YOUTH &ARTS WEB | SOCIAL NETWORK TRAINING

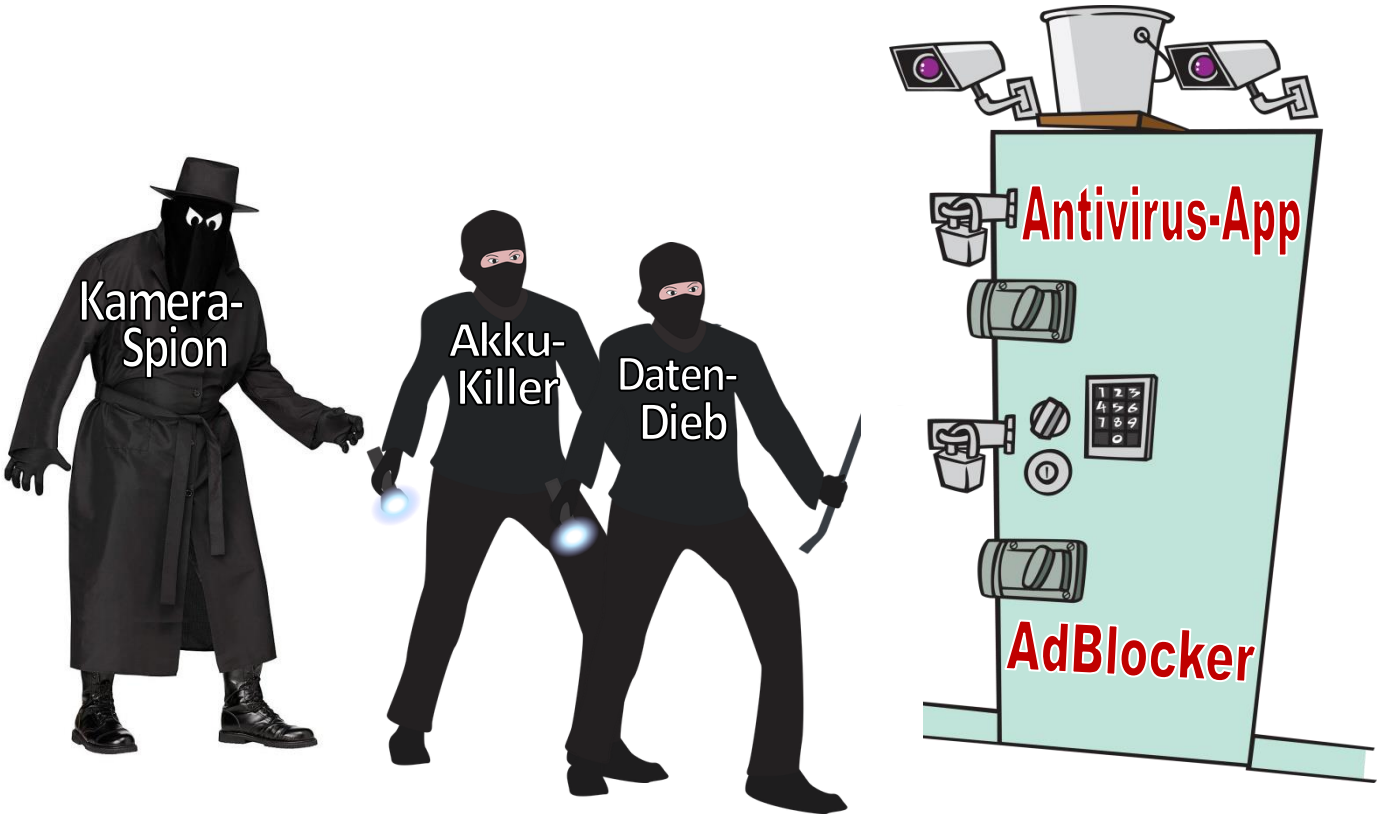
Inhaltsverzeichnis

1. Übersicht der Gefahren

Schütze dich vor Viren!

Computerviren sind so genannte Schadsoftware. Sie schleichen sich auf Computern und Smartphones ein, um es sich dort gemütlich zu machen und dir zu schaden:

- Viele Viren sind ferngesteuert: sie spionieren dich aus und klauen deine Daten.
- Sie können Daten löschen und Hardware zerstören: Dein Handyakku kann z.B. so stark überhitzen, bis er kaputt geht.
- Viren und andere Malware verbrauchen Platz: Deine Geräte werden langsamer.

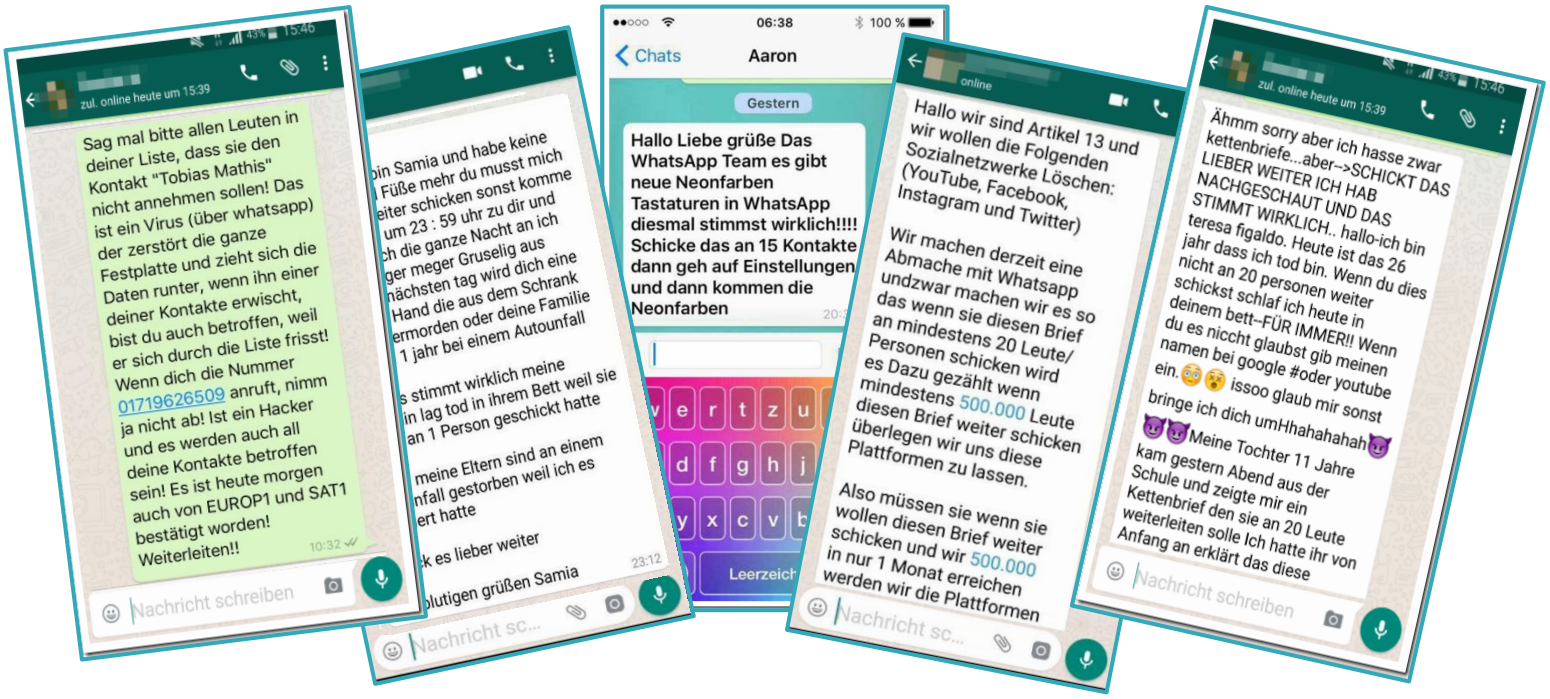


Installiere dir unbedingt eine Antivirus-App und einen AdBlocker!

Bitte nur EINE Antivirus-App installieren, denn sie bekämpfen sich gegenseitig!

YOUTH &ARTS WEB | SOCIAL NETWORK TRAINING

Kettenbriefe sind Lügengeschichten!

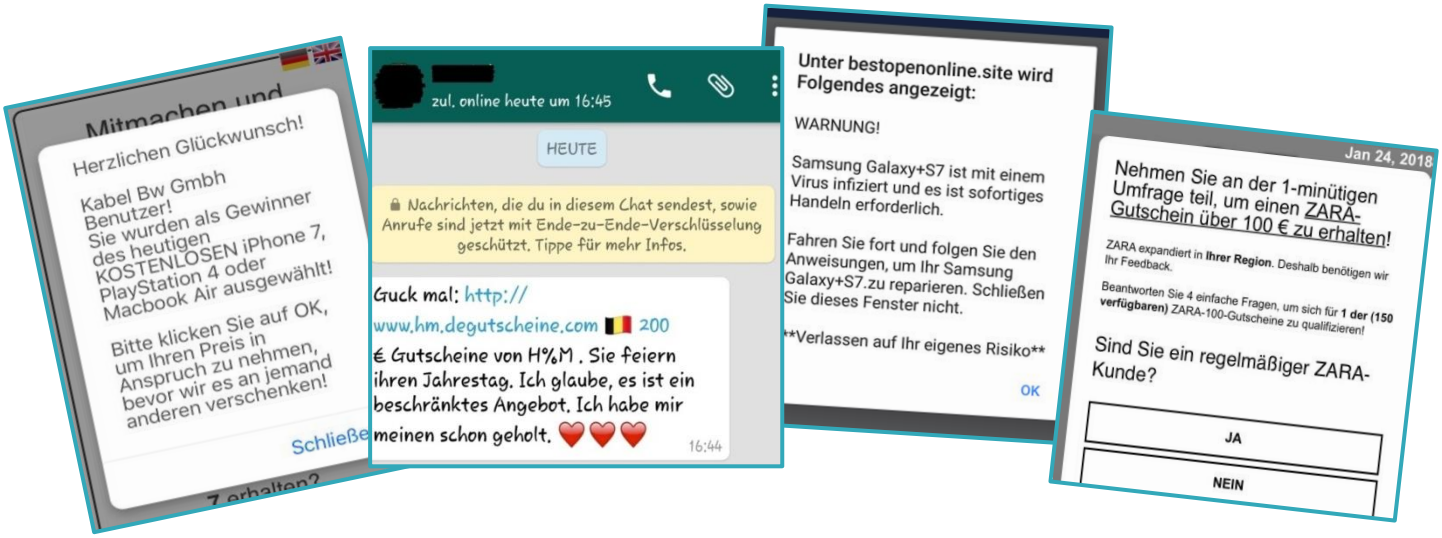


So genannte „Kettenbriefe“ sind Nachrichten, die Du an so viel Freunde wie möglich weiterschicken sollst. Manchmal versprechen sie coole Add-Ons, manchmal sollst Du kranken Kindern helfen, manchmal bedrohen sie Dich sogar. Egal was drin steht: Kettenbriefe sind erfunden, um damit Viren zu verbreiten.

Kettenbriefe niemals weiterleiten, sondern sofort löschen und den Absender informieren!

Kettenbriefe sind oft erfunden, um Viren zu verbreiten!

Nervig und gefährlich: Pop-Ups!



Ihr öffnet eine neue Seite im Netz und plötzlich blockiert ein neues Fenster den kompletten Bildschirm. Hauptgewinn, Gutscheine, Sonderangebote? Diese „Pop-Ups“ wollen, dass ihr auf einen Link klickt, meist läuft sogar ein Timer ab, damit ihr schnell und ohne nachzudenken eure Daten eingebt. Immer seid ihr die „Auserwählten“, und immer haben die Pop-Ups ähnliche Themen:

FAKE WERBUNG	Einkaufsgutscheine (oft auch über WhatsApp) von bekannten Firmen
FAKE VIRENWARNUNG	„Achtung, dein Handy ist infiziert!“
FAKE GEWINNSPIELE	„Herzlichen Glückwunsch, Sie haben gewonnen!“
FAKE UMFRAGEN	„Nehmen Sie an dieser Umfrage teil, um einen Gutschein zu erhalten“
FAKE CHALLENGES	„Ich fordere dich heraus: Poste das letzte Selfie aus deiner Gallerie!“

→ In Umfragen und Challenges werden Informationen über euch gesammelt

→ hinter den Links zu angeblichen Gewinnen und Sonderangeboten verstecken sich sehr oft Viren

→ Oft ist es ganz schön schwer, diese Fenster wieder zu schließen!

Fallt nicht auf Pop-Ups herein: keine Umfragen ausfüllen, keine Links zu Gewinnen oder Gutscheinen anklicken! Installiert euch eine Antivirus-App und einen AdBlocker!

Meistens sieht man schon am Link, dass es sich um einen Fake handelt. Seiten, die nicht mit *https* beginnen, unbedingt meiden!

Fake Videos und Fake Hacks verprechen viel und halten wenig!

Habt ihr schon mal so einen Link mit so einer ähnlichen Überschrift angeklickt?

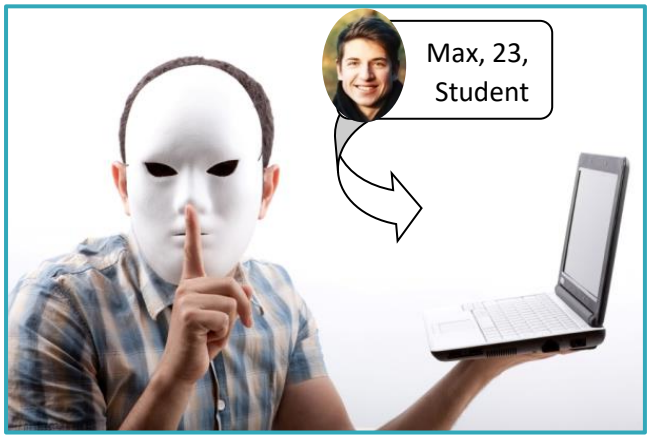
- „DU WIRST ES NICHT SCHAFFEN, NICHT ZU LACHEN!!!“
- „Ich dachte, es wäre alles nur fake. Aber dann war ich überrascht!“
- „OMG!! Diese 15 Dinge hast Du IMMER falsch benutzt!
- „10 Beauty-Tipps für eine schönere Haut, NUMMER 5 WIRD DICH SCHOCKIEREN!

Lasst euch nicht ködern! Manche Menschen, die Fotostrecken, Artikel oder Videos ins Netz stellen, verdienen durch Werbung viel Geld damit und wollen euch dazu kriegen, auf ihren Content zu klicken.

Vorsicht vor Clickbait-Videos und angeblichen Life-Hacks: Lass Dir Deine Zeit nicht klauen, damit andere Geld verdienen!

Achtung Fake Profile!

Was genau sind Fake-Profile? „Fake“ bedeutet Fälschung oder Täuschung, diese Profile sind also nicht „echt“. Der Name, die Fotos, das Alter und alle anderen Informationen darin sind meist frei erfunden. Anfang 2018 hat Facebook 580 Millionen Fake-Profile gelöscht, im Juli 2018 haben Forscher bei Instagram 95 Millionen gezählt.[1]



So erkennst Du Fake-Profile:

- Das Profil wurde erst vor Kurzem erstellt, hat kein Profilbild und ist wenig aktiv (wenig Posts).
- Die Person hat nur sehr wenige Freunde oder fast nur Freunde aus fernen Ländern.
- Bei Instagram haben Fake-Profile kaum oder gar keine eigenen Follower, folgen aber sehr vielen anderen.
- In Suchmaschinen gibt es die Möglichkeit der „Bilder-Suche“, dort könnt ihr checken, wo im Netz das Profilbild sonst noch auftaucht.

[1] Die Firma „Ghost Data“ hat diese Zahl im Juli 2018 auf der Nachrichtenseite „The Information“ veröffentlicht. https://goo.gl/RNwYpd (Stand: 18.10.2018).

Eine hohe Anzahl an Freunden und Followern zu haben ist also gar nicht mehr so cool, wenn man weiß, dass viele davon nicht „echt“ sind. Checkt genau, wer welche Infos von euch sehen kann!

Stellt euer Profil von „öffentlich“ auf „privat“. Fake Profile als Spam melden, löschen und blockieren.

Nehmt nur Freunde und Follower an, die ihr persönlich kennt.

2. Was verrätst Du dem Internet?

Deine Email-Adresse soll dich schützen, nicht verraten!

Lisa Rotenberg ist 14 Jahre alt, wohnt in Bonn und spielt Basketball. Ihre Eltern und Freunde nennen sie Lissy. Ihre ersten Ideen für ihre Email-Adresse sind:

lisa.rotenberg14@web.de ✗

Lisa_Bonn@web.de ✗

Beide Adressen verraten viel zu viele Informationen über Lisa! Besser sind folgende Beispiele:

lissy_jordan@web.de ✓

basketballgirl@web.de ✓

Dein Profil ist ein Tarnmantel!

Für euer Profil gilt dasselbe wie für eure Email-Adresse: verratet nicht zu viel über euch! Es geht niemanden etwas an, wie ihr ausseht, wo ihr wohnt und wann ihr geboren seid. Eure Freunde kennen euch persönlich und brauchen diese Infos nicht online zu sehen.

Name:	Lisa Rotenberg
Email-Adresse:	lisa.rotenberg14@web.de
Adresse:	Neue Strasse 20 53111 Bonn
Mobilnummer:	0176 12345678
Geburtstag:	15. Januar 2004
Hobbies:	Badminton, lesen

Name:	Lissy Jordan
Email-Adresse:	basketballgirl@web.de
Adresse:	
Telefonnummer:	
Geburtstag:	
Hobbies:	

Kostenlose Apps sind teuer

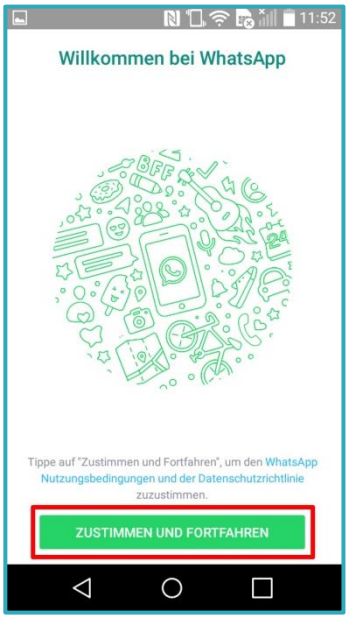
Habt ihr euch schon Mal gefragt, warum manche Apps Geld kosten, andere aber nicht? Ihr bezahlt dafür nicht mit Geld, sondern mit euren Daten.

Beispiel: WhatsApp darf...

- ...alle Bilder, Texte, Videos und Audiodateien **nutzen**, die ihr verschickt oder empfangt.
- ...eure Telefonnummer, Email-Adresse, Telefonnummern aus euren Kontakten und euer Profilbild **nutzen**.
- ...Nutzungsinformationen (wie oft und wie lange ihr WhatsApp benutzt) **abspeichern**.
- ...Informationen darüber **sammeln**, welches Smartphone-Modell ihr benutzt und welches Mobilfunknetz.
- ...eure Standortinformationen **abrufen.**

Aber wie machen diese Apps jetzt Geld damit? Sie verkaufen die gesammelten Daten weiter. Dürfen Die das? Ja, und ihr habt es sogar selbst erlaubt!

Nach dem Download von WhtasApp z.B. habt ihr den „Nutzungsbedingungen“ zugestimmt und damit einen Vertrag unterschrieben, mit nur einem Klick.



Alternative A:

Es gibt kostenpflichtige Alternativen zu WhatsApp, die aber eure privaten Daten schützen. Sie funktionieren genau gleich wie WhatsApp: z.B. Threema, Signal, SIMSme und noch viele andere.

Alternative B:

Es gibt leider immer noch viele Menschen, die nur WhatsApp nutzen. Wir empfehlen deswegen die 2-Geräte-Strategie:

UNTERWEGS

Auf dem Smartphone, auf dem private Dateien (Fotos, Videos, Kontakte...) und sensible Daten (Passwörter, Standort...) gespeichert sind, installiert ihr eine sichere App mit geprüften AGBs.

ZUHAUSE

Auf einem alten Gerät zuhause, auf dem vorher alle privaten Dateien gelöscht wurden, kann WhatsApp installiert werden.

Installiert euch eine sichere Messenger-App. Mit der 2-Geräte-Taktik bleibt ihr trotzdem mit allen in Kontakt!

Ungefähr dieselben Rechte haben andere kostenlose Apps wie z.B. Talking Tom, Talking Angela, Hay Day uvm.

Das Netz vergisst nichts!

- Alles, was ihr in sozialen Netzwerken hochladet oder verschickt, bleibt für immer gespeichert.
- Auch wenn ihr sie wieder löscht, können Fotos trotzdem weiterhin in Suchmaschinen auftauchen, oft noch Jahre später.
- Überlegt euch ganz genau, welche Fotos ihr mit anderen teilt. Würdet ihr diese Fotos auch auf Plakate drucken und in der Stadt verteilen?

Leider verschicken Mädchen und Jungs immer öfter intime Fotos von sich an ihren Schwarm. Diese Fotos können mit nur einem Kllick weitergeleitet werden. Viele Jugendliche haben sich im Anschluss so geschämt, dass sie nicht nur die Schule, sondern sogar den Wohnort wechseln mussten.

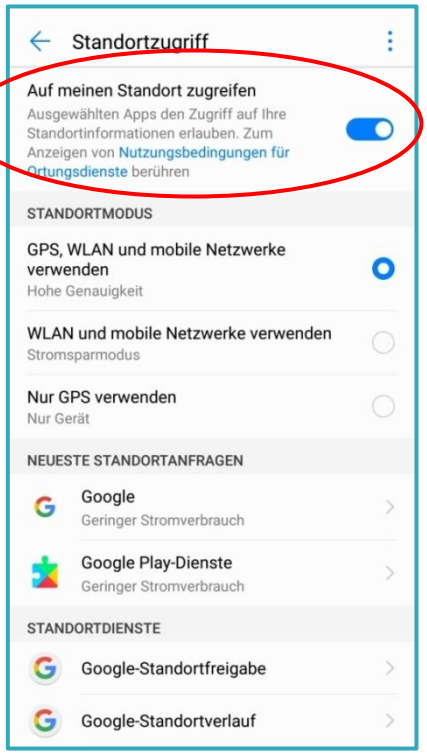
Überlegt euch gut, was ihr für die Ewigkeit mit der Welt teilen möchtet. Intime Fotos von einem selbst oder von anderen sollten niemals verschickt oder weitergeleitet werden!

3. Installationsanleitungen und Geräteeinstellungen

Macht euch unsichtbar!

Sind die Ortungsdienste auf eurem mobilen Gerät aktiviert, werden ständig Informationen darüber gesendet, wo ihr gerade seid:

- bei jedem Foto, das ihr macht, wird auch der Ort gespeichert
- bei jeder Suche auf einer Suchmaschine wird euer momentaner Aufenthaltsort gesendet



Bei **Android** findet ihr unter *Einstellungen* den Menüpunkt *Datenschutz und Sicherheit.* Hier wählt ihr die Option *Standortzugriff*, um Ortungsdienste zu deaktivieren oder bestimmten Apps den Zugriff zu erlauben.

Bei **iOS** findet ihr unter *Einstellungen* den Punkt *Datenschutz* – auch hier könnt ihr unter *Ortungsdienste* Standortinformationen generell deaktivieren oder für jede App individuell Einstellungen vornehmen.

Deaktiviert die Standortinformationen!

Nur das GPS zu deaktivieren reicht nicht, Standortinformationen werden auch über WLAN und mobile Daten gesendet.

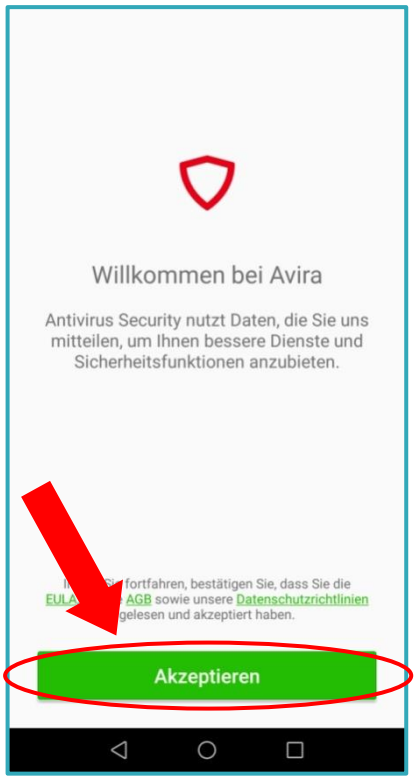
Die Sicherheitstür für's Smartphone: Antivirus-Apps

iPhones brauchen keine zusätzliche Antivirus-App. Für Android gibt es viele verschiedene kostenlose und kostenpflichtige Apps, kostenlose Varianten sind beispielsweise:

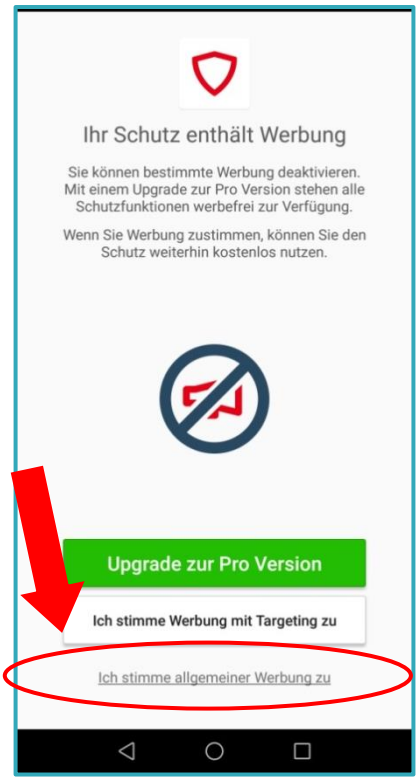
Avast Mobile Antivirus & Virenschutz 2019

Avira Antivirus Security 2019

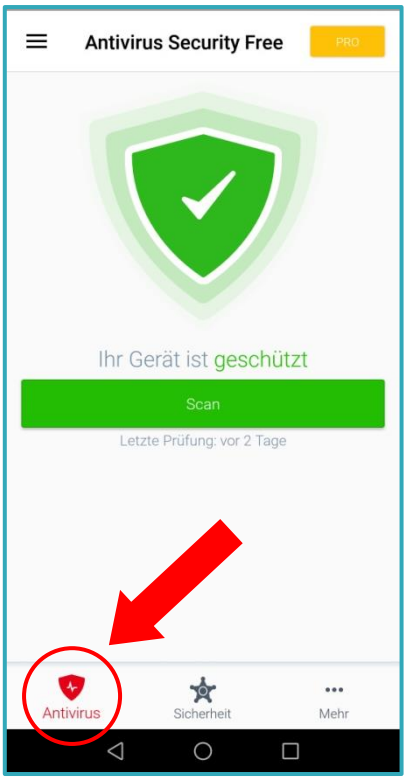
Diese beiden Programme bilden Platz 1 und 2 in den „Top 100 Antivirus-Downloads aller Zeiten" beim Computermagazin CHIP[2]. **Avira Antivirus Security** auf einem Android-Handy zu installieren sieht z.B. so aus:



① Zuerst die AGBs akzeptieren



② Dann allgemeiner Werbung zustimmen!



③ Ihr braucht nur den Button links unten.

Lasst euch nicht verwirren: Man braucht nur die Funktion „Antivirus", die bei Bild 3 eingekreist ist. Hier könnt ihr ab und zu euer Gerät scannen.

[2] http://www.chip.de/Downloads-Download-Charts-Top-100-aller-Zeiten_32417798.html?xbl_category=39008. Stand: 23.10.2018.

Der Türsteher für's Smartphone: AdBlocker

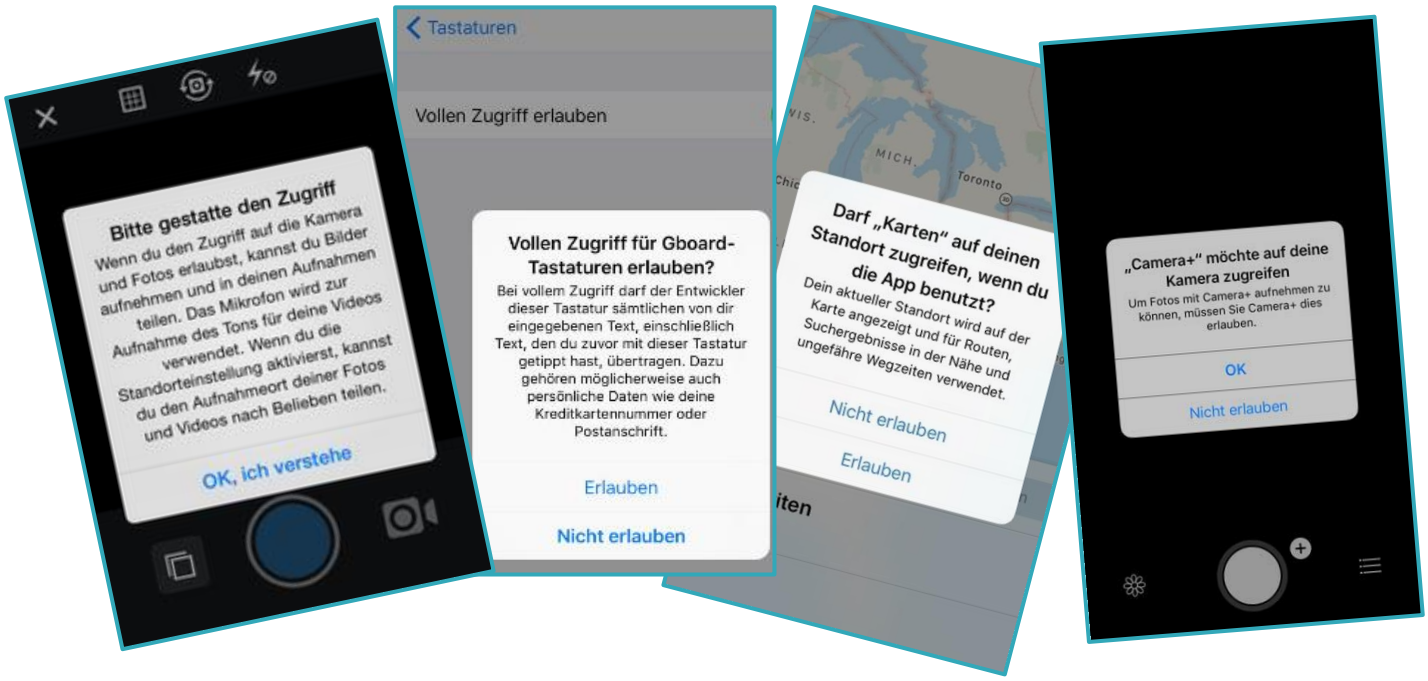
Ein so genannter AdBlocker hält einen Großteil nerviger Werbung und Pop-Ups von Dir fern. Auch hier gibt es einige kostenlose Varianten, z.B.

AdBlock Plus (iOS)

AdBlockBrowser (Android)

Zugriffsberechtigungen

Viele Apps wollen schon beim Installieren oder beim Öffnen Zugriff auf bestimmte Bereiche Deines Smartphones. Es hört sich immer so an, als muss die App das unbedingt tun, damit sie richtig funktioniert:



Erlaubt euren Apps nicht automatisch Zugriff auf euren Standort, eure Fotos oder Kontakte! Unter *Einstellungen* könnt ihr für jede App die Zugriffsrechte anpassen.

Benutzt euren Kopf: braucht eine Kamera-App euren Standort? Braucht ein Spiel Zugriff auf eure Kamera? Wieso interessieren Google eure Kontakte?

4. Was heißt wirklich cool?

So etwas passiert ganz schnell: In der WhatsApp-Gruppe eurer Klasse hat jemand einen Witz über einen Mitschüler gemacht. Die anderen sind miteingestiegen und er oder sie hat einen richtigen Shitstorm abbekommen. Auch am nächsten Tag in der Klasse machen viele noch Witze über ihn oder sie. Was könnt ihr tun?

SEID KEINE....

...Hater: Nicht drauftreten!
...Mitläufer: Nicht mitlachen!
...Feiglinge: Nicht wegschauen!

SONDERN: **Seid cool, seid mutig, helft!**

Cool ist, wer sich für andere einsetzt! Erinnert eure Klasse daran, dass ihr eine gute Klassengemeinschaft sein wollt, in der alle dazu gehören.

5. Tipps für Eltern

Hintergründe

Die Nutzung von Smartphones beginnt heute in der Regel mit dem Übergang in die weiterführenden Schulen, immer häufiger schon davor. Ohne Anleitung entstehen erste Schäden meist sofort mit Beginn der Nutzung, vor allem in Bezug auf:

- Umgang mit sensiblen persönlichen Daten
- Preisgabe von kritischen Inhalten wie Fotos und Videos
- Viren, Schadsoftware und fehlenden Kenntnissen über die Standardeinstellungen
- negative soziale Erfahrungen in der Gruppe

Nachfolgend haben wir einige Tipps zusammengestellt, wie Sie als Eltern Ihre Kinder im Umgang mit den Neuen Medien unterstützen und voneinander lernen können.

Virenschutz & AdBlocker

Viren können nicht nur großen Schaden am Gerät anrichten sondern auch alle möglichen Daten ausspionieren. Installieren Sie deshalb unbedingt eine Antivirus-App. Es gibt eine Vielzahl an kostenlosen und kostenpflichtigen Apps für Android. Eine beispielhafte Installationsanleitung finden Sie weiter vorn in der Broschüre. Es lohnt sich, darüber nachzudenken, eine kostenpflichtige App zu installieren: diese sind werbefrei. Für iPhones gibt es keine Antivirus-Apps, da sie ein eigenes Schutzsystem integriert haben.

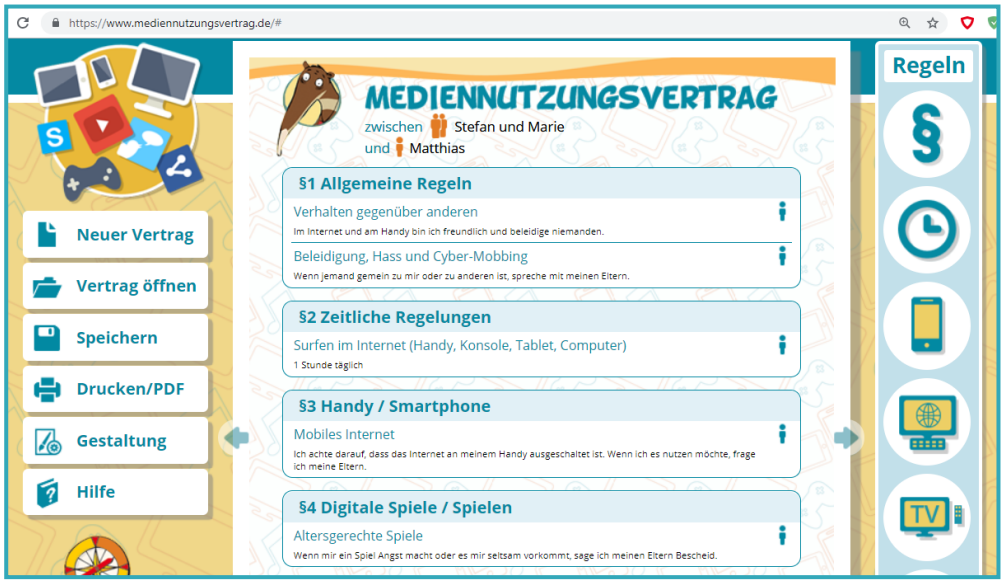
Nutzungsgewohnheiten

Erwachsene können Jugendliche wesentlich darin bestärken, verantwortungsbewusst im Netz zu handeln. Sie wiederum können von Ihren Kindern viel über den Umgang mit sozialen Netzwerken lernen: Unterstützen Sie Ihr Kind darin, sich zu informieren und Angebote gezielt auszuwählen. Lassen Sie sich das aktuelle Lieblingsspiel zeigen! Kinder genießen es meistens, wenn sie Erwachsenen etwas vorführen können und Sie können besser nachvollziehen, was Ihr Kind besonders mag. Haben Sie keine Angst vor der Expertise Ihres Kindes!

Bleiben Sie im Austausch mit den Eltern der anderen Kinder, mit den Klassenlehrern und vor allem mit Ihren Kindern. Schaffen Sie eine Vertrauensbasis, so dass Ihr Kind sich nicht schämt und keine Strafe fürchtet, wenn es sich Ihnen bspw. zum Thema Cybermobbing anvertrauen möchte.

Vereinbaren Sie Regeln zur Nutzung des Internets:

Sie können hierfür das Angebot der EU-Initiative klicksafe.de nutzen: Über ein Baukastensystem kann hier ein altersgerechter und für die jeweilige Familie passender Vertrag erstellt werden. Vorbereitete Regeln für die Altersgruppen 6–12 Jahre und für über 12-Jährige erleichtern die Erstellung: www.mediennutzungsvertrag.de



Zwei Regeln jedoch sollten auch ohne Vertrag unbedingt beachtet werden:

1. ***Intime Fotos von einem selbst oder von anderen dürfen niemals verschickt oder weitergeleitet werden!***

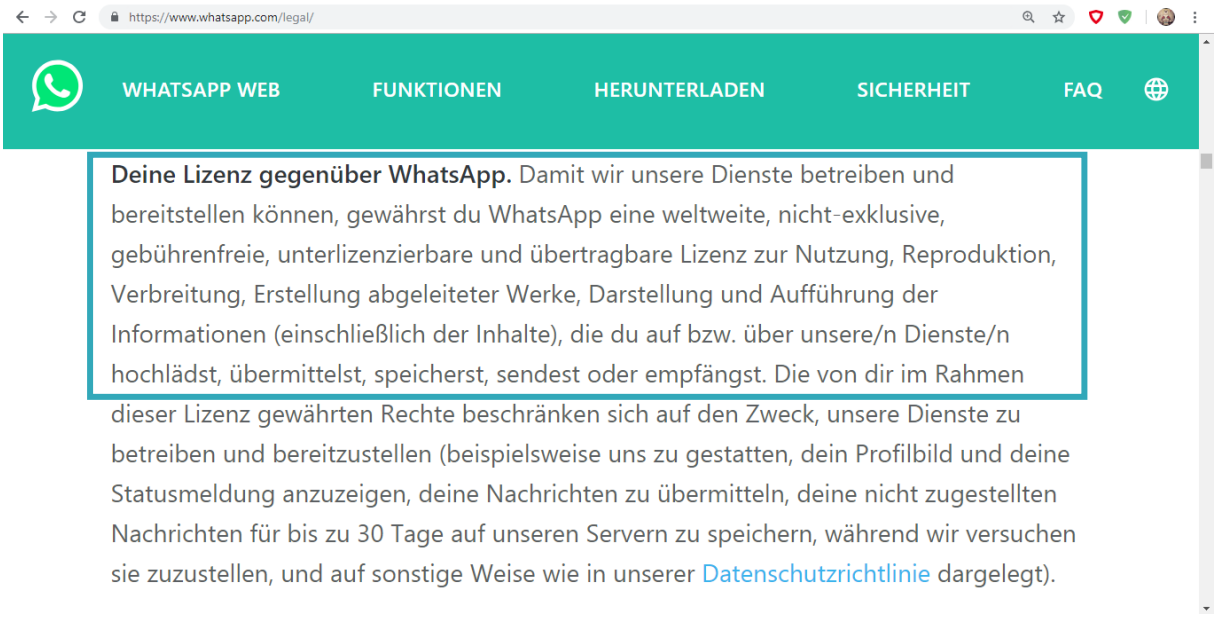
   Leider verschicken Mädchen und Jungs immer öfter und immer früher intime Fotos von sich selbst an ihren Schwarm. Dass diese Fotos dann weitergeleitet werden, belastet die Betroffenen oft jahrelang, viele wechseln sogar Schule und Wohnort. Klären Sie Ihr Kind darüber auf und besprechen Sie mit ihm, was es tun kann, wenn von einem Mitschüler solche Fotos auftauchen: nicht lachen, sondern helfen!

2. Sich für andere einsetzen, die gemobbt werden!

In WhatsApp-Gruppen und anderen sozialen Netzwerken schlägt ein flapsiger schnell in einen beleidigenden Kommentar um und durch die Gruppendynamik schaukelt sich die Stimmung hoch. Ermutigen Sie Ihr Kind dazu, bei solchen Beleidigungs-Fluten nicht mitzumachen, sondern die anderen dazu aufzufordern, damit aufzuhören. Generell gilt es, so gut es geht darauf zu achten, welchen Umgangston ihr Kind in sozialen Netzwerken pflegt und welchem es ausgesetzt ist. Wenn jemand gemobbt wird reicht es nicht aus, nicht mitzumachen – am wirkungsvollsten ist es als Gruppe hinter dem Opfer zu stehen.

WhatsApp & Co

Kostenlose Apps bezahlt man meist mit seinen Daten. WhatsApp, Instagram und Co. haben in ihren AGBs genau festgelegt, welche Rechte die Programme an den Daten ihrer Nutzer haben. In den Nutzungsbedingungen von WhatsApp beispielsweise findet man folgende Informationen[3]:



Dieser Satz bedeutet im Prinzip, dass WhatsApp alles, was man dort hochlädt, (Bilder, Texte, Videos oder Audiodateien) nutzen darf, und zwar ganz offiziell mit der Erlaubnis des Nutzers.

Es gibt kostenpflichtige Alternativen zu WhatsApp, die aber garantieren, alle privaten Daten zu schützen. Sie funktionieren fast genau gleich wie WhatsApp und bieten dieselben Möglichkeiten. Überlegen Sie mit anderen Eltern und dem Klassenlehrer, ob die gesamte Klasse für den Klassenchat zu einem der folgenden Dienste wechselt:

Threema **Signal** **SimsMe**

Beachten Sie hierzu auch die „2-Geräte-Strategie“ in dieser Broschüre!

[3] In: www.whatsapp.com/legal, Nutzungsbedingungen, Absatz „Lizenzen“. Stand: 18.10.2018.

Weiterführende Informationen:

Noch mehr Informationen zum Thema finden Sie auf den folgenden Internetseiten:

http://www.klicksafe.de:	Umfassende Infos für Eltern zu sozialen Medien, inkl., App-Tipps, Datenschutz, Möglichkeiten der Kindersicherung, Flyer-Download uvm.
http://www.mimikama.at:	Hier werden Infos über Internetmissbrauch, Internetbetrug (auch Kettenbriefe) und über aktuelle Falschmeldungen bzw. Fakes gesammelt
http://www.elternguide.online:	Unterstützung bei der Medienerziehung, Infos zur Bedeutung von Medien in unterschiedlichen Lebensaltern, Beratung bei Fragen.
http://www.handysektor.de:	Website für Jugendliche rund ums Thema Smartphone, z.B. aktuelle Apps, Reparaturanleitung, Artikeln über Lifestyle-Themen und Phänomenen wie Influencern.
http://www.schau-hin.info:	Infos zu den Themen Surfen, Chatten, Hören (Podcasts), Spielen, Schauen (Streaming) sowie Artikel zu Cybermobbing und einem „Elterntest“.