# E-Mailing – aber sicher

Ein Workshop der studentischen Gruppe

***ITS Us.***


der ***Technischen Hochschule Lübeck***


durchgeführt von

***Michael Georg Schmidt (Stud. B. Sc. IT Sicherheit)***

# Präambel

ich lege äußersten Wert auf die Gleichberechtigung aller Geschlechter und halte sie für zwingend notwendig!

Dennoch verwende ich in diesem Skript in der Regel nur eine Geschlechtsform, um den Text leichter lesbar zu machen. Davon abgesehen, geht es bei Texten immer um den *Genus* und nicht um den *Sexus*.

Alle Angaben beziehen sich auf den Zeitpunkt der Erstellung dieses Skripts im Sommer 2022. Es können danach durchaus Änderungen eintreten.

Sämtliche Empfehlungen sind ***nicht abschließend*** und vermutlich gibt es noch viele andere Anbieter, die den beschriebenen Service sicher und gut anbieten.

Die Empfehlungen zu Anbietern denen man aus dem Weg gehen sollte, sollten ernst genommen werden.

Dieses Skript ist modular aufgebaut, so dass alle Punkte separat nachgelesen werden können, wenn Fragen entstehen. Es ist zwar ***wünschenswert***, aber ***nicht notwendig***, dass Sie das gesamte Skript lesen, um einen Nutzen hieraus zu ziehen.

Die *Quellen* sind für diejenigen gedacht, die es ganz genau wissen möchten, oder Zweifel an der Richtigkeit der hier getroffenen Aussagen haben.

# Immer und für alles wichtig

- Halten Sie Ihre Software auf dem neuesten Stand
- Machen Sie regelmäßig Datensicherungen (Backups) – möglichst in Echtzeit

# Inhaltsverzeichnis

# 1. E-Mailing

*E-Mails* sind im Normalfall wie Postkarten. Daher sollten sie verschlüsselt sein.

## 1.1 Verschlüsseltes E-Mailing

E-Mails sollten *Ende-zu-Ende (E2EE – End-to-End-Encryption)* verschlüsselt sein. Das bedeutet, dass sie auf dem Rechner des Absenders verschlüsselt werden und erst beim Empfänger wieder entschlüsselt werden können.

Dafür gibt es zwei grundlegende Möglichkeiten

- asymmetrishe Verschlüsselung mit einem *öffentlichen* und einem *privaten Schlüssel*
  → dieses Verfahren könnte mit *PGP (Pretty Good Privacy – ziemlich gute Privatsphäre - https://de.wikipedia.org/wiki/Pretty_Good_Privacy)* umgesetzt werden.
- symmetrische Verschlüsselung bei der sowohl der Absender als auch der Empfänger den *selben geheimen Schlüssel* verwenden. Dabei kommt *AES-Verschlüsselung (Advanced Encryption Standard - https://de.wikipedia.org/wiki/Advanced_Encryption_Standard)* zum Einsatz.

Beide Verfahren sind als ausgesprochen sicher zu betrachten. Da die Verwendung der *symmetrischen Verschlüsselung* für Endbenutzer deutlich einfach ist, als der Einsatz von *PGP*, beschränkt sich dieses Skript auf eine nähere Beschreibung der Verschlüsselung mit dem *symmetrischen Verschlüsselungsverfahren AES*.

Hier stelle ich zwei E-Mailanbieter näher vor, die eine E2EE-Verschlüsselung mit AES umsetzen. Sofern Sie PGP vorziehen könnten Sie *mailbox.org* oder *posteo* nutzen. Alle Anbieter haben individuelle Eigenschaften, die möglicherweise ein wichtigeres Kriterium als eine „einfache“ E2EE sind. Sehe Sie sich die Angebote am besten selbst an.

Auch diese Auflistung ist ***nicht*** vollständig. Es gibt sicherlich mehr gute und sichere Anbieter für E-Mailaccounts. Anbieter von denen Sie unbedingt Abstand nehmen sollten erwähne ich später. Grundsätzlich ist es ***keine*** *gute Idee*, amerikanische Anbieter zu verwenden.

## 1.2 Sichere E-Mailanbieter

### 1.2.1 mailbox.org

*mailbox.org* ist ein deutscher Anbieter. Damit bietet er ein hohes Maß an gesetzlich garantiertem Datenschutz an. mailbox.org bietet für die Verschlüsselung das *asymmetrische Verfahren* mit *PGP* an.

### 1.2.2 Posteo

*Posteo* ist ebenfalls ein deutscher Anbieter und garantiert daher ebenfalls ein hohes Niveau an Datenschutz. Auch Posteo verschlüsselt E-Mails mit dem *asymmetrischen Verfahren PGP*. Posteo bietet die Möglichkeit an, E-Mailaccount anonym zu bezahlen.

Sowohl *ProtonMail* als auch *Tutanota* bieten die Möglichkeit an, ein *kostenloses E-Mailkonto* einzurichten.

## 1.2.3 ProtonMail

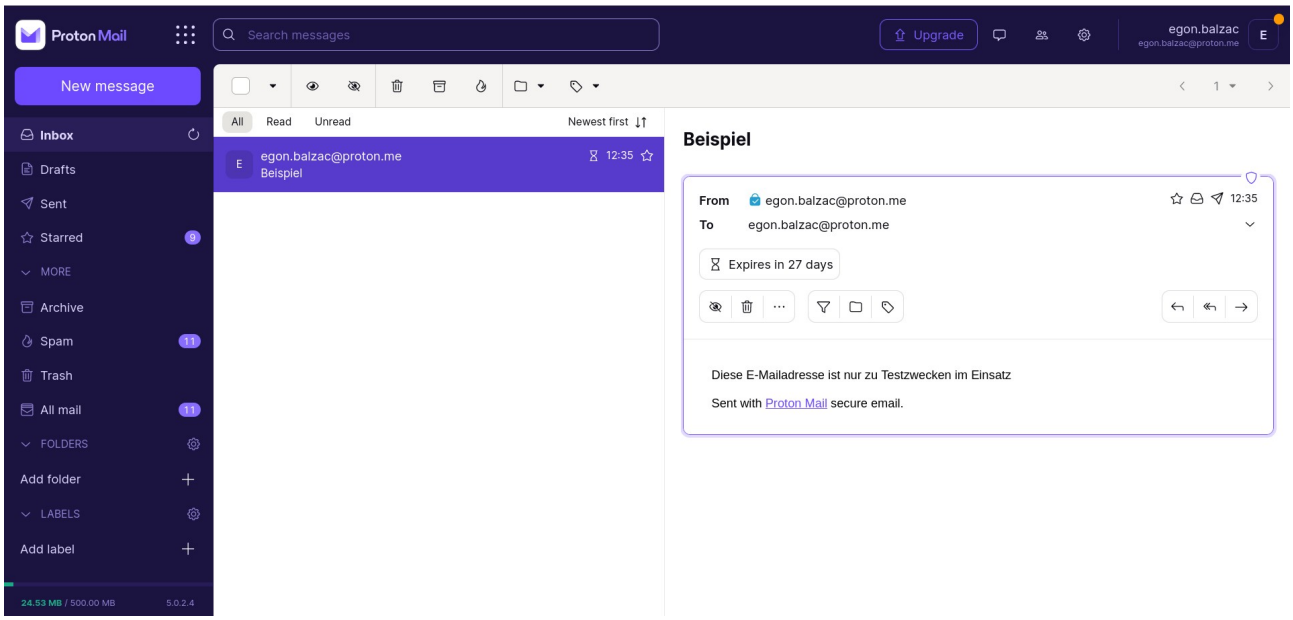
*Proton(Mail)* ist ein schweizer Anbieter der unter dem Oberbegriff *Proton* firmiert. Proton bietet nicht nur sichere E-Mailkonten an, sondern auch sichere *Online-Kalender* und sichere *VPN*.

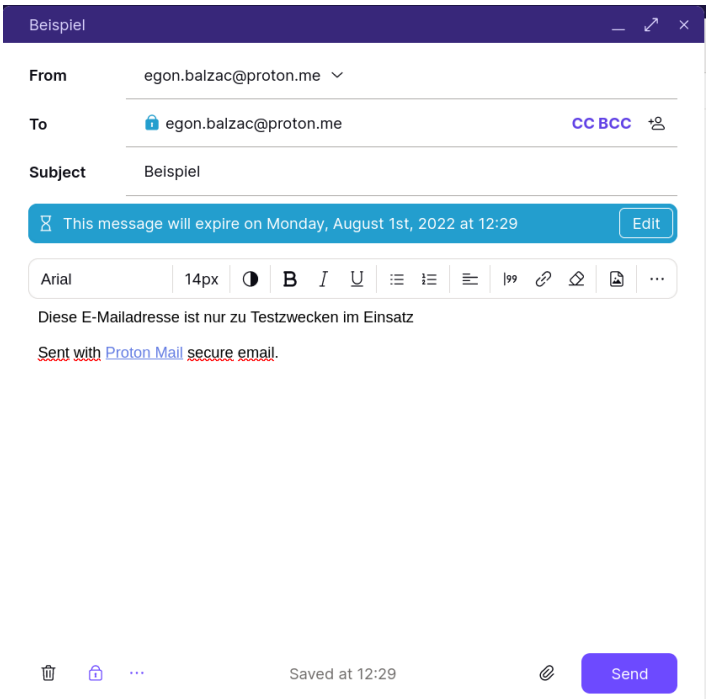
*ProtonMail* garantiert das Datenschutzniveau der Schweiz, da Proton ein Schweizer Anbieter ist. Damit ist es mit dem Datenschutzniveau der *DSG-VO (DSG-VO - https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679)* zu vergleichen (*Bundesgesetz über den Datenschutz - https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de*) und empfehlenswert.

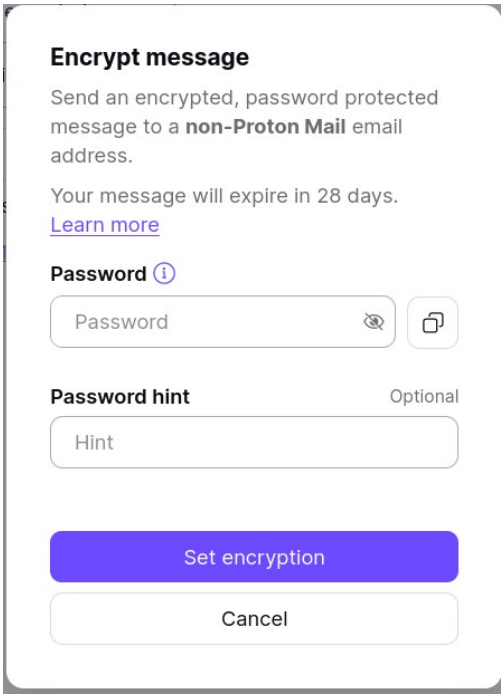
ProtonMail verwendet für die Verschlüsselung von E-Mails und deren Anhängen das *symmetrische Verfahren AES-256 (Wikipedia, Advanced Encryption Standard - https://de.wikipedia.org/wiki/Advanced_Encryption_Standard)*.

### *1.2.3.1 Verschlüsselte E-Mails mit ProtonMail*

Öffnen Sie in Ihrem Protonmail-Account ein *E-Mailformular*, indem Sie *oben links* auf *New Message* bei deutschsprachigen Accounts *Neue Nachricht* klicken. Bei deutschsprachigen Acconts ist auch das vollständige Menü deutschsprachig.





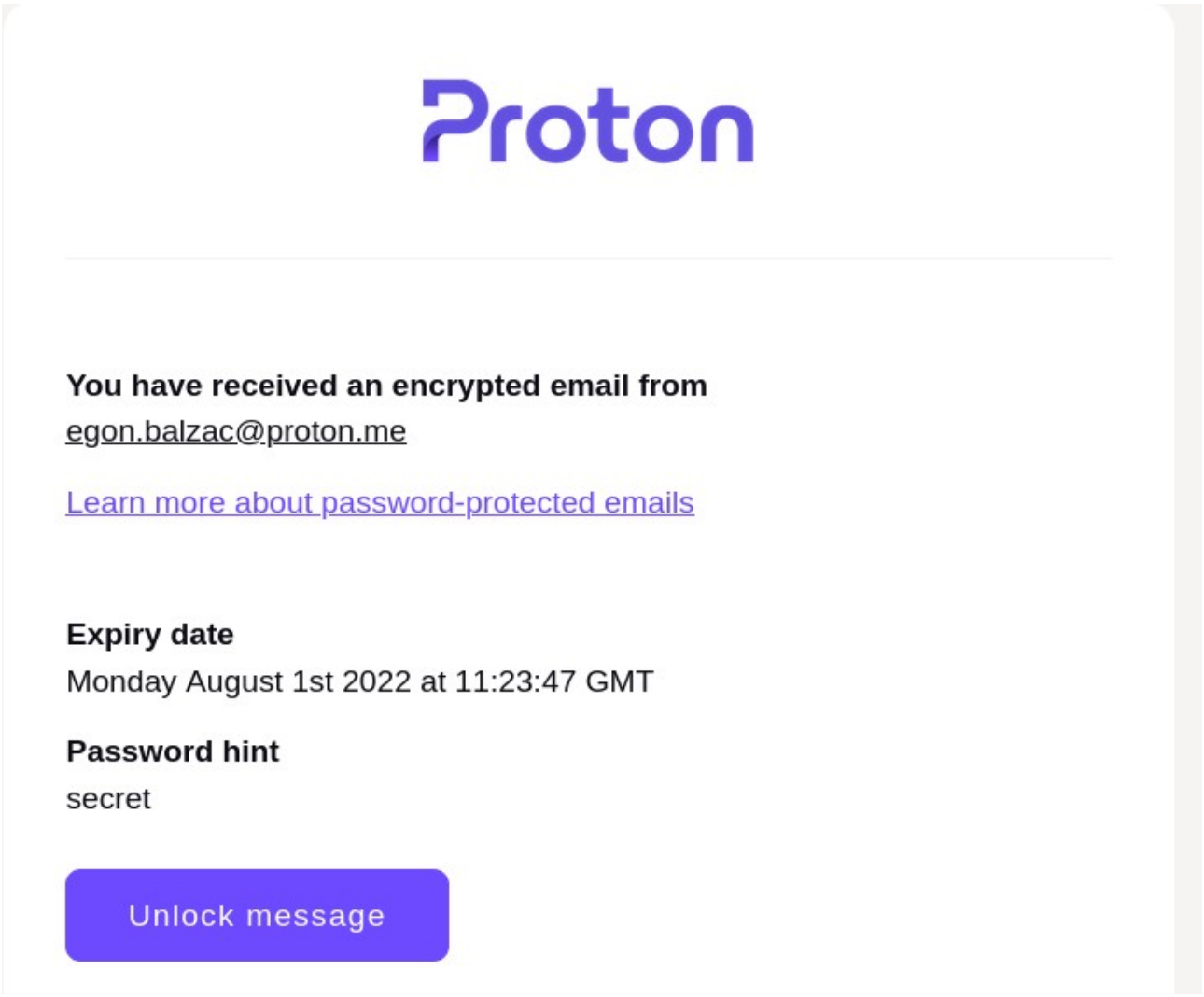

Links sehen Sie das *E-Mailformular* von *Protonmail*. Um eine Nachricht zu verschlüsseln, klicken Sie am unteren Rand auf das hier blau markierte Schlosssymbol. Sie erhalten dann eine Maske, die wie in der rechten Abbildung aussieht. Hier geben Sie Ihr geheimes Passwort ein. Zusätzlich können Sie für den Empfänger auch noch einen *Passworthinweis* eingeben. Bestätigen Sie Ihre Eingaben mit *Set encryption* der dem deutschsprachigen Pendant.

Im *E-Mailformular* erkennen Sie oben in der Zeile *To / An* an dem *Schlosssymbol*, dass diese E-Mail verschlüsselt versandt wird.

Schicken Sie Ihre E-Mail mit einem Klick auf *Send / Absenden* ab.

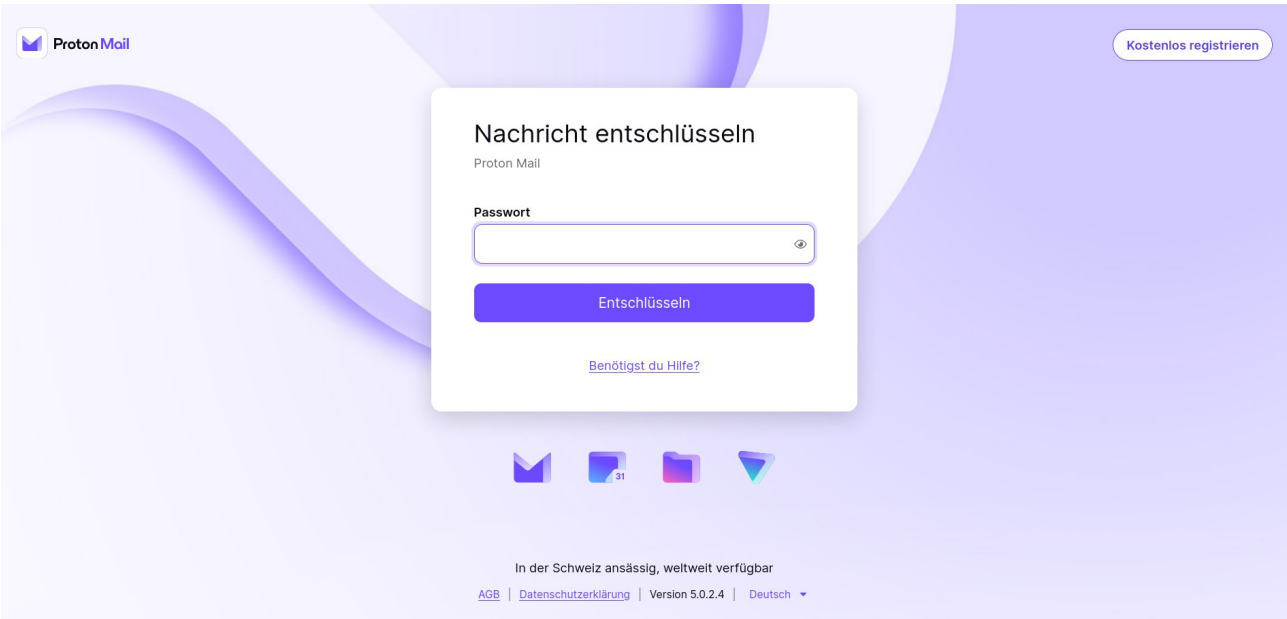
Der Empfänger Ihrer E-Mail muss ***bevor*** er diese lesen kann, das dazugehörige Passwort kennen. Das könnten Sie ihm per *sicherem Messenger*, per *Telefon* oder auf anderem Weg, nur ***nicht per E-Mail*** mitteilen.

Die E-Mail die der Empfänger erhält sieht so aus

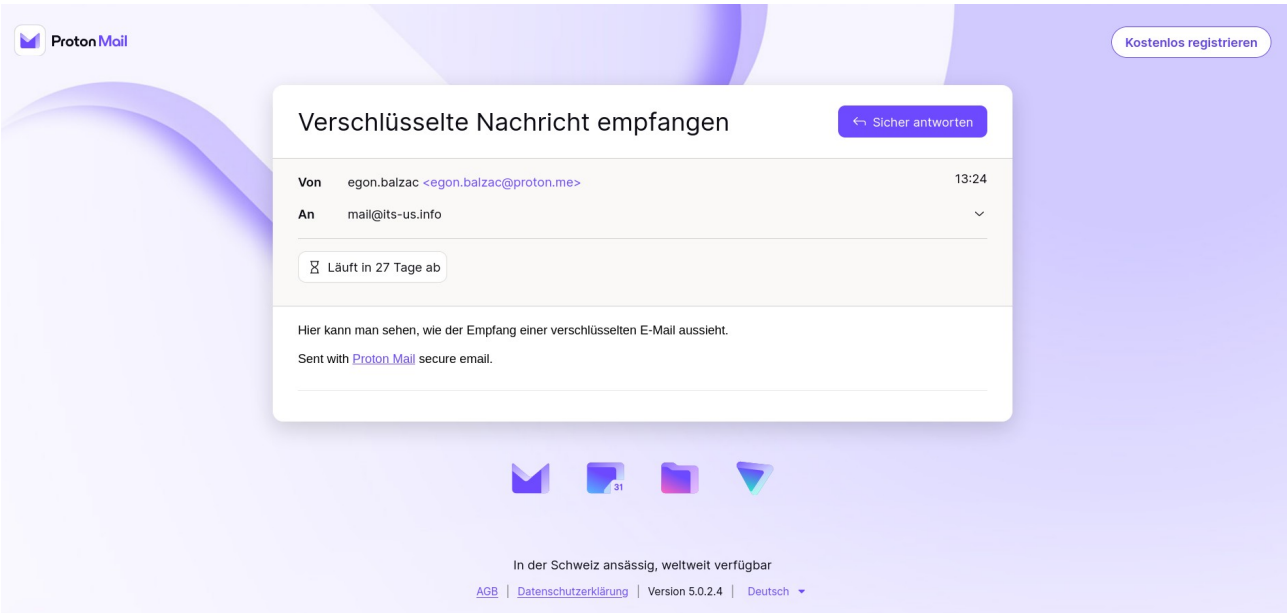



Der Empfänger sieht also, von wem die Nachricht kommt und kann diese durch einen Klick auf den Button am Ende der E-Mail öffnen. Die E-Mail bleibt ungeöffnet *vier Wochen* bei Protonmail gespeichert, bevor sie automatisch gelöscht wird.

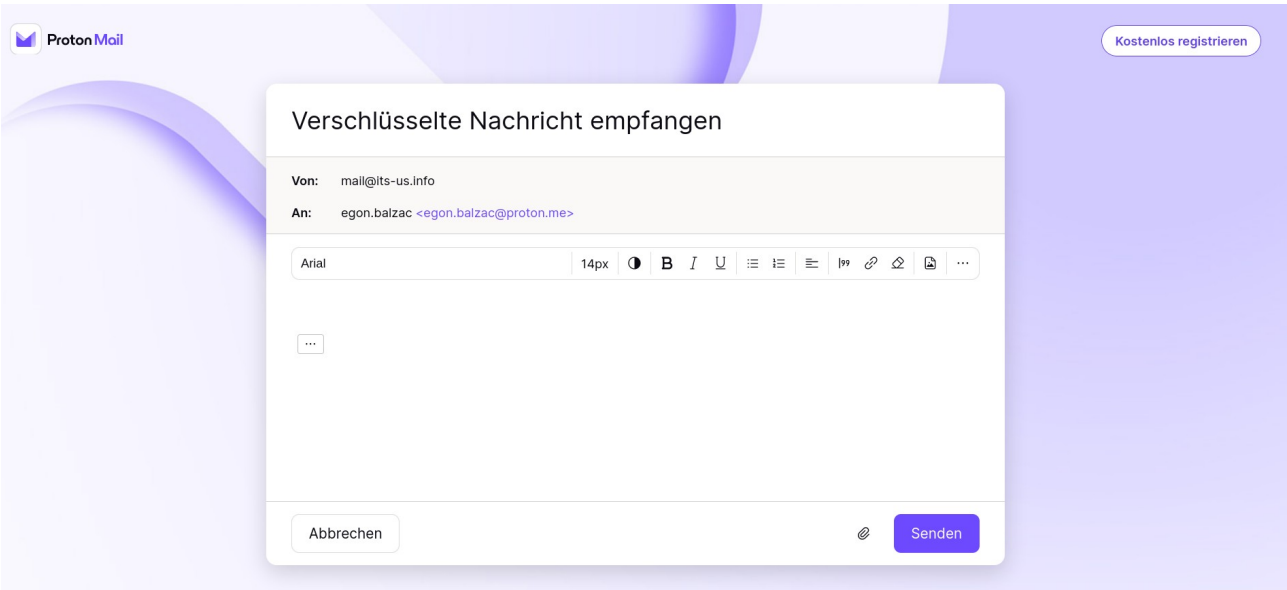
Nachdem der Empfänger den Button angeklickt hat, gelangt er auf diese Seite




Nachdem er das Passwort eingegeben hat sieht er die entschlüsselte E-Mail



Auf diese E-Mail kann der Empfänger mit einem Klick auf *sicher antworten*, ebenfalls verschlüsselt antworten.



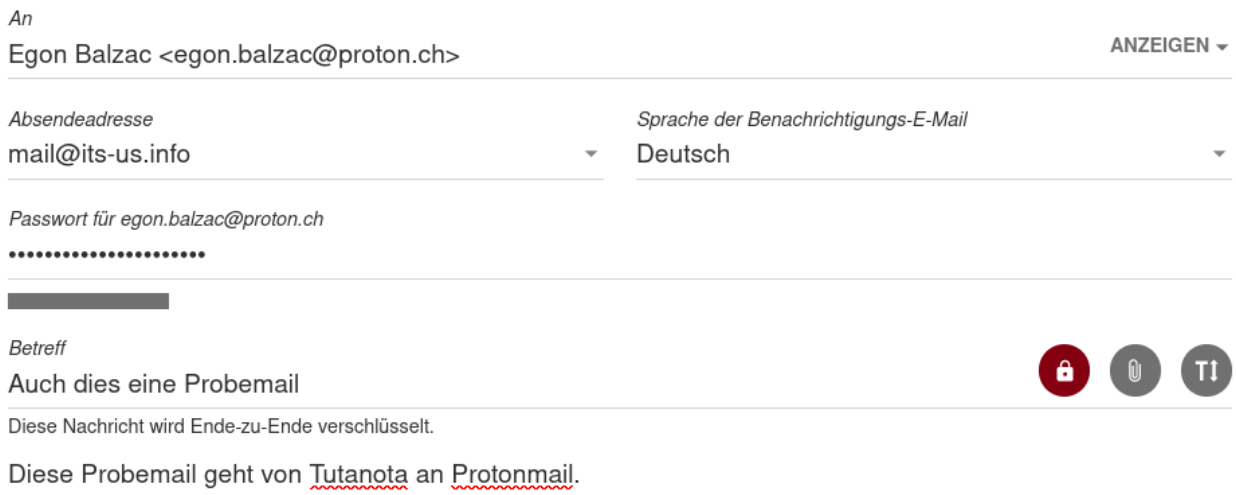

Wenn zwei Leute sich von Protonmail zu Protonmail schreiben, sind die Nachrichten ***immer automatisch*** E2EE.

Die Kommunikation zwischen einem E-Mailkonto bei Protonmail und einem Empfänger bei einem anderen Anbieter bleibt E2EE, weil die E-Mail, die von dem Protonkon-E-Mailkonto versandt wird, auf den Protonservern liegen bleibt, wo sie sicher verschlüsselt ist. Gleiches gilt für Tutanota.

### *1.2.3.2 Verschlüsseltes E-Mailing mit Tutanota*

*Tutanota* ist ein deutsches Unternehmen, das den strengen Anforderungen der DSG-VO (*https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679)* unterliegt. Tutanota setzt ebenfalls auf eine *symmetrische Verschlüsselung mit AES-256*.

Von der Funktionsweise arbeitet Tutanota genauso, wie ich es für Protonmail beschrieben habe. Das *E-Mailformular* bei Tutanota sieht wie folgt aus




In diesem E-Mailformular steht ausdrücklich *Passwort für (E-Mailadresse des Empfängers)*. Darunter zeigt ein Balken die Stärke des Passworts an.

Im weiteren Verlauf sind die Schritte genauso wie bei Protonmail. Aus Platzgründen verzichte ich jedoch darauf, dies zu illustrieren. Zusätzlich haben Sie die Möglichkeit die Sprache der Benachrichtigungs-E-Mail einzustellen.

## 1.2.4 Unsichere Anbieter

Grundsätzlich gilt, dass Ihre Daten bei *amerikanischen Unternehmen* ***nicht sicher*** sind. Das liegt daran, dass amerikanische Behörden an Hand zweier Rechtsgrundlagen von amerikanischen Unternehmen die Herausgabe aller Daten ihrer Kunden verlangen können. Dabei spielt es keine Rolle, wo die Niederlassung der amerikanischen Firma sich befindet oder aus welchem Land die Kunden stammen (FISA – Foreign Intelligence Surveiliance Act, section 702, § 1881a - https://www.law.cornell.edu/uscode/text/50/1881a) und dem USA Patriot Act – 2001 – (USA Patriot Act – https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act).

Eine ***Ausnahme*** sind amerikanische Unternehmen, die glaubhaft zusichern, dass Sie gar keine Daten von Ihnen speichern und so wenig wie notwendig erheben. Dazu zählen Anbieter wie ***Firefox***.
Ursprünglich zählte auch ***DuckDuckGo*** zu diesen Anbietern, bis herauskam, dass DuckDuckGo einen *Tracking-Vertrag mit Microsoft* abgeschlossen hat – https://global.techradar.com/de-de/news/duckduckgo-in-der-kritik-wegen-versteckter-tracking-vereinbarung-mit-microsoft.

Bei Anbietern wie

- Google – gmail
- Facbebook
- outlook.com - @outlook.com
- Yahoo

müssen Sie davon ausgehen, dass Ihre Daten

- gespeichert werden
- mit anderen Daten verknüpft werden
- Profile erstellt werden
- die Inhalte Ihrer Nachrichten ebenfalls verarbeitet werden
- Ihre Metadaten für die Erstellung von Profilen missbraucht werden
- Ihre (Meta)Daten verkauft werden

Google bietet seit einiger Zeit eine E2EE an. Das ist gut, wenn sie aktiviert ist. Dennoch sagen Ihre Metadaten immer viel zu viel über Sie aus, als dass es gerechtfertigt wäre, ein gmail-Konto zu nutzen.

### 1.2.5 Alle meine Kontakte kennen meine „gmail-Adresse“

Wenn *alle Ihre Kontakte* Ihre gmail-Adresse oder etwas Ähnliches kennen, ist auch das kein Problem.

1. Richten Sie sich eine neue E-Mailadresse bei einem *empfehlenswerten E-Mailanbieter* ein
2. Richten Sie bei Ihrer „bekannten“ E-Mailadresse eine *E-Mailumleitung* zu Ihrer neuen, *sicheren E-Mailadresse* ein
3. Antworten und schreiben Sie ab sofort nur von Ihrer *neuen / sicheren E-Mailadresse*

Schon nach kurzer Zeit ist Ihre neue *sichere E-Mailadresse* allen Kontakten bekannt. Sie verpassen keine Nachrichten, weil alle Nachrichten umgeleitet sind und Ihre Privatsphäre wird immer besser geschützt.

## 1.2.6 Tracker

*Tracker* sind Programmschnippsel, die Ihre Aktivitäten aufzeichnen und diese Daten automatisch an Dritte weiterleiten. Tracker sind häufig in Bildern oder E-Mails eingebaut. Als Nutzer bemerken Sie sie nicht, dennoch spionieren Tracker Sie aus.

### *1.2.6.1 Trackern entkommen*

Trackern kann man vor allem auf zwei Arten entgehen. Entweder

- Sie nutzen als E-Mailformat *nur Text* oder
- Sie verwenden E-Mail(Relay)anbieter, die Tracker für Sie automatisch löschen

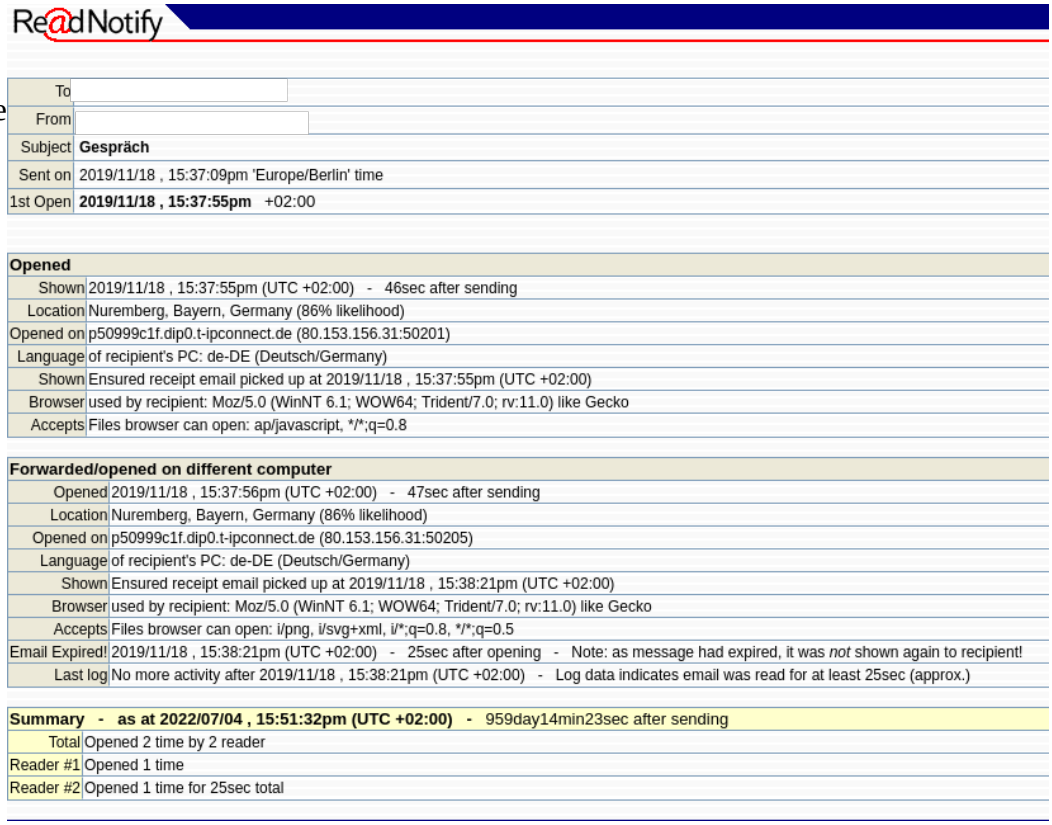
Wenn Sie als E-Mailformat *nur Text* nutzen, können Sie keine Bilder, keine Emojis und keine Formatierungen wie **fett**, *kursiv* oder farbigen Text verwenden.

Wenn Sie stattdessen E-Maianbieter wie *Protonmai* oder E-Mailrelayanbieter wie *RelayFirefox* verwenden, dann können Sie arbeiten wie Sie es gewohnt sind und die Dienstleister filtern für Sie die Tracker heraus.

### *1.2.6.2 Beispiel für Tracker*

Der amerikanische E-Maildienstleister *readnotify.com (Readnotify - https://www.readnotify.com/)*

Hier sehen Sie ein Beispiel, bei dem eine E-Mail



ReadNotify

| | |
|---|---|
| To | |
| From | |
| Subject | **Gespräch** |
| Sent on | 2019/11/18 , 15:37:09pm 'Europe/Berlin' time |
| 1st Open | **2019/11/18 , 15:37:55pm** +02:00 |

| **Opened** | |
|---|---|
| Shown | 2019/11/18 , 15:37:55pm (UTC +02:00) - 46sec after sending |
| Location | Nuremberg, Bayern, Germany (86% likelihood) |
| Opened on | p50999c1f.dip0.t-ipconnect.de (80.153.156.31:50201) |
| Language | of recipient's PC: de-DE (Deutsch/Germany) |
| Shown | Ensured receipt email picked up at 2019/11/18 , 15:37:55pm (UTC +02:00) |
| Browser | used by recipient: Moz/5.0 (WinNT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko |
| Accepts | Files browser can open: ap/javascript, */*;q=0.8 |

| **Forwarded/opened on different computer** | |
|---|---|
| Opened | 2019/11/18 , 15:37:56pm (UTC +02:00) - 47sec after sending |
| Location | Nuremberg, Bayern, Germany (86% likelihood) |
| Opened on | p50999c1f.dip0.t-ipconnect.de (80.153.156.31:50205) |
| Language | of recipient's PC: de-DE (Deutsch/Germany) |
| Shown | Ensured receipt email picked up at 2019/11/18 , 15:38:21pm (UTC +02:00) |
| Browser | used by recipient: Moz/5.0 (WinNT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko |
| Accepts | Files browser can open: i/png, i/svg+xml, i/*;q=0.8, */*;q=0.5 |
| Email Expired! | 2019/11/18 , 15:38:21pm (UTC +02:00) - 25sec after opening - Note: as message had expired, it was *not* shown again to recipient! |
| Last log | No more activity after 2019/11/18 , 15:38:21pm (UTC +02:00) - Log data indicates email was read for at least 25sec (approx.) |

| **Summary - as at 2022/07/04 , 15:51:32pm (UTC +02:00) -** 959day14min23sec after sending | |
|---|---|
| Total | Opened 2 time by 2 reader |
| Reader #1 | Opened 1 time |
| Reader #2 | Opened 1 time for 25sec total |

automatisch mit einem Tracker angereichert wurde. Der Empfänger hat dies nicht mitbekommen. Der Absender hat sehr viele Informationen erhalten, die er eigentlich nicht haben dürfte. Der Informationsstrom geht weiter, solange die abgeschickte E-Mail nicht dauerhaft gelöscht wurde.

Bei dem gezeigten Beispiel handelt es sich um eine alte und „einfache“ Version des „Dienstes“ readnotify.com. Bei entsprechender Bezahlung können noch sehr viel mehr Informationen ausspioniert werden. Außerdem ist der „Dienst“ inzwischen auch aktualisiert worden. Es könnte also noch mehr Möglichkeiten zur Spionage geben.

Wenn Sie einen E-Mail-Relayanbieter oder einen sicheren E-Mailanbieter nutzen, ist die Wahrscheinlichkeit, dass Ihnen Ähnliches passiert sehr gering.

Wenn Sie als E-Mailformat *nur Text* oder Entsprechendes einsetzen, ist diese Art der Spionage ausgeschlossen.

### 1.2.7 E-Mail-Relays

E-Mail-Relays verbergen die tatsächliche E-Mailadresse von Nutzern. Diese können stattdessen die E-Mail-Relay-Adresse angeben, damit E-Mails an die E-Mail-Relay-Adresse an die eigene Adresse weitergeleitet werden können. Damit ist Spam leichter zu filtern, außerdem entfernen die meisten E-Mail-Relay-Anbieter in E-Mails enthaltene Tracker. Antworten kann man auch über die E-Mail-Relay-Adressen.

Empfehlenswert ist für E-Mail-Relays der Anbieter Firefox (Relay Firefox – https://relay.firefox.com/).
***DuckDuckGo*** hat auch ein Angebot für E-Mail-Relays. Bislang galt DuckDuckGo als zuverlässiger Datenschützer. Leider kam inzwischen heraus, dass die Suchmaschine DuckDuckGo Nutzerdaten an Microsoft verkauft. Angeblich soll sich dies nur auf die Suchmaschine beziehen und angeblich soll diese immer noch besser sein, als alle anderen Suchmaschinen. Entscheiden Sie selbst, ob Sie DuckDuckGo weiterhin vertrauen wollen oder nicht. Einen Artikel hierzu finden Sie hier - https://global.techradar.com/de-de/news/duckduckgo-in-der-kritik-wegen-versteckter-tracking-vereinbarung-mit-microsoft

### 1.2.8 Wegwerf-E-Mailadressen

Das Wort *Wegwerf-E-Mailadressen* klingt so vollkommen unzeitgemäß, wo alle auf Nachhaltigkeit achten. Das was dahinter steckt ist jedoch ausgesprochen nachhaltig, denn Sie können damit Ihre Privatsphäre schützen.

Bei einigen Diensten muss man eine E-Mailadresse angeben, um sie nutzen zu können. Oftmals hat das eine Belästigung mit Spam-E-Mails zur Folge. Das will niemand.

Daher gibt es Anbieter von *Wegwerf-E-Mailadressen*. Das sind E-Mailadressen, die man für wenige Minuten aktiviert. Hier können Sie in diesem Zeitraum Nachrichten empfangen. Das ist wichtig, weil Dienste oft eine *Bestätigungs-E-Mail* versenden, die einen Code zur Verifikation enthalten. Den können Sie so empfangen. Danach verfällt die E-Mailadresse, Sie können den gewünschten Dienst nutzen und potentielle Spam-E-Mails verschwinden im Nichts.

Einige Anbieter von Wegwerf-E-Maildressen sind

- @mail.tm - https://mail.tm/de/
- byom.de (byom - https://www.byom.de/)
- Müllmail (Müllmail - https://muellmail.com/)
- Spamgourmet (Spamgourmet - https://www.spamgourmet.com/index.pl)
- tempr.email – (tempr.email - https://tempr.email/)
- Trashmail – (Trashmail - https://trashmail.com/)

Nutzen Sie diese E-Mailanbieter nur für die beschrieben Zwecke, denn es ist davon auszugehen, dass auch diese Anbieter Sie tracken und Profile erstellen wollen. Die bezahlten Angebote dieser Anbieter könnten „sicher“ sein.

Bevor Sie die Möglichkeit anonymen E-Mailings nutzen, überlegen Sie ***ganz genau***, ob das gerechtfertigt ist. Sie dürfen diese Option ***auf keinen Fall für illegale Zwecke nutzen!***

Es gibt Situationen in denen man den Bedarf hat eine E-Mail zu versenden, aber auf jeden Fall anonym bleiben möchte. Um das zu erreichen, sollten Sie die folgenden Optionen nur in Zusammenhang mit einem

- *VPN (Virtual Private Network)* und dem
- *anonymisierenden TOR Browser*

nutzen. Dafür gibt es im Wesentlichen zwei Möglichkeiten:

### *1.2..8.1 Kurzfristig und einmalig*

Es gibt Anbieter, die es ermöglichen, eine Webmail ohne Anmeldung abzusenden. Früher galt hier *Anonymouse.org* als empfehlenswert. Das ist aktuell nicht mehr so, denn dieser Anbieter verschlüsselt seinen Datenverkehr nicht – zu erkennen am *http*-Protokoll. Für sicheren Datenverkehr müsste es ein http**s**-Protokoll sein.

Eine Möglichkeit E-Mails anonym zu versenden sind *Trashmail-Anbieter*. Es ist aber fraglich, wie sicher und anonym Sie dabei wirklich sind. Ich würde nicht darauf vertrauen, dass Ihre Anonymität bei diesen Anbietern gewährleistet ist.

Daher empfehle ich als echte Alternative *Protonmail über TOR* (s. 2.4.8.2.1).

### *1.2.8.2 Dauerhafte Nutzung*

Für eine dauerhafte anonyme Nutzung eines E-Maildienstes – das macht vor allem für Dissidenten Sinn – bietet sich der anonyme E-Maildienst von *Protonmail* an.

#### 1.2.8.2.1 Anonymes E-Mailkonto mit Protonmail

Protonmail bietet einen besonderen Service für Menschen an, die äußersten Wert auf ihre Privatsphäre legen. Nutzer können eine anonyme Protonmail-E-Mailadresse anlegen, wenn Sie über den anonymisierenden Browser TOR (TOR - https://www.torproject.org/de/download/) die Website von Protonmail im TOR-Netzwerk (Protonmail über TOR - https://proton.me/news/tor-encrypted-email) aufrufen. Dann benötigen Sie nur noch eine „Wegwerf-E-Mailadresse“, die Sie auch über TOR aufrufen, und schon ist ein vollständig anonymes E-Mailkonto eingerichtet.

**Vorgehensweise**

1. VPN starten
2. TOR-Browser starten
3. Wegwerf-E-Maildresse einrichten (s. 2.4.7)
4. Protonmail über TOR aufrufen (https://proton.me/news/tor-encrypted-email) und E-Mailadresse einrichten
5. Bestätigungs-E-Mail über Wegwerf-E-Mailadresse empfangen

### 1.2.9 Phishing E-Mails

*Phishing E-Mails* sind E-Mails mit denen Dritte versuchen an Informationen zu gelangen, die nicht für sie bestimmt sind. Das können Passwörter sein, das können Informationen über Personen oder über andere Dinge wie Gebäudeaufbau, oder Überweisungen oder vieles andere, sein. Daher

- Überlegen Sie, ob die Nachricht die Sie bekommen haben, wirklich von dem genannten Absender kommen könnte und ob der Inhalt korrekt sein könnte
    - Immer, wenn Ihnen der Inhalt seltsam vorkommt, ziehen Sie dies in Zweifel und prüfen es genau nach
        - Durch persönliche Nachfrage
        - Ansicht der E-Mailheader – wie das geht, erkläre ich etwas weiter unten
        - Sehen Sie sich die Absenderadresse ganz genau an
          steht da *noreply@sparkase.de* oder steht noreply@sparkasse.de?
          Der entscheidende Unterschied ist das *doppelte s*, das die echte *Sparkasse* verwendet.
- Lassen Sie sich nicht durch einen harschen Ton oder Drohungen einschüchtern
    - Wenn in E-Mails gedroht wird, egal womit, ist oft etwas nicht korrekt
- Seien Sie genauso skeptisch, wenn E-Mails zu freundlich sind und Sie um einen Gefallen gebeten werden
- Geben Sie nie und nirgends persönliche Daten an, wenn Sie per E-Mail dazu aufgefordert werden
- … vor allem keine Kontodaten
- Mitteilungen über Gewinne per E-Mail sind immer Anlass zum Zweifeln
- E-Mails mit schockierendem Inhalt lassen Sie erst einmal liegen und lesen Sie diese etwas später erneut und beurteilen dann, ob Handlungsbedarf besteht. Wenn es um eine echte Notlage geht, ist die Wahrscheinlichkeit, dass man Sie persönlich kontaktiert deutlich größer, als dies per E-Mail zu tun.
- Wenn Sie aufgefordert werden *Makros* zu aktivieren, ***löschen Sie diese E-Mail sofort!***, ohne die Makros aktiviert zu haben.
- Klicken Sie keine Anhänge mit der Endung ***.exe*** an. Löschen Sie auch diese E-Mails sofort.
- Achten Sie darauf, ob die *Empfängeradrsse* korrekt ist. Wenn Sie bei *Amazon* mit der E-Mailadresse *ich@kaufen.de* registriert sind, aber an die E-Mailadresse *ich@freunde.de* eine E-Mail von *Amazon* bekommen, ist hier vermutlich etwas falsch.
- Wenn in E-Mails *Links* enthalten sind, öffnen Sie diese nur, wenn Sie ganz sicher sind, dass es sich um einen vertrauenswürdigen Link handelt. Sehen Sie sich die Schreibweise ganz genau an. Hier gilt das Gleiche wie bei der *sparkase* und der *sparkasse*.
- Kommen Ihnen E-Mails merkwürdig vor, die auch noch Adressen im *CC-Feld* der E-Mail enthalten, löschen Sie diese am besten gleich.

- Achten Sie darauf, ob Sie von Absendern, die Sie normalerweise persönlich ansprechen, plötzlich mit *Sehr geehrte Damen und Herren* oder ähnlichem angesprochen werden
- Achten Sie auf ungewöhnliche Formulierungen – Syntax – oder falsche Rechtschreibung
- Sind Umlaute *ä, ö, ü* als *a, o, u* geschrieben?
- Finden Sie in der E-Mail seltsamen Sonderzeichen, vor allem ■?
- Sind in der E-Mail Zeichenfolgen in spitzen Klammern vorhanden <b>?
- Oder Rückstriche /, die dort nicht hingehören?
- Haben Sie eine E-Mail als „schädlich“ identifiziert, markieren Sie deren Absender als *Spam*, so dass Sie Absender Sie nicht mehr belästigen kann
- Wenn E-Mails *verlinkten Text* enthalten wie hier, dann klicken Sie mit der *rechten Maustaste* darauf um sich anzeigen zu lassen, welche *URL – Internetadresse* – dahinter steckt
- Sollten Sie eine E-Mail als *gefälscht* identifiziert haben, melden Sie dies direkt dem betroffenen Unternehmen, damit dieses entsprechende Gegenmaßnahmen ergreifen kann
- Nutzen Sie so oft es geht ein *VPN (Virtuelles Privates Netzwerk – s. 2.3.3)*

## 1.2.10 E-Mail-Header

*E-Mailheader* sind die Informationen, die ein System benötigt, um eine E-Mail von A nach B zustellen zu können. Diese Informationen verraten uns viel über den Absender und technische Daten.

### *1.2.10.1 E-Mail-Header anzeigen*

Es gibt verschiedene Möglichkeiten E-Mailheader anzeigen zu lassen. Hier stelle ich einige der gebräuchlichsten Möglichkeiten vor

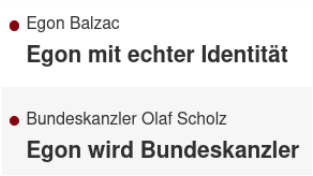
- Gmail (Gmail, Vollständige E-Mail-Header lesen - https://support.google.com/mail/answer/29436?hl=de)
  - Öffnen Sie die E-Mail, deren Header Sie überprüfen möchten.
  - Klicken Sie neben „Antworten“  auf das Dreipunkt-Menü  **Original anzeigen**.
  - Kopieren Sie den Text auf der Seite.
  - Öffnen Sie das Tool „Nachrichten-Header“.
  - Fügen Sie im Abschnitt "E-Mail-Header hier einfügen" Ihren Header ein.
  - Klicken Sie auf **Header oben analysieren**.
- GMX und Web.de
  - Klicken Sie auf das *Infosymbol* der betreffenden E-Mail
- Outlook(.com) und MS Exchange in allen Varianten (Microsoft - https://support.microsoft.com/de-de/office/anzeigen-von-kopfzeilen-f%C3%BCr-internetnachrichten-in-outlook-cd039382-dc6e-4264-ac74-c048563d212c)
  - auf E-Mailnachricht doppelklicken um sie außerhalb des Lesebereichs zu öffnen
  - klicken auf *Datei → Eigenschaften*
  - Header werden im Feld *Internetkopfzeilen* angezeigt
- ProtonMail
  - klicken Sie auf die betreffende E-Mail
  - klicken Sie auf die drei Punkte neben dem *Mülleimersymbol* in der Kopfzeile
  - klicken Sie auf *Kopfzeilen anzeigen*
- Thunderbird
  - doppelklicken Sie auf eine E-Mail
  - klicken Sie im Menü *Ansicht → Nachrichten-Quelltext*
- Tutanota
  - klicken Sie auf die betreffende E-Mail
  - klicken Sie auf die drei Punkte in der Kopfzeile

- klicken Sie auf *Öffne die E-Mail-Header*

Sie sehen eine Menge Informationen mit denen Sie möglicherweise spontan nichts anfangen können. Darum kümmern wir uns im Folgenden:

### *1.2.10.2 E-Mail-Header interpretieren*

Bevor wir E-Mail-Header interpretieren, zeige ich Ihnen an einem Beispiel, wie leicht es ist, einen angezeigten Absender zu fälschen.




Dies ist ein Ausschnitt aus dem Posteingang einer *Tutanota* E-Mailadresse. Hier hat *Egon Balzac* zwei E-Mails geschickt. Die obere E-Mail hat Egon mit seiner echten Identität versandt. Bei der zweiten ist er *Bundeskanzler Olaf Scholz*. Das ist natürlich Unsinn. Es zeigt aber, wie leicht jeder den angezeigten Absendernamen fälschen kann

Sollten Sie Zweifel an der Korrektheit eines *angezeigten Absendernamens* haben, sehen Sie sich die *E-Mail-Header* an. Wie das funktioniert habe ich unter Punkt *2.4.9.1.1 E-Mail-Header anzeigen* erläutert.

Der *E-Mail-Header* von *„Bundeskanzler Olaf Scholz“* sieht so aus

*Authentication-Results: w3.tutanota.de (dis=neutral; info=dmarc domain policy); dmarc=pass (dis=neutral p=quarantine; aspf=s; adkim=s; pSrc=dns) header.from=proton.me; dkim=pass header.d=proton.me header.s=3nlisfwx55fdhct6a2nltdul4u.protonmail header.b=eKGY54Zp Received: from w4.tutanota.de ([192.168.1.165]) by w3.tutanota.de with SMTP (SubEthaSMTP 3.1.7) id L59DBSZF for mgschmidt@its-us.info; Wed, 06 Jul 2022 10:58:59 +0200 (CEST) Received-SPF: Pass (mailfrom) identity=mailfrom; client-ip=185.70.40.140; helo=mail-40140.protonmail.ch; envelope-from=egon.balzac@proton.me; receiver=<UNKNOWN> Received: from mail-40140.protonmail.ch (mail-40140.protonmail.ch [185.70.40.140]) by w4.tutanota.de (Postfix) with ESMTPS id 0CB90106040D for <mgschmidt@its-us.info>; Wed, 6 Jul 2022 08:58:59 +0000 (UTC) Date: Wed, 06 Jul 2022 08:58:53 +0000 DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=proton.me; s=3nlisfwx55fdhct6a2nltdul4u.protonmail; t=1657097938; x=1657357138; bh=upLrFf2hHiaLDURKAypePFW3jhCKbTIkWTuE2RayN1M=; h=Date:To:From:Reply-To:Subject:Message-ID:Feedback-ID:From:To:Cc: Date:Subject:Reply-To:Feedback-ID:Message-ID;*
*b=eKGY54ZpK7BBKI8VTRCftEU2thc843Ok9htE7gN81UvoycvuY2ggvvLZdAZykzfea*
*cS9bQLmJzjmc3rYcOZdawfzahcYaAmqRWMJMrU5DD4Hc6pw0S40w0KyIsqz6JAVN3B*
*Ird72aW5nV2nxa1Hb/iXCk4jRqZvWxdPpbaM2FBBECnHbgt73CY23oH+sDXp8cD5XV*
*ipyXK7hUKRcXMjGhFLU8vVfVThfI6EuvoAO9MLIgv8v9YmodKAt3/eTb8u8yr3J19z*
*oHSuZS7VcRd4Va+Ie8lqdaFYbjZKhag4yRcYk3thV+EwWoMbRQxOf6dTaV+PJ463XM*
*Vp5iboZnbQ7MQ== To: "mgschmidt@its-us.info" <mgschmidt@its-us.info> From: Bundeskanzler Olaf Scholz <egon.balzac@proton.me> Reply-To: Bundeskanzler Olaf Scholz <egon.balzac@proton.me> Subject: Egon wird Bundeskanzler Message-ID: <1AO21DTH_HxK08g0zdLk8HCSJzNt20d_1VhOAYkMM8ARfO9yujg9V4SI6n9GCkwg_3oxTNnTv Ex8Er77biorL12-tkfLzZaZ0qFxIbiLPa0=@proton.me> Feedback-ID: 48040964:user:proton MIME-Version: 1.0 Content-Type: multipart/alternative; boundary="b1_bCXXTP0t1l9Nkg522kMfGNDXPJ7RWjVpbq7AUL48n8"*

Das wirkt zunächst erdrückend, ist aber recht einfach zu lesen. Die wichtigsten Informationen im Einzelnen

- header.from=proton.me → dieser Header sagt, von welchem E-Mailanbieter diese E-Mail kommt. Das ist hier *proton.me*, also *Protonmail*
- *for mgschmidt@its-us.info* → an diese E-Mailadresse ist die Nachricht gesandt worden
- envelope-from=egon.balzac@proton.me → *„Bundeskanzler Olaf Scholz“* schreibt vom E-Mailkonto *egon.balzac@proton.me*. Das ist vollkommen unglaubwürdig.
- From: Bundeskanzler Olaf Scholz <egon.balzac@proton.me> Reply-To: Bundeskanzler Olaf Scholz <egon.balzac@proton.me> → hier wird die Fälschung noch deutlicher.

Es ist also recht einfach, nachzuvollziehen, ob der angezeigte Absender auch der tatsächliche Absender ist. Prüfen Sie das, sobald Sie auch nur geringe Zweifel haben.

Hier sehen Sie die E-Mailheader, die der anonyme Versender *Anonymouse.org* übermittelt:

*Authentication-Results: w3.tutanota.de (dis=neutral; info=spf); dmarc=pass (dis=neutral p=quarantine; aspf=r; adkim=r; pSrc=config) header.from=dizum.com Received: from w4.tutanota.de ([192.168.1.165]) by w3.tutanota.de with SMTP (SubEthaSMTP 3.1.7) id L59F1Q8M for mgschmidt@its-us.info; Wed, 06 Jul 2022 11:47:10 +0200 (CEST) Received-SPF: Pass (mailfrom) identity=mailfrom; client-ip=45.66.35.221; helo=sewer.dizum.com; envelope-from=remailer@dizum.com; receiver=<UNKNOWN> Received: from sewer.dizum.com (sewer.dizum.com [45.66.35.221]) by w4.tutanota.de (Postfix) with ESMTP id 6DE4010603C8 for <mgschmidt@its-us.info>; Wed, 6 Jul 2022 09:47:09 +0000 (UTC) Received: by sewer.dizum.com (Postfix, from userid 1001) id DA86C601EA; Wed, 6 Jul 2022 11:47:08 +0200 (CEST) From: Nomen Nescio <nobody@dizum.com> Comments: This message did not originate from the Sender address above. It was remailed automatically by anonymizing remailer software. Please report problems or inappropriate use to the remailer administrator at <abuse@dizum.com>. To: mgschmidt@its-us.info Subject: Anonyme E-Mail Message-ID: <ff0fd608b0a8b9b7583157151ed27fbe@dizum.com> Date: Wed, 6 Jul 2022 11:47:08 +0200 (CEST)*

Die für uns wichtigste Information dieser *E-Mail-Header* ist

- Comments: This message did not originate from the Sender address above. It was remailed automatically by anonymizing remailer software. → Diese Nachricht stammt nicht von der oben angegebenen Adresse (sewer.dizum.com). Sie ist von anonymisierender Mailer-Software automatisch weiter gleitet worden.

E-Mailheader geben noch sehr viel mehr Informationen preis, die spielen hier aber keine Rolle.

# Quellen


1. *@mail.tm* - Trashmailanbieter
   https://mail.tm/de/
2. *AES-Verschlüsselung* - Wikipedia (Advanced Encryption Standard)
   https://de.wikipedia.org/wiki/Advanced_Encryption_Standard)
3. *Bundesgesetz über den Datenschutz*
   *https://www.fedlex.admin.ch/eli/cc/1993/1945_1945_1945/de*
4. *byom.de* - byom
   https://www.byom.de/
5. *DSG-VO* – DSG-VO
   *https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32016R0679*
6. *FISA* – Foreign Investigation Surveilliance Act, section 702, § 1881a
   https://www.law.cornell.edu/uscode/text/50/1881a
7. *Gmail* – Vollständige Header anzeigen
   https://support.google.com/mail/answer/29436?hl=de
8. *mailbox.org* – Mailbox.org
   https://mailbox.org/de/
9. *MS Exchange* – alle E-Mailheader anzeigen lassen
   https://support.microsoft.com/de-de/office/anzeigen-von-kopfzeilen-f%C3%BCr-internetnachrichten-in-outlook-cd039382-dc6e-4264-ac74-c048563d212c
10. *Müllmail* - Müllmail
    https://muellmail.com/
11. *Outlook.com* – alle E-Mailheader anzeigen
    https://support.microsoft.com/de-de/office/anzeigen-von-kopfzeilen-f%C3%BCr-internetnachrichten-in-outlook-cd039382-dc6e-4264-ac74-c048563d212c
12. *Patriot Act* -
    https://www.fincen.gov/resources/statutes-regulations/usa-patriot-act
13. *Posteo* – Posteo
    https://posteo.de/de
14. *Pretty Good Privacy (PGP)* – Wikipedia
    https://de.wikipedia.org/wiki/Pretty_Good_Privacy
15. *ProtonMail* – Proton.me
    https://proton.me/mail?ref=icnbtn
16. *ProtonMail über TOR*
    https://proton.me/news/tor-encrypted-email
17. *Readnotify.com* – Readnotify
    *https://www.readnotify.com/*

18. *Relay Firefox* – Firefox E-Mail-Relay
    https://relay.firefox.com/
19. Spamgourmet - Spamgourmet
    https://www.spamgourmet.com/index.pl
20. *Tech Radar* – Franziska Schaub, unterstützt von Sead Fadilpašić – (2022-05-25, DuckDuckGo in der Kritik wegen versteckter Tracking-Vereinbarung mit Microsoft)
    https://global.techradar.com/de-de/news/duckduckgo-in-der-kritik-wegen-versteckter-tracking-vereinbarung-mit-microsoft
21. *tempr.email* – tempr.email
    https://tempr.email/
22. *TOR* – Tor Onion Routing
    https://www.torproject.org/de/download/
23. Trashmail – Trashmail
    https://trashmail.com/
24. *Tutanota* – Tutanota
    https://tutanota.com/de/