

## Schütze dein Smartphone/ Tablet und deine Daten

Beim Surfen im Internet solltest du darauf achten, dass Websites **https** verwenden.

Https steht für **HyperText Transfer Protocol Secure** und sorgt dafür, dass Daten die zwischen deinem PC oder Smartphone und dem Server, mit dem du kommunizierst, verschlüsselt übertragen werden.

Websites, die https verwenden, erkennst du an dem Schloss in der Adressliste des Browsers. Diese können grau oder grün sein, wobei grün die höchste "Sicherheitsstufe" darstellt.

## Passwörter

- Verwende zufällige und lange Passwörter oder Passsätze. Ein Erklärvideo zur Verwendung sicherer Passwörter findest du über den QR-Code.
- Verwende für jeden Dienst ein separates Passwort, damit bei einem Passwortdiebstahl der Schaden so gering wie möglich gehalten wird.
- Verwende einen Passwortmanager, wenn du viele Passwörter verwalten musst. Wähle für den Passwortmanager ein langes und komplexes Masterpasswort.
- In bestimmten Fällen ist es hilfreich, wenn deine Eltern oder die Polizei z.B. in einem Notfall Zugriff auf deine Passwörter haben. Überlege dir mit deinen Eltern, ob ihr z. B. das Masterpasswort deines Passwortmanagers in einem versiegelten Umschlag an einem geheimen Ort aufbewahren wollt.



[YouTube](#)



[Test Passwortmanager](#)

## 2-Faktor-Authentifizierung



[Authy-App](#)

Viele Dienste bieten inzwischen die Möglichkeit einer sogenannten 2-Faktor-Authentifizierung.

Das bedeutet, dass du zu deinem Benutzernamen und Passwort noch eine **zusätzliche Sicherheitsschranke** hast. Dies kann z.B. eine SMS mit einem nur kurz gültigen Zahlencode sein, den du bei der Anmeldung an einem Dienst eingeben musst.

Die zusätzlichen Codes können auch über bestimmte Apps, wie z.B. Authy (siehe QR-Code), generiert werden.

## Vorsicht in offenen WLANs

In Hotels, auf dem Campingplatz, am Bahnhof oder an Flughäfen hast du oft die Möglichkeit, ein kostenfreies WLAN zu nutzen.

Diese sind in aller Regel **nicht verschlüsselt**. Das bedeutet, dass alle Daten, die zwischen deinem Smartphone und dem WLAN-Punkt ausgetauscht werden, theoretisch abgefangen und mitgelesen werden können. Abhilfe schaffen sogenannte **VPN-Dienste**. Sie verhindern, dass deine Daten von Unbefugten abgegriffen werden können.

## https - HyperText Transfer Protocol Secure

---

**Beim Surfen im Internet solltest du darauf achten, dass Webseiten https verwenden.**

Https steht für **HyperText Transfer Protocol Secure** und sorgt dafür, dass Daten die zwischen PC/Smartphone und dem Server, mit dem du kommunizierst, verschlüsselt werden. So hat niemand die Möglichkeit "mitzulesen".

Du erkennst Webseiten mit https an dem Schlosssymbol in der Adressleiste deines Browsers.

Achte darauf, dass du keine persönlichen oder wichtigen Daten übermittelst, auf

Nicht sicher — spiegel.de

kein https - nicht sicher



mz-mittelbaden.de



gls.de

https - sicher

https - sicher

Das Schlosssymbol zeigt dir ebenfalls an, dass der Betreiber der Website der ist, für den er sich ausgibt.

**Doch Vorsicht.**

Das Zertifikat gilt immer nur für den Teil der URL, der links vor dem letzten Punkt der Adresse steht. Überprüfe also immer die komplette URL, bevor du dem Schlosssymbol blind vertraust.

## Verwende Ad-Blocker

---

Sicherlich kennst du Seiten, bei denen dir **Werbung** eingeblendet wird. Das stört oft nicht nur den Lesefluss, sondern birgt zudem auch die Gefahr, dass unliebsame Werbung eingeblendet wird. Es kann sogar passieren, dass du bei einem Klick auf die Werbung auf einer Seite landest, deren Betreiber mit **betrügerischen Absichten** handeln.

Ein Ad-Blocker (Werbeblocker) versucht, diese Werbemeldungen im Browser zu unterdrücken.

**Achtung:** Manche Webseiten funktionieren inzwischen leider nur mit deaktiviertem Ad-Blocker. Du kannst ihn für bestimmte Seiten auch **deaktivieren**.

## Aufgaben

### ① Überlege mit einem Partner

Wo im Alltag begegnen uns Passwörter und Codes? Denkt dabei nicht nur an Computer und Smartphones. Notiert eure Ergebnisse.

### ② Welche Kriterien sollte ein sicheres Passwort erfüllen?

### ③ Für wie sicher hältst du folgende Passwörter?

|                     | sehr gut              | gut                   | unsicher              |
|---------------------|-----------------------|-----------------------|-----------------------|
| Anne2010            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Fh#;jjWUrv3NfoRz8   | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| IhPuba25021980g!    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| DasistmeinPasswort! | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Passwort123         | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

### ④ Notiere drei weitere Beispiele für sichere Passwörter/ Passsätze. (Die solltest du danach besser nicht mehr verwenden).

### ⑤ Diskutiert in eurer Klasse

In welchen Fällen kann es sinnvoll sein, dass z.B. deine Eltern Zugriff auf deine Passwörter haben?

Denkt dabei an unterschiedliche Situationen und begründet eure Antworten.

### ⑥ Diskutiert in eurer Klasse

Manche Websites unterbinden, dass du mit aktiviertem Ad-Blocker Inhalt auf der Seite lesen kannst.

1) Was könnten Gründe dafür sein?

2) Für wie sinnvoll haltet ihr diese Maßnahme?