

Social Media Sicherheit

Konten schützen, Risiken kennen, Privatsphäre bewahren — was jede Nutzerin und jeder Nutzer über die sichere Nutzung sozialer Netzwerke wissen sollte.

THEMEN IM ÜBERBLICK

Konten & Passwörter

Privatsphäre-Einstellungen

Fake-Profile & Betrug

Datenweitergabe verstehen

Kinder & Jugendliche

Notfallmaßnahmen

Die Broschüre lässt sich von vorne nach hinten lesen oder kapitelweise nachschlagen. Kapitel 13 ist ein Spickzettel zum Heraustrennen.

01	Die wichtigsten Regeln auf einen Blick	3
02	Konten richtig absichern	4
03	Privatsphäre-Einstellungen verstehen	5
04	Was Plattformen über Sie sammeln	6
05	Fake-Profilе und Betrug erkennen	7
06	Sicherheitseinstellungen je Plattform	8
07	Weniger preisgeben — Datensparsamkeit	9
08	Belästigung, Mobbing und richtig melden	10
09	Kinder und Jugendliche schützen	11
10	Desinformation und Manipulation erkennen	12
11	Wenn das Konto übernommen wurde	13
12	Digitaler Nachlass und Konten im Todesfall	14
13	Spickzettel zum Ausdrucken	15
14	Quellen und weiterführende Hinweise	16



Menüpfade altern schnell

Die Pfadangaben im Kapitel „Sicherheitseinstellungen je Plattform“ waren zum genannten Stand korrekt. Plattformen bauen ihre Einstellungen regelmäßig um — wenn ein Pfad nicht mehr passt, hilft die Suche in den App-Einstellungen nach Stichworten wie „Zweistufig“, „Privat“ oder „Sitzungen“.

Die wichtigsten Regeln auf einen Blick

Konto absichern

Starkes einzigartiges Passwort und 2FA für jedes soziale Netzwerk. Die E-Mail-Adresse des Kontos ebenfalls absichern.

Wer sieht was?

Privatsphäre-Einstellungen aktiv prüfen. Standard ist oft „öffentlich“ — das ist selten sinnvoll.

Vor dem Posten denken

Was einmal online ist, lässt sich kaum vollständig löschen. Screenshots existieren weiter.

Fake erkennen

Gefälschte Profile, Gewinnspiele und Hilfesuche sind häufige Betrugsmaschen auf allen Plattformen.

GOLDENE REGEL

Soziale Netzwerke sind keine privaten Räume — auch bei engen Privatsphäre-Einstellungen. Teilen Sie nichts, das Sie nicht auch einem Fremden auf der Straße zeigen würden. Das gilt für Fotos, Standorte, Reisepläne und persönliche Daten.

Mini-Checkliste vor dem Posten

- ? Bin ich sicher, wer das sehen wird?
- ? Enthält das Bild unbeabsichtigt Adressen, Kennzeichen oder andere Personen?
- ? Würde ich das in drei Jahren noch posten wollen?
- ? Betrifft der Post andere Personen, die nicht gefragt wurden?

Konten richtig absichern

Ein übernommenes Social-Media-Konto kann für Betrug, Identitätsdiebstahl und Rufschädigung genutzt werden – oft ohne dass die betroffene Person es sofort bemerkt.

Absicherung in der richtigen Reihenfolge

- 1 E-Mail-Adresse zuerst:** Das verknüpfte E-Mail-Konto ist der Schlüssel zur Kontoübernahme. Dieses mit 2FA und starkem Passwort sichern.
- 2 Einzigartiges Passwort:** Nie dasselbe Passwort für mehrere Plattformen. Passwortmanager nutzen.
- 3 Zwei-Faktor-Authentifizierung aktivieren:** Authenticator-App oder Passkey bevorzugen, SMS als Mindeststandard.
- 4 Angemeldete Geräte prüfen:** In den Sicherheitseinstellungen alle unbekannten Sitzungen beenden.
- 5 Backup-Codes sichern:** Offline aufbewahren – für den Fall, dass das zweite Gerät verloren geht.
- 6 Telefonnummer und Recovery-E-Mail aktuell halten:** Veraltete Angaben blockieren die Wiederherstellung.

! „Konto bestätigen“ – häufige Phishing-Falle

Nachrichten, die angeblich von Instagram, Facebook oder TikTok kommen und Sie zur Bestätigung Ihres Kontos auffordern, sind häufig Phishing. Melden Sie sich immer direkt in der App an – nie über einen Link aus einer Nachricht oder E-Mail.

i Passend dazu

Wie starke Passwörter entstehen, wie ein Passwortmanager eingerichtet wird und worin sich SMS-Code, Authenticator-App, Passkey und Hardwarekey unterscheiden, steht ausführlich in der Schwesterbroschüre „Cybersecurity im Alltag“, Kapitel „Passwörter ohne Kopfschmerzen“ und den beiden folgenden.

i Tipp

Viele Plattformen bieten eine Login-Benachrichtigung an – aktivieren Sie diese, um bei fremden Anmeldeversuchen sofort informiert zu werden.

Privatsphäre-Einstellungen verstehen

Die meisten Plattformen stellen neue Konten auf „öffentlich“. Das bedeutet: Profil, Beiträge und oft auch Freundeslisten sind für jeden weltweit sichtbar. Überprüfen Sie diese Einstellungen aktiv.

EINSTELLUNG	EMPFEHLUNG	WARUM?
Profil-Sichtbarkeit	Nur Freunde / Privat	Verhindert, dass Fremde Ihre Beiträge und Fotos einsehen können.
Freundesliste / Follower	Verborgен oder eingeschränkt	Öffentliche Kontaktlisten können für Social Engineering genutzt werden.
Standort-Tagging	Deaktivieren	Präziser Standort in Echtzeit ist ein Sicherheitsrisiko.
Suchbarkeit per E-Mail/ Telefon	Deaktivieren	Verhindert, dass Unbekannte Sie über Ihre Kontaktdaten finden.
Verknüpfte Apps & Dienste	Regelmäßig prüfen	Alte Apps mit Zugriff auf Ihr Konto regelmäßig entfernen.
Gesichtserkennung / KI-Features	Bewusst entscheiden	Viele Plattformen nutzen Fotos zum Training von KI-Modellen.
Aktivitätsstatus	Je nach Bedarf	„Zuletzt online“ und „tippt gerade“ können Rückschlüsse ermöglichen.

Einmal im Jahr nachsehen

Plattformen ändern ihre Datenschutzeinstellungen regelmäßig — oft nach Updates oder Änderungen der Nutzungsbedingungen. Prüfen Sie die Einstellungen mindestens einmal pro Jahr.

Was Plattformen über Sie sammeln

Soziale Netzwerke sind kostenlos — weil das Produkt die Daten der Nutzerinnen und Nutzer sind. Das Wissen darüber hilft, bewusster zu entscheiden, was man teilt und was nicht.

Standort & Bewegung

Standort bei App-Nutzung, Geo-Tags in Fotos, WLAN-Netzwerke in der Nähe, Reismuster.

Verhalten & Interesse

Was Sie liken, wie lange Sie bei einem Post verweilen, wem Sie folgen, was Sie suchen.

Gerät & Netzwerk

Gerätemodell, Betriebssystem, Browser, IP-Adresse, Mobilfunkanbieter.

Plattformübergreifend

Viele Plattformen verfolgen Sie auch außerhalb — durch „Gefällt mir“-Buttons, Pixel und Login-Buttons auf fremden Webseiten.

Datensammlung reduzieren

- ✓ App-Berechtigungen prüfen: Mikrofon, Kamera und Standort nur bei echter Notwendigkeit erlauben.
- ✓ „Login mit Facebook/Google“ vermeiden — dadurch werden Konten und Daten verknüpft.
- ✓ Werbe-Tracking in den Einstellungen einschränken oder deaktivieren.
- ✓ Geo-Tags in Fotos vor dem Hochladen entfernen (EXIF-Daten).
- ✓ Browser-Erweiterungen wie uBlock Origin oder Privacy Badger reduzieren plattformübergreifendes Tracking.

i Was Sie verlangen können

Auskunft über gespeicherte Daten, Löschung und ein Export in maschinenlesbarer Form sind Rechte, keine Kulanz. Wie man sie geltend macht, steht in „**Deine Rechte an deinen Daten**“.

i EXIF-Daten in Fotos

Viele Smartphones speichern GPS-Koordinaten, Uhrzeit und Gerätemodell direkt in der Bilddatei. Wer das Foto erhält, kann damit den genauen Aufnahmeort bestimmen. Plattformen entfernen diese Daten teils automatisch — teils nicht.

Fake-Profil und Betrug erkennen

Soziale Netzwerke sind ein bevorzugtes Umfeld für Betrug, weil Vertrauen schnell entsteht – durch gemeinsame Kontakte, geteilte Interessen oder ein ansprechendes Profil.

ROMANCE SCAM

Attraktives Profil, schnelle emotionale Nähe, dann Geldforderung.

Häufig über Wochen oder Monate aufgebaut. Bilder sind meist gestohlen. Niemals Geld an Personen senden, die man nur online kennt.

GEFÄLSCHTE GEWINNSPIELE

„Sie wurden ausgewählt! Klicken Sie hier zum Einlösen.“

Oft mit echtem Logo von Firmen oder Prominenten. Ziel ist die Phishing-Seite, auf der Zugangsdaten abgefangen werden.

GEHACKTE BEKANNTHE

„Ich stecke in der Klemme – kannst du mir schnell helfen?“

Nachrichten von Freunden oder Verwandten, die plötzlich um Geld oder Gutschein-Codes bitten. Immer über einen anderen Kanal rückfragen.

FAKE-SHOPS & INVESTITIONEN

„Limitiertes Angebot, nur heute!“ mit Markenlogo.

Werbeanzeigen für nicht existierende Produkte oder Krypto-Investments mit garantiertem Gewinn. Anbieter vor Zahlung unabhängig prüfen.

Profil auf Echtheit prüfen

- ✓ Profilbild per Rückwärts-Bildersuche prüfen (Google Bilder, TinEye).
- ✓ Wenige Posts, junges Konto, kaum Kontakte – häufige Merkmale von Fake-Profilen.
- ✓ Nachrichten mit ungewöhnlichen Links oder Dateianhängen grundsätzlich misstrauen.
- ✓ Bei Geldforderungen: immer telefonisch über eine bekannte Nummer rückfragen.

Sicherheitseinstellungen je Plattform

Jede Plattform hat eigene Wege zu den Sicherheitseinstellungen. Die wichtigsten Punkte im Überblick.

Instagram & Facebook (Meta)

Einstellungen → Sicherheit

2FA aktivieren	Einstellungen → Sicherheit → Zweistufige Authentifizierung → Authenticator-App wählen
Angemeldete Geräte	Einstellungen → Sicherheit → Wo du angemeldet bist → unbekannte Sitzungen beenden
Profil auf privat	Einstellungen → Privatsphäre → Konto → Privates Konto aktivieren
App-Verknüpfungen	Einstellungen → Apps und Websites → nicht genutzte Apps entfernen

X (ehemals Twitter)

Einstellungen → Sicherheit

2FA aktivieren	Einstellungen → Sicherheit und Kontozugriff → Zwei-Faktor-Authentifizierung
Sichtbarkeit einschränken	Einstellungen → Privatsphäre → Beiträge schützen (nur Follower sehen Beiträge)
Standort-Tagging	Einstellungen → Privatsphäre → Standortdaten für Beiträge deaktivieren

TikTok

Profil → Einstellungen

Konto auf privat	Einstellungen → Privatsphäre → Privates Konto aktivieren
2FA aktivieren	Einstellungen → Sicherheit → Bestätigung in zwei Schritten
Duett / Stitch	Einstellungen → Privatsphäre → auf „Nur Freunde“ oder „Niemand“ setzen

WhatsApp

Einstellungen → Datenschutz

Zweistufige Verifizierung	Einstellungen → Konto → Verifizierung in zwei Schritten → PIN vergeben
Profilbild & Info	Einstellungen → Datenschutz → auf „Meine Kontakte“ begrenzen
Gruppen-Einladungen	Einstellungen → Datenschutz → Gruppen → „Meine Kontakte, außer ...“
Verknüpfte Geräte	Menü → Verknüpfte Geräte → unbekannte Sitzungen abmelden

Weniger preisgeben — Datensparsamkeit

Das Prinzip der Datensparsamkeit: Nur das teilen, was wirklich nötig ist. Jede Information, die online nicht existiert, kann nicht missbraucht werden.

Wohnort & Adresse

Nie die vollständige Adresse im Profil. Stadtteil oder Stadt reicht — falls überhaupt.
Paketzustellungen nicht öffentlich kommentieren.

Reisen & Abwesenheit

Urlaubsfotos erst nach der Rückkehr posten.
Echtzeitstandort ist eine Einladung für Einbrüche.

Kinder & Familie

Fotos von Kindern nie ohne Nachdenken posten.
Schulname, Sportverein oder Wohnort des Kindes sind sensible Daten.

Beruf & Arbeitgeber

Detaillierte Arbeitgeberdaten erleichtern gezielte Phishing-Angriffe. Interne Informationen, Projekte und Kollegen nicht öffentlich diskutieren.

Informationen, die Sie nie teilen sollten

- ✗ Vollständiges Geburtsdatum (Monat und Jahr reichen Identitätsdieben oft).
- ✗ Telefonnummer im öffentlichen Profil.
- ✗ Fotos von Ausweisen, Tickets oder Kreditkarten.
- ✗ Antworten auf typische Sicherheitsfragen (Name des Haustieres, Geburtsstadt).
- ✗ Aktueller Aufenthaltsort in Echtzeit.

! Der Mosaik-Effekt

Einzelne Informationen wirken harmlos — Vorname, Arbeitgeber, Wohnort, Haustier. Zusammengesetzt ergeben sie ein detailliertes Profil, das für gezielte Angriffe oder Identitätsdiebstahl genutzt werden kann. Kriminelle sammeln diese Puzzleteile gezielt aus verschiedenen Quellen.

Belästigung, Mobbing und richtig melden

Cybermobbing, Stalking und Belästigung sind auf sozialen Netzwerken verbreitet. Zu wissen, welche Werkzeuge die Plattformen bereitstellen, hilft schnell zu reagieren.

Sofortmaßnahmen

- ✓ **Blockieren:** verhindert jeglichen Kontakt über die Plattform.
- ✓ **Melden:** Jeder Beitrag und jedes Profil kann gemeldet werden. Nutzen Sie diese Funktion aktiv.
- ✓ **Beweise sichern:** vor dem Blockieren dokumentieren — Datum, Uhrzeit, Nutzernamen sichtbar.
- ✓ **Nicht eskalieren:** Antworten verschlimmert die Situation oft. Schweigen und melden ist wirkungsvoller.

Bei ernsthafteren Vorfällen

- ✓ Profil vorübergehend auf privat stellen oder deaktivieren.
- ✓ Vertrauensperson informieren — allein damit umzugehen ist schwerer.
- ✓ Bei Bedrohungen: Anzeige bei der Polizei, Screenshots als Beweise mitbringen.
- ✓ Plattform-Support kontaktieren — bei schwerwiegenden Fällen gibt es oft gesonderte Meldewege.

BEWEISE RICHTIG SICHERN

Screenshot so aufnehmen, dass Profilname, Datum und der vollständige Inhalt sichtbar sind. Speichern Sie zusätzlich die URL des Beitrags. Manche Plattformen bieten auch einen offiziellen Bericht-Download an (etwa für Behörden).

Anlaufstellen in Deutschland

Klicksafe.de bietet Beratung bei Cybermobbing. Das Bundeskriminalamt nimmt Anzeigen zu Online-Straftaten entgegen. Die Verbraucherzentrale hilft bei Datenmissbrauch.

Kinder und Jugendliche schützen

Die meisten Plattformen haben ein Mindestalter von 13 Jahren — in der Praxis wird es kaum kontrolliert. Aufklärung und offene Gespräche sind wirkungsvoller als reine Verbote.

Offen reden

Kinder berichten eher von Problemen, wenn sie keine Konsequenzen befürchten. Regelmäßige, urteilsfreie Gespräche über Erlebnisse online.

Gemeinsam einrichten

Privatsphäre-Einstellungen zusammen konfigurieren. Kinder verstehen so, warum bestimmte Einstellungen sinnvoll sind.

Regeln vereinbaren

Klare Absprachen: Was darf gepostet werden? Wer darf Freundschaftsanfragen schicken? Was passiert bei unangenehmen Nachrichten?

Grooming erkennen

Erwachsene, die gezielt Vertrauen bei Kindern aufbauen, nach Fotos fragen oder zur Geheimhaltung auffordern — sofort Eltern oder Vertrauenspersonen informieren.

Technische Schutzmaßnahmen

- ✓ Jugendschutzeinstellungen und Family-Funktionen der Plattformen und Geräte nutzen.
- ✓ Konto auf privat stellen — Follower nur nach manueller Bestätigung.
- ✓ Nachrichten von Fremden deaktivieren (bei Instagram, TikTok und anderen möglich).
- ✓ Standort-Sharing und Live-Funktionen ausschalten.
- ✓ Bildschirmzeit-Funktionen bewusst einsetzen — nicht als Strafe, sondern als vereinbarte Grenze.

! Für Begleitpersonen

Eine eigene Broschüre richtet sich an Eltern und Sorgeberechtigte: „Kinder online begleiten“ — mit Altersgrenzen, gemeinsamer Einrichtung, Grooming, Kostenfallen und Anlaufstellen.

! Erpressung mit Bildern

Jugendliche werden zu Aufnahmen überredet und danach damit erpresst — teils mit KI-erzeugten Bildern, für die nie ein Foto nötig war. Wichtig: Es ist nie die Schuld der betroffenen Person, es wird nicht gezahlt, und Erwachsene helfen ohne Vorwürfe. Beweise sichern, Kontakt abbrechen, melden.

! Anlaufstelle bei Missbrauch

Bei sexueller Belästigung oder Missbrauchsmaterial: Meldung an die Plattform und an die Meldestelle jugendschutz.net oder direkt an die Polizei. Beweise sichern, aber betroffene Kinder nicht zwingen, alles nochmals anzuschauen.

Desinformation und Manipulation erkennen

Soziale Netzwerke verbreiten Fehlinformationen schneller als Korrekturen. Algorithmen priorisieren emotionale, aufmerksamkeitsstarke Inhalte — unabhängig von deren Wahrheitsgehalt.

MUSTER	ERKENNUNGSZEICHEN	WAS TUN?
Falschmeldung	Reißerische Überschrift, kaum Quellenangaben, unbekannte Seite	Primärquelle suchen. Faktencheck-Seiten nutzen (correctiv.org, dpa-factchecking).
Manipuliertes Bild/Video	Kontextfremde Verwendung, Deepfake-Anzeichen, fehlende Metadaten	Rückwärts-Bildersuche, InVID-Plugin für Videos.
Koordinierte Bots	Viele gleichartige Accounts, identische Texte, junges Konto mit vielen Posts	Nicht teilen, melden.
Emotionaler Bait	Starke Empörung, Angst oder Mitgefühl als Hauptaussage	Innehalten. Inhalt auf den faktenbasierten Kern prüfen, bevor man teilt.

VOR DEM TEILEN PRÜFEN

Wer eine Meldung teilt, trägt Verantwortung für ihre Verbreitung. Ein kurzer Check vor dem Teilen — Quelle, Datum, andere Berichte — verhindert, dass man unfreiwillig zur Verbreitung von Falschinformationen beiträgt.



Nützliche Werkzeuge

correctiv.org und dpa-factchecking.com für deutschsprachige Faktenchecks. TinEye.com und die Google-Bildersuche für Bildprüfung. InVID/WeVerify für Videoverifikation.

Wenn das Konto übernommen wurde

Schnelles Handeln begrenzt den Schaden. Die Reihenfolge ist entscheidend.

- 1 Passwort sofort ändern — von einem anderen Gerät.** Wenn noch Zugriff besteht: Passwort sofort ändern. Kein verknüpftes Gerät des Angreifers nutzen.
- 2 Alle aktiven Sitzungen beenden.** Sicherheitseinstellungen → „Überall abmelden“ / „Alle Sitzungen beenden“. Entfernt den Angreifer vom Konto.
- 3 Verknüpfte E-Mail-Adresse und 2FA prüfen.** Angreifer ändern oft die Recovery-E-Mail. Prüfen und zurücksetzen. Anschließend 2FA aktivieren oder neu einrichten.
- 4 Freunde und Follower warnen.** Angreifer senden oft Nachrichten oder Betrugs-Links an Kontakte. Eine kurze öffentliche oder direkte Warnung verhindert weiteren Schaden.
- 5 Zugriff verloren? Wiederherstellungs-Prozess der Plattform nutzen.** Alle großen Plattformen haben offizielle Formulare für Kontodiebstahl. Ausweis-Verifizierung ist möglich. Offizielle Support-Seite direkt aufrufen — nie über Links in E-Mails.

! Geld oder Identität betroffen?

Wurden über das Konto betrügerische Nachrichten verschickt oder wurden Betroffene um Geld gebeten? Empfänger sofort informieren, Beweise sichern, gegebenenfalls Anzeige bei der Polizei erstatten.

Digitaler Nachlass und Konten im Todesfall

Was passiert mit Social-Media-Konten, wenn jemand stirbt? Viele Plattformen bieten Regelungen — die meisten Menschen kennen sie nicht.

PLATTFORM	OPTION	VORGEHEN
Facebook / Instagram	Gedenkseite oder Löschung	Nachlasskontakt vorab festlegen unter Einstellungen → Gedenkseite. Angehörige können Löschung beantragen.
Google (YouTube etc.)	Inaktivitätsmanager	Im Google-Konto unter „Daten & Datenschutz“ → Inaktivitätsmanager festlegen, was nach X Monaten Inaktivität passiert.
X / Twitter	Nur Löschung möglich	Angehörige können per Support-Anfrage mit Sterbeurkunde die Löschung beantragen.
TikTok / LinkedIn	Löschantrag durch Angehörige	Support-Formular mit Nachweisen. Keine automatische Gedenkfunktion vorhanden.

Was Sie jetzt tun können

- ✓ Nachlasskontakt bei Facebook einrichten.
- ✓ Google-Inaktivitätsmanager konfigurieren.
- ✓ Zugangsdaten sicher hinterlegen — etwa in einem versiegelten Umschlag oder einem digitalen Nachlass-Dienst.
- ✓ Vertrauenspersonen informieren, wo diese Informationen zu finden sind.

i Rechtslage in Deutschland

Es gibt keinen gesonderten gesetzlichen Anspruch von Erben auf Konto-Inhalte sozialer Netzwerke — das regelt jede Plattform über ihre Nutzungsbedingungen. Ein BGH-Urteil von 2018 stärkte die Rechte von Erben zumindest im Fall Facebook.

Spickzettel zum Ausdrucken

Diese Seite lässt sich einzeln ausdrucken und neben den Rechner legen.

KONTOSICHERHEIT

- ☐ Einzigartiges Passwort
- ☐ 2FA aktiviert
- ☐ Angemeldete Geräte geprüft
- ☐ Kein gleiches Passwort überall

PRIVATSPHÄRE

- ☐ Profil auf privat gestellt
- ☐ Standort-Tagging deaktiviert
- ☐ Telefonnummer nicht öffentlich
- ☐ Suchbarkeit per E-Mail/Tel. aus

VOR DEM POSTEN

- ☐ Sichtbarkeit geprüft
- ☐ Keine Adressen im Bild
- ☐ Keine Urlaubsfotos in Echtzeit
- ☐ Kinderfoto bewusst entschieden

BEI VERDACHT / NOTFALL

- ☐ Screenshot sichern
- ☐ Blockieren & melden
- ☐ Passwort ändern (anderes Gerät)
- ☐ Sitzungen beenden

ERSTE HILFE BEI KONTOÜBERNAHME

Passwort ändern → alle Sitzungen beenden → 2FA prüfen und aktivieren → Kontakte warnen → bei Verlust des Zugriffs den offiziellen Wiederherstellungsprozess der Plattform nutzen, nie über Links aus E-Mails.

Quellen und weiterführende Hinweise

BSI: Soziale Netzwerke sicher nutzen

bsi.bund.de → Verbraucher → Soziale Netzwerke

BSI: Identitätsdiebstahl

bsi.bund.de → Methoden der Cyberkriminalität → Identitätsdiebstahl

Klicksafe: Cybermobbing und Beratung

klicksafe.de/cybermobbing

jugendschutz.net: Meldestelle für problematische Online-Inhalte

jugendschutz.net

Correctiv: Faktencheck

correctiv.org/faktencheck/

dpa Faktencheck

dpa.com/de/faktencheck

Verbraucherzentrale: Datenschutz in sozialen Netzwerken

verbraucherzentrale.de/soziale-netzwerke

Meta: Sicherheitscenter

facebook.com/safety

Google: Inaktivitätsmanager einrichten

myaccount.google.com/inactive-account-manager

Have I Been Pwned: E-Mail und Passwort auf Datenlecks prüfen

haveibeenpwned.com

TinEye: Rückwärts-Bildersuche

tineye.com

InVID / WeVerify: Videoverifikation

weverify.eu/verification-plugin/

Weitergabe und Lizenz

Herausgeber

[Plotspace.eu](https://plotspace.eu) · info@plotspace.eu

Anschrift und Verantwortlicher im Impressum:

plotspace.eu/impressum

Lizenz

CC BY 4.0 — Kopieren, Weitergeben und Bearbeiten ausdrücklich erlaubt. Bitte „Plotspace.eu“ als Quelle nennen und Änderungen kenntlich machen; bearbeitete Fassungen dürfen nicht so wirken, als kämen sie von [Plotspace.eu.creativecommons.org/licenses/by/4.0/deed.de](https://plotspace.eu.creativecommons.org/licenses/by/4.0/deed.de)

Schriften: Public Sans und IBM Plex Mono, SIL Open Font License 1.1.

Diese Broschüre darf einzeln weitergegeben werden. Sie ist so aufgebaut, dass sie für sich allein verständlich bleibt; Querverweise auf die Schwesterbroschüre sind Ergänzung, keine Voraussetzung.

** Hinweis**

Diese Broschüre ersetzt keine individuelle Rechts- oder IT-Beratung. Plattformen ändern ihre Einstellungen und Datenschutzbedingungen regelmäßig. Prüfen Sie die aktuellen Einstellungen direkt in der jeweiligen App.