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

Für die Jahrgangsstufe 10

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

1. Hast du ein Geheimnis?

Beantworte diese Frage nur für Dich allein und erzähl niemandem Deine Überlegungen.

2. Wie fühlt es sich an, wenn du dir vorstellst, jeder würde dieses Geheimnis kennen?

Stell dir vor, du hast 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 du mit *Smartphones*, *Tablets* oder auf andere Weise mit dem *Internet* umgegangen bist, hast du diese Geheimnisse im persönlichen Gespräch geteilt. Das war gut so!

3. Dinge, die du über das Internet erzählst, sind keine Geheimnisse mehr!

Selbst, wenn du deinen besten Freunden etwas über das Internet, also Messenger, E-Mail, Foren oder Ähnliches erzählst, weißt du 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 deine Geschichten und Fotos speichern und ein *Profil* von dir anlegen. Das ist nicht gut, weil diese Stellen dann ganz schnell, ganz viel über dich erfahren.

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

Stell dir vor, du hast deiner besten Freundin oder deinem besten Freund von einem Geheimnis per Messenger, Chat oder E-Mail berichtet. Jetzt gibt es Streit zwischen euch. Sie oder er will dich ärgern und schickt das Geheimnis an ganz viele andere Leute weiter. Schon ist dein Geheimnis *kein Geheimnis* mehr.

Wenn du davon nur persönlich berichtet hast, ist es viel schwerer, dein 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 du unbedingt berücksichtigen solltest***

- Alles was du über ein Smartphone, Tablet oder Rechner erzählst und postest, ***muss die ganze Welt wissen dürfen.***
- Verhalte dich so, wie du das auch von anderen dir gegenüber erwarten würdest.
- Wer ***droht,*** ist ***draußen****!*
  Niemand hat das Recht, dir zu drohen oder dich zu beleidigen! Wenn das vorkommt, brich den Kontakt sofort ab und blockiere diese Person! Wende dich an einen Erwachsenen, dem du vertraust.
  Gleiches gilt für üble Scherze und alles, was dir *komisch* vorkommt.
- Sei skeptisch, wenn jemand zu freundlich ist.
- Wenn jemand etwas von dir will, ***lehne es ab! Egal was es ist.*** Kommunikation über Smartphone, Tablet oder Rechner sollte nur wie ein normales Gespräch sein.
- Sei skeptisch, wenn jemand dir erzählt, dass du etwas gewonnen hast oder du etwas geschenkt bekommen sollst. Niemand verschenkt „einfach“ so etwas an jemanden, den sie / er kaum kennt.
- Bevor du Leute triffst, die du im Internet kennen gelernt hast, halte mit denen einige ***Videochats*** ab, damit du sicher sein kannst, wer die Person ist, die du treffen willst. Fotos reichen ***nicht*** aus, denn da kann jeder jedes beliebige Foto schicken.

- Sprich unbedingt vorher mit einem Erwachsenen deines Vertrauens, bevor du dich verabredest!
- Wenn die Person, mit der du dich verabredest, von dir will, dass du dich besonders anziehst oder zurecht machst, ***brich den Kontakt sofort ab! Du bist gut, so wie du immer bist! Wer dich nicht nimmt, wie du bist, ist deiner Aufmerksamkeit nicht wert!***

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

6.1 Apps

Sicher kennst du ganz viele *Apps*, die alle tolle Funktionen anbieten.
Dennoch ist es wichtig, dass du *Apps* mit Bedacht einsetzt. Installiere nicht jede *App*, die als *tolle Sache* beworben wird oder weil irgendwer sie dir 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 du aber für die Nutzung nichts bezahlst, muss das Geld auf andere Weise zu den Programmierern kommen.

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

Daher – bevor du eine App installierst, lies dir die ***Nutzungsbedingungen*** durch. Eine *Taschenlampen-App*, die auf deine *Kontakte* zugreifen will, solltest du nicht installieren. Genauso solltest du eine App, die dein Surfverhalten aufzeichnen will, nicht installieren.

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

6.1.1 Was Apps machen dürfen

Guck dir in den *Einstellungen* deines Smartphones einmal den Punkt *Apps* an. Da gibt es irgendwo auch einen Punkt, der etwas über die *Berechtigungen von Apps* aussagt. Sieh genau hin, was die einzelnen Apps dürfen, die auf deinem Telefon installiert sind. Überlege genau, ob die App die gewährten Berechtigungen braucht, um richtig funktionieren zu können.

Wenn du der Meinung bist, dass eine App zu viel darf, dann nimm ihr die Berechtigung weg. Im Zweifel solltest du immer lieber eine Berechtigung erst mal wegnehmen. Wenn du den Eindruck hast, dass die App dann nicht mehr so gut funktioniert, kannst du 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 dich, wenn du auf TikTok verzichtest.

6.1.2.2 Kalender, die vorinstalliert sind

Kalender, die vorinstalliert sind, solltest du 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, eure Daten auszuwerten. Besser sind extra installierte Kalender, deren Inhalte verschlüsselt werden können.

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

6.1.3 Trackende Apps

Grundsätzlich gilt, dass du so wenig wie möglich Apps installiert haben solltest, denn viele Apps *tracken* euch. Sie verfolgen euer Verhalten und erstellen hieraus Profile über dich.

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 deine Daten missbrauchen und verkaufen. Daher solltest du ganz vorsichtig mit dem sein, was du über Messenger erzählst, verschickst, postest und mit wem du überhaupt Kontakt per App hast.

*Sei dir 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 deine Daten ***nicht missbrauchen***. Das sind

- Signal

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

- Threema

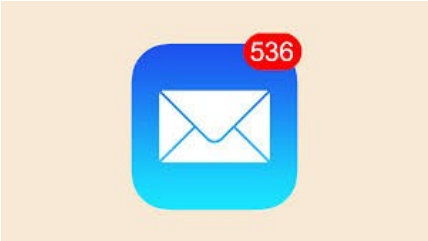
  Threema. https://threema.ch/de

Natürlich kann man aber auch bei diesen Messengern Screenshots machen.

6.2.2 Gefährlicher Messenger

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

6.3 E-Mailanbieter



E-Mails sind wie Postkarten, wenn man sie nicht verschlüsselt. Daher musst du bei E-Mails besonders vorsichtig sein, was du darin schreibst. Den Inhalt kann alle Welt mitlesen.

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

6.4 Foren und Chats

Bei Foren und Chats ist es sinnvoll, erst einmal nur ***mitzulesen*** und ***zuzuhören***. Beteilige dich ***nicht sofort selbst*** an Diskussionen, sondern beobachte erst einmal, wie sich die Leute im Forum oder Chat verhalten und wie sie miteinander umgehen. Erst wenn du sicher bist, dass sich dort alle so benehmen, wie du das im Alltag auch erwarten würdest, überlege dir mitzumachen.

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

6.5 Browser

Wenn du im Internet surfst, ist es wichtig, dass du einen Browser benutzt, der *sparsam* mit deinen persönlichen Daten umgeht. Das ist nicht bei allen so.

Empfehlenswert sind

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

Ganz ***schlimm*** sind dabei

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

6.6 Surfen

Wenn du im Internet surfst, E-Mails abfragst oder Messenger nutzt, ***nutze immer mobile Daten***, es sei denn, du bist zu Hause. ***Wenn du in einem WLAN surfst, können alle, die das gleiche WLAN nutzen, alle deine Daten mitlesen***.

6.6.1 Geschützt surfen

Wenn du im Internet surfst, sendest du deine Anfragen mit einer so genannten *Transportweg Verschlüsselung (TLS – Transport Layer Security)* ins Internet, damit nicht jeder mitlesen kann, was dich interessiert. Denn anhand deines elektronischen Absenders bist du eindeutig identifizierbar.

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

6.6.1.1 Empfehlenswerter VPN-Anbieter

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

Sicherlich gibt es auch andere empfehlenswerte Anbieter, leider aber auch sehr viele schwarze Schafe, die deine Daten ausnutzen. Daher beschränke dich lieber auf *ProtonVPN*.

6.7 Geschenke – Gewinne – Freundschaft

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

Niemand schenkt dir etwas, obwohl er dich nicht kennt.

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

Niemand bringt dir echte Freundschaft entgegen, obwohl er dich überhaupt nicht kennt.

Wenn also solche Nachrichten, egal auf welchem Weg, dich 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 deine Daten. Ein *Pseudonym* in Chats und Foren ist eine sinnvolle Sache, damit nicht jede/r Nutzer/in dich gleich identifizieren kann. Aber Firmen und Anbieter von Seiten können dich mit Hilfe vielfältiger Möglichkeiten leicht identifizieren. Aus deinen „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 solltest du ***immer*** ganz genau überlegen, was du im Netz schreibst oder postest. ***Lästereien, Mobbing*** oder ***Gemeinheiten*** gegenüber anderen sind ein ***absolutes Tabu***! Im Moment glaubst du vielleicht, dass niemand weiß, wer dahinter steckt. Das täuscht, denn man kann dich im Ernstfall relativ leicht identifizieren. Vor allem musst du damit rechnen, dass diese Gemeinheiten in dein persönliches Profil wandern, das später vielleicht irgendwer kauft und veröffentlicht.

Wenn du selber Opfer von Mobbing oder Beschimpfungen bist, wende dich umgehend an einen vertrauenswürdigen Erwachsenen und erstattet 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 dir nicht passieren! - Daher überlege dir genau, was du veröffentlichst, und schick nichts ins Internet, was du nicht auch im persönlichen Leben von dir geben würdest.

Abgesehen davon, dass du dir mit Gemeinheiten im Netz auf jeden Fall immer selber schadest, überlege dir vorher, was so etwas mit anderen machen kann. Das ist nicht fair!

7.2 Noch mehr Tracker

Um möglichst wenige *Datenspuren* von dir zu hinterlassen, ist es sinnvoll, wenn du an deinem Smartphone die *GPS-Funktion* – die Ortungsfunktion abschaltest. Wenn du nicht gerade navigierst, brauchst du die nämlich eigentlich nicht. Die benötigen nur Apps, die ein Bewegungsprofil von dir erstellen wollen. Daran hast ***du*** 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 deinem Smartphone und anderen Bluetooth-Geräten ausgetauscht werden, ohne dass du es merkst.

Perfekte Tracker sind auch *Smartwatches*, denn die sammeln richtig viele Daten über dich und von dir und übertragen sie oftmals ins Internet zu irgendwelchen Firmen, die die Daten verarbeiten und

speichern. Damit sind wir wieder bei den persönlichen Profilen, die du gar nicht von dir haben willst.

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 Deine Daten da nicht sicher sind. Google und Co. sind einfach zu neugierig.

Es gibt aber Alternativen bei denen du deine Daten *Ende-zu-Ende-Verschlüsselt (E2EE – End-to-End-Encryption)* in verschlüsseltem, sicherem Cloudspeicher ablegen und teilen kannst. Es gibt viele gute Anbieter. Wichtig ist, dass du darauf achtest, 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

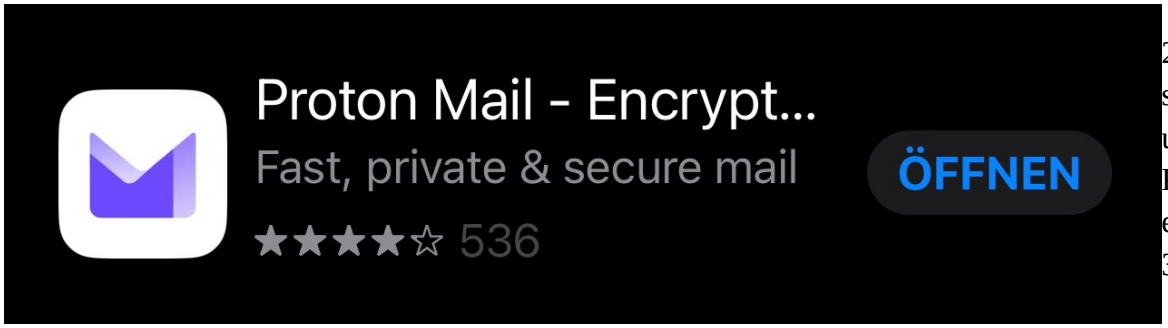
- **ProtonDrive** (gibt es auch im Zusammenhang mit ProtonMail) - https://proton.me/
- **Tresorit** (kostenloser kleiner Speicher unter https://web.tresorit.com/signup
  Hauptseite unter https://tresorit.com/de

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

9.1 ProtonMail E-Mailadresse

Als erstes richte dir bitte eine E-Mailadresse bei *ProtonMail* ein. Im Folgenden siehst du den Vorgang Schritt für Schritt in Bildern dargestellt, wenn du die E-Mailadresse über die *ProtonMail* App einrichtest.

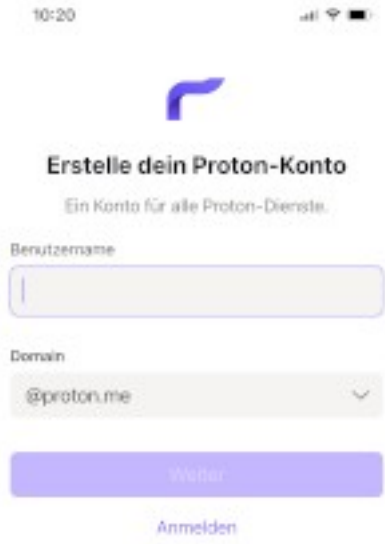
1. App herunterladen



2. App starten und ein Konto erstellen

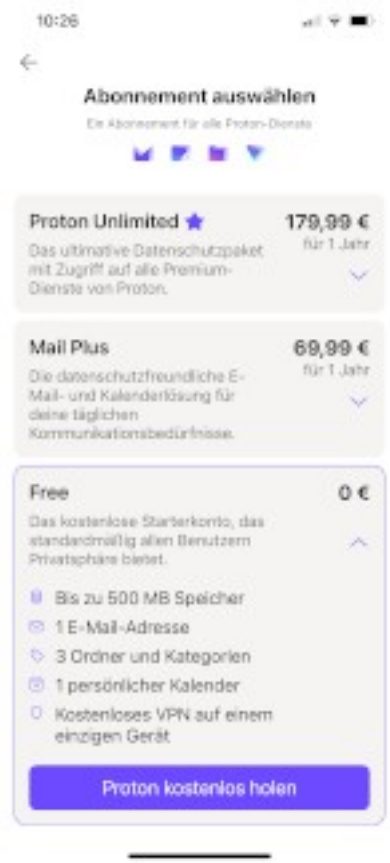
3. Benutzernamen und E-Mailadresse erstellen

4. Passwort erstellen



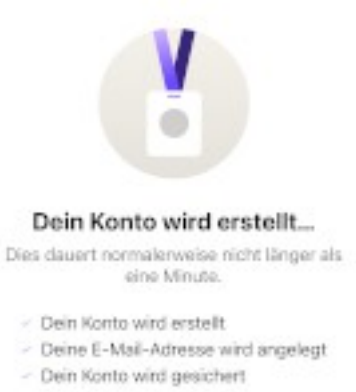
5. E-Mailadresse für Wiederherstellung eingeben

6. Abonnement auswählen – Free



7. Captcha – ich bin ein Mensch

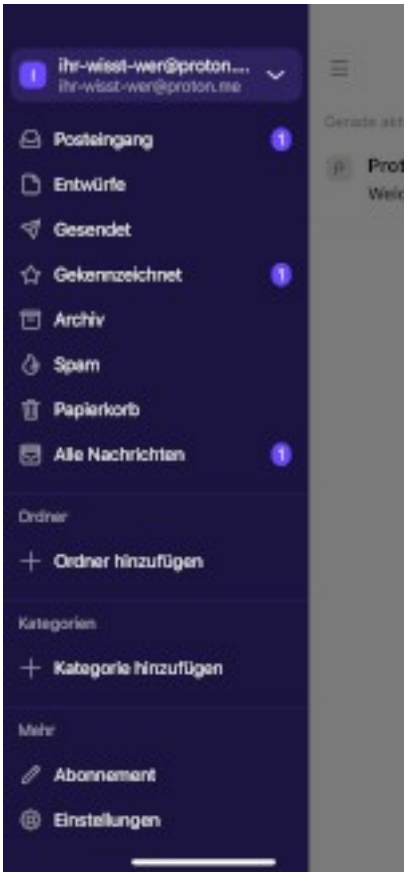
8. Das E-Mailkonto wird erstellt



9. Jetzt kann es losgehen

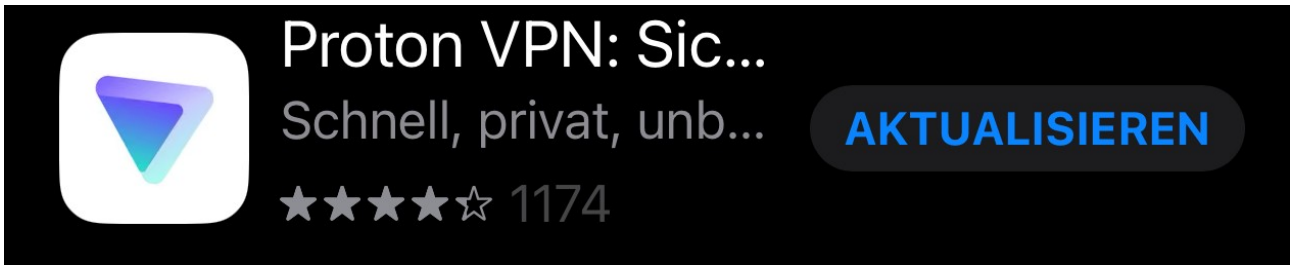
10. Der *Posteingang*
11. Die *Einstellungen* – im Postfach oben links Klicken


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
1
Entwürfe
Gesendet
Gekennzeichnet
1
Archiv
Spam
Papierkorb
Alle Nachrichten
1
Ordner
Ordner hinzufügen
Kategorien
Kategorie hinzufügen
Mehr
Abonnement
Einstellungen

9.2 ProtonVPN

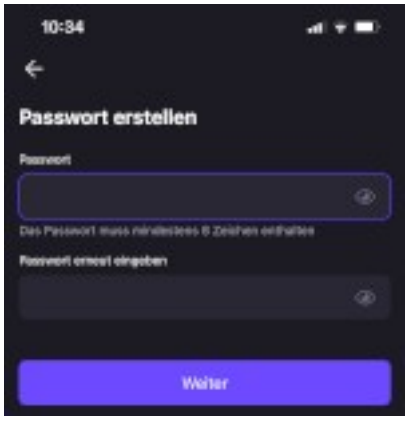
1. App herunterladen und installieren



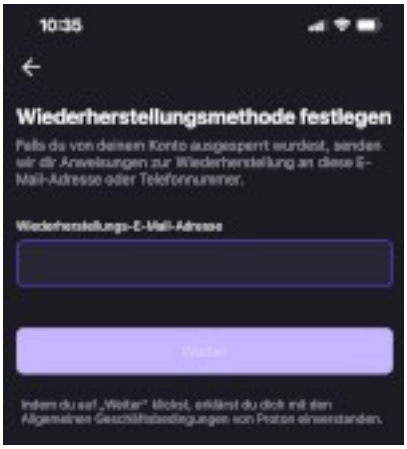
2. App starten

3. Benutzernamen überlegen und eintragen

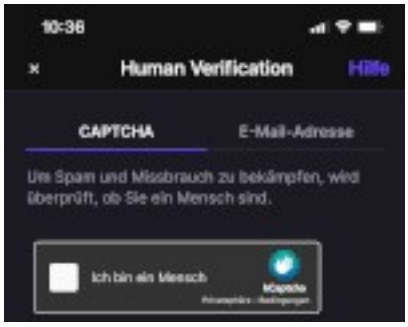
4. Passwort erstellen



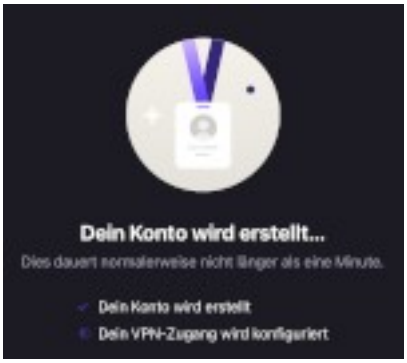
5. Wiederherstellungs E-Mailadresse eintragen



6. Captcha – ich bin ein Mensch

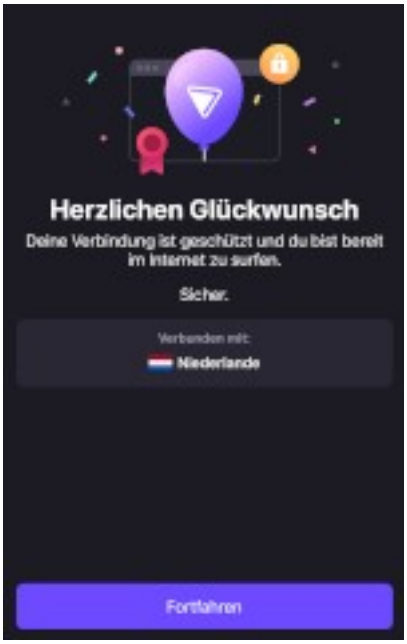


7. Das Konto wird erstellt

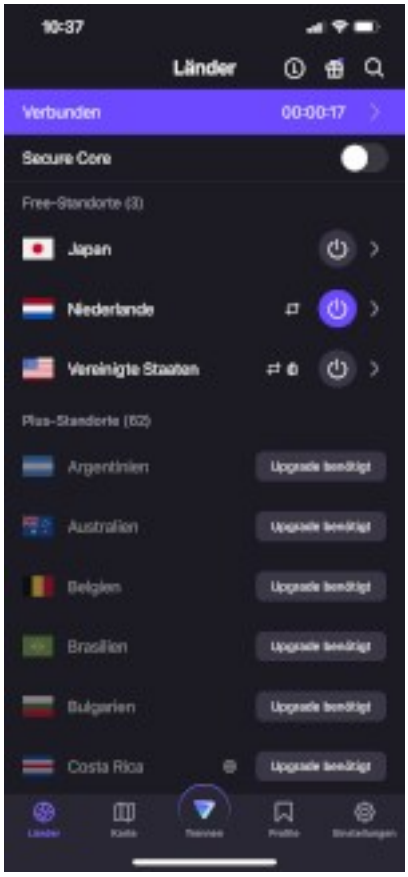


8. *Rundgang* – oder *Überspringen*

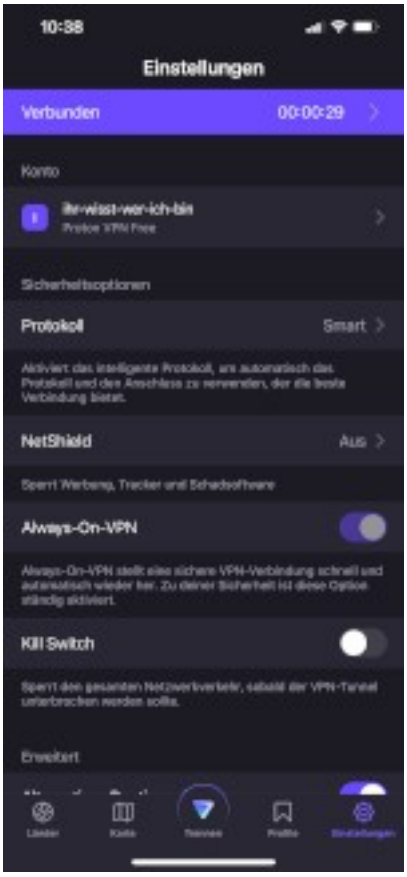
9. Es kann losgehen



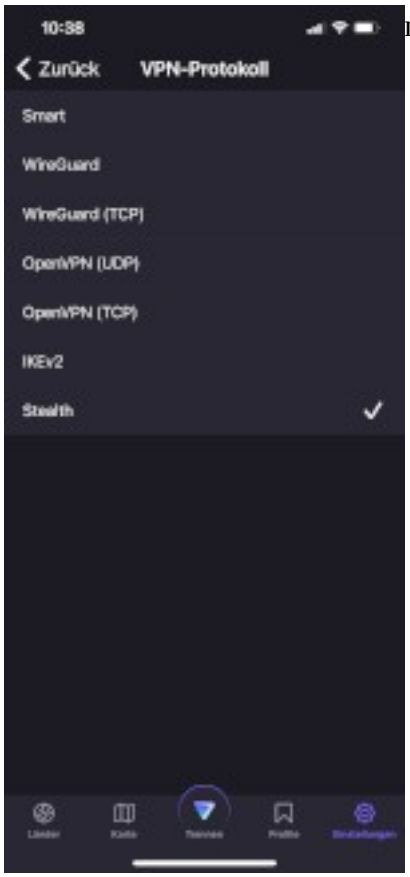
10. Land und Server auswählen



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.



9.3 Signal – sicherer Messenger

Signal herunterladen und gemäß der Anleitung installieren.

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. Firefox - https://www.mozilla.org/de/firefox/new/
5. 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
6. Posteo - https://posteo.de/de
7. Proton - https://proton.me/
8. ProtonMail/Calendar/Drive/VPN - https://proton.me/
9. ProtonVPN - https://protonvpn.com/
10. Signal für PC (gibt es auch für Smartphones) - https://signal.org/de/download/
11. Threema für PC (gibt es auch für Smartphones) - https://threema.ch/de
12. TikTok bei BuzzFeedNews - TikTok bei Forbes - https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/
13. TikTok bei Forbes - https://www.forbes.com/sites/emilybaker-white/2022/12/22/tiktok-tracks-forbes-journalists-bytedance/
14. 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
15. 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
16. TikTok bei heise security - https://www.heise.de/news/Tiktok-ueberwacht-Journalisten-per-App-7441812.html
17. Tresorit Cloudspeicher kostenlos - https://web.tresorit.com/signup
18. Tresorit Homepage - https://tresorit.com/de
19. Tutanota - https://tutanota.com/de/
20. Web.de - https://tutanota.com/de/