

# **Cyberstalking & Digitale Selbstverteidigung**

*Effektiv und selbstbewusst digitale  
Sicherheit stärken*

v1.1

Yvette Muszynski <yvette@srlabs.de>  
Nina Piontek <nina@srlabs.de>



**Security  
Research  
Labs**

**Stand:** 26.02.2024

**Version:** v1.1

**Hinweis:** Diese Datei wird unregelmäßig aktualisiert.

Die aktuelle Version findest du unter

<https://raw.githubusercontent.com/srlabs/resources/main/antistalking-guidelines-de.pdf>

# Baue dir deine Festung - Mit ein paar Schritten zu 1A Sicherheit

Stufe 1 - Grundsicherung	Stufe 2 - Kontrolle	Stufe 3 - Beständigkeit
Wenig Aufwand, große Wirkung	Ergänzende Maßnahmen	Für die extra Sicherheit
<div>A1</div> Passwörter ändern	<div>A2</div> MFA	<div>A3</div> Passwort-Manager einrichten
<div>B1</div> Laufende Sitzungen beenden	<div>B2</div> Chronik und Browserdaten löschen	<div>B3</div> Browser sicher einstellen
<div>C1</div> Google/Apple Konto Zugriffe verwalten	<div>C2</div> Kontos aufräumen und Datensammeln limitieren	<div>C3</div> Social-Media Privacy-Einstellungen
<div>D1</div> Smartphone Zugang absichern	<div>D2</div> Smartphone aufräumen	<div>D3</div> Smartphone zurücksetzen
<div>E1</div> Telefonnummern blockieren	<div>E2</div> Nutzer blockieren	
<div>F1</div> Backups machen		

## Das sind wir



**Nina Piontek**  
 Security Consultant


[nina@srlabs.de](mailto:nina@srlabs.de)



**Yvette Muszynski**  
 Security Consultant


[yvette@srlabs.de](mailto:yvette@srlabs.de)  

[@iyskierka@23.social](https://www.instagram.com/iyskierka)

## A: Zugriff schützen

- A1 Passwörter ändern ..... 6
- A2 MFA ..... 8
- A3 Passwort-Manager einrichten..... 8

## B: Private Geräte und Browser

- B1 Laufende Sitzungen beenden
  - Messenger - Angemeldete Geräte entfernen ..... 9
  - Browser - Sitzungen löschen..... 10
- B2 Chronik und Browserdaten löschen ..... 10
- B3 Browser sicher einstellen
  - Browserdaten automatisch löschen ..... 11
  - Privater Modus ..... 11

## C: Cloud Konto absichern

- C1 Cloud Konto Zugriffe verwalten
  - Unerwünschte Personen aus dem Konto schmeißen ..... 12
  - Standort teilen Funktion kontrollieren ..... 13
- C2 Kontos aufräumen und Datensammeln limitieren
  - Google das Datensammeln verbieten ..... 14
  - Google Standortfreigabe unterbinden ..... 15
  - Standortdaten aus iCloud entfernen ..... 15
- C3 Privacy Einstellungen
  - Goldene Regeln ..... 16
  - Metadaten entfernen ..... 16
  - WhatsApp Privacy-Einstellungen vornehmen ..... 17
  - Instagram Privacy-Einstellungen vornehmen ..... 18

## D: Smartphone schützen

- D1** Smartphone Zugang absichern
  - Sicheren PIN code ..... 19
  - SIM-Karten sperre ..... 19
- D2** Smartphone aufräumen
  - App-Berechtigungen verwalten ..... 20
  - Unerwünschte Apps deinstallieren ..... 20
- D3** Smartphone zurücksetzen
  - Einen Jailbreak erkennen ..... 21
  - Zurück auf Werkseinstellungen ..... 21

## E: Belästigung unterbinden

- E1** Anrufe blockieren
  - Eine Rufnummer blockieren ..... 22
  - Unbekannte Anrufe blockieren ..... 22
- E2** Nutzer blockieren
  - WhatsApp Anrufer stummschalten ..... 23
  - Social-Media Accounts blockieren ..... 23

## F: Daten sichern

- F1** Daten sichern
  - Ein Backup deines Smartphones und automatische Backups einrichten ..... 24
  - Ein Backup deines Laptops machen..... 25

## Extrkapitel

- Sind Informationen von mir online? ..... 26
- War da jemand an meinem Laptop? ..... 26

# A1 Passwörter ändern

## Wann:

- ✓ Die Person hatte in der Vergangenheit dein Passwort
- ✓ Du befürchtest die Person hat Zugriff auf deine Konten

## Warum:

- ✓ Durch das ändern des Passwortes kann sich niemand mehr in deinen Account einloggen – außer dir

## Schritt 1: Dein Mail-Account



### Mail

1. Logge dich in deinem Mail-Account ein
2. In den **Einstellungen des Accounts** findest du die Funktion **Passwort ändern**
3. Für iCloud Mails, ändere das iCloud-Account Passwort
4. Tue dies für alle Mail-Accounts, die du aktiv nutzt und welche als Login für andere Accounts hinterlegt sind

Es ist wichtig mit dem Mail Account anzufangen, da die meisten Online Accounts eine Funktion zum Zurücksetzen des Passworts haben, welche das neue Passwort an deine Mail Adresse schickt.

## Schritt 2: Cloud-Accounts



### Apple

Auf deinem Smartphone, gehe zu:

1. **Einstellungen > [Dein Name] > Anmeldung & Sicherheit.**
2. Tippe auf **Passwort ändern**
3. Gib dein bisheriges **Passwort** oder den Gerätecode ein
4. Tippe auf **Ändern** oder **Passwort ändern**

### G Google

Auf deinem Smartphone, gehe zu:

1. **Einstellungen** und tippe auf **Google > Google-Konto verwalten > Sicherheit**
2. Tippe unter **Bei Google anmelden** auf **Passwort** und melde dich neu an
3. Geben das neue **Passwort** ein und tippe auf **Passwort ändern**

## Schritt 3: Alles andere



### Social-Media und der Rest

Logge dich nun in **alle anderen wichtigen Accounts** ein und **ändere die Passwörter**. Es ist sinnvoll, eine **Liste anzufertigen** und diese nach und nach abzuarbeiten. Zum Beispiel so::

- Facebook
- Instagram
- Twitter
- Amazon
- ...

# A1) Passwörter ändern – aber wie wird es sicher?

## Wann:

- ✓ Sichere Passwörter sollten immer gesetzt werden

## Warum:

- ✓ Ein sicheres Passwort garantiert, dass niemand das Schloss an deinem Account knacken kann

**Nutze für jeden Login ein eigenes Passwort.** Egal wie sicher dein Passwort ist, Wiederverwendung kann alle Sicherheitsvorkehrungen aushebeln.

### Je komplexer und länger, desto besser!

Mehr als 8 Zeichen, Zahlen, Symbole sowie Groß- und Kleinbuchstaben

### Keine Klassiker nutzen!

„123456“, „Passw0rt!“ und „qwertz“ sind No-Gos

### Keine Inhalte aus deinem Leben!

Benutzername, Name des Haustiers oder Geburtstag sind einfach zu raten

**Vergesst den Term „Passwort“ – es sollte „Passphrase“ oder „Passsatz“ heißen!**

Länge trumpft Komplexität – wähle lieber ein langes Passwort statt eines mit vielen Sonderzeichen. Am einfachsten machst du dein Passwort sicher, wenn du ein möglichst langes Wählst! Nutze dazu zum Beispiel diese Techniken:

## A: Nimm etwas aus dem Umfeld

Schau dich einmal im Raum um, in dem du bist: Steht irgendwo ein Text oder Satz, der gut einzuprägen ist? Nimm diesen als Passwortsatz, zum Beispiel: **24/7-rund-um-die-Uhr**  
Verbinde die Wörter mit einem Leerzeichen oder einem Sonderzeichen deiner Wahl.

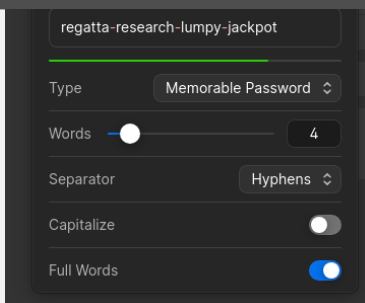
## B: Passsätze würfeln

Mithilfe einer Wortliste und einem Würfel generierst du eine zufällige Passphrase bestehend aus mehreren Wörtern, zum Beispiel: **merken-boom-ragt-hurra**

Die Bedeutung der Wörter sollte bekannt sein und mit Hilfe einer Eselsbrücke fällt das merken einfach. Eine ausführliche Anleitung gibt es im Anhang (Seite 27)

## C: Der Passwort-Manager macht die ganze Arbeit

Wenn du einen Passwort-Manager nutzt (siehe A3) übernimmt dieser die ganze Arbeit für dich. Du kannst automatisch ein langes, sicheres Passwort generieren lassen. Der zusätzliche Vorteil des Passwort-Managers: Das merken übernimmt er auch!



regatta-research-lumpy-jackpot

Type: Memorable Password

Words: 4

Separator: Hyphens

Capitalize: ☐

Full Words: ☒

## A2 Multi-Faktor Authentifizierung einrichten

### Wann:

- ✓ Du willst sicher sein, dass sich niemand ohne deine Bestätigung in dein Konto einloggen kann

### Warum:

- ✓ Durch die zweite Abfrage auf deinem Smartphone ist kein Login ohne Bestätigung möglich

Die Einstellung kann in verschiedenen Online-Accounts unterschiedlich zu finden sein, meist jedoch findet sie sich so:

- **Einstellungen > Passwort und Sicherheit > Zwei-Faktor-Authentifizierung**

oder

- **Einstellungen > Sicherheit > Multi-Faktor-Authentifizierung**

**Apple und Google** nutzen schon ohne, dass du etwas machen musst, **dein Gerät als zweiten Faktor**. Es wird ein 6-stelliger Code an dein Gerät / eine Google-App geschickt, wenn du dich versuchst einzuloggen.

## A3 Passwort-Manager einrichten

### Wann:

- ✓ Du magst Passwörter nicht und möchtest dir am liebsten nur ein einziges Merken

### Warum:

- ✓ Mit einem Passwort-Manager können komplexere Passwörter mit weniger Aufwand verwaltet werden

Jeder Passwort-Manager ist besser als keiner. **Wähle den, der deine Geräte gut und bequem unterstützt.** Die meisten Browser bieten auch Erweiterungen an, mit welchen die Passwörter bequem im Browser ausgefüllt werden können. Die Anleitung findest du auf der jeweiligen Website.

Auch **iCloud Schlüsselbund** und **Google Passwort-Manager** kommen hier in Frage!

Wichtig ist, dass der Passwort-Manager mit einer zusätzlichen, einzigartigen und langen Passphrase geschützt ist.

Beliebte Beispiele:



1Password



KeePassXC



Bitwarden

„Mit Google anmelden“ ist zwar eine praktische Funktion (Single-Sign-On), die Nutzung führt jedoch dazu, dass eine Anwendung der Schlüssel für alle anderen wird!



# **B1** Laufende Sitzungen beenden: Messenger - angemeldete Geräte entfernen

## ▶ Wann:

- ✓ Du hast das Gefühl, jemand liest deine online Gespräche mit

## ▶ Warum:

- ✓ Messenger Apps erlauben mehrere aktive Sitzungen auf verschiedenen Geräten gleichzeitig. Dadurch könnte eine Person deine Chats mitlesen.

### WhatsApp

*In WhatsApp, gehe zu:*

1. **Einstellungen > Verknüpfte Geräte**
2. Tippe auf die jeweiligen Geräte und klicke auf **Abmelden**

### Telegram

*In Telegram, gehe zu:*

1. **Einstellungen > Geräte**
2. Tippe unter deinem Gerät auf **Alle anderen Sitzungen beenden**

### Signal

*In Signal, gehe zu:*

1. Tippe auf **dein Profil > Gekoppelte Geräte**
2. Tippe auf die jeweiligen Geräte und klicke auf **Verknüpfung aufheben**

### Facebook Messenger

*In der Facebook App, gehe zu:*

1. **Einstellungen und Privatsphäre > Einstellungen > Sicherheit und Login > Wo du derzeit angemeldet bist**
2. Tippe auf die **drei Punkte** neben der Sitzung und dann auf **Abmelden**

## B1 Laufende Sitzungen beenden: Browser - Sitzungen löschen

### ► Wann:

- ✓ Du hast das Gefühl, jemand liest deine online Gespräche mit UND
- ✓ Jemand hat Zugriff auf deinen Laptop

### ► Warum:

- ✓ Messenger Apps erlauben lange aktive Sitzungen im Browser. Dadurch könnte jemand deine Chats ausspähen.

#### Firefox

1. **Einstellungen > Datenschutz und Sicherheit > Cookies und Website-Daten**
2. Klicke auf **Daten entfernen ...**
3. Setze alle Häkchen und klicke auf **Leeren**

#### Edge

1. **Einstellungen > Datenschutz, Suche und Dienste**
2. **Browserdaten löschen**
3. Wähle **Cookies und andere Websitedaten** und **gesamten Zeitraum** aus > **Löschen**

#### Google Chrome

1. **Einstellungen > Datenschutz und Sicherheit > Drittanbieter-Cookies**
2. **Alle Websitedaten und -Berechtigungen ansehen > Alle Daten löschen**

#### Safari

1. **Safari > Einstellungen > Datenschutz**
2. Klicke auf **Website-Daten verwalten > Alle Entfernen > Jetzt entfernen**

## B2 Chronik und Browserdaten löschen

### ► Wann:

- ✓ Jemand hat Zugriff auf deinen Laptop

### ► Warum:

- ✓ Der Browser merkt sich besuchte Seiten und den Login, lösche diese regelmäßig

#### Firefox

1. **Menü > Chronik > Neuste Chronik löschen**
2. Wähle die Zeitspanne **Alles** aus und klicke alle Häkchen an
3. Klicke auf **Jetzt löschen**

#### Edge

1. **Einstellungen > Datenschutz, Suche und Dienste > Browserdaten löschen > Browserdaten jetzt löschen**
2. Wähle den **gesamten Zeitbereich** und **alle Browsing-Daten** aus > **Jetzt löschen**

#### Google Chrome

1. **Menü > Verlauf > Verlauf**
2. Klicke auf **Browserdaten löschen**
3. Wähle den **gesamten Zeitraum** und **alle Daten** zum Löschen aus
4. Klicke auf **Daten löschen**

#### Safari

1. **Safari > Verlauf > Verlauf löschen**  
Und anschließend:
2. **Safari > Einstellungen > Datenschutz**
3. Klicke auf **Website-Daten verwalten > Alle Entfernen > Jetzt entfernen**

## B3 Browser sicher einstellen: Browserdaten automatisch löschen

### Wann:

- ✓ Wenn du dir nicht jedes Mal selbst die Arbeit machen möchtest, die Daten manuell zu löschen

### Warum:

- ✓ Mit diesen Einstellungen werden alle beim Schließen des Browsers alle Browserdaten automatisch gelöscht

### Firefox

1. **Einstellungen > Datenschutz und Sicherheit > Chronik**
2. Setze das Häkchen bei **Die Chronik löschen, wenn Firefox geschlossen wird**
3. Rechts in den **Einstellungen**, wähle alle Häkchen an
4. Bestätige mit **OK**

### Edge

1. **Einstellungen > Datenschutz, Suche und Dienste**
2. **Browserdaten löschen**
3. Wähle die Option **Auswählen, was bei jedem Schließen des Browsers gelöscht werden soll**
4. Setze alle Schalter auf **Ein**

### Google Chrome

Chrome bietet keine Option an automatisch beim Schließen des Browsers Daten zu löschen. Nur Daten aus Inkognito-Fenstern werden nicht gespeichert.

### Safari

Auch Safari bietet keine Option an automatisch beim Schließen des Browsers Daten zu löschen. Nur Daten aus privaten Fenstern werden nicht gespeichert.

---

## B3 Browser sicher einstellen: Privater Modus

### Wann:

- ✓ Wenn du dir nicht selbst die Arbeit machen möchtest, die Daten manuell zu löschen

### Warum:

- ✓ Es werden keine Sitzungen oder sonstige Browserdaten gespeichert und automatisch gelöscht, wenn du den Browser schließt

### Firefox

**Menü (oben rechts)**  
> **Neues privates Fenster**

### Edge

**Menü (oben rechts)**  
> **Neues InPrivate-Fenster**

### Google Chrome

**Menü (oben rechts)**  
> **Neues Inkognitofenster**

### Safari

**Ablage > Neues privates Fenster**

# c1 Zugriffe verwalten: Unerwünschte Personen aus dem Konto schmeißen

<b>Wann:</b> <ul style="list-style-type: none"><li>✓ Wenn du das Gefühl hast, dass jemand viel über dein Leben weiß</li></ul>	<b>Warum:</b> <ul style="list-style-type: none"><li>✓ Dein Cloud-Konto kann ein Sammelpunkt für viele deiner persönlichen Daten sein: Fotos, Dokumente, Passworte &amp; Standortinfos</li></ul>
---	---

 <b>Android</b>	 <b>iPhone</b>
--	---

## Schritt 1: Account Passwort ändern

<ol style="list-style-type: none"><li>1. <b>Einstellungen &gt; Google &gt; Google-Konto verwalten</b></li><li>2. Klick auf <b>Sicherheit &gt; Passwort</b></li><li>3. Wähle ein neues, starkes Passwort [3]</li></ol>	<ol style="list-style-type: none"><li>1. <b>Einstellungen &gt; [Dein Name] &gt; Anmeldung &amp; Sicherheit</b></li><li>2. Klicke auf <b>Passwort ändern</b></li><li>3. Wähle ein neues, starkes Passwort [3]</li></ol>
---	--

## Schritt 2: Eingeloggte Geräte prüfen

<ol style="list-style-type: none"><li>1. <b>Einstellungen &gt; Google &gt; Google-Konto verwalten</b></li><li>2. Klick auf <b>Sicherheit</b></li><li>3. Scrolle nach unten zur Liste <b>eingeloggter Geräte</b></li><li>4. Kennst du die Geräte? Falls nein: Logge dich aus</li></ol>	<ol style="list-style-type: none"><li>1. <b>Einstellungen &gt; [Dein Name]</b></li><li>2. Scrolle hinunter zur Liste aller eingeloggten Geräte</li><li>3. Entferne alle unbekannten Geräte, in dem du sie anklickst und anschließend auf <b>Aus dem Account entfernen</b> klickst</li></ol>
---	---

## Schritt 3: Wiederherstellungsemail prüfen

<ol style="list-style-type: none"><li>1. <b>Einstellungen &gt; Google &gt; Google-Konto verwalten</b></li><li>2. Click auf <b>Sicherheit &gt; Wiederherstellungsemail</b></li><li>3. Stelle sicher, dass dies deine eigene E-Mail-Adresse ist. Ändere auch für diese E-Mail-Adresse das Passwort.</li></ol>	<ol style="list-style-type: none"><li>1. <b>Einstellungen &gt; [Dein Name] &gt; Anmeldung &amp; Sicherheit</b></li><li>2. Unter E-Mail und Telefonnummern, klicke auf <b>Bearbeiten</b></li><li>3. Entferne E-Mails und Telefonnummern, die veraltet oder nicht deine sind</li></ol>
---	--

# c1 Zugriffe verwalten: Standort teilen Funktion kontrollieren

## Wann:

- ✓ Wenn du das Teilen deines Live-Standorts beenden möchtest

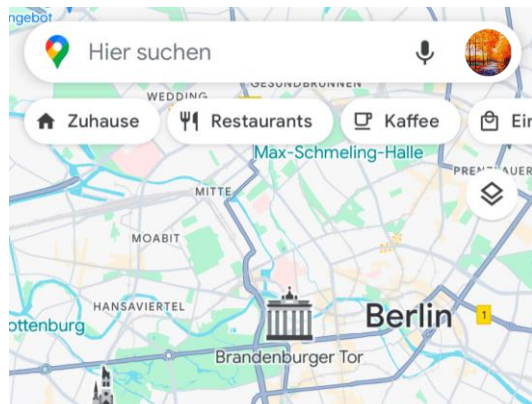
## Warum:

- ✓ Es ist wichtig Einsicht zu haben, mit wem der Standort geteilt wird

### Android

Gehe zu:

1. Öffne **Google Maps**
2. Klicke auf dein Profilbild und wähle **Standortfreigabe**
3. Du siehst eine Liste von Personen, mit denen dein Standort geteilt wird
4. Wähle **Beenden** neben den Namen der Personen, die deinen Standort nicht mehr sehen sollen



**Max Mustermann**

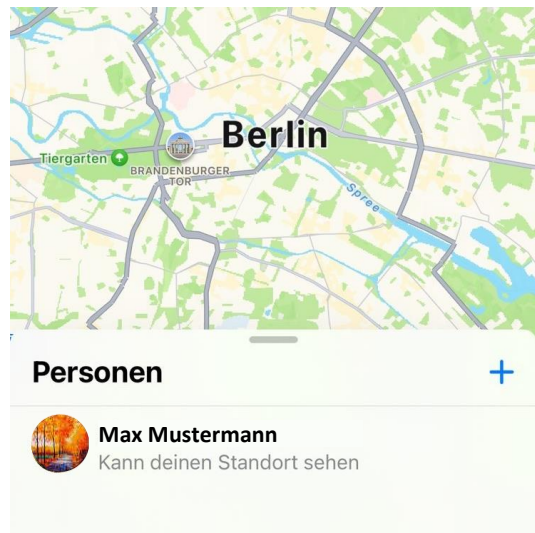
Kann deinen Standort sehen  
für 1 Stunde

 Beenden

### iPhone

Gehe zu:

1. Öffne die **Wo ist? App**
2. Unter **Personen** findest du alle Menschen, die deinen Live-Standort sehen können
3. Entferne unerwünschte Personen



**Personen**



**Max Mustermann**

Kann deinen Standort sehen

## c2 Cloud Konto aufräumen: Standortdaten Speicherung einschränken



### ▶ Wann:

- ✓ Wenn du das Sammeln deiner Standortdaten in deinem Google-Konto minimieren möchtest

### ▶ Warum:

- ✓ Vorsorge. Wenn keine Daten vorhanden sind, dann kann auch keiner sie sehen

### ▶ Schritt 1: Standortverlauf/Timeline ausschalten

1. Gehe zu <https://myactivity.google.com> und logge dich mit deinem Google-Konto ein
2. Wähle **Standortverlauf** > **Deaktivieren**; hier kannst du ebenfalls deine bisherige Standorthistorie löschen

### ▶ Schritt 2: Web- & App-Aktivitäten ausschalten

1. Gehe zu <https://myactivity.google.com> und logge dich mit deinem Google-Konto ein
2. Wähle **Web- & App-Aktivitäten** > **Deaktivieren und Aktivitäten löschen**; hier kannst du auch bisherige Aktivitäten löschen

### ▶ Schritt 3: Mein Gerät Finden deaktivieren

1. Smartphone **Einstellungen** > **Mein Gerät finden** > **Deaktivieren**
2. Jetzt kann dein Gerät nicht mehr über <https://www.google.com/android/find> geortet werden

▶ **Tip: Direkt eingegebene Webadressen werden nicht im Verlauf gespeichert!**



## c2 Cloud Konto aufräumen: Google Standortfreigabe unterbinden



Die Standortfreigabe kann nur von deinem Smartphone aus freigegeben werden.

### Wann:

- ✓ Du hast die Vermutung, dass jemand immer deinen Aufenthaltsort kennt

### Warum:

- ✓ Der Live-Standort sollte nicht öffentlich einsehbar sein

### Android

Gehe zu:

1. **Einstellungen** > **Google** > **Konto verwalten** > **Informationen** die du mit anderen teilen kannst. Dort siehst du eine Liste von Menschen mit denen du gerade deinen Standort teilst.
2. Klicke auf **Stopp**. Jetzt hat das Teilen ein Ende.

### Achtung!

Auch wenn du nur mit der in der Liste aufgeführten Person deinen Standort teilen möchtest, **jeder der den Link besitzt kann deinen Standort sehen**.

Wenn der Link weiter gegeben wird, ist dein Standort auch für weitere Menschen sichtbar.

## c2 Cloud Konto aufräumen: Standortdaten aus iCloud entfernen



### Wann:

- ✓ Du hast die Vermutung, dass jemand immer deinen Aufenthaltsort kennt

### Warum:

- ✓ Je weniger Daten gespeichert werden, desto unwahrscheinlicher, dass jemand diese in die Finger bekommt

### iCloud

Historische Standortdaten löschen und Speicherung einschränken:

1. **Einstellungen** > **Datenschutz & Sicherheit** > **Ortungsdienste**
2. Ganz unten, klicke auf **Systemdienste** > **Wichtige Orte**
3. Klicke auf **Verlauf löschen** und deaktiviere den Schalter **Wichtige Orte**

Live Standortdaten ausschalten:

1. **Einstellungen** > **[Dein Name]** > **Wo ist?**
2. Deaktiviere **Standort teilen**
3. Klicke auf **Mein iPhone suchen** und deaktiviere alle Optionen

## Privacy-Einstellungen: Goldene Regeln

Sei dir bewusst, was du mit der Welt teilst! Privacy beginnt mit Eigenverantwortung.

Ein paar goldene Regeln für dein Online-Dasein:

Teile im Internet niemals ...

- ... dein Passwort
- ... deine Adresse, Arbeits- oder Schuladresse
- ... Bilder deines Ausweises oder Ausweisnummer
- ... deinen Geburtstag oder Geburtsort
- ... Kreditkartennummer oder Bankdaten
- ... Antworten zu typischen Sicherheitsfragen (was ist der Mädchenname deiner Mutter)
- ... deine Telefonnummer

## Privacy-Einstellungen: Metadaten entfernen

**Wann:**

- ✓ Erweiterte Privatsphäre ist erwünscht

**Warum:**

- ✓ Meta-Daten in Fotos können Zeit und Ortsinformationen beinhalten

Metadaten können mit speziellen Programmen entfernt werden. Lade sie für deinen Laptop oder dein Smartphone herunter und befolge die Anleitung des jeweiligen Programms.

### Laptop

*Alle Betriebssysteme:*

Programm: ExifTool

*Windows:*

Im Explorer: Rechtsklick auf die Bilder > Eigenschaften > Details > Eigenschaften und persönliche Informationen entfernen

*Mac:*

Programm: ImageOptim

### Smartphone

*Android:*

App:

- Scrambled Exif
- Photo Exif Editor

*iPhone:*

App:

- Apple Shortcuts-App
- ViewExif

**Mehr Infos:** <https://www.heise.de/ratgeber/Metadaten-aus-Fotos-entfernen-4657362.html>



# c3 Privacy-Einstellungen: WhatsApp Privacy-Einstellungen vornehmen



## Wann:

- ✓ Grundsätzliche Privatsphäre

## Warum:

- ✓ WhatsApp neigt dazu deine Informationen freizügig zu teilen. Dies kann eingeschränkt werden

## Profilbild für Fremde unsichtbar machen

1. **Einstellungen > Datenschutz > Profilbild**
2. Hier kannst du zwischen der Sichtbarkeit für Alle, Meine Kontakte und Niemand auswählen.

## „Zuletzt online“ verbergen

1. **Einstellungen > Datenschutz > Zuletzt Online**
2. Hier kannst du zwischen der Sichtbarkeit für Alle, Meine Kontakte und Niemand auswählen.

## Lesebestätigung deaktivieren

1. **Einstellungen > Datenschutz > Lesebestätigung**
2. Hier kannst du die Lesebestätigung Aus- oder Einschalten.

## Status verbergen

1. **Einstellungen > Datenschutz > Status**
2. Hier kannst du zwischen der Sichtbarkeit für Alle, Meine Kontakte und Niemand auswählen.

## Einladung in Gruppen verhindern

1. **Einstellungen > Datenschutz > Gruppen**
2. Hier kannst du kontrollieren, wer dich Gruppen hinzufügen darf: Alle oder Meine Kontakte.

# Privacy-Einstellungen: Instagram Privacy-Einstellungen vornehmen



## ► Wann:

- ✓ Grundsätzliche Privatsphäre

## ► Warum:

- ✓ Instagram ist prima, um viele Infos über dein Leben zu sammeln. Nicht jeder sollte das können.

## ► Privates Konto einstellen

Mit einem privaten Konto können nur von dir bestätigte Follower deinen Content sehen:

1. Auf deinem Profil, klicke auf das **Menü** oben rechts und auf **Einstellungen und Privatsphäre**
2. Klicke auf **Konto-Privatsphäre** und aktiviere **Privates Konto**

## ► Story und Live-Videos verbergen oder nur für enge Freunde anzeigen

1. Du kannst beim Teilen einer Story einstellen, dass diese nur mit engen Freunden geteilt werden soll. Diese Gruppe an Menschen kannst du hier einstellen:  
**Einstellungen und Privatsphäre > Enge Freunde**
2. Zusätzlich kannst du bestimmte Accounts davon ausschließen, überhaupt Storys und Live-Videos von dir zu sehen:  
**Einstellungen und Privatsphäre > Story und Live verbergen**
3. Konten können auch komplett blockiert werden:  
**Einstellungen und Privatsphäre > Blockiert > +**

## ► Einschränken, wie andere mit dir interagieren können

In den **Einstellungen und Privatsphäre** kannst du bestimmen welche Personengruppen mit dir wie interagieren können:

Unter Nachrichten und Story-Antworten: Wer dich kontaktieren kann, wer sehen kann, dass du online bist und Lesebestätigungen erhält

Unter Markierungen und Erwähnungen: Wer dich wie Markieren kann oder ob du öffentlich in einer Story, Kommentaren u.Ä. von anderen erwähnt werden kannst.

## ► Instagrams Anti-Belästigungsfunktionen

In den **Einstellungen und Privatsphäre** erlaubt dir die Funktion **Eingeschränkte Konten** Interaktionen mit einem **Account heimlich einzuschränken**, ohne dass die andere Person informiert wird. Kommentare, die diese Person schreibt, müssen von dir manuell freigegeben werden und dein Aktivitätsstatus wird verborgen.

Um sich auf selbe Weise vor **Personengruppen** zu schützen, kann die Funktion **Limitierte Interaktionen** genutzt werden.

# D1 Smartphone absichern: Sichere PIN-Code einstellen

**Lasse dein Smartphone niemals entsperrt unbeaufsichtigt liegen!**

## Wann:

- ✓ Die Person hat die Möglichkeit auf dein Gerät zuzugreifen, wenn du nicht hinschaust

## Warum:

- ✓ Mit einem sicheren PIN ist es nicht so einfach



## Android

Gehe zu:

1. **Einstellungen > Bildschirmsperre**
2. Wähle die folgenden Einstellungen aus:



## iPhone

Gehe zu:

1. **Einstellungen > Face ID & Code** (Auf älteren iPhones: Touch ID & Code)
2. Deaktiviere Touch ID oder Face ID
3. Wähle die folgenden Einstellungen aus:

- Displaysperre: Alphanummerischer Code
- Mindestens 6 Zeichen, NICHT 123456, 000000, deinen Namen oder ähnliches
- Automatisch sperren: hier kann man angeben, nach wie vielen Minuten gesperrt werden soll. 2 Minuten ist ein guter Wert.

# D1 Smartphone absichern: SIM Karten Sperre einrichten

## Wann:

- ✓ Die Person hat die Möglichkeit auf dein Gerät zuzugreifen, wenn du nicht hinschaust

## Warum:

- ✓ Sollte jemand deine SIM-Karte stehlen, ist es nicht möglich die SIM-Karten zu nutzen



## Android

Gehe zu:

1. **Einstellungen > Nutzer > Sicherheit**
2. Wählen **SIM-Sperre einrichten** aus
3. Tippe auf **PIN ändern**
4. Geben deine **neue PIN** ein und tippe auf **OK**



## iPhone

Gehe zu:

1. **Einstellungen > Mobilfunk > SIM-PIN**
2. Schalte SIM-Pin auf **Ein**
3. Vergebe eine **neue PIN**

## D2 Smartphone aufräumen: App-Berechtigungen verwalten

### Wann:

- ✓ Du hast Sorge, dass deine (Standort-) Daten ohne dein Wissen geteilt werden

### Warum:

- ✓ Apps horten Berechtigungen, selbst wenn sie diese nicht gebraucht werden. Je weniger Daten übertragen werden, desto weniger Risiko.



### Android

Gehe zu:

1. **Einstellungen > Apps**
2. Hier findest du nun alle installierten Programme – tippe dazu auf **Alle**
3. Wähle unbekannte App aus und deinstalliere sie über den Button **Deinstallieren**. Je nach Smartphone-Modell musst du dazu lange den Namen der App gedrückt halten.



### iPhone

Gehe zu:

1. **Einstellungen** und scrolle herunter zu den **Apps**.
2. Hier kannst du pro App einsehen, **welche Berechtigungen erteilt** worden sind.
3. **Deaktiviere** unerwünschte Berechtigungen für Apps, die Sie nicht brauchen (z.B. Standort Berechtigungen für Spiele-Apps)

## D2 Smartphone aufräumen: Unerwünschte Apps deinstallieren

### Wann:

- ✓ Du bist dir unsicher, was alles auf deinem Smartphone installiert ist
- ✓ Du hast Sorge, dass eine Spionage-App installiert sein könnte

### Warum:

- ✓ Es schadet nicht, Apps die du nicht kennst zu löschen! Dein Smartphone wird dich vom Löschen von notwendigen Apps abhalten!



### Android

Gehe zu:

1. **Einstellungen > Apps**
2. Hier findest du nun alle installierten Programme – tippe dazu auf **Alle**
3. Wähle unbekannte App aus und deinstalliere sie über den Button **Deinstallieren**. Je nach Smartphone-Modell musst du dazu lange den Namen der App gedrückt halten.



### iPhone

Gehe zu:

1. **Wische nach rechts**, auf die aller letzte Seite. Nun siehst du eine **Liste aller installierten Apps**, eingeteilt in Kategorien.
2. **Deinstalliere** unbekannte Apps, in dem du fest auf das App-Icon drückst (iPhone 3D-Touch)

## D3 Smartphone zurücksetzen: Zurück auf Werkseinstellungen

### Wann:

- ✓ Die Person hatte in der Vergangenheit unüberwachten Zugriff auf dein Gerät
- UND
- ✓ Du bist besorgt, dass etwas auf deinem Smartphone ist, was da nicht sein sollte

### Warum:

- ✓ Das Smartphone auf den Zustand zurückzusetzen, in dem es beim Kauf war, ist die sicherste Möglichkeit sicherzustellen, dass nichts unerwünschtes auf dem Gerät ist

**Mache zunächst ein Backup deiner Daten! Mehr dazu bei [F3](#)**



### Android

Gehe zu:

1. **Einstellungen > System > Optionen zum Zurücksetzen**
2. Wähle **Alle Daten löschen** (auf Werkseinstellungen zurücksetzen)
3. Tippe auf **Alle Daten löschen**





### iPhone

Gehe zu:

1. **Einstellungen > Allgemein > iPhone übertragen/zurücksetzen**
2. Wähle **Zurücksetzen**

## E1 Anrufe blockieren: Eine Rufnummer blockieren

<b>Wann:</b> <ul style="list-style-type: none"><li>✓ Wenn dich Personen mit unerwünschten Anrufen belästigen</li></ul>	<b>Warum:</b> <ul style="list-style-type: none"><li>✓ Blockierte Rufnummern können dich nicht mehr anrufen</li></ul>
--	--

 <b>Android</b>	 <b>iPhone</b>
<b>Gehe zu:</b> <ol style="list-style-type: none"><li>1. Öffne die <b>Telefon-App</b></li><li>2. Tippe auf das <b>Dreipunkt-Menü</b> &gt; <b>Anrufliste</b></li><li>3. Tippe auf einen Anruf von der Nummer, die blockiert werden soll</li><li>4. Tippe auf <b>Blockieren/Spam melden</b></li></ol>	<b>Gehe zu:</b> <ol style="list-style-type: none"><li>1. Tippe in der App <b>Telefon</b> auf Favoriten, Anrufliste oder Voicemail</li><li>2. Tippe auf ⓘ <b>neben der Nummer</b> oder <b>der Person</b>, die blockiert werden soll</li><li>3. Scrolle nach unten und tippe auf <b>Anrufer blockieren</b></li><li>4. Um blockierte Nummern zu verwalten, wähle <b>Einstellungen</b> &gt; <b>Telefon</b> &gt; <b>Blockierte Kontakte</b></li></ol>

## E1 Anrufe blockieren: Unbekannte Anrufe blockieren

<b>Wann:</b> <ul style="list-style-type: none"><li>✓ Wenn dich Personen mit unerwünschten Anrufen belästigen</li></ul>	<b>Warum:</b> <ul style="list-style-type: none"><li>✓ Verdeckte Rufnummern und unbekannte Rufnummern können dich nicht mehr erreichen</li></ul>
--	---

 <b>Android</b>	 <b>iPhone</b>
<b>Gehe zu:</b> <ol style="list-style-type: none"><li>1. Öffnen die <b>Telefon App</b></li><li>2. Tippe auf das <b>Dreipunkt-Menü</b></li><li>3. <b>Einstellungen</b> und dann <b>Blockierte Nummern</b></li><li>4. Aktiviere <b>Anrufe von nicht identifizierten Anrufern blockieren</b></li></ol>	<b>Gehe zu:</b> <ol style="list-style-type: none"><li>1. <b>Einstellungen</b> &gt; <b>Telefon</b></li><li>2. <b>Unbekannte Anrufer stummschalten:</b> Unbekannte Nummern und Rufnummern, die nicht in deinen Kontakten oder deiner Anruf-Historie sind, werden automatisch auf deine Mailbox geleitet.</li></ol>

## E2) Nutzer blockieren: WhatsApp Anrufer stummschalten

### Wann:

- ✓ Wenn dich Personen mit unerwünschten Anrufen belästigen

### Warum:

- ✓ Anrufe, die über WhatsApp getätigt werden, müssen separat eingeschränkt werden



### WhatsApp

Um unbekannte Nummern zu blockieren, gehe zu:

- **Einstellungen > Datenschutz > Anrufe**
- Hier kannst du Anrufe von unbekannten Nummern stummschalten

Um eine Person zu blockieren, gehe zu:

1. Öffne den **Chat** mit der Person
2. **Optionen > Kontakt ansehen > Blockieren > Blockieren**

## E2) Nutzer blockieren: Social-Media Accounts blockieren

### Wann:

- ✓ Wenn dich Personen auf Social-Media belästigen

### Warum:

- ✓ Blockierte Accounts können nicht mehr mit dir in Kontakt treten und sehen nicht mehr was du teilst



### Facebook

Gehe zu:

1. Klicke auf **dein Profilbild**
2. **Einstellungen und Privatsphäre > Einstellungen > Blockieren**
3. Gib **den Namen** des Profils ein, das du blockieren möchtest, und klicke auf **Blockieren**



### Instagram und Twitter

Gehe zu:

1. **Öffne den Account**, den du blockieren möchtest
2. Klicke auf die drei Punkte oben Rechts
3. **Blockieren**



# F1 Daten sichern: Ein Backup deines Smartphones und automatische Backups einrichten

## Wann:

- ✓ Du hast Sorge, dass eine Person deine Daten löschen könnte
- ODER
- ✓ Vor dem zurücksetzen deines Smartphones

## Warum:

- ✓ Mit einem Backup kannst du verlorene Daten jederzeit wiederherstellen

## Android

Gehe zu:

1. Öffne die **Einstellungen**
2. Wählen **Google** und dann **Sicherung** aus
3. Tipp: Wenn du die automatische Sicherung zum ersten Mal einrichtest, **aktiviere Google One-Back-up** und folge der Anleitung auf dem Bildschirm
4. Tippe auf **Jetzt sichern**

*Fotos und Dateien müssen separat gesichert werden:*

Variante A: Auf deinen Laptop

Schließe dein Smartphone mit einem Kabel an deinen Rechner an und ziehe die Dateien und Fotos, die du sichern möchtest, auf diesen.

Variante B: Google Cloud

Richte Google Drive ein, deine Dateien und Fotos automatisch zu synchronisieren.

Beachte, dass jeder mit Zugriff auf dein Google Konto auch Zugriff hat auf die Dateien und Fotos, die du hier sicherst!

Befolge die Hinweise aus Kapitel A1!

## iPhone

Gehe zu:

1. **Einstellungen > [Benutzername] > iCloud > iCloud-Backup**
2. Aktiviere den Schalter rechts neben iCloud-Backup

Ist dein **iCloud Speicherplatz** voll?

Variante A: Häufig ist der iCloud Speicher durch alte Backups verstopft, die kann man löschen!

1. **Einstellungen > [dein Name] > iCloud**
2. **Speicher verwalten > Backups**
3. Tippe auf den Namen des Geräts, dessen Backup du löschen möchtest
4. Tippe auf **Backup löschen > Deaktivieren & Löschen**

Variante B: Backup am Laptop über iTunes

1. iPhone an den Laptop oder PC mit einem Kabel anschließen. iTunes öffnet sich automatisch
2. In iTunes wähle **Übersicht > Backup jetzt erstellen**



# **Daten sichern: Ein Backup deines Laptops machen**

 <b>Wann:</b> ✓ Du hast Sorge, dass deine Daten verloren gehen könnten	 <b>Warum:</b> ✓ Mit einem Backup kannst du verlorene Daten jederzeit wiederherstellen
--	--

## **Windows 11**

Unter **Windows 11** mit **OneDrive**

1. In der Suchleiste, tippe **Windows-Sicherung** ein
2. Klicke auf **Sichern**

## **Linux Ubuntu**

Nutze die vorinstallierte Anwendung **Datensicherungen** und **Google Drive** oder eine **externe Festplatte** (siehe unten – Universalmethode)

1. Tippe in die Suchleiste in der Anwendungsübersicht **Datensicherungen** ein
2. Gib **den Ort** ein, in dem deine Daten gesichert werden sollen (Google Drive / Festplatte)
3. Richte ein, wie häufig automatische Backups vorgenommen werden sollen

## **Mac**

Variante A: **Backup mit Time Machine**

1. Schließe eine **externe Festplatte** an (siehe unten – Universalmethode)
2. Wähle **Systemeinstellungen > Allgemein > Time Machine**
3. Klicke auf **Backup-Volume hinzufügen**
4. Wähle deine externe Festplatte aus, und klicke auf **Volume konfigurieren**
5. Öffne **Time Machine > Backup jetzt erstellen** oder warte auf das automatische Backup

Variante B: **Wichtige Dateien in der iCloud**

1. **Systemeinstellungen > Apple-ID > iCloud > Apps, die iCloud verwenden > iCloud Drive**
2. Überprüfe unter **iCloud Drive**, ob **Diesen Mac synchronisieren** aktiviert ist
3. Aktiviere **Ordner ‚Schreibtisch‘ & ‚Dokumente‘**

## **Die Universalmethode – für einen Laptop jeder Art**

Diese **manuelle Methode** nimmt mehr Zeit in Anspruch, funktioniert aber immer.

1. Kaufe dir eine **externe Festplatte** (Suche nach „1TB externe SSD-Festplatte“)
2. Schließe die Festplatte an deinen Laptop an. Sie verhält sich wie ein angeschlossener USB-Stick
3. Nun **kopiere alle Ordner, die für dich wichtige Daten beinhalten, auf die Festplatte**

## Extra: Sind Informationen von mir online?

### ▶ Wann:

- ✓ Du möchtest gerne wissen, welche Informationen von dir im Netzkursieren

### ▶ Warum:

- ✓ Häufig ist uns gar nicht bewusst, welche Informationen nur eine Google-Suche entfernt sind

### Google Me!

*Gehe zu Google:*

1. Google deinen Namen in „Anführungszeichen“, z.B. „Melina Müller“
2. Suche auf dieselbe Weise nach deiner Nummer und deiner Wohnadresse

Wenn du Webseiten oder Plattformen entdeckst, die deine Informationen ungewollt veröffentlichen: Logge dich ein und entferne die Informationen oder kontaktiere die Seitenbetreiber.

*Gehe zu den Social-Media Plattformen, die du nutzt:*

1. Logge dich aus oder öffne ein neues privates Fenster. Gehe auf dein Profil und schau dir an, welche Informationen nicht eingeloggte Besucher über dich herausfinden können
2. Registriere einen neuen Account oder bitte eine/n FreundIn mit dir dein Profil zu besuchen. Schau dir an, welche Informationen ein anderer Nutzer auf der Plattform über dich herausfinden kann.

Wenn du Informationen entdeckst, die du lieber nicht öffentlich sehen würdest: Logge dich ein und lösche diese Informationen oder ändere die Privacy-Einstellungen.

---

## Extra: War da jemand an meinem Laptop?

### ▶ Wann:

- ✓ Du möchtest gerne wissen, ob jemand an deinem Laptop war, während du nicht hingeschaut hast

### ▶ Warum:

- ✓ Manchmal ist es möglich, die Spuren unwillkommener Schnüffler zu finden

### Simple Laptop Forensik

*Logge dich auf deinem Laptop ein:*

1. Drücke auf das Windows Symbol und prüfe, welche die zuletzt genutzten Apps sind
2. Tippe jeden Buchstaben aus dem Alphabet in die Suchleiste ein und beobachte, welche Suchanfragen zuletzt geschrieben worden sind
3. Öffne deinen Papierkorb und prüfe, welche Dateien zuletzt gelöscht worden sind

# Weitere Informationen



## Antistalking Haecksen

Technische Hilfe gegen Cyberstalking

<https://antistalking.haecksen.org/>



## Privacy Guides

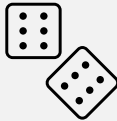
The guide to restoring your online privacy.

<https://www.privacyguides.org/>



## Informationen um das Thema sichere Passwörter (BSI)

<https://www.bsi.bund.de/dok/6596574>



## Erstelle mit Würfeln einen zufälligen Passwortsatz

<https://de.wikipedia.org/wiki/Diceware>