweigerlich vor einer verschlossenen Tür.

Die amtierende Politik drängt uns zwar in eine totale Abhängigkeit von staatlich kontrollierten Identitäts-Apps. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) betont in seinen Empfehlungen zum Accountschutz jedoch ausdrücklich, dass wir diese echten Schutzmaßnahmen selbst in die Hand nehmen müssen – anstatt den Kontroll-Systemen der Machthaber zu vertrauen.
Man muss sich lediglich einmal die Mühe machen, diese Funktion in den Einstellungen des eigenen Mail-Anbieters einzuschalten, um seine digitale Festung gegen den staatlichen und kriminellen Zugriff zu sichern.

3.3 Offizielle Hilfsmittel des BSI

Wer das System der zwei Faktoren genauer verstehen oder einrichten möchte, findet verbraucherfreundliche und unabhängige Informationen direkt auf den staatlichen Portalen:

- **Informationsseite**: Die offizielle Informationsseite des BSI zum Thema Accountschutz erreichst du unter:
  🔗 bund.de
- **Erklärvideo**: Wie dieses Prinzip genau funktioniert und warum es jeden Login bombensicher macht, zeigt das offizielle Erklärvideo direkt beim BSI-Verbraucherportal:
  🔗 bund.de

MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

🏰 KAPITEL 4: PASSWORT-SICHERHEIT UND DIE FESTUNG DER VERSCHLÜSSELTEN ANBIETER

4.1 Das große Risiko einfacher Passwörter

Der häufigste Fehler im Internet ist die Bequemlichkeit bei Passwörtern. Viele Menschen nutzen extrem einfache Passwörter oder verwenden ein und dasselbe Kennwort für mehrere Seiten gleichzeitig.
Wird dann nur ein einziger Anbieter gehackt, bricht dein gesamtes digitales Kartenhaus zusammen. Ein sicheres Passwort muss folgende Kriterien erfüllen:

- Es muss lang sein.
- Es muss aus einer wirren Kombination von Zeichen bestehen.
- Es darf niemals ungeschützt im Browser gespeichert werden.

4.2 Die sichere Alternative zu den alten Anbietern

Wer den traditionellen Großanbietern nach den vielen Datenskandalen und der offensichtlichen Zusammenarbeit mit Behörden nicht mehr vertrauen möchte, findet heute extrem sichere Alternativen.
Ein hervorragendes Beispiel ist der Anbieter **Proton Mail**. Dieser hat seinen expliziten Sitz in der Schweiz – und liegt damit außerhalb der direkten EU-Zensurgewalt. Proton Mail bietet zudem einen komplett kostenlosen und werbefreien Grundzugang an.

4.3 Die Null-Zugriff-Verschlüsselung

Der riesige Vorteil wird in den offiziellen Sicherheitsfunktionen von Proton Mail erklärt: Durch eine sogenannte *Null-Zugriff-Verschlüsselung* sind deine E-Mails so stark geschützt, dass nicht einmal der Anbieter selbst oder Behörden deine Nachrichten mitlesen können.
Kombiniert mit einem starken Passwort und der Zwei-Faktor-Authentisierung (2FA) wird dein Postfach damit für Angreifer und staatliche Überwachungssysteme so gut wie unangreifbar. Es ist der direkte Mittelfinger gegen die Brüsseler Schikane.
Die offizielle Seite von Proton Mail erreichst du unter:
🔗 proton.me

🌐 KAPITEL 5: ANONYM SURFEN – VPNS UND DATENSCHUTZFREUNDLICHE BROWSER

5.1 Die Tarnkappe für die eigene Internetleitung (VPN)

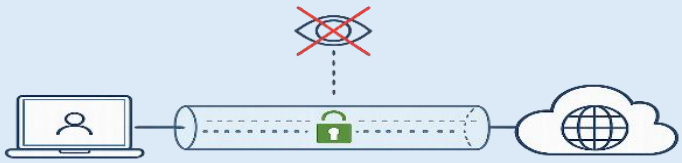
Wenn sich Nutzer ganz normal im Internet bewegen, hinterlassen sie bei jedem Klick digitale Spuren. Der jeweilige Internetanbieter sowie jede besuchte Webseite kennen die genaue IP-Adresse und können das gesamte Surfverhalten lückenlos protokollieren.
Ein virtuelles privates Netzwerk, kurz VPN, funktioniert an dieser Stelle wie ein digitaler Tunnel. Das Bundesamt für Sicherheit in der Informationstechnik (BSI)

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

erklärt die präzise Funktionsweise eines VPN ausführlich: Die Daten zwischen dem Endgerät und dem Server werden komplett verschlüsselt und sind für Außenstehende zu keinem Zeitpunkt mehr einsehbar.
Die offizielle BSI-Erklärung zum VPN-Schutz kann hier nachgelesen werden:
🔗 bund.de

5.2 Volle Legalität durch EU-Urteil bestätigt

Dass diese Technologie ein vollkommen legales Werkzeug zum Schutz der eigenen Privatsphäre ist, hat der Europäische Gerichtshof (EuGH) in einem Grundsatzurteil ausdrücklich bestätigt.
Das offizielle Urteil zur Rechtmäßigkeit von VPN-Verbindungen kann jederzeit in der Rechtsprechungs-Datenbank des EuGH eingesehen werden:
🔗 europa.eu



5.3 Alternative Browser statt Datenkraken

Die standardmäßig auf den Geräten vorinstallierten Browser leiten massenhaft Daten über das individuelle Nutzungsverhalten an die großen Tech-Konzerne weiter. Es existieren jedoch hervorragende, datenschutzfreundliche Alternativen für die tägliche Praxis:

- **Brave Browser**: Diese quelloffene Anwendung blockiert Tracker und Werbeanzeigen von Haus aus konsequent.
- **Tor Browser**: Wer nach der maximalen Anonymität sucht, greift zum Tor Browser. Wie das BSI zum Thema des Tor-Netzwerks ausführt, leitet dieser spezielle Browser die Verbindung dreifach verschlüsselt über verschiedene, dezentrale Knotenpunkte um. Dadurch wird es für Werbenetzwerke und staatliche Überwachungssysteme so gut wie unmöglich, die echte IP-Adresse oder den physischen Standort zurückzuverfolgen.

🚀 KAPITEL 6: ANONYM SURFEN UND STAATLICHE VPN-SPERREN IM NOTFALL UMGEHEN

6.1 Der Ernstfall: Was tun bei aktiver Netzzensur?

Sollte der Staat oder der eigene Provider versuchen, normale VPN-Verbindungen flächendeckend zu blockieren, bricht die gewohnte digitale Schutzmauer ein.
In einem solchen Fall von akuter Netzzensur lässt sich die staatliche Sperre mithilfe ausländischer Sicherheitssoftware durch drei konkrete, praktische Handgriffe sofort wirksam umgehen.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

6.2 Schritt 1 – „Verschleierte Server“ in der Anwendung aktivieren

Normale VPN-Verbindungen werden von staatlichen Blockadesystemen anhand ihrer Datenstruktur sofort erkannt und automatisch abgeschaltet. Große, ausländische Premium-Anbieter haben für dieses Szenario jedoch eine hocheffektive Tarnfunktion integriert.

- **Die Umsetzung**: Öffnen Sie die erweiterten Einstellungen Ihrer VPN-App und stellen Sie das verwendete Protokoll manuell auf *OpenVPN* um. Nun wird in der Serverliste der Menüpunkt „Spezialserver“ sichtbar.
- **Der Effekt**: Klicken Sie dort auf *verschleierte Server* oder aktivieren Sie den sogenannten *„Camouflage Mode“* des Anbieters. Diese Funktion verändert die Struktur der Datenpakete so grundlegend, dass sie für den Provider wie ganz normaler, harmloser Internetverkehr aussehen. Die staatliche Sperre greift somit vollkommen ins Leere.

Die genaue Funktionsweise dieser Technologie wird auf der offiziellen Hilfeseite von NordVPN detailliert aufgeschlüsselt:

🔗 nordvpn.com

6.3 Schritt 2 – Das Protokoll manuell auf „TCP-Port 443“ umstellen

Zensur-Sperren blockieren in vielen Fällen lediglich das standardmäßige Übertragungsprotokoll des VPN-Dienstes. Betroffene können den verschlüsselten Tunnel jedoch manuell umleiten.

- **Die Umsetzung**: Navigieren Sie in die erweiterten Verbindungseinstellungen Ihrer Sicherheitssoftware. Schalten Sie dort das Protokoll von *UDP* auf *TCP* um und wählen Sie als Ausgang den *Port 443*.
- **Der Effekt**: Port 443 ist exakt derselbe Kanal, über den das gesamte weltweite Online-Banking und alle sicheren, verschlüsselten HTTPS-Webseiten laufen. Ein Provider kann diesen spezifischen Port unmöglich sperren, ohne das gesamte wirtschaftliche und gesellschaftliche Internet des eigenen Landes komplett lahmzulegen.

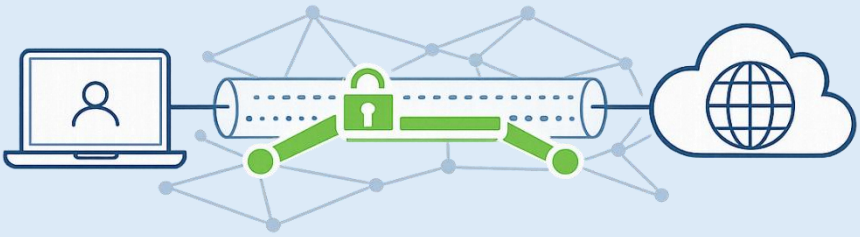
6.4 Schritt 3 – Den Tor-Browser mit „Bridges“ (digitalen Brücken) starten

Sollten kommerzielle VPN-Anbieter flächendeckend verboten und deren bekannte Server-IP-Adressen blockiert werden, hilft als letzte Instanz nur noch das dezentrale, unzensierbare Tor-Netzwerk.

- **Die Umsetzung**: Laden Sie den kostenlosen Tor Browser herunter. Wenn das normale Laden des Netzwerks blockiert wird, klicken Sie beim Starten der Anwendung auf den Button „Konfigurieren“ und navigieren Sie zum Abschnitt „Brücken“. Klicken Sie dort auf die Option „Brücken anfordern“.
- **Der Effekt**: Das System nutzt ab diesem Moment geheime, private Relays. Wie diese privaten Brücken-IPs im Detail funktionieren und warum sie von staatlichen Zensoren unmöglich flächendeckend erfasst oder blockiert werden können, erklärt die offizielle Dokumentation zur Zensurumgehung im Tor

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

Project Support Portal:
🔗 torproject.org



📋 KAPITEL 7: DIE CHECKLISTE FÜR DIE DIGITALE FREIHEIT

7.1 Die tägliche Verteidigungslinie im Netz

Sicherheit im Internet ist kein statischer Zustand, sondern ein fortlaufender Prozess. Nachdem die realen Mechanismen der Überwachung aufgedeckt und analysiert wurden, liegt es an den Bürgern selbst, aktiv zu bleiben. Nutzen Sie die folgende Checkliste, um Ihre Konten Schritt für Schritt in eine unknackbare digitale Festung zu verwandeln.

7.2 Konkrete Schritte für den digitalen Alltag

- **Das E-Mail-Postfach konsequent sichern**: Aktivieren Sie unverzüglich die Zwei-Faktor-Authentisierung (2FA) bei Ihrem bisherigen Provider oder wechseln Sie zu einem komplett verschlüsselten Anbieter.

- **WhatsApp-Backups lokal verschlüsseln**: Generieren Sie den 64-stelligen Sicherheitsschlüssel in den Chat-Einstellungen. Schreiben Sie diesen Code per Hand ab und legen Sie ihn sicher in einer analogen Dokumentenmappe ab. Vertrauen Sie keinem unverschlüsselten Cloud-Backup.

- **Digitale Datenspuren effektiv verwischen**: Nutzen Sie im Alltag konsequent einen datenschutzfreundlichen Browser sowie ein verschlüsseltes VPN, um Ihre IP-Adresse vor den Augen von Mobilfunkriesen und Werbenetzwerke zu verbergen.

- **Sperren im Ernstfall gezielt umgehen**: Prägen Sie sich die Notfall-Schritte für Ihren VPN-Dienst ein. Schalten Sie bei aktiven Blockaden auf verschleierte Server (Camouflage Mode) um oder nutzen Sie den Tor-Browser mit privaten Brücken (Bridges).

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

7.3 Den Druck auf die Politik erhöhen und die eigenen Rechte kennen

- **Das Recht auf ein Girokonto einfordern**: Das sogenannte De-Banking darf Bürger nicht finanziell isolieren. Informieren Sie sich unabhängig über das Recht auf ein Basiskonto, das jedem Bürger gesetzlich zusteht, direkt beim Bundesministerium der Justiz:
  🔗 bmj.de
- **Die regionalen Abgeordneten direkt kontaktieren**: Nutzen Sie Ihr gesetzliches Recht auf Gehör. Über die offizielle Abgeordnetensuche des Deutschen Bundestages können Sie Ihre regionalen Vertreter heraussuchen und Ihren Unmut über die digitale Totalüberwachung sowie den Kontrollverlust auf den Straßen direkt an die politischen Gremien senden:
  🔗 bundestag.de

- **Wahlprogramme kritisch prüfen**: Übernehmen Sie auch im realen Leben Verantwortung. Informieren Sie sich unabhängig abseits der etablierten Medien und setzen Sie an der Wahlurne ein bewusstes Zeichen für Freiheit und den Erhalt der Bürgerrechte.

🎯 KAPITEL 8: DAS FAZIT

Warum digitale Selbstverteidigung Pflicht ist!

8.1 Die Kehrseite der fortschreitenden Digitalisierung

Die Digitalisierung hat der Gesellschaft viele Erleichterungen gebracht. Aber sie hat die Menschen auch so verletzlich gemacht wie nie zuvor. Wer heute die Augen verschließt und blind den Standardeinstellungen der großen Tech-Konzerne, Mobilfunkriesen und politischen Vorgaben vertraut, gibt freiwillig den Schlüssel zur eigenen Freiheit ab.

8.2 Drei unumstößlichen Gründe für Ihr Schutzschild

Es existieren drei fundamentale Pfeiler, warum Sie Ihre digitale Festung ab heute niemals mehr herunterfahren dürfen:

1. **Die Privatsphäre ist Ihr persönliches Eigentum**: Wenn Bürger ihre Daten nicht selbst aktiv schützt, macht der Staat sie durch Gesetze wie die geplante europäische Chatkontrolle vollkommen gläsern. Was einmal im Netz gelandet ist, lässt sich nie wieder zurückholen.

2. **Der Schutz durch Konzerne und Politik ist eine reine Illusion**: Die ständigen Skandale und massiven Datenlecks bei Traditionsanbietern belegen, dass niemand Ihre Konten für Sie sichert. Ein gehacktes Postfach ist der Generalschlüssel zu Ihrem gesamten Leben – die Riegel dafür müssen Sie mit der Zwei-Faktor-Authentisierung selbst vorschieben. Während die herrschende Politik das Volk im realen Alltag auf den Straßen nicht mehr schützen kann, versucht sie im digitalen Raum die totale Ausspionierung.

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

3. **Konsequente Vorsorge statt reiner Schadensbegrenzung**: Es ist weitaus einfacher und sicherer, die digitale Festung durch dauerhaft eingeschaltete VPNs und datenschutzfreundliche Browser von vornherein hochgezogen zu lassen. Machen Sie es Angreifern, Datenkraken und staatlichen Überwachungssystemen im Alltag von der ersten Sekunde an systematisch so schwer wie möglich.

8.3 Der finale Appell an die Leserschaft

Über diese gefährlichen Entwicklungen und die drastischen Pläne der Politik wurde bereits im Vorfeld ausführlich und detailliert berichtet. Den vollständigen, unzensierten Leitfaden zur Absicherung Ihrer Konten finden Sie unter:
🔗 klartext-info.online
Nehmen Sie Ihre digitale Selbstbestimmung jetzt selbst in die Hand.
Wer wegschaut, wird kontrolliert. Wer handelt, bleibt frei!

Zurück zum Anfang

Mit freundlichen Grüßen

Michael B. Barnes

Michael B. Barnes

Impressum / Kontakt:

Michael B. Barnes
Hengeloer Str.1
49565 Bramsche
📧 E-Mail: info@klartext-info.online

Rechtlicher Hinweis

Dieses Dokument ist Teil des privaten Informations- und Aufklärungsprojekts **KLARTEXT** von Michael B. Barnes.

Der Bericht dient ausschließlich der Information sowie der öffentlichen Meinungs- und Diskussionsbildung. Er enthält eine Kombination aus dokumentierten Tatsachen, öffentlich zugänglichen Quellen, rechtlichen Einordnungen sowie persönlichen Bewertungen, Schlussfolgerungen, Vermutungen und Hypothesen des Autors. Diese sind entsprechend im Gesamtzusammenhang des jeweiligen Dossiers zu verstehen.

Alle Inhalte wurden nach bestem Wissen und Gewissen auf Grundlage der zum Zeitpunkt der Veröffentlichung verfügbaren Informationen erstellt. Trotz sorgfältiger Recherche kann keine Gewähr für Vollständigkeit, Aktualität oder die fortdauernde Richtigkeit sämtlicher Angaben übernommen werden. Neue Erkenntnisse oder spätere Entwicklungen können eine Überarbeitung oder Neubewertung einzelner Inhalte erforderlich machen.

Eine unveränderte Weitergabe des vollständigen Dokuments über den offiziellen Veröffentlichungsweg ist ausdrücklich erwünscht. Veränderungen, Kürzungen, aus dem Zusammenhang gerissene Zitate oder Bearbeitungen, die den Sinn oder die Aussage des Dokuments verfälschen, sind ohne ausdrückliche Zustimmung des Autors nicht gestattet.

Stand der Quellen und Rechtslage: Veröffentlichungsdatum des jeweiligen Dossiers.

Version: 1.1

Impressum:

https://www.klartext-info.online/impressum/

Zur Klartext-Info-Website

QR-Code

Weitere Beiträge, Aktualisierungen und Quellen:

www.klartext-info.online

Michael B. Barnes

Stand: 08.08.2026

MBB ← Zur Themenübersicht
WWW.KLARTEXT-INFO.ONLINE

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

⚠ WICHTIGER HINWEIS FÜR ALLE VERBRAUCHER:

Dieses Schreiben ist universell gültig!
Die journalistischen Enthüllungen in diesem Leitfaden nutzen die Deutsche Telekom lediglich als aktuelles Praxis-Beispiel. Die offizielle Beweislage der EU-Kommission zeigt unmissverständlich, dass **alle großen Netzanbieter und Mobilfunkkonzerne** (wie Vodafone, O2, 1&1 etc.) gleichermaßen als tragende Säulen in diese digitale Kontrollinfrastruktur eingebunden werden.
Sollten Sie Ihren Vertrag bei einem anderen Anbieter abgeschlossen haben, können Sie diese Vorlage **eins zu eins für Ihren Protest nutzen**. Tauschen Sie beim Kopieren des Textes im Adressfeld und im Fließtext einfach den Namen „Deutsche Telekom“ gegen den Namen Ihres jeweiligen Vertragspartners aus. Lassen Sie sich nicht täuschen: Der Schutz der Privatsphäre betrifft jeden Mobilfunk- und Internetnutzer, völlig unabhängig vom Logo auf der monatlichen Rechnung!

🗁 ANHANG: PRAXIS-BEISPIEL FÜR DIE DIGITALE SELBSTBESTIMMUNG

RECHTLICH UNWIDERRUFLICHE KÜNDIGUNG

Kundennummer: [Ihre Kundennummer]
Vertragsverhältnis: Mobilfunk / Festnetz / Internet
Kündigungstermin: Zum Ende der Mindestvertragslaufzeit

Sehr geehrte Damen und Herren,
ich habe erst vor Kurzem einen Vertrag mit Ihrem Unternehmen abgeschlossen. Nach intensiver Beschäftigung mit den aktuellen, öffentlich zugänglichen Entwicklungen rund um die europäische Digital-ID sowie die neue EU-Altersverifikations-App bin ich zu dem unumstößlichen Entschluss gekommen, meinen Vertrag nach Ablauf der Mindestvertragslaufzeit nicht fortzuführen.
Ich lehne jede technologische Entwicklung entschieden ab, die dazu führt, dass private Endgeräte der Bürger für staatliche Identitäts-, Verifikations- oder Kontrollfunktionen instrumentalisiert werden. Mein Smartphone ist mein persönliches Eigentum. Ich allein entscheide, welche Anwendungen sich darauf befinden und welchen Zweck sie erfüllen.

Mein Vertrauen in die Unabhängigkeit großer Netzanbieter wurde bereits während der Corona-Zeit nachhaltig erschüttert. Auf meinem eigenen Endgerät befand sich nachweislich die Corona-Warn-Infrastruktur, ohne dass ich einer Installation jemals bewusst zugestimmt hätte. Dieses Erlebnis hat mein Vertrauen in den respektvollen Umgang mit der Privatsphäre von Verbrauchern dauerhaft beschädigt. Ich werde

MBB MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com

nicht tatenlos abwarten, bis sich diese Form der digitalen Schikane unter dem Deckmantel neuer Verordnungen wiederholt.

Die offiziellen Pläne der EU-Kommission zur Verknüpfung von Internetzugängen mit digitalen Identitätsstrukturen sehe ich in tiefer Sorge vor einer lückenlosen digitalen Überwachung. Ich bin nicht bereit, ein Unternehmen finanziell zu unterstützen, dessen Infrastruktur nach den Erfahrungen der Vergangenheit als tragende Säule für die Umsetzung solcher Kontrollnetzwerke dient.

Aus diesen Gründen kündige ich meinen Vertrag vorsorglich zum nächstmöglichen Ende der Mindestvertragslaufzeit. Bitte bestätigen Sie mir den exakten Kündigungstermin schriftlich innerhalb der gesetzlichen Frist. Von telefonischen oder schriftlichen Rückgewinnungsversuchen bitte ich ausdrücklich Abstand zu nehmen. Darüber hinaus werde ich meine Beweggründe sowie meine persönliche und journalistische Bewertung dieser Infrastrukturpläne auf meiner eigenen Internetseite veröffentlichen, damit sich auch andere Verbraucher anhand der offiziellen EU-Beweislage ein eigenes Bild machen können.
Mit freundlichen Grüßen,
[Ihr Vorname] (Ihr Nachname)

MBB
MICHAEL B. BARNES
BÜRGERANLIEGEN · STELLUNGNAHMEN · KORRESPONDENZ
Hengelorstraße 1 | 49565 Bramsche | mbarnes61@outlook.com