



## IT-Sicherheit | Datenschutz | Hacking

Suchen

→ Wirf einen Blick in die Empfehlungsecke



MIKE KUKETZ



19. FEBRUAR 2021



11 ERGÄNZUNGEN



# Ungewöhnliche IT-Sicherheits- und Datenschutztipps – Teil1

## 1. Follower-Power



Über das [Fediverse](#) (Mastodon) hab ich gebeten, mir eure ungewöhnlichen IT-Sicherheits- und Datenschutztipps zu nennen. Es sind eine Menge an Tipps eingegangen, die das komplette Spektrum abdecken. Von sinnvoll über skurril bis hin zu gefährlich ist alles dabei. Es kamen so viele Tipps rein, dass ich diese in zwei Artikel aufgeteilt habe. Im vorliegenden ersten Teil habe ich eure Tipps in verschiedene Kategorien sortiert und sie ebenfalls kurz kommentiert. Auch habe ich mir erlaubt kleine Rechtschreib- und Grammatikfehler zu korrigieren.

Vorab sei gesagt: Es gibt keine allgemeingültigen Vorgehensweisen und Tipps, mit denen ihr euch vor allen Gemeinheiten schützen könnt, die in der IT-Welt lauern. Die vorgestellten Tipps können euch aber dabei helfen, euer persönliches Risiko zu minimieren. Allerdings solltet ihr immer bedenken, dass IT-Sicherheit und auch Datenschutz ein ständiger Prozess ist, der es notwendig macht, umgesetzte Maßnahmen regelmäßig kritisch zu hinterfragen und sich an neue Herausforderungen bzw. Gegebenheiten anzupassen.



Copyright © 2012 -2021 [Kuketz IT-Security](#)

IT-Sicherheit aus Karlsruhe

## 2. Allgemeine Sicherheit / Datenschutz

### 2.1 Zum Warmwerden ein paar Klassiker – nicht wirklich ungewöhnlich



Stecke keinen USB-Stick in deinen Rechner, den du irgendwo gefunden hast!

Der Tipp ist mindestens genauso alt, wie das damit einhergehende Problem: [BadUSB](#) . Es gibt noch weitere USB-Angriffsvektoren bzw. Risiken. Bleeping Computer hat eine schöne Übersicht zusammengestellt: [Here's a List of 29 Different Types of USB Attacks](#) . Allgemeiner Rat: Unbekannte USB-Sticks sollten nur in kontrollierten Umgebungen eingesteckt bzw. untersucht werden.



Neue Geräte wie Notebooks, Computer und Smartphones immer verschlüsseln, so ist das Problem viel geringer, wenn mal ein Gerät verkauft wird, in die Reparatur muss oder eben geklaut wird.

Die Aktivierung der geräteseitigen (Voll-)Verschlüsselung ist grundsätzlich eine gute Idee – sofern man selbst immer an die Daten rankommt. Gerade bei mobilen Geräten wie Notebooks oder Smartphones, die auch mal verloren gehen oder gestohlen werden. Die Vollverschlüsselung kann Angreifern den Zugriff / Zugang auf die Daten des Geräts erschweren. Wer sich allein auf die Verschlüsselung verlässt, begeht allerdings einen fatalen Fehler. Denn die Sicherheit der Geräteverschlüsselung ist von einem ganz entscheidenden Faktor abhängig: Die Geräteverschlüsselung bzw. der Schutz, den sie bietet, ist nur so gut, wie das verwendete Passwort / PIN. Das bedeutet: Der Sinn und insbesondere die Sicherheit der Geräteverschlüsselung steht und fällt mit der **Qualität** des verwendeten Passworts, Musters bzw. der PIN. Behaltet dies bitte stets im Hinterkopf.

Bei eBay könnt ihr Speichermedien erwerben, die von den ehemaligen Besitzern nur »oberflächlich« gelöscht wurden. In der Regel bedeutet das: Die Daten wurden in den Papierkorb verschoben und gelöscht. Die so gelöschten Daten sind nach wie vor vorhanden und lassen sich mit [Recovery-Tools](#) einfach wiederherstellen. Das [korrekte Löschen von SSD- bzw. Flashspeicher-Medien](#) ist in der Praxis gar nicht so einfach. Auch in diesem Fall kann die Verschlüsselung der Speichermedien helfen.



Weniger ist mehr. Es kann nichts angegriffen werden, was nicht da ist.  
Daher das KISS-Prinzip beachten und Komplexität vermeiden.

Das Prinzip »[Keep it small and simple / Keep it simple, stupid!](#)» (KISS) ist relativ effektiv, weil zu viel Komplexität meist mit dem Verlust der Übersicht und damit der Kontrolle einhergeht. Wendet das Prinzip möglichst in allen Lebensbereichen an – besonders aber in der digitalen Welt. Ein Beispiel zu KISS: Unsere Haushaltsgeräte (Fernseher, Kühlschrank, Radio, Waschmaschine etc.) sind allesamt »dumm« und können somit auch nie Teil des [Internet of Shit](#) werden.

Oder ein anderes Beispiel: Für eure WordPress-Seite könnt ihr euch ein optisch eindrucksvolles Theme mit vielen Funktionen einkaufen. Aber versteht ihr, wozu all die ganzen Funktionen eigentlich da sind? Komplexität bzw. zu viel (unnötige) Funktionen ist der größte Feind der IT-Sicherheit. Nehmt ein kleines, handliches Theme und seid bei der Auswahl eurer Plugins umsichtig.



Kein Backup – kein Mitleid

Ein hart formulierter Tipp, von dem man zumindest den ersten Teil beherzigen sollte: Das Anfertigen eines Backups. Erpresserische Schadsoftware ([Ransomware](#)) hat über die letzten Jahre massiv zugenommen. Ransomware befällt Rechner und **verschlüsselt** die Daten, die anschließend für den Nutzer dann nicht mehr abrufbar sind. Das Ziel: Für die Entschlüsselung der Daten fordert ein Angreifer üblicherweise einen Geldbetrag, der über ein Online-Bezahlungssystem zu entrichten ist. Es kann aber auch sein, dass eine Ransomware Daten ausschließlich verschlüsselt und euch nicht mehr die Möglichkeit einräumt, die Daten »freizukaufen«. Insbesondere vor diesem Hintergrund spielen Backups bzw. Datensicherungen eine essenzielle Rolle.

Aber auch bei ganz klassischen Problemen, wie einem Hardware-Defekt der Festplatte oder dem unbeabsichtigten Löschen von Daten kann euch ein Backup im wahrsten Sinne des Wortes »den Arsch retten«.

In der Praxis unterscheidet man zwischen verschiedenen [Sicherungsarten](#), wie der [Komplettsicherung](#) oder der [inkrementellen Sicherung](#). Gekoppelt mit einer passenden [Backupstrategie](#) kann daraus schon fast eine Obsession werden – je nachdem wie wichtig eure Daten eben sind. Gerade das Backup im Privatumfeld sollte

nach meiner Auffassung leicht zu händeln sein. Mein Backup ist nach dem KISS-Prinzip aufgebaut:

**Speicherort:** Externes USB-Gehäuse mit zwei Festplatten, die über [RAID-1](#) ↗ gespiegelt sind ([Icy Box IB-RD3621U3](#) ↗)

**Sicherungssoftware:** [BorgBackup](#) ↗

**Sicherungsart / Backupstrategie:** Während der Laufzeit werden automatisch [inkrementelle Backups](#) ↗ erstellt / einmal wöchentlich ein [vollständiges Backup](#) ↗

Persönlich rate ich euch von Backups in irgendwelchen flauschigen »Clouds« ab. Je nach Anforderung muss ein Backup auch nicht ständig über ein Network Attached Storage ([NAS](#) ↗) im Netzwerk erreichbar sein oder sogar über irgendein Web-Interface mit dem Internet verbunden sein.

“

Klick nicht einfach auf jeden Dialog. Lies dir die Meldung vorher durch.

Wer kennt das nicht? Auf AGB bzw. auch kurze Hinweise wird meist nur ein flüchtiger Blick geworfen und man redet sich unterbewusst ein: »Wird schon passen...« – gefolgt von einem Klick / Fingertipp. Die Folgen davon können ganz unterschiedlich sein. Sagen wir mal so: Wenn sich jeder an diesen Tipp halten würde, dann wären ganze Heerscharen von Admins / Service-Mitarbeitern vermutlich über Nacht arbeitslos. In der Praxis ist dieser Tipp im Grunde genommen eine essenzielle Grundvoraussetzung für die Nutzung eines jeden IT-Geräts bzw. Dienstes.

## 2.2 Windows-Tipps

“

Keine AV-Scanner einsetzen.

AV-Scanner gelten bei vielen Ottonormalanwendern noch immer als eines der Hauptschutzmaßnahmen im Kampf gegen Schadsoftware. Gleiches ist auch in Unternehmen und Organisationen zu beobachten, bei denen sich IT-Verantwortliche am [Stand der Technik](#) ↗ orientieren. In der Artikelserie »[Snakeoil](#)« zeige ich auf, dass sich AV-Scanner jedoch nur bedingt eignen, um ein System und die darauf befindlichen Daten nachhaltig vor Schadsoftware zu schützen. Vielmehr sollte diesbezüglich immer

auch bedacht werden, dass eine AV-Software selbst, aufgrund der Menge an möglicherweise in ihr schlummernden und noch nicht gefundenen bzw. veröffentlichten Sicherheitslücken, ein **Einfallstor** für Schadsoftware darstellen kann.

Insgesamt sicherlich ein Tipp, der polarisiert und nicht jeder so unterschreiben würde.

“

Für Windows: Dateierweiterungen immer anzeigen lassen.

Das Ausblenden von Dateierweiterungen ist eine Designentscheidung, die ich nicht nachvollziehen kann. Gerade Schadsoftware macht sich bspw. die Tatsache zunutze, dass der Windows-Dateimanager in der Standardeinstellung, bei bekannten Dateitypen, die Dateierweiterung nicht mehr anzeigt. Die harmlose Bilddatei `nackter_hintern_2021.jpg` wird entsprechend nur als `nackter_hintern_2021` angezeigt. Es ist allerdings auch möglich, Dateien eine doppelte Dateiendung zu geben.

Eine ausführbare Datei wie `nackter_hintern_2021.exe`, die Schadsoftware enthält, wird von einem Angreifer einfach in `nackter_hintern_2021.jpg.exe` umbenannt. Im Dateimanager wird die Datei dann als `nackter_hintern_2021.jpg` angezeigt. Ahnungslose Nutzer klicken die vermeintliche Bilddatei dann an und führen damit die Schadsoftware aus – mit ungewissen Folgen. Daher ist die dauerhafte Einblendung von Dateiendungen bzw. Dateierweiterungen mehr als empfehlenswert.

---

Der Kuketz-Blog ist spendenfinanziert!

**Mitmachen →**

---

## 2.3 Spezielle Tipps

“

Für manche Personen kann ein analoger Passwortsafe die bessere Wahl sein, denn sie verstehen, wie man ihn schützen kann/muss.

Dem schließe ich mich an. Denn gerade Anwender, die wenig technikaffin sind, tun sich mit dem Umstieg auf einen Passwort-Manager oft schwer. Wer damit partout nicht zurechtkommt, der nimmt sich ein Notizbuch und verwaltet darüber seine Online-Zugänge inkl. Passwörter. Diese Lösung ist natürlich mit diversen Nachteilen verbunden – insgesamt ist das allerdings allemal besser, als ein einfaches Passwort, das bei jedem Account zum Einsatz kommt.

In der [Empfehlungsecke](#) findet ihr zum Thema [Passwort-Manager](#) mehr Hintergrundwissen.



“

Wenn man Pakete in gebrauchten Versandverpackungen verschickt, sollte man vorher alte Adressaufkleber abreißen oder unkenntlich machen.

Das kann sinnvoll sein, wenn ihr nicht wollt, dass der Empfänger Details über eure letzte Bestellung bzw. die Adresse des vorigen Absenders erfährt.

“





RFID-blockierende Kartenhüllen im Portemonnaie und für den Reisepass.

Die meisten EC-/Kredit-Karten bieten das kontaktlose Bezahlen über [NFC](#)  an. Damit gehen allerdings Risiken für die Sicherheit und den Datenschutz einher. Man kann den RFID- / NFC-Chip nun entweder brachial außer Betrieb setzen, indem man die [Karte an der korrekten Stelle durchbohrt](#) oder man nutzt weniger invasive Techniken. Dazu zählt unter anderem die Deaktivierung des Chips über die Bank ([unter anderem die GLS-Bank bietet solch einen Service](#)) oder man nutzt einfach eine RFID-Kartenschutzhülle, [wie sie bspw. Digitalcourage anbietet](#) .

Aber auch in Personalausweisen und Reisepässen sind diese kleinen Chips anzutreffen. Auch hier können RFID-Kartenschutzhüllen vor dem unberechtigten / unbemerkten Auslesen schützen.



“

Am Router UPnP vollständig deaktivieren, damit nicht jeder Ranz-IoT-Kram einen Portforward einrichten kann.

[UPnP](#)  vereint diverse Protokolle, die eine IP-basierte Ansteuerung von Geräten ermöglichen – das [IGD-Protokoll](#)  (Internet Gateway Device) zählt bspw. dazu. Es wird benutzt, um bspw. dem Router anzuweisen, welche [Ports](#)  zu öffnen sind, damit eine Anfrage aus dem Internet den entsprechenden Rechner bzw. Dienst / Anwendung erreichen kann. Dies machen sich unter anderem Anwendungen für Filesharing, Videokonferenzen oder auch Messenger zu Nutze. Quasi in Eigenregie werden dann am Router Ports geöffnet. Und nicht nur Anwendungen, sondern eben auch Geräte wie Waschmaschinen, Überwachungskameras und Co., die man unter dem Begriff [Internet of Things](#)  (IoT) zusammenfasst, reißen zunehmend »Lücken« in den Router. Dazu interessant: [Shodan: Suchmaschine für das »Internet of Shit«](#).


Die automatische Portkonfiguration ist eine Komfortfunktion und insbesondere unbedarfte Anwender, die keine Kenntnis darüber besitzen, was eine Portweiterleitung überhaupt ist, profitieren von UPnP. Versierte Nutzer bzw. solche, die auf Sicherheit bedacht sind, sollten allerdings in Erwägung ziehen UPnP auf ihrem Router zu deaktivieren – im Router-Handbuch wird die Deaktivierung in der Regel erklärt.

“ Besucht online und später wieder offline CryptoPartys.

Auf [CryptoPartys](#)  treffen sich Menschen mit dem Ziel, Verschlüsselungs- und Verschleierungstechniken zu erlernen. Dazu zählt bspw. die [E-Mail-Verschlüsselung via GnuPG / OpenPGP](#) oder auch die korrekte Verwendung des Tor-Netzwerks. Wer Lust hat solch eine CryptoParty zu besuchen, kann sich über anstehende [Termine](#)  informieren. Insgesamt meist sehr empfehlenswert.

### 3. Mobiles Endgerät / Apps

“ Handy mal ausgeschaltet zu Hause lassen.

Nicht immer möglich, aber wenn, dann einfach machen. Bewusst entschleunigen und [Digital Detox](#)  betreiben.

“ Wenn z.B. eine Nachrichtenseite eine gute mobile Webseite hat, nutze diese und erstelle dir ein Bookmark auf dem Homebildschirm des Smartphones und installiere NICHT die passende App bei der

Trackingblocker oft nicht greifen.

Ein guter Tipp, den ich regelmäßig auf Workshops zum Thema »Apps und Datenschutz« gebe. Es muss nicht immer eine App sein. Oftmals kann man Informationen direkt von einer Webseite abfragen, ohne dafür eine App installieren zu müssen. Erstellt euch doch einfach mithilfe des mobilen Firefox-Browsers (oder einem Browser eurer Wahl) einen Starter direkt auf dem Homescreen. Öffnet dazu einfach die Webseite, bei der ihr euch häufig Informationen besorgt (bspw. Wetter, Deutsche Bahn etc.) und drückt auf die drei Pünktchen, bis das Optionsmenü erscheint. Anschließend wählt ihr dort:

Zu Startbildschirm hinzufügen

Die gewünschten Informationen sind jetzt nur noch einen Fingertipp vom Homescreen entfernt – vergleichbar mit einer App. Mit diesem Tipp entgeht ihr nicht nur dem In-App-Tracking und der In-App-Werbung, sondern auch dem [perfiden Android-Berechtigungsmodell](#). Auf der Webseite bzw. über den mobilen Browser könnt ihr Tracker und Werbung anschließend ganz einfach mit [uBlock Origin](#) loswerden.

Wer sich partout nicht von seiner App trennen möchte / kann, der sollte einen Blick in die Rubrik [Werbe- und Trackingblocker](#) der Empfehlungsecke werfen. Dort wird kompakt erklärt, wie sich Werbung und Tracking mit bestimmten Tools auch innerhalb von Apps vermeiden lassen.

“ Installiert euch nicht jeden »Scheiß« nur weil dies so vom Anbieter gewollt ist. Das Mensch für alles eine App haben soll, ist noch fix in den Köpfen drin, gilt übrigens auch auf dem Desktop. Macht auch nicht für alles ein Konto wenn ihr nicht wirklich einen Zugang benötigt.

In die gleiche Kerbe schlägt der Tipp:



“ Einmal digitalen Minimalismus pflegen und hinterfragen: Brauche ich diese App wirklich? Kann ich auch ohne auskommen und die »Leere« stattdessen mit weniger privatsphäreschädigendem füllen, wenn überhaupt nötig?




Beide Tipps müssen eigentlich nicht weiter kommentiert werden. Ich möchte nur ergänzen: Fragt euch einfach, brauche ich App XY wirklich? Und wenn nein, dann einfach löschen. Jede App, die von eurem Smartphone verschwindet, zieht nicht unnötig Aufmerksamkeit auf sich. Dazu interessant: [Digitaler Minimalismus: Ein Weg zu mehr Datenschutz und Zeit.](#)



Lade dein Smartphone an öffentlichen USB-Ports nie mit einem USB-Datenkabel.

Ein berechtigter Tipp. Vermutlich wissen die meisten allerdings nicht, weshalb dieser beherzigt werden sollte. Das Problem: [Juice Jacking](#)  oder auch [BadUSB](#) . Eine Angriffsform, die schon auf das Jahr 2009 zurückgeht, aber bis dato noch relativ unbekannt ist. Über den USB-Anschluss eines Smartphones lässt sich nicht nur der Akku aufladen, sondern er dient auch zur Datenübertragung. Eben über diese Datenverbindung ist es möglich das Smartphone anzusprechen, sobald es an eine öffentliche Ladestation angesteckt wird. Vordergründig liefert die Ladestationen nur Strom, im Hintergrund wird das Smartphone allerdings zusätzlich über die Datenschnittstelle angesprochen. Das Ziel: Das Smartphone zu entriegeln, Zugriff auf die Daten zu erhalten und weitere Operationen durchzuführen.

2013 hat das via [Mactans](#)  auf iOS-Geräten ganz hervorragend funktioniert. Und auch wenn Systeme wie iOS oder Android mittlerweile Gegenmaßnahmen ergriffen haben, bleibt nicht ausgeschlossen, dass dieser Angriffsvektor unter bestimmten Voraussetzungen weiterhin erfolgreich ist. Daher ist es empfehlenswert sein Gerät immer über das mitgelieferte Netzteil zu laden.



WLAN, Bluetooth, mobile Daten, NFC und persönlicher Hotspot deaktivieren, wenn es nicht gebraucht wird. Verringert die Angriffsfläche und Trackingmöglichkeiten werden minimiert. Der Akku hält ebenfalls länger.

Moderne Rechner und auch Smartphones sind mit einer Vielzahl an Schnittstellen und Sensoren wie WiFi, Bluetooth, Kamera, Mikrofon, NFC usw. ausgestattet. Insbesondere die nicht verwendeten Schnittstellen sollten, da sie durchaus weitere **Angriffsvektoren** darstellen, nur dann aktiv sein, wenn ihr sie wirklich benötigt. Für die meisten Android-Geräte bedeutet das: Generell solltet ihr die WiFi-, Bluetooth- und auch NFC-

Schnittstelle nur bei Bedarf aktivieren und bei längerer Nichtbenutzung das Smartphone in den Flugmodus versetzen.

## 4. Fazit

Einige Tipps waren euch sicherlich noch unbekannt bzw. eventuell war euch bisher nicht klar, weshalb es sinnvoll sein kann, diese umzusetzen. Ob ein Tipp letztendlich in eurem Kontext bzw. Umfeld umgesetzt werden kann, müsst ihr selbst entscheiden. Es ist wie so oft in der IT: Die Verbesserung der IT-Sicherheit / Datenschutz geht meist mit dem Verlust von Komfort einher.

Im zweiten Teil der Artikelserie schauen wir uns die Tipps zum Thema »Accounts / Konten« und »E-Mail« an – natürlich ebenfalls kommentiert und um Zusatzinformationen ergänzt.

---

## Weitersagen | Unterstützen

Wenn dir der Beitrag gefallen hat, dann **teile** ihn mit deinen Freunden, Bekannten und Mitmenschen. Nutze dafür soziale Netzwerke, Foren, Messenger, E-Mails oder einfach die nächste Feier / Veranstaltung. Gerne darfst du meine Arbeit auch [unterstützen](#)!

## Über den Autor | Kuketz



*Mike Kuketz*

In meiner freiberuflichen Tätigkeit als Pentester / Sicherheitsforscher ([Kuketz IT-Security](#)) schlüpfe ich in die Rolle eines »Hackers« und suche Schwachstellen in IT-Systemen, Webanwendungen und Apps (Android, iOS). Des Weiteren bin ich **Lehrbeauftragter** für IT-Sicherheit an der [dualen Hochschule Karlsruhe](#) [↗](#), schärfe durch [Workshops und Schulungen](#) das **Sicherheits-** und **Datenschutzbewusstsein** von Personen und bin unter anderem auch als Autor für die Computerzeitschrift [c't](#) [↗](#) tätig.

Der Kuketz-Blog bzw. meine Person ist regelmäßig in den [Medien](#) (heise online, Spiegel Online, Süddeutsche Zeitung etc.) vertreten.

Mehr Erfahren →

---

## Unterstützung erhalten

Wenn du Fragen hast oder Hilfe suchst sind das offizielle [Forum](#) oder der [Chatraum](#) geeignete Anlaufstellen, um den Sachverhalt dort zu erörtern.



### FOLGE DEM BLOG

Wenn du über aktuelle Beiträge informiert werden möchtest, hast du verschiedene Möglichkeiten, dem Blog zu folgen:

**Bleib aktuell →**

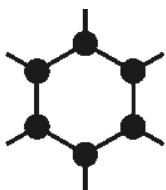
### ÄHNLICHE BEITRÄGE



**1. MÄRZ 2021**

#### **Ungewöhnliche IT-Sicherheits- und Datenschutztipps – Teil2**

Weitere IT-Sicherheits- und Datenschutztipps: Von sinnvoll über skurril bis hin zu gefährlich - da ist für jeden etwas dabei.



**17. NOVEMBER 2020**

#### **GrapheneOS: Das Android für Sicherheits- und Datenschuttfreaks**

Wer bereit ist, die »bittere Pille« zu schlucken und in ein Google-Pixel-Gerät zu investieren, der erhält mit GrapheneOS das wohl sicherste Android.



**13. APRIL 2013**

#### **Basisschutz – WordPress absichern Teil1**

WordPress lässt sich mit einfachen Mitteln gut absichern - ein Basisschutz für alle Blogger und WordPress-Betreiber.



**12. OKTOBER 2012**

#### **aSpotCat – Datenschutz für Android Teil1**



Welche App hat welche Berechtigungen? aSpotCat zeigt es euch! Die App listet alle Berechtigungen auf und bietet detaillierte Informationen.



 18. SEPTEMBER 2017

## Android: Viele VPN-Apps sind ein Sicherheits- und Datenschutzproblem

Die Studie »An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps« ist zwar schon etwas älter...

### WEITERE THEMEN

---

Android	Audit	Autonomie	Backup	Browser	Cloud
Datenschutz	Digitalpolitik	E-Mail	Firewall	Hacking	
Härten	iOS	Kuketz-Blog	Linux	macOS	Messenger
OpenWrt	Passwort	Pentest	RaspberryPi		
Sicherheitslücke	Sicherheitsmaßnahme	Tor	Tracking		
Überwachung	Verschlüsselung	Windows	WordPress		
XMPP					

---

### ERGÄNZUNGEN

## 11 Ergänzungen zu "Ungewöhnliche IT-Sicherheits- und Datenschutztipps – Teil1"



Anonymous sagt:

20. Februar 2021 um 17:21 Uhr

Zu dem Tipp „RFID-blockierende Kartenhüllen im Portemonnaie und für den

Reisepass.“ könnte noch der folgende Artikel interessant sein: ([Achtung, um den kompletten Artikel lesen zu können, wird leider ein heise+-Konto benötigt. Alternativ ist er in der Printausgabe der c't 3/2021, S. 164 zu finden.](#)) [↗](#). Nach dieser Art von „Behandlung“ lassen sich die Karten auch ganz normal weiterverwenden.



Mia sagt:

21. Februar 2021 um 20:01 Uhr

Da ich nicht auf Mastodon unterwegs bin, noch ein Tipp anbei:

Wenn du den Freundeskreis Vorratsdatenspeicherung et. al. in die sprichwörtliche Röhre gucken lassen willst, lege dir eine zweite und ausschließlich nur für diesen Zweck(!) zu verwendende Tor-Browser-Installation zu, bearbeite/editiere die torrc-Datei, indem du festlegst, über welche (vertrauenswürdigen) Exit-Nodes die Verbindung erfolgen soll – dann kannst du den Tor-Browser auch dazu verwenden, dich bei den Online-Diensten deines Vertrauens anzumelden, ohne dass die Dienste, denen du misstraust (oder: es solltest; also Zitronenfalter aka Verfassungsschützer bspw.) davon Kenntnis erlangen. Das Addon HTTPS-Everywhere sollte hierbei von „können“ auf „müssen“ scharf gestellt werden. Die Sicherheitsstufe des Browsers sollte stets mindestens auf „mittel“ gestellt sein. -„Reversed anonymity“ quasi – geht mit Tor auch. :-)

Mehr dazu auch hier: [https://www.privacy-handbuch.de/handbuch\\_24n.htm](https://www.privacy-handbuch.de/handbuch_24n.htm) [↗](#)



Anonymous sagt:

22. Februar 2021 um 11:43 Uhr

Statt der RFID-Shutzhüllen kann man auch RFID-Blocker benutzen, die wie ein Störsender das Auslesen verhindern.



dkf sagt:

23. Februar 2021 um 07:54 Uhr



Lade dein Smartphone an öffentlichen USB-Ports nie mit einem USB-Datenkabel.

Gibt's Ladekabel ohne Datenübertragung überhaupt zu kaufen?

Bastler können sich natürlich mit etwas Geschick ein reines Ladekabel selber herstellen:

[\[How-To\] Reines USB-Ladekabel basteln](#)



Mike Kuketz sagt:

23. Februar 2021 um 08:56 Uhr

Oder fertig kaufen. So etwas zum Beispiel: <https://portablepowersupplies.co.uk/product/usb-data-blocker>



Justin sagt:

24. Februar 2021 um 10:49 Uhr

Gibt es auch immer mal wieder beim örtlichen Discounter.

Ich habe „USB-Ladekabel“ (sie heissen dort dann genau so) bereits bei ALDI/LIDL/Netto/NORMA gesehen.

Kosten dann <<5€.



Luca sagt:

23. Februar 2021 um 13:20 Uhr

Zu „RFID-Blocker“: ich meine gelesen zu haben, dass es reicht, mehrere Karten mit RFID-Funktion im Portemonnaie zu haben, um geschützt zu sein. Die Auslesegeräte können den Mix an Daten nicht mehr korrekt auswerten.



Crey sagt:

23. Februar 2021 um 20:33 Uhr

Leider stimmt das nicht. Gab schon mehrere Versuche dazu auf unter anderem in Youtube zu finden.

Lustigerweise wird manchmal die Erste, mal die Letzte und mal eine Karte dazwischen ausgelesen.



Klaus sagt:

23. Februar 2021 um 13:37 Uhr

Auf meinem Phone (Moto G6) kann ich den USB-Anschluss konfigurieren. Steht bei mir immer auf ‚Nur Laden‘. Zur Datenübertragung muss ich diese erst erlauben.

Bei anderen Phones gibt es diese Option eventuell auch.

Diese Einstellung habe ich eher zufällig entdeckt, da sie bei mir erst in Nachrichtenfenster angeboten wird, wenn ich ein USB-Kabel anschlieÙe.



Stefan K. sagt:

24. Februar 2021 um 17:01 Uhr

Nachtrag 2, diesmal zu Digital Detox:

Benutzt uBlock Origin um Kommentarsektionen auf Webseiten zu sperren! Je nachdem wie ihr gestrickt seid ziehen Kommentare einen eher runter, weil sie meist negativ sind.

Positiver Nebeneffekt: Ich verbringe nur noch die Zeit den Artikel zu lesen.

Was mich dazu bewegt eine Webseite die ich häufig besuche wieder rasch zu schließen.

Bei Kuketz sind die Kommentare moderiert, das verhindert das hier Zustände wie bei einem Hannoveraner Verlag ausbrechen.

Dafür danke ich!



Robert sagt:

26. Februar 2021 um 23:05 Uhr

Generell würde ich gerne anmerken wollen, dass im Netz immer noch eine gefühlte Mehrheit von Leuten existiert, die denken man müsse (verpflichtend) immer und überall seine korrekten privaten Daten (Name, Email, geb. Datum, Adresse, etc.) angeben. Sofern man keine verbindlichen Rechtsgeschäfte abschließt, sollte man jedoch -falls möglich- besser Fakedaten benutzen. Andernfalls kann auch mal einfach ein oder besser zwei Buchstaben falsch schreiben, wodurch eine Rückverfolgung bei unerwünschter Werbung recht einfach wird. Und die Verwendung von kostenlosen temporären Email-Adressen zur Anmeldung bei irgendwelchen Internet-Diensten sollte selbstverständlich ebenso mit zum allgemeinen standardisierten Datenschutzverhalten zählen.

## Ergänzungen sind geschlossen / Aktualität

Dieser Beitrag ist älter als vier Wochen. **Hinweis:** Die Blog-Beiträge haben nicht wie Enzyklopädie-Einträge (bspw. Wikipedia) den Anspruch, dauerhaft aktuell und richtig zu sein, sondern beziehen sich wie Zeitungsartikel auf den Informationsstand zum Redaktionsschluss.

Wenn du Fragen hast oder Hilfe suchst sind das offizielle [Forum](#) oder der [Chatraum](#) geeignete Anlaufstellen, um den Sachverhalt dort zu erörtern. Kritik, Anregungen oder Korrekturvorschläge zum Beitrag nehme ich gerne per [E-Mail](#) entgegen.

### Kuketz-Forum

---



Artikel (293)



Datenschutz (161)

Sicherheitsmaßnahme (83)



**NACH OBEN ↑**

**SITEMAP IMPRESSUM DATENSCHUTZHINWEIS**