

# 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 die Jahrgangsstufen 5 / 6**

## **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](mailto:mail@its-us.info)

*Threema-ID: WYH86UFA*

# Inhaltsverzeichnis

1. Hast Du ein Geheimnis?.....	4
2. Wie fühlt es sich an, wenn Du Dir vorstellst, jeder würde dieses Geheimnis kennen?.....	4
3. Dinge die Du über das Internet erzählst, sind keine Geheimnisse mehr!.....	4
4. Es gibt Streit mit der besten Freundin, dem besten Freund.....	5
5. Wichtige Regeln für alles.....	5
6. Apps – Messenger – E-Mail - Foren - Chats - Browser.....	7
6.1 Apps.....	7
6.1.1 Was Apps machen dürfen.....	7
6.1.2 Apps auf die man verzichten sollte.....	7
6.2 Messenger.....	8
6.2.1 Vertrauenswürdige Messenger.....	8
6.2.2 Gefährlicher Messenger.....	8
6.3 E-Mailanbieter.....	9
6.3.1 Empfehlenswerte E-Mailanbieter.....	9
6.4 Foren und Chats.....	10
6.5 Browser.....	10
6.6 Surfen.....	11
6.6.1 Geschützt surfen.....	11
6.6.1.1 Empfehlenswerter VPN-Anbieter.....	11
6.7 Geschenke – Gewinne – Freundschaft.....	12

# 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 an jemanden etwas, 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 machen 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

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.

## 6.2 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



<https://threema.ch/de>

Natürlich kann man aber auch bei diesen Messengern Screenshots machen.

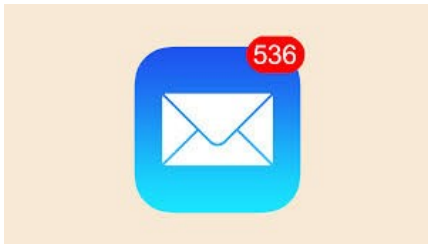
### 6.2.2 Gefährlicher Messenger



**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 das die Gegenseite etwas dazu tun muss.  
Protonmail bietet zusätzlich zur kostenlosen E-Mailadresse ein kostenloses VPN (**V**irtual **P**riate **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 das 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 an Hand 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 zurückverfolgbar. 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!