

## LEITFADEN FÜR ELTERN

### Wichtige Information zum Schutz Ihres Kindes nach dem Hackerangriff

Liebe Eltern,

wie bereits über Ihre Schulleitungen mitgeteilt, wurden bei einem Hackerangriff auf das Schulsystem umfangreiche personenbezogene Daten entwendet und teilweise im Internet veröffentlicht.

#### Dazu können gehören:

- ✿ Namen, Adressen und Kontaktdaten
- ✿ Schuldaten (Klasse, Lehrkräfte)
- ✿ ggf. auch sensible Informationen (z. B. Förderbedarfe, Gutachten oder Gesundheitsdaten)

#### Was bedeutet das konkret?

Unbekannte könnten diese Informationen nutzen, um gezielt Vertrauen aufzubauen oder Druck auszuüben. Zum Beispiel:

- ✿ Ihr Kind persönlich ansprechen und Details nennen
- ✿ sich als bekannte Person ausgeben
- ✿ Informationen verwenden, um Nähe oder Autorität vorzutäuschen

Auf Anregung der Schulen und den SEBs haben wir Ihnen folgenden Leitfaden erstellt.

### WAS JETZT BESONDERS WICHTIG IST

#### 1. Sprechen Sie offen mit Ihrem Kind

- ✿ Erklären Sie altersgerecht, dass Fremde möglicherweise persönliche Dinge wissen
- ✿ Betonen Sie: Wissen über eine Person bedeutet **kein Vertrauen**

#### 2. Klare Sicherheitsregeln vereinbaren

- ✿ Keine Treffen mit Unbekannten
- ✿ Keine Weitergabe persönlicher Informationen
- ✿ Keine Reaktion auf Druck („Sag niemandem etwas“)
- ✿ Unter [www.notinsel.de](http://www.notinsel.de) schauen, welche Notinseln es für Kind auf dem Schulweg gibt

Vereinbaren Sie ein **Familien-Codewort** sowie ein **Safe-Emoji** für Ausnahmesituationen, das nur Sie und ihr Kind kennen.

#### 3. Digitale Sicherheit erhöhen

- ✿ Passwörter ändern (auch bei Eltern-Accounts)
- ✿ Zwei-Faktor-Anmeldung aktivieren
- ✿ Privatsphäre-Einstellungen prüfen
- ✿ Vorsicht bei unbekanntem Nachrichten oder Anrufen



### **Mögliche Warnsignale**

- ✿ Ungewöhnliche Kontaktaufnahmen (online oder offline)
- ✿ Personen, die viele persönliche Details kennen
- ✿ Versuche, Vertrauen oder Druck aufzubauen

### **Was tun bei Auffälligkeiten?**

- ✿ Gespräch mit dem Kind suchen
- ✿ Kontakt abbrechen lassen
- ✿ Beweise sichern (Screenshots etc.)
- ✿ Schule und ggf. Polizei informieren

### **Wichtig für Ihr Kind**

- ✿ Fremde können Dinge wissen – das macht sie nicht vertrauenswürdig
- ✿ Ihr Kind kann jederzeit zu Ihnen kommen



## LEITFADEN FÜR FÖRDERSCHÜLER

### Wichtige Regeln für Dich

Fremde Menschen könnten Dinge über Dich wissen.

Zum Beispiel:

- ✿ Deine Namen oder den Deiner Eltern bzw. Lehrerinnen und Lehrer
- ✿ Deine Schule
- ✿ andere persönliche Dinge

#### Wichtig:

Auch wenn jemand viel über Dich weiß:

→ Das ist ein Fremder!

#### Das darfst Du nicht tun:

- ✿ Nicht mit Fremden mitgehen – auch nicht wenn sie den Namen Deiner Eltern kennen
- ✿ Keine persönlichen Dinge erzählen
- ✿ Keine Geschenke annehmen

#### Das sollst Du tun:

- ✿ Weggehen
- ✿ Sag laut: „**NEIN!**“
- ✿ Dir Hilfe holen

#### Wer hilft Dir?

- ✿ Eltern
- ✿ Lehrerinnen und Lehrer
- ✿ vertraute Erwachsene
- ✿ „Notinseln“ ([www.notinsel.de](http://www.notinsel.de))

#### Ganz wichtig:

Wenn Dich jemand anspricht und viel weiß:

→ **Immer zuhause davon erzählen!**



## **LEITFADEN FÜR GRUNDSCHÜLER**

### **Bleib sicher – das solltest Du wissen**

Fremde Menschen könnten Informationen über Dich kennen.

Zum Beispiel:

- ✿ Deinen Namen oder den Deiner Eltern bzw. Lehrerinnen und Lehrer
- ✿ Deine Schule
- ✿ andere persönliche Dinge

#### **Wichtig:**

Auch wenn jemand Dir unbekanntes Dich kennt oder Dinge über Dich weiß:

→ Du musst dieser Person nicht vertrauen.

#### **Deine Regeln:**

- ✿ Geh nicht mit fremden Menschen mit – auch nicht wenn sie den Namen Deiner Eltern kennen
- ✿ Gib keine persönlichen Infos weiter
- ✿ Triff Dich nicht mit Fremden
- ✿ Nimm keine Geschenke an

#### **Im Internet:**

- ✿ Schreibe nicht mit Unbekannten
- ✿ Nimm keine fremden Kontakte an
- ✿ Schicke keine persönlichen Infos oder Fotos

#### **Achtung:**

Manche Menschen tun so, als wären sie nett oder würden Dich kennen.

#### **Wenn Dir etwas seltsam vorkommt:**

- ✿ Geh weg
- ✿ Antworte nicht
- ✿ Sag Deinen Eltern oder Lehr\*innen Bescheid

#### **Wichtig:**

Du kannst immer Hilfe holen.

Erzähle es immer zuhause!



## LEITFADEN FÜR JUGENDLICHE

### Deine Daten könnten im Umlauf sein – bleib aufmerksam

Durch einen Hackerangriff könnten umfangreiche persönliche Daten von Dir im Internet verfügbar sein: Dazu können gehören:

- ✿ Name, Adresse, Schule – auch die Deiner Eltern oder Lehrer\*innen
- ✿ Kontaktdaten
- ✿ ggf. auch sensible Informationen (z. B. Gesundheitsdaten oder Gutachten)

#### Was bedeutet das?

- ✿ Diese Daten können gezielt genutzt werden, um:
- ✿ Vertrauen aufzubauen
- ✿ Dich zu manipulieren
- ✿ Druck auszuüben oder einzuschüchtern
- ✿ Das nennt man **Social Engineering**.

#### Mögliche Situationen:

- ✿ Jemand schreibt Dir und kennt viele Details über Dich
- ✿ Fake-Accounts geben sich als bekannte Personen aus
- ✿ Jemand nutzt persönliche Infos, um Dich unter Druck zu setzen

#### Warnzeichen:

- ✿ „Ich weiß viel über Dich...“
- ✿ „Vertrau mir, ich kenne Dich“
- ✿ „Sag niemandem etwas“
- ✿ Drohungen oder Druck

#### So schützt Du Dich:

- ✿ Teile keine sensiblen Informationen
- ✿ Reagiere nicht auf Druck oder Drohungen
- ✿ Ändere Deine Passwörter
- ✿ Aktiviere Zwei-Faktor-Anmeldung
- ✿ Prüfe Deine Privatsphäre-Einstellungen

#### Online:

- ✿ Unbekannte blockieren
- ✿ Keine fremden Kontakte annehmen
- ✿ Verdächtige Accounts melden



**Wenn etwas passiert:**

- ✿ Screenshots machen
- ✿ Kontakt abbrechen
- ✿ Hilfe holen (Eltern, Schule, Vertrauenspersonen)

**Wichtig:** Persönliche Informationen können missbraucht werden.  
Bleib aufmerksam und hol Dir Unterstützung.



## KONKRETE SZENARIEN („WAS TUN, WENN...“)

### Deine Daten könnten im Umlauf sein – bleib aufmerksam

#### Szenario 1: „Jemand kennt meinen Namen, den Namen bzw. Wohnort meiner Eltern und Bezugspersonen oder meine Schule“

**Situation:**

Eine fremde Person spricht ein Kind an oder schreibt eine Nachricht und kennt persönliche Details.

**Botschaft:**

→ Wissen ≠ Vertrauen

**Was tun:**

- ✿ Nicht weiter reden oder schreiben
- ✿ Keine Informationen bestätigen
- ✿ Abstand halten / Chat beenden
- ✿ Erwachsenen informieren

#### Szenario 2: „Jemand ist besonders nett und macht ein Angebot“

**Situation:**

Geschenke, Hilfe, Mitfahrgelegenheit („Ich soll Dich abholen“)

**Was tun:**

- ✿ Nicht mitgehen
- ✿ Nichts annehmen
- ✿ Immer Rücksprache mit Eltern/Schule
- ✿ Codewort-Regel nutzen

#### Szenario 3: „Unbekannte schreiben mir online“

**Situation:**

Nachrichten über Social Media, Messenger oder Gaming-Plattformen

**Was tun:**

- ✿ Nicht antworten
- ✿ Account prüfen (Fake möglich)
- ✿ Blockieren und melden
- ✿ Screenshots machen



#### Szenario 4: „Jemand setzt mich unter Druck“

##### Situation:

- ✿ „Sag niemandem etwas“
- ✿ „Ich weiß Dinge über Dich“
- ✿ Drohungen oder Erpressung

##### Was tun:

- ✿ Nicht reagieren
- ✿ Beweise sichern
- ✿ Sofort einer Vertrauensperson sagen
- ✿ Hilfe holen (Eltern, Schule)

#### Szenario 5: „Jemand gibt sich als bekannte Person aus“

##### Situation:

- ✿ angeblich Lehrer\*in
- ✿ angeblich Verwandte
- ✿ angeblich Bekannte

##### Was tun:

- ✿ Immer überprüfen (nachfragen, auf der Dir bekannten Nummer zurückrufen)
- ✿ Keine Infos weitergeben
- ✿ Im Zweifel: abbrechen

#### Szenario 6: „Ich bin unsicher“

##### Wichtigste Regel überhaupt:

→ Lieber einmal zu viel fragen als einmal zu wenig

##### Was tun:

- ✿ Gespräch mit Eltern / Lehrer\*innen
- ✿ Situation schildern
- ✿ gemeinsam entscheiden

#### KINDGERECHTE KURZFORMEL

STOPP – DENKEN – FRAGEN

- ✿ **STOPP** → Nicht reagieren
- ✿ **DENKEN** → Woher weiß die Person das?
- ✿ **FRAGEN** → Erwachsene um Hilfe bitten



## **HILFREICHE LINKS ZUM THEMA „DATENSCHUTZ“**

### **Unterrichtsreihe „Was ist Datenschutz?“ (2026)**

- Herausgeber: Bundesbeauftragte für den Datenschutz (BfDI)
- Zielgruppe: Klassen 4–7
- Inhalte:
  - Was sind persönliche Daten?
  - Was ist privat / öffentlich?
  - Datenspuren & Suchmaschinen
  - sichere Passwörter
  - Social Media & Cybermobbing

### **„Datenschutz geht zur Schule“ (klicksafe / EU-Initiative)**

- Umfangreiches Handbuch (~200+ Seiten)
- Enthält:
  - komplette Unterrichtseinheiten
  - Checklisten für Schüler & Eltern
  - Themen wie:
    - Datenmissbrauch
    - Profiling
    - Social Media Risiken
    - Recht am eigenen Bild

### **„Data Kids“ – Unterrichtsmodule**

- Zielgruppe: Klassen 4–6 (anpassbar)
- Inhalte:
  - personenbezogene Daten verstehen
  - Rechte von Kindern
  - Datennutzung & Werbung
  - Sicherheit bei Lernplattformen
  - Cybermobbing

### **BSI: „Cybersicherheit für 10–14-Jährige“**

- Fokus: konkrete Sicherheitskompetenzen
- Inhalte:
  - sichere Nutzung digitaler Systeme
  - Schutz vor Angriffen
  - Verhalten im Ernstfall



## **ERGÄNZENDE LEITFÄDEN UND RATGEBER:**

### **„Jugendliche online – Persönliche Daten“**

- Schwerpunkt:
  - Welche Daten gebe ich preis?
  - Risiken von Datenspuren
  - Missbrauch durch Dritte

### **Allgemeiner Ratgeber Datenschutz für Kinder & Jugendliche**

- erklärt:
  - warum Datenschutz wichtig ist
  - typische Gefahren (Phishing, Datenmissbrauch)
  - Rolle von Schule & Eltern

Liebe Eltern,  
dieser Leitfaden wurden von der Stadt Speyer erstellt und kann selbstverständlich auch unabhängig des Hackerangriffs verwendet oder an andere Eltern weitergeben werden.

Wenn Sie Ergänzungen oder Tipps für diesen Leitfaden haben, senden Sie uns Ihr Feedback bitte per Mail unter dem Betreff „Schülerleitfaden“ an das Büro der Oberbürgermeisterin. Ansprechpartnerin ist Sabrina Albers: [sabrina.albers@stadt-speyer.de](mailto:sabrina.albers@stadt-speyer.de)

Vielen Dank!

