Digitale Kompetenz für Schüler/innen, Lehrer/innen und Eltern des Leibniz Gymnasiums Bad Schwartau

ein Beitrag von

Michael Georg Schmidt
mit präsentiert von Antje Hänzelmann und Patrycja Kupiec

von der studentischen Gruppe

der

Für Lehrer/innen und Eltern

Stress im Netz? Hier gibt es Hilfe

Nummer gegen Kummer - https://www.nummergegenkummer.de/
Kostenloses Telefon für Kinder und Jugendliche – 116 111
Kostenloses Telefon für Erwachsene – 0800-1110550

mobbing – schluss damit! - https://mobbing-schluss-damit.de/

Stress im Netz – für Jugendliche - https://jugend.support/

Fragen & Kontakt

mail@its-us.info

Threema-ID: WYH86UFA

Inhaltsverzeichnis

0. Vorbemerkung

Dieser Text ist von der Ansprache auf Erwachsene abgestellt, die Sprache ist jedoch so gehalten, dass sie für Kinder und Jugendliche gut nachvollziehbar sein sollte.

1. Haben Sie ein Geheimnis?

Beantworten Sie diese Frage nur für sich allein.

2. Wie fühlt es sich an, wenn Sie sich vorstellen, jeder würde dieses Geheimnis kennen?

Stellen Sie sich vor, Sie haben ein Geheimnis, was ganz normal ist. Jede/r hat mindestens ein Geheimnis, das kommt im Laufe der Zeit. Denn nicht alles, was man denkt und fühlt, möchte man mit anderen Menschen teilen.

Dennoch erzählt man Geheimnisse auch mal anderen Menschen, denen man vertraut. Auch das ist normal und sehr gut, denn manchmal ist es hilfreich, ein Geheimnis los zu werden.

Bevor Sie mit *Smartphones*, *Tablets* oder auf andere Weise mit dem *Internet* umgegangen sind, haben Sie diese Geheimnisse im persönlichen Gespräch geteilt. Das war gut so!

3. Dinge, die Sie über das Internet erzählen, sind keine Geheimnisse mehr!

Selbst wenn Sie Ihren besten Freunden etwas über das Internet, also Messenger, E-Mail, Foren oder Ähnliches erzählen, wissen Sie nie, ob nicht auch andere, die das gar nichts angeht, „mithören“.

Nachrichten nehmen im Internet selten den direkten Weg von einer Stelle zur nächsten, also vom *Sender* zum *Empfänger*. Da gibt es viele *Zwischenstationen*, von denen man den meisten *nicht trauen* kann. Die könnten Ihre Geschichten und Fotos speichern und ein *Profil* von Ihnen anlegen. Das ist nicht gut, weil diese Stellen dann ganz schnell, ganz viel über Sie erfahren.

4. Es gibt Streit mit der besten Freundin, dem besten Freund

Stellen Sie sich vor, Sie haben Ihrer besten Freundin, oder Ihrem besten Freund von einem Geheimnis per Messenger, Chat oder E-Mail berichtet. Jetzt gibt es Streit zwischen Ihnen. Sie oder er will Sie ärgern und schickt das Geheimnis an ganz viele andere Leute weiter. Schon ist Ihr Geheimnis *kein Geheimnis* mehr.

Wenn Sie davon nur persönlich berichtet haben, ist es viel schwerer, Ihr Geheimnis weiterzugeben.

Stress im Netz? Hier gibt es Hilfe

Nummer gegen Kummer - https://www.nummergegenkummer.de/
Kostenloses Telefon für Kinder und Jugendliche – 116 111
Kostenloses Telefon für Erwachsene – 0800-1110550

Mobbing – Schluss damit! - https://mobbing-schluss-damit.de/

Stress im Netz – für Jugendliche - https://jugend.support/

5. Wichtige Regeln für alles

Für all diese Bereiche gibt es ein paar ***Regeln, die Sie unbedingt berücksichtigen sollten:***

- Alles was Sie über ein Smartphone, Tablet oder Rechner erzählen und posten, ***muss die ganze Welt wissen dürfen.***
- Verhalten Sie sich so, wie Sie das auch von anderen Ihnen gegenüber erwarten würden.
- Wer ***droht*** ist ***draußen!***
  Niemand hat das Recht, Ihnen zu drohen oder Sie zu beleidigen! Wenn das vorkommt, brechen Sie den Kontakt sofort ab und blockieren diese Person!
  Gleiches gilt für üble Scherze und alles, was Ihnen *komisch* vorkommt.
- Seien Sie skeptisch, wenn jemand zu freundlich ist.
- Wenn jemand etwas von Ihnen will, ***lehnen Sie es ab, egal, was es ist!*** Kommunikation über Smartphone, Tablet oder Rechner sollte nur wie ein normales Gespräch sein.
- Seien Sie skeptisch, wenn jemand Ihnen erzählt, dass Sie etwas gewonnen haben oder Sie etwas geschenkt bekommen sollen. Niemand verschenkt „einfach“ so an jemanden etwas, den sie / er kaum kennt.
- Bevor Sie Leute treffen, die Sie im Internet kennen gelernt haben, halten Sie mit denen einige ***Videochats*** ab, damit Sie sicher sein können, wer die Person ist, die Sie treffen wollen. Fotos reichen ***nicht*** aus, denn da kann jeder jedes beliebige Foto schicken.

- Wenn die Person, mit der Sie sich verabreden, von Ihnen will, dass Sie sich besonders anziehen oder zurecht machen, ***brechen Sie den Kontakt sofort ab! Sie sind gut, so wie Sie immer sind! Wer Sie nicht nimmt, wie Sie sind, ist Ihrer Aufmerksamkeit nicht wert!***

6. Apps – Messenger – E-Mail - Foren - Chats - Browser

6.1 Apps

Sicher kennen Sie ganz viele *Apps*, die alle tolle Funktionen anbieten.
Dennoch ist es wichtig, dass Sie *Apps* mit Bedacht einsetzen. Installieren Sie nicht jede *App*, die als *tolle Sache* beworben wird oder weil irgendwer sie Ihnen empfohlen hat.

Eine *App* zu programmieren kostet Geld. Nur selten programmieren Leute *Apps*, um sie dann zu verschenken. Meistens wollen die Programmierer damit auch Geld verdienen. Wenn Sie aber für die Nutzung nichts bezahlen, muss das Geld auf andere Weise zu den Programmierern kommen.

Meistens funktioniert das so, dass Sie ganz viele Dinge gefragt werden, bevor Sie die *Apps* nutzen können. Oft stimmen Sie auch – unwissentlich – zu, dass all Ihre Daten geschäftlich genutzt werden dürfen. Das bringt den Anbietern richtig viel Geld ein. Denn Ihre Daten sind wertvoll. Wer glaubt, nichts zu verbergen zu haben, irrt sich. Jede/r hat etwas zu verbergen, denn so können Dritte viel über Sie erfahren, auch Ihre Geheimnisse.

Daher – bevor Sie eine App installieren, lesen Sie die ***Nutzungsbedingungen*** durch. Eine *Taschenlampen-App*, die auf Ihre *Kontakte* zugreifen will, sollten Sie nicht installieren. Genauso sollten Sie eine App, die Ihr Surfverhalten aufzeichnen will, nicht installieren.

Apps wie *Snapchat* oder Ähnliches speichern Ihre Fotos in großen Datenbanken, ohne dass Sie das merken. Das sollte auch nicht so sein. Vor allem nicht, wenn es auch mal „peinliche“ Fotos sind.

6.1.1 Was Apps machen dürfen

Gucken Sie sich in den *Einstellungen* Ihres Smartphones einmal den Punkt *Apps* an. Da gibt es irgendwo auch einen Punkt, der etwas über die *Berechtigungen von Apps* aussagt. Sehen Sie genau hin, was die einzelnen Apps, die auf Ihrem Telefon installiert sind, dürfen, und überlegen Sie genau, ob die App die gewährten Berechtigungen braucht, um richtig funktionieren zu können.

Wenn Sie der Meinung sind, dass eine App zu viel darf, dann nehmen Sie ihr die Berechtigung weg. Im Zweifel sollten Sie immer lieber eine Berechtigung erst einmal wegnehmen. Wenn Sie den Eindruck haben, dass die App dann nicht mehr so gut funktioniert, können Sie die Berechtigung wieder neu gewähren.

6.1.2 Apps, auf die man verzichten sollte

6.1.2.1 TikTok

Die App *TikTok* ist sehr beliebt. Leider überwacht der Konzern hinter *TikTok* seine Nutzer manchmal auch – https://www.heise.de/news/Tiktok-ueberwacht-Journalisten-per-App-7441812.html – daher ist es besser für Sie, wenn Sie auf TikTok verzichten.

6.1.2.2 Kalender die vorinstalliert sind

Kalender, die vorinstalliert sind, sollten Sie nicht nutzen, weil Kalender viele persönliche Informationen enthalten. Diese Kalender speichern die eingetragenen Daten aber nicht verschlüsselt, sondern machen es den Anbietern wie *Google (Android), Apple (iOS)* und den Herstellern der Mobiltelefone *(Samsung, Huawei & Co.)* möglich, Ihre Daten auszuwerten. Besser sind extra installierte Kalender, deren Inhalte verschlüsselt werden können.

Empfehlenswert sind der **Proton Calendar** und der **Tutanota Kalender**.

6.1.3 Trackende Apps

Grundsätzlich gilt, dass Sie so wenig wie möglich Apps installiert haben sollten, denn viele Apps *tracken* Sie. Sie verfolgen Ihr Verhalten und erstellen hieraus Profile über Sie.

Oft ist das Argument zu hören, dass das ja alles *anonyme Daten* seien. Das stimmt, nur reichen ***4*** anonyme Daten aus, um eine Person mit Namen, Adresse und allem, was dazu gehört, zu identifizieren.

Ein prominentes Beispiel ist der amerikanische Bischof *Jeffrey D. Burril*, der die App *grindr* anonym genutzt hat. Journalisten kauften *anonyme Daten* von einem Datenhändler und personalisierten diese Daten. Damit hatte der Bischof dann ein Problem – https://www.pillarcatholic.com/pillar-investigates-usccb-gen-sec/ und https://www.faz.net/aktuell/politik/ausland/eine-dating-app-wuehlt-amerikas-katholiken-auf-17460619.html.

Vermeintlich *anonyme Daten* kann jede/r frei kaufen und *deanonymisieren*. Einer der größten Datenhändler der Welt ist *Acxiom* – https://www.acxiom.com/.

6.2 Messenger

Instagram, Facebook, WhatsApp & Co. Wer nutzt die nicht?! Die Meisten tun das früher oder später. Leider sind das alles Vertreter, die davon leben, dass Sie Ihre Daten missbrauchen und verkaufen. Daher sollten Sie ganz vorsichtig mit dem sein, was Sie über Messenger erzählen, verschicken, posten und mit wem Sie überhaupt Kontakt per App haben.

*Seien Sie sich auch bewusst, dass von Nachrichten ganz leicht **Screenshots** gemacht werden können, die sich genauso leicht an ganz viele andere Leute weiterleiten lassen*.

6.2.1 Vertrauenswürdige Messenger

Zwei Messenger gibt es, die Ihre Daten ***nicht missbrauchen***. Das sind

- Signal

  Signal https://signal.org/de/download/

- Threema

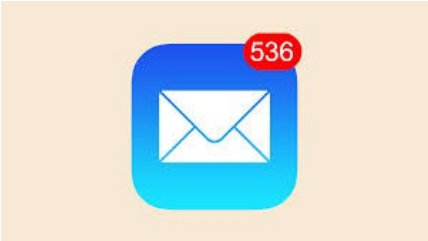
  Threema. https://threema.ch/de

Natürlich kann man aber auch bei diesen Messengern Screenshots machen.

6.2.2 Gefährlicher Messenger

Telegram ist der derzeit wohl gefährlichste Messenger. Sobald Sie dort etwas eintippen, geht es sofort unverschlüsselt zu den Telegram Servern und wird dort gespeichert. Auch, wenn Sie das, was Sie eintippen, nie abschicken.

6.3 E-Mailanbieter



E-Mails sind wie Postkarten, wenn man sie nicht verschlüsselt. Daher müssen Sie bei E-Mails besonders vorsichtig sein, was Sie darin schreiben. Den Inhalt kann alle Welt mitlesen. Das gilt vor allem für den Kontakt mit der Schule, mit Ärzten oder ähnlichem.

Einige E-Mailanbieter machen das sogar standardmäßig. Dazu gehören *Gmail* & Co, *Yahoo*, *outlook.com* und andere amerikanische E-Mailanbieter. Das hat nichts mit Fremdenfeindlichkeit zu tun. Das liegt einfach daran, dass in Amerika ganz andere Gesetze zum Datenschutz gelten, als bei uns in Europa. Daher ist es immer eine gute Idee, einen *europäischen E-Mailanbieter* zu nutzen.

6.3.1 Empfehlenswerte E-Mailanbieter

- Posteo - https://posteo.de/de
- Protonmail - https://proton.me/mail?ref=icnbtn
- Tutanota - https://tutanota.com/de/
- Web.de - https://tutanota.com/de/

Diese Auflistung ist ausschließlich alphabetisch sortiert. Es gibt noch viele andere empfehlenswerte E-Mailanbieter, aber eine zu große Auswahl wäre sicherlich nicht hilfreich.

Besonders hervorzuheben sind die Anbieter

- ***Protonmail***
  Protonmail bietet die Möglichkeit ***ganz einfach*** seinen E-Mailverkehr zu verschlüsseln, ohne dass die Gegenseite etwas dazu tun muss.
  Protonmail bietet zusätzlich zur kostenlosen E-Mailadresse ein kostenloses VPN (**V**irtual **P**rivate **N**etwork – zum sicheren Surfen) und ein wenig sicheren Onlinespeicher und einen verschlüsselt gespeicherten Kalender.
- ***Tutanota***
  Tutanota bietet auch eine ***ganz einfache*** Möglichkeit, seine E-Mails zu verschlüsseln, ohne dass die Gegenseite etwas dazu beitragen muss. Einen verschlüsselten Kalender gibt es hier auch.

Wenn Ihre E-Mails *verschlüsselt* sind, sind sie *nicht mehr wie Postkarten, sondern niemand kann sie dann mehr mitlesen.*

Hierzu stelle ich mein Skript *E-Mailing – aber sicher* zur Verfügung. Es erklärt, wie Sie sicher E-Mailen können und wie Sie sich eine *wirklich anonyme* E-Mailadresse einrichten können.

6.3.2 Verraten Sie nicht jedem Ihre private E-Mailadresse – nutzen Sie Relays

Oftmals muss man eine E-Mailadresse angeben, wenn man sich irgendwo anmelden will. Das führt schnell zu Spam E-Mails, die man nicht haben möchte. Dem können Sie aus dem Weg gehen, indem Sie sich eine so genannte *Relay-E-Mailadresse* einrichten. Das ist eine E-Mailadresse, die Sie nicht abfragen müssen. Diese E-Mailadresse reicht eingehende E-Mails nämlich gleich weiter und zwar an eine von Ihnen vorgegebene E-Mailadresse, die Sie abfragen. Wenn Ihnen die Spam-Flut zu groß wird, löschen Sie die *Relay-Adresse* und schon sind Sie den Spam los. Wenn Sie auf E-Mails über das Relay antworten müssen, ist das auch möglich.

Der Anbieter *DuckDuckGo* filtert zudem in E-Mails enthaltene bekannte Tracker aus den eingehenden E-Mails heraus. Daher ist es sinnvoll, sich bei DuckDuckGo ein Relay einzurichten – https://duckduckgo.com/email/.

6.4 Foren und Chats

Bei Foren und Chats ist es sinnvoll, erst einmal nur ***mitzulesen*** und ***zuzuhören***. Beteiligen Sie sich ***nicht sofort selbst*** an Diskussionen, sondern beobachten Sie erst einmal, wie sich die Leute im Forum oder Chat verhalten und wie sie miteinander umgehen. Erst, wenn Sie sicher sind, dass sich dort alle so benehmen, wie Sie das im Alltag auch erwarten würden, überlegen Sie sich mitzumachen.

Achten Sie aber auch hier darauf, nur das zu erzählen, was alle Welt wissen darf! Auch sogenannte ***private Nachrichten*** sind alles andere als wirklich privat.

6.5 Browser

Wenn Sie im Internet surfen, ist es wichtig, dass Sie einen Browser benutzen, der *sparsam* mit Ihren persönlichen Daten umgeht. Das ist nicht bei allen so.

Hierzu stelle ich meine Skripte

- Mein Browser – was erzählt die Plaudertasche über mich?

  und

- Mein Browser – wie bringe ich die Plaudertasche zum Schweigen

zur Verfügung.

Empfehlenswert sind

- ***Firefox*** - https://www.mozilla.org/de/firefox/new/
- ***Brave*** - https://brave.com/de/

Ganz ***schlimm*** sind

- ***Microsoft Edge***
- ***Microsoft Internet Explorer***
- ***Opera***
- **Vivaldi**

6.6 Surfen

Wenn Sie im Internet surfen, E-Mails abfragen oder Messenger nutzen, n***utzen Sie immer mobile Daten***, es sei denn Sie sind zu Hause. ***Wenn Sie in einem WLAN surfen, können alle, die das gleiche WLAN nutzen, alle Ihre Daten mitlesen***.

6.6.1 Geschützt surfen

Wenn Sie im Internet surfen, senden Sie Ihre Anfragen mit einer sogenannten *Transportweg Verschlüsselung (TLS – Transport Layer Security)* ins Internet, damit nicht jeder mitlesen kann, was Sie interessiert. Denn anhand Ihres elektronischen Absenders sind Sie eindeutig identifizierbar.

Diese TLS-Verschlüsselung wird jedoch an jedem Zwischenstopp auf dem Weg zum Ziel entschlüsselt, geprüft, wieder neu verschlüsselt und weitergeleitet. Damit haben Sie keine Kontrolle mehr darüber, wer was von Ihnen weiß. Um das zu verhindern, setzt man so genannte *VPN (Virtual Private Network)* ein. Bei einer Anfrage über ein VPN werden Ihre Anfrage- / E-Mail- und sonstigen Daten auf Ihrem Gerät verschlüsselt, direkt zu einem Server geleitet und von dort ins Internet geschickt. Vorher entschlüsselt dieser Server Ihre Daten, um zu sehen, welche Seite Sie suchen. Das hat den Vorteil, dass es *keine Zwischenstationen* gibt und den Server, den Sie nutzen, ganz viele andere auch nutzen. Das heißt, dass eine Website nicht mehr sehen kann, dass die Anfrage von Ihnen kommt, sondern nur sehen kann, dass die Anfrage von einem Server kommt, den ganz viele Leute nutzen. Damit ist Ihre Anfrage nur noch von dem Server zu Ihnen zurück verfolgbar. Daher muss dieser Server vertrauenswürdig sein. Außerdem können Sie nahezu jedes Land der Erde als Absende-Ort Ihrer Anfrage vortäuschen, indem Sie einen entsprechenden Server auswählen.

6.6.1.1 Empfehlenswerter VPN-Anbieter

ProtonVPN ist ein empfehlenswerter Anbieter für VPN, der sogar kostenlos ein VPN für Sie zur Verfügung stellt https://protonvpn.com/. Bei *Google Play* oder im *App-Store* finden Sie es als App unter der Bezeichnung ***ProtonVPN***.

Sicherlich gibt es auch andere empfehlenswerte Anbieter, leider aber auch sehr viele schwarze Schafe, die Ihre Daten ausnutzen. Daher beschränken Sie sich lieber auf *ProtonVPN*.

6.7 Geschenke – Gewinne – Freundschaft

Geschenke, Gewinne und Freundschaft brauchen Zeit, um zu wachsen.

Niemand schenkt Ihnen etwas, obwohl er Sie nicht kennt.

Niemand kann etwas gewinnen, wenn er nicht vorher an einem Gewinnspiel bewusst teilgenommen hat.

Niemand bringt Ihnen echte Freundschaft entgegen, obwohl er Sie überhaupt nicht kennt.

Wenn also solche Nachrichten, egal auf welchem Weg, Sie erreichen, ist das ein Grund, mehr als skeptisch zu sein!

7. „Anonymität“ im Netz

Wer glaubt, im Internet *anonym* handeln zu können, täuscht sich. Das ist so gut wie unmöglich, denn Websites und Apps sammeln Ihre Daten. Ein *Pseudonym* in Chats und Foren ist eine sinnvolle Sache, damit nicht jede/r Nutzer/in Sie gleich identifizieren kann. Aber Firmen und Anbieter von Seiten können Sie mit Hilfe vielfältiger Möglichkeiten leicht identifizieren. Aus Ihren „anonymen“ Daten (s. 6.1.1 Trackende Apps) werden schnell persönliche Daten, die Firmen zu einem Profil verarbeiten.

7.1 Vorsicht bei Äußerungen im Netz

Daher sollten Sie ***immer*** ganz genau überlegen, was Sie im Netz schreiben oder posten. ***Lästereien, Mobbing*** oder ***Gemeinheiten*** gegenüber anderen sind ein ***absolutes Tabu***! Im Moment glauben Sie vielleicht, dass niemand weiß, wer dahinter steckt. Das täuscht, denn man kann Sie im Ernstfall relativ leicht identifizieren. Vor allem müssen Sie damit rechnen, dass diese Gemeinheiten in Ihr persönliches Profil wandern, das später vielleicht irgendwer kauft und veröffentlicht.

Wenn Sie selber Opfer von Mobbing oder Beschimpfungen sind, erstatten Sie umgehend Anzeige bei der Polizei.

Alexi McCammond hat mit 16 eine Äußerung über Twitter von sich gegeben, die sie später bitter bereut hat – https://www.spiegel.de/kultur/neue-chefredakteurin-der-teen-vogue-muss-vor-ihrem-start-schon-wieder-gehen-a-ef89d18c-9978-4b8c-9c6e-ab742ab2b85e.

Sie sollte Chefredakteurin der *Teen Vogue* werden. Kurz bevor sie ihren Job antreten konnte, hat jemand ihr Profil gekauft und veröffentlicht, dass sie sich rassistisch und homophob im Alter von 16 Jahren bei Twitter geäußert hat. Sie wurde keine Chefredakteurin mehr.

Das sollte Ihnen nicht passieren! - Daher überlegen Sie sich genau, was Sie veröffentlichen, und schicken Sie nichts ins Internet, was Sie nicht auch im persönlichen Leben von sich geben würden.

Abgesehen davon, dass Sie sich mit Gemeinheiten im Netz auf jeden Fall immer selber schaden, überlegen Sie sich vorher, was so etwas mit anderen machen kann. Das ist nicht fair!

7.2 Noch mehr Tracker

Um möglichst wenige *Datenspuren* von sich zu hinterlassen, ist es sinnvoll, wenn Sie an Ihrem Smartphone die *GPS-Funktion* – die Ortungsfunktion abschalten. Wenn Sie nicht gerade navigieren, brauchen Sie die nämlich eigentlich nicht. Die benötigen nur Apps, die ein Bewegungsprofil von Ihnen erstellen wollen. Daran haben ***Sie*** jedoch kein Interesse.

Ebenso ist es sinnvoll *Bluetooth* abzuschalten, denn wenn das aktiv ist, verbraucht das zum einen Strom und zum anderen können Daten zwischen Ihrem Smartphone und anderen Bluetooth-Geräten ausgetauscht werden, ohne dass Sie es merken.

Perfekte Tracker sind auch *Smartwatches*, denn die sammeln richtig viele Daten über Sie und von Ihnen und übertragen sie oftmals ins Internet zu irgendwelchen Firmen, die die Daten verarbeiten und speichern. Damit sind wir wieder bei den persönlichen Profilen, die Sie gar nicht von sich haben wollen.

8. Online Zusammenarbeit

Oft ist es hilfreich, wenn man mit anderen online zusammenarbeiten und Dokumente austauschen kann. Anbieter wie *Google Drive* oder *DropBox* sind dabei keine gute Idee, weil Ihre Daten da nicht sicher sind. Google und Co. sind einfach zu neugierig.

Es gibt aber Alternativen bei denen Sie Ihre Daten *Ende-zu-Ende-Verschlüsselt (E2EE – End-to-End-Encryption)* in verschlüsseltem sicheren Cloudspeicher ablegen und teilen können. Es gibt viele gute Anbieter. Wichtig ist, dass Sie darauf achten, dass der Anbieter seinen Hauptsitz in *Europa* oder der *Schweiz* hat, weil diese Regionen guten Datenschutz gewährleisten.

8.1 Zwei der empfehlenswerten Anbieter für Cloudspeicher

- **ProtonDrive** (gibt es auch im Zusammenhang mit ProtonMail) - https://proton.me/
- **Tresorit** (kostenloser kleiner Speicher unter https://web.tresorit.com/signup Hauptseite unter https://tresorit.com/de

9. Sicheres Anmelden und Authentisieren

Das Wort *Authentisierung* ist kein Schreibfehler. In Deutschland unterscheidet man zwischen *Authentisierung* und *Authentifizierung*. Die Authentisierung ist, wenn man Informationen zur Verfügung stellt, die nachweisen sollen, wer die Person, die diese herausgibt, ist. Die Authentifizierung ist der Prozess, der prüft, ob die zur Verfügung gestellten Daten korrekt sind.

9.1 Sichere Passwörter

Sichere Passwörter sollten sowohl bestimmte Voraussetzungen erfüllen, als auch sicher aufgehoben werden und nur für ein/en ***einziges Konto / Zugang*** gelten.

9.1.1 Passwort-Tresor

Ein *Passwort-Tresor* ist ein Programm, das Passwörter für die Nutzer sicher speichert. Viele Passwort-Tresore bieten auch die Option an, sichere Passwörter zu erstellen. Bei Passwort-Tresoren unterscheidet man zwischen

- ***lokalen*** Passwort-Tresoren und
- ***online*** Passwort-Tresoren

Den ***lokalen*** Passwort-Tresoren ist der Vorrang zu geben, weil sie sicherer sind als *Online*-Passwort-Tresore.

Lokale Passwort-Tresore sind auf dem Gerät, dass Sie nutzen, installiert. Damit ein Angreifer Ihren Passwort-Tresor angreifen kann, muss er Zugang zu ihrem Gerät haben. Das kann ein *physischer*

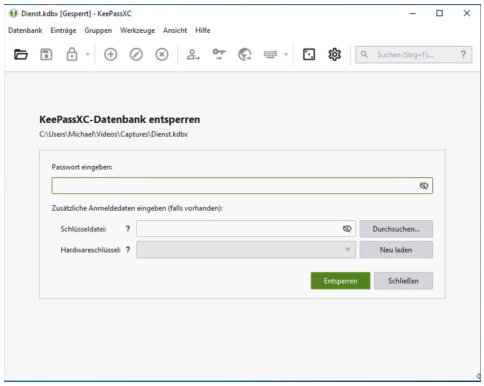
Zugriff sein, aber auch durch einen *Hacking-Angriff* erfolgen. Die Anzahl der potentiellen Personen, die dies erreichen könnten, ist in der Regel überschaubar.

Online-Passwort-Tresore stehen im Internet, so dass jeder sie erreichen und damit auch theoretisch angreifen kann. Also ist die Zahl der potentiellen Angreifer riesig.

9.1.1.1 KeePassXC

KeePassXC ist ein kostenloser Passwort-Tresor, den Sie hier - https://keepassxc.org/ - herunterladen können.

Der Startbildschirm von *KeePassXC*



Hier tragen Sie Ihr Passwort ein oder nutzen eine *Passwortdatei* oder einen *Token* (als 2Faktor).

In KeePassXC können Sie beliebig viele Passwörter sicher speichern. KeePassXC erzeugt für Sie auf Wunsch auch sichere Passwörter. Für Ihre einzelnen Konten und Accounts können Sie Ordner anlegen wie *E-Mail*, *Bank*, *Social Media* und anderes.

Sie können es sich aber noch leichter machen, indem Sie das *Add-on* von KeePassXC für *Firefox* oder *Chrome* installieren. Dann brauchen Sie nur einmal Ihr Zugangspasswort einzutragen und KeePassXC erkennt automatisch, wo Zugangsdaten erforderlich sind, und trägt diese für Sie ein.

Add-ons sind kleine Programme, die *Browser* wie Firefox oder Chrome erweitern. Sie sind mit wenigen Klicks installierbar.

KeePassXC ist *Open Source Software (OSS)*. Das heißt, dass der Programmcode für jeden einsehbar ist. Es ist also wahrscheinlich, dass Fehler und mögliche Schadfunktionen von Experten schnell gefunden werden würden. Jedoch ist dies ***kein*** Garant dafür. Bei Programmen, deren Code nicht frei einsehbar ist, muss man dem Anbieter vertrauen. Das ist hier nicht notwendig.

Noch mehr Sicherheit erlangt man, wenn es ein allgemein zugängliches *Audit* gibt. Das ist ein Bericht, den eine als vertrauensvoll eingestufte Instanz erstellt hat, der bescheinigt, dass die Software fehlerfrei ist und das gewährt, was sie verspricht. Da KeePassXC von Freiwilligen erstellt wird, fehlt der Gruppe das Geld ein solches – kostspieliges – Audit erstellen zu lassen. Dennoch ist KeePassXC allgemein als *sicher* anerkannt.

Es gibt noch andere Zweige dieses Passwort-Tresors wie *KeePass*, die auch nicht schlecht sind, aber die Entwicklung ist bei KeePassXC am aktivsten und es ist auf verschiedenen Plattformen wie Windows, Mac und Linux einsetzbar.

Es mag der Gedanke aufkommen, dass es gefährlich ist, wenn der Programmcode frei zugänglich ist. Das ist jedoch nicht der Fall, denn es gilt das bereits 1883 von *Auguste Kerkhoffs* formulierte Prinzip (Wikipedia, 2021-06-20 – Kerkhoffs' Prinzip – https://de.wikipedia.org/wiki/Kerckhoffs%E2%80%99_Prinzip), das besagt, dass die Sicherheit eines *symmetrischen Verschlüsselungsverfahrens* auf der *Geheimhaltung des Schlüssels* beruht und **nicht** auf der *Geheimhaltung des Verschlüsselungsalgorithmus*.

Bei KeePassXC kommt ein *symmetrisches Verschlüsselungsverfahren* zum Einsatz und der erwähnte Schlüssel ist das Passwort, das Sie brauchen, um Zugang zu KeePassXC zu bekommen. Der *Verschlüsselungsalgorithmus* ist hier das Programm KeePassXC selbst.

Sie erlangen also mit ***nur einem sicheren Passwort*** eine sehr große Sicherheit und können für ***all*** Ihre Anwendungen individuelle Passwörter verwenden, ohne sich diese merken zu müssen.

9.1.1.2 Zweiter Faktor – 2FA (2 Factor Authentication)

Es gibt immer wieder neue Möglichkeiten, Passwörter zu knacken. Daher gilt aktuell die Empfehlung, einen *zweiten Faktor* zu verwenden. Das ist, neben dem Passwort, eine weitere Möglichkeit, nachzuweisen, dass eine berechtigte Person Zugang zu einem „Konto" zu erlangen versucht.

Um einen *zweiten Faktor* zu verwenden, gibt es mehrere Möglichkeiten. Sie könnten sich eine SMS zusenden lassen, in der ein Code steht, das Gleiche per E-Mail. Beides ist jedoch relativ unsicher.

KeePassXC bietet dafür *sichere* Möglichkeiten an, die Sie auch beide gemeinsam nutzen ***können***, so dass Ihr Zugang *dreifach* abgesichert ist.

Die eine Möglichkeit ist eine ***Passwortdatei***. Diese Datei kann auf einem externen Datenträger wie einem *USB-Stick* oder besser noch einer *SD-Karte* gespeichert sein oder auf dem Gerät, das Sie verwenden. Sie müssen in diesem Fall nur den Pfad zu dieser Datei angeben. Jedoch ist es eher unsicher, eine Passwortdatei auf dem gleichen Gerät wie dem Passworttresor zu speichern.

Eine weitere Möglichkeit ist der Einsatz eines ***Tokens***. Das ist ein Gerät, das aussieht wie ein USB-Stick, auf dem Sie aber vorher einen einmaligen Code erzeugt haben, der Sie als rechtmäßigen Nutzer ausweist. Den Code richten Sie einmalig mit einer dafür vorgesehenen Software ein. Der Vorgang erfolgt weitgehend automatisch, so dass er auch für absolute Laien kein Problem ist.

Bekannte Anbieter für Token sind *Nitrokey* - *https://www.nitrokey.com/de* – und *Yubico* - *https://www.yubico.com/der-yubikey/?lang=de* – mit seinen Yubikeys.

Beide Anbieter haben qualitativ hochwertige Geräte. Yubico ist die Luxusversion. Beide haben unterschiedliche Funktionalitäten. Interessant könnte die Möglichkeit sein, den Token per *NFC (Near Field Communication)* zu nutzen. Das ist eine Funktechnik für kurze Strecken, die die meisten Smartphones beherrschen. Dabei reicht es aus, den Token an das Smartphone zu halten, um den Zugang zu einem Konto zu erlangen.

9.1.1.3 Alternativer Faktor

Wer sich Passwörter nicht merken kann oder will, der kann als Zugangsschutz bei KeePassXC auch ***allein*** eine *Passwortdatei* oder einen *Token* benutzen. Das ist immer noch sicherer, als ein Passwort mehr als einmal zu benutzen. Um so zu verfahren, lassen Sie das *Passwort-Feld* leer. Jetzt brauchen Sie aber zwingend einen 2Faktor, denn sonst sind Ihre Daten vollkommen ungeschützt. Allerdings ist auch ein einfaches Passwort, das man sich leicht merken kann, immer noch besser als gar kein Passwort.

9.1.1.4 Passworttresore, die man meiden sollte

Immer wieder in den Schlagzeilen ist der Anbieter *LastPass*. Seine Tresore wurden in der Vergangenheit schon mehrfach gehackt. Hierbei handelt es sich um einen *online Passwort-Tresor*. https://www.heise.de/news/Passwortmanager-LastPass-Hacker-haben-Zugriff-auf-Kennworttresore-von-Kunden-7441929.html.

9.2 Passwort-Generatoren

Passwortgeneratoren sind Programme, die (sichere) Passwörter erzeugen. Das ist hilfreich, weil menschliche Überlegungen oft leicht nachvollziehbar sind. Wenn das Passwort der Name des Haustiers ist oder ein Geburtstag, sind dies Passwörter, die leicht zu erraten sind, denn diese Informationen sind über *Social Engeneering* leicht zu bekommen, auch aus Ihrem persönlichen Umfeld.

Passwortgeneratoren benutzen hingegen *Pseudozufallsgeneratoren*, die aus (pseudo)zufälligen Daten bestehen. *Pseudo*zufällig sind diese Daten, weil auch die Programme zur Erstellung von Passwörtern einem vorgegebenen Schema folgen. Dabei gibt es jedoch qualitative Unterschiede. Ein guter Pseudopasswortgenerator erzeugt Passwörter, die mit aktuellen Mitteln nicht zu erraten sind.

9.2.1 PWGen

Das Programm *PWGen* – ein *lokaler* Passwortgenerator – ist auf der Website der Firma *Password Tech* - https://pwgen-win.sourceforge.io/ - zu finden.

Achten Sie unbedingt darauf, nur dieses Programm zu verwenden! Es gibt auch Programme die sich *PWGen* nennen und *online* Passwörter erstellen. Damit weiß ein potentieller Angreifer gleich, welche Passwörter Sie verwenden. Denn an Hand der übertragenen Metadaten (s. 1.5.1 Metadaten) weiß der Betreiber der Webseite sofort, wer Sie sind und wie er Sie finden kann. Dies gilt für ***alle online-Passwortgeneratoren***.

9.2.2 Passwort-Aufbau

Passwörter sollten folgende Kriterien erfüllen:

- möglichst lang sein
- aus GROSS- und Kleinbuchstaben
- aus Sonderzeichen ! “ § $ % ~ - = (/) und anderen
- aus Ziffern 0-9

bestehen.

Mit Hilfe eines Passwort-Tresors kann ein Passwort ***sehr lang*** sein, da der Passwort-Tresor das Passwort automatisch für Sie bei Anmeldungen einsetzt. Sie müssen sich nur noch das Passwort für den Passwort-Tresor merken.

Passwörter müssen lang sein, weil das einzige Hindernis, um ein Passwort zu knacken, nur noch in der Rechenleistung der Computer liegt, die sie brechen wollen. Es gibt vielfältige Programme und spezialisierte Hardware, um dies zu erledigen.

Als *aktuelle Sicherheitsempfehlung für Passwörter* gilt, dass Passwörter *lang* sein sollen. Zusätzlich sollten sie gerne möglichst *komplex* sein. Passwörter können unter diesen Voraussetzungen *gern lebenslang* genutzt werden.

Die Maßgabe, sein Passwort regelmäßig zu wechseln, gilt ***nicht mehr!***, da dies in der Regel dazu führt, dass unsichere Passwörter gewählt werden.

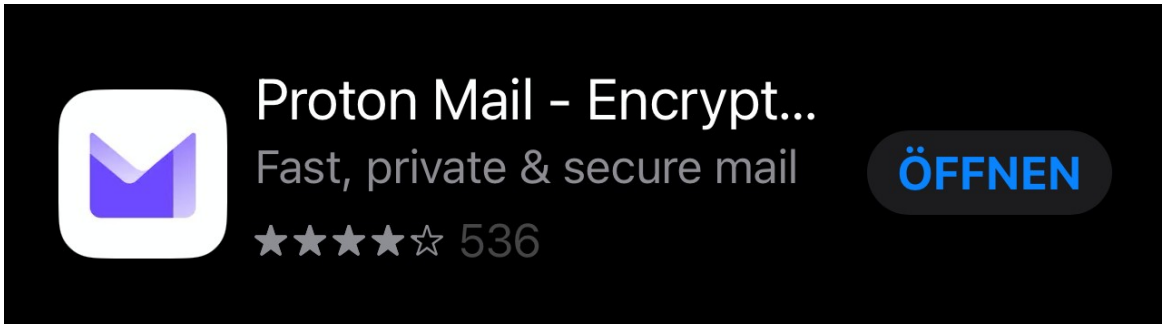
Aus Gründen der Sicherheit ist es unbedingt zu empfehlen, dass Sie sich nicht nur mit einem Passwort authentisieren, sondern auch noch mit einem zweiten Faktor – 2FA. Das kann eine SMS sein, die sie bekommen, um einen Code einzugeben, ein *Hardwaretoken* – ein Gerät, das aussieht wie ein USB Stick – oder ein *One Time Password (OTP)*.

10. Workshop – sicheres E-Mailing – sicheres VPN - sicherer Messenger

10.1 ProtonMail E-Mailadresse

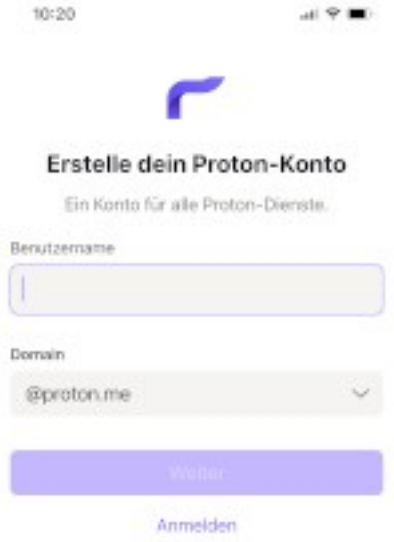
Als erstes richten Sie sich bitte eine E-Mailadresse bei *ProtonMail* ein. Im Folgenden sehen Sie den Vorgang Schritt für Schritt in Bildern dargestellt, wenn Sie die E-Mailadresse über die *ProtonMail* App einrichten.

1. App herunterladen

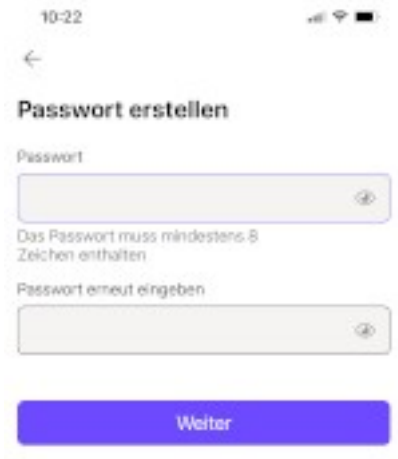


2. App starten und ein Konto erstellen

3. Benutzernamen und E-Mailadresse erstellen

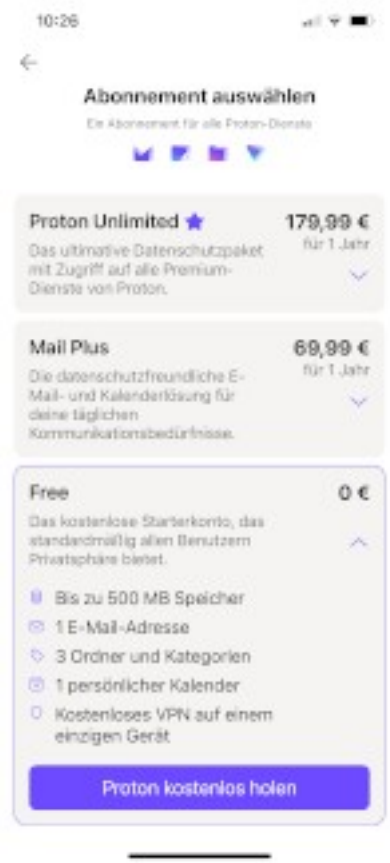


4. Passwort erstellen



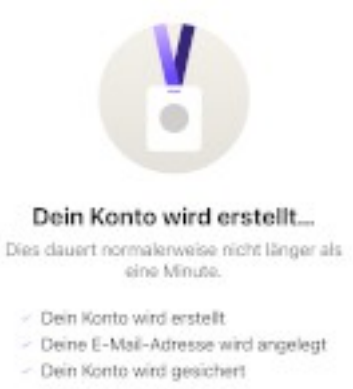
5. E-Mailadresse für Wiederherstellung eingeben

6. Abonnement auswählen – ***Free***



7. Captcha – ich bin ein Mensch

8. Das E-Mailkonto wird erstellt

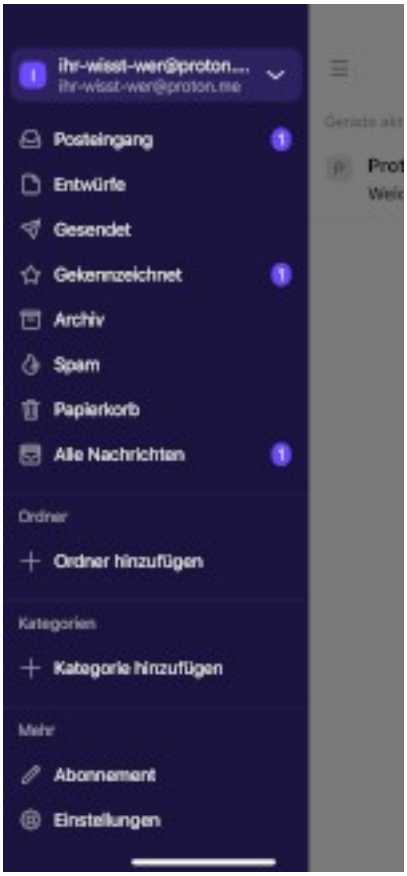


9. Jetzt kann es losgehen

10. Der *Posteingang*

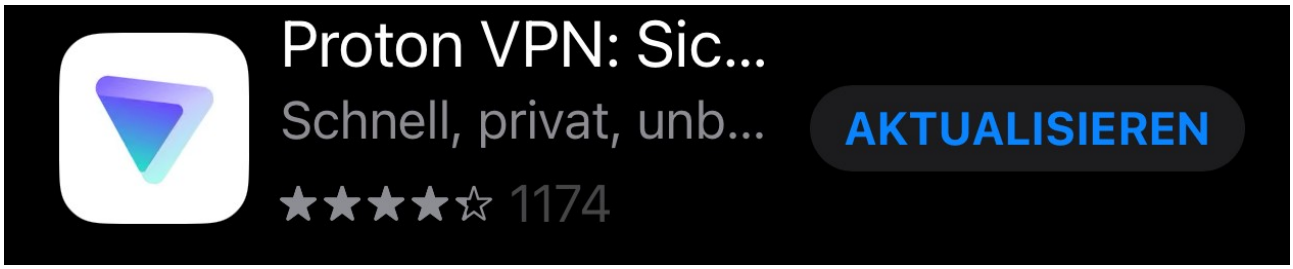
11. Die *Einstellungen* – im Postfach oben links klicken


10:27
Posteingang
Gerade aktualisiert
1 ungelesen
Proton
10:26
Welcome to the future of email


ihr-wisst-wer@proton...
ihr-wisst-wer@proton.me
Posteingang
Entwürfe
Gesendet
Gekennzeichnet
Archiv
Spam
Papierkorb
Alle Nachrichten
Ordner
Ordner hinzufügen
Kategorien
Kategorie hinzufügen
Mehr
Abonnement
Einstellungen

10.2 ProtonVPN

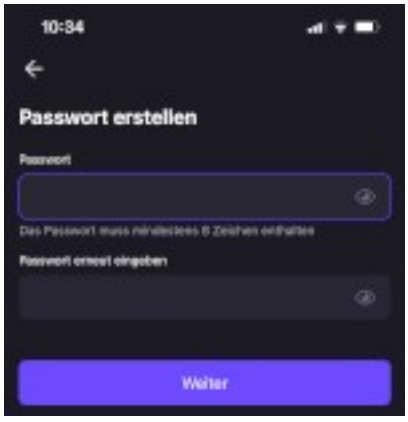
1. App herunterladen und installieren



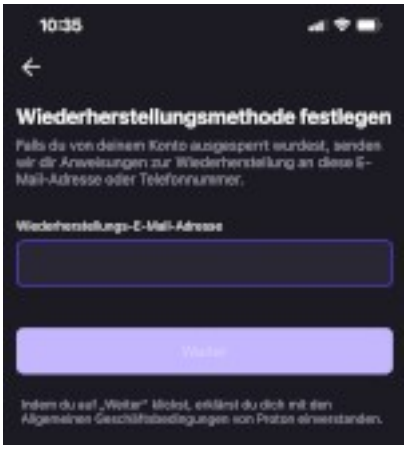
2. App starten

3. Benutzernamen überlegen und eintragen

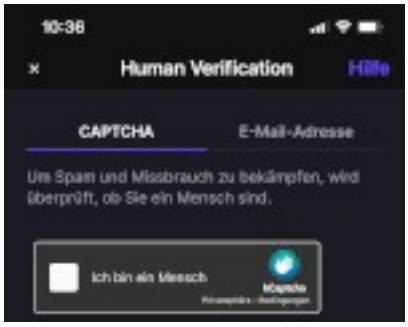
4. Passwort erstellen



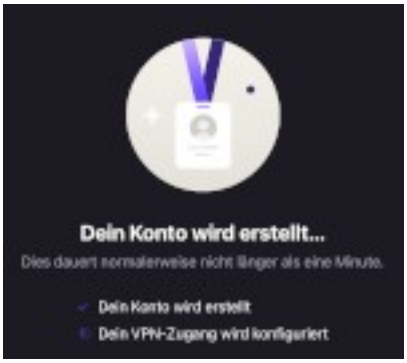
5. Wiederherstellungs-E-Mailadresse eintragen



6. Captcha – ich bin ein Mensch

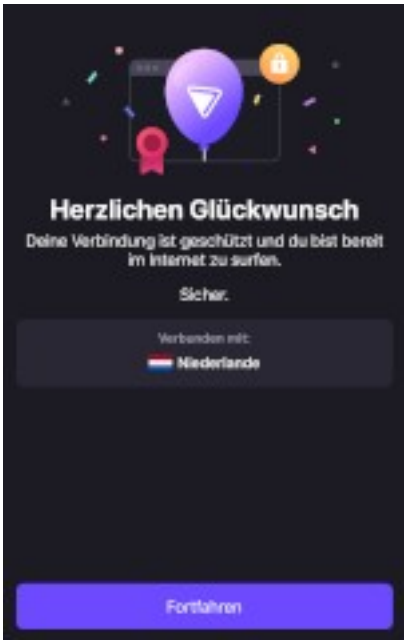


7. Das Konto wird erstellt

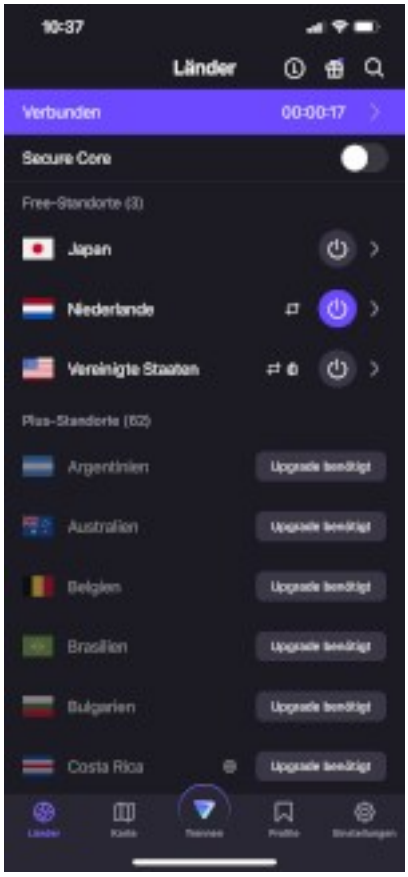


8. *Rundgang* – oder *Überspringen*

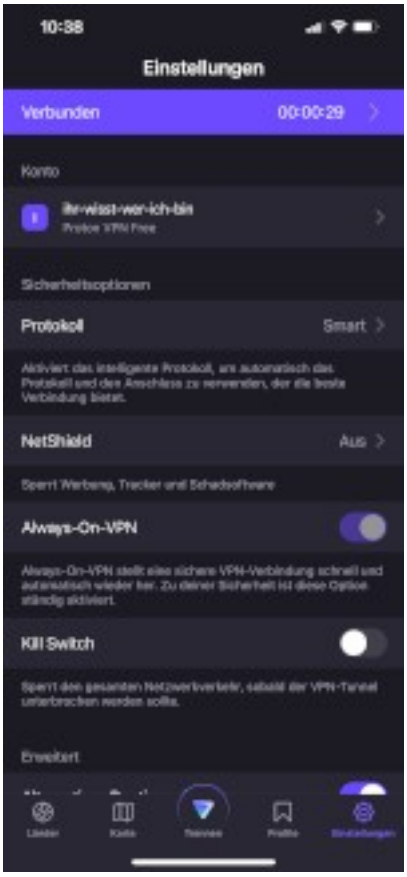
9. Es kann losgehen



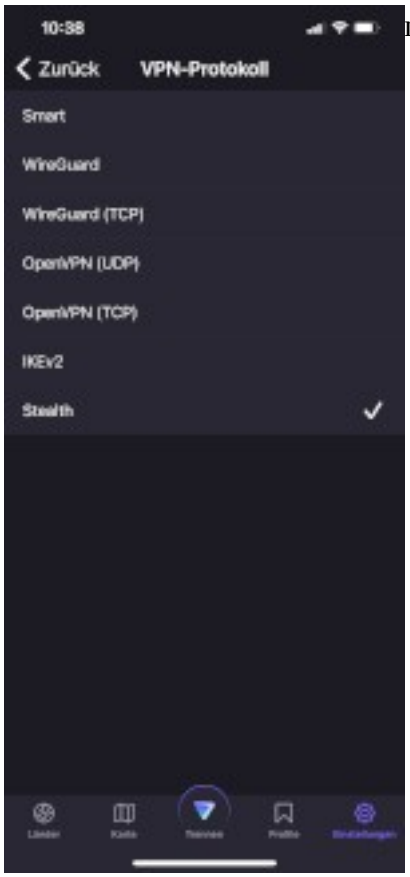
10. Land und Server auswählen



11. *Protokoll Einstellungen* anpassen



12. *VPN-Protokoll* einstellen. Hier ist es wichtig, als Protokoll ***stealth*** zu nehmen. Einige Websites erkennen VPN und lassen die Nutzer dann nicht auf deren Inhalte zugreifen, weil die Seiten dann nicht deren Daten ergaunern können.



Das kann man weitgehend mit dem ***stealth-Protokoll*** umgehen.

10.3 Signal – sicherer Messenger

Signal herunterladen und gemäß der Anleitung installieren.

11. Kindersicherungs-Apps für Mobilgeräte

Vom Einsatz von Kindersicherungs-Apps für Mobilgeräte ist eher abzuraten, da es bei vielen Apps „kinderleicht“ ist, die Sicherungsmaßnahmen zu umgehen. Sind die Kinder etwas IT versiert, könnten sie sogar die Mobilgeräte der Eltern angreifen.

Hierzu mehr bei Heise Security - https://www.heise.de/news/Kindersicherungs-Apps-Smarte-Kids-koennten-Eltern-attackieren-7435146.html und SEC Consult – https://sec-consult.com/de/blog/detail/ueberwachungs-apps-fuer-kinder-welchen-preis-die-totale-kontrolle-mit-sich-bringt/.

12. Kinder, Jugendliche und das Internet

Zu diesem Thema gibt es bei Heise-online einen sehr guten Artikel von *Kristina Beer* und *Bernd Mewes* – https://www.heise.de/ratgeber/Safer-Internet-Day-FAQ-Internetsicherheit-fuer-Kinder-und-Jugendliche-7333482.html?seite=all.

Den Großteil der dort verlinkten Angebote finden Sie in den ***Quellen*** unter ***Spezielle Angebote für den Kinderschutz*** ab Ziffer 27.

Quellen

1. Alexi McCommand - https://www.spiegel.de/kultur/neue-chefredakteurin-der-teen-vogue-muss-vor-ihrem-start-schon-wieder-gehen-a-ef89d18c-9978-4b8c-9c6e-ab742ab2b85e
2. Brave - https://brave.com/de/
3. Datenhändler – Acxiom - https://www.acxiom.com/
4. DuckDuckGo – E-Mailrelay - https://duckduckgo.com/email/
5. Firefox - https://www.mozilla.org/de/firefox/new/
6. Jeffrey D. Burril - https://www.pillarcatholic.com/pillar-investigates-usccb-gen-sec/ und https://www.faz.net/aktuell/politik/ausland/eine-dating-app-wuehlt-amerikas-katholiken-auf-17460619.html
7. Kindersicherungs-Apps - https://www.heise.de/news/Kindersicherungs-Apps-Smarte-Kids-koennten-Eltern-attackieren-7435146.html
8. Kindersicherungs-Apps - https://sec-consult.com/de/blog/detail/ueberwachungs-apps-fuer-kinder-welchen-preis-die-totale-kontrolle-mit-sich-bringt/
9. LastPass – Passwort-Tresor - https://www.heise.de/news/Passwortmanager-LastPass-Hacker-haben-Zugriff-auf-Kennworttresore-von-Kunden-7441929.html
10. Nitrokey - https://www.nitrokey.com/de
11. Posteo - https://posteo.de/de
12. Proton - https://proton.me/
13. ProtonMail/Calendar/Drive/VPN - https://proton.me/
14. ProtonVPN - https://protonvpn.com/
15. Signal für PC (gibt es auch für Smartphones) - https://signal.org/de/download/
16. Threema für PC (gibt es auch für Smartphones) - https://threema.ch/de
17. TikTok bei BuzzFeedNews - TikTok bei Forbes - https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/
18. TikTok bei Forbes - https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/
19. TikTok bei heise online – immer mehr Verbote von TikTok in den USA - https://www.heise.de/news/TikTok-Immer-mehr-Verbote-in-US-Bundesstaaten-auf-mehr-Geraeten-blockiert-7432797.html
20. TikTok bei heise online – über 200 chinesische Apps in Indien gesperrt - https://www.heise.de/news/Indien-sperrt-bereits-ueber-200-chinesische-Apps-4971277.html
21. TikTok bei heise security - https://www.heise.de/news/Tiktok-ueberwacht-Journalisten-per-App-7441812.html

22. Tresorit Cloudspeicher kostenlos - https://web.tresorit.com/signup
23. Tresorit Homepage - https://tresorit.com/de
24. Tutanota - https://tutanota.com/de/
25. Web.de - https://tutanota.com/de/
26. Yubico - https://www.yubico.com/?lang=de

Spezielle Angebote zum Kinderschutz

27. Act-on – Medienschutz für 10-14 Jährige - https://www.schau-hin.info/
28. Add-ons – nicht alle Add-ons sind empfehlenswert – heise.de – Affiliate-Betrug: Chrome-Browser-Add-ons mit 1,4 Millionen Installationen - https://www.heise.de/news/Affiliate-Betrug-Browser-Erweiterungen-mit-1-4-Millionen-Installationen-7247888.html
29. Apple – Kindersicherung auf dem iPhone, iPad oder iPod touch deines Kindes verwenden - https://support.apple.com/de-de/HT201304
30. bsi.de – Kindersicherung für Tablet, Smartphone und Computer - https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Checklisten/BSI-Checkliste-Kinderschutz.pdf?__blob=publicationFile&v=1
31. Bundesministerium für Familie, Senioren, Frauen und Jugend – Sicher Surfen: Schutz für Kinder im Netz - https://www.bmfsfj.de/bmfsfj/aktuelles/alle-meldungen/sicher-surfen-schutz-fuer-kinder-im-netz-89786
32. BvD e.V. - führ Lehrende – Datenschutz leicht erklärt - https://www.datenschutz-leicht-erklaert.de/
33. Der Bundesbeauftragte für den Datenschutz und Informationsfreiheit – Pixi Bücher zur Sensibilisierung für Datenschutz - https://www.bfdi.bund.de/DE/Service/Publikationen/Pixi/Pixi_node.html
34. Gesetze im Internet – Jugendschutzgesetz - https://www.gesetze-im-internet.de/juschg/BJNR273000002.html
35. Google – Auch online zum Schutz Ihrer Familie beitragen - https://families.google/intl/de_ALL/familylink/
36. heise.de – Safer Internet Day: FAQ Internetsicherheit für Kinder und Jugendliche - https://www.heise.de/ratgeber/Safer-Internet-Day-FAQ-Internetsicherheit-fuer-Kinder-und-Jugendliche-7333482.html?seite=all
37. Jugend Support – Hilfe für Jugendliche bei Problemen im Netz - https://jugend.support/
38. Kinder Ministerium – für Kinder zwischen 7 und 12 Jahren – Kinderrechte, Menschenrechte, grundlegendes Wissen zur Bundesrepublik Deutschland, - https://www.kinder-ministerium.de/
    wie sich Kinder sicher im Internet bewegen können - https://www.kinder-ministerium.de/familie-und-du

39. Kinder-Suchmaschine – Blinde Kuh - https://www.blinde-kuh.de/index.html
40. Kinder-Suchmaschine – FragFinn - https://eltern.fragfinn.de/eltern/fragfinn-als-startseite/#1548856918580-4c0cf33d-9cc0
41. Kinder-Suchmaschinen Klick safe - https://www.klicksafe.de/fuer-kinder
42. Klick safe – eine europäische Initiative - https://www.klicksafe.de/
43. Klick safe für Kinder – mit zwei Kindersuchmaschinen - https://www.klicksafe.de/fuer-kinder
44. Microsoft – Microsoft Family Safety - https://www.microsoft.com/de-de/microsoft-365/family-safety?market=de
45. Mobbing – Schluss damit! - https://mobbing-schluss-damit.de/
46. Mozilla Firefox – Jugendschutz - https://support.mozilla.org/de/kb/Jugendschutz
47. Nummer gegen Kummer - https://www.nummergegenkummer.de/
48. Projekt „gut aufwachsen mit Medien“ für 14-18 Jährige und Eltern – Schützen, Handeln, Stärken - https://www.schau-hin.info/
49. schau-hin.info – Eltern macht Euch medienfit - https://www.schau-hin.info/