

Smartphone absichern

Das Gerät, auf dem alles zusammenläuft: Konten, Fotos, Bezahlen und der zweite Faktor. Was es schützt — und was passiert, wenn es weg ist.

THEMEN IM ÜBERBLICK

Sperre & Biometrie

App-Berechtigungen

Sichere App-Quellen

Updates & Gerätealter

Verlust & Diebstahl

Gerätewechsel mit 2FA

Backups

Gerät weitergeben

Diese Broschüre ergänzt „**Cybersecurity im Alltag**“ um das Gerät, das die meisten Menschen am häufigsten benutzen. Passwörter, Phishing und 2FA werden dort ausführlich behandelt und hier nicht wiederholt.

01	Warum das Handy der Hauptschlüssel ist	3
02	Bildschirmsperre und Biometrie	4
03	App-Berechtigungen verstehen	5
04	Woher Apps kommen dürfen	6
05	Updates und die Lebensdauer des Geräts	7
06	Verlust und Diebstahl	8
07	Gerätewechsel mit zweitem Faktor	9
08	Backups, die im Ernstfall taugen	10
09	Unterwegs: fremde Netze und Ladepunkte	11
10	Gerät weitergeben, verkaufen, entsorgen	12
11	Spickzettel zum Ausdrucken	13
12	Quellen und weiterführende Hinweise	14
13	Impressum und Weitergabe	15

i Android und iPhone

Die Wege heißen auf beiden Systemen unterschiedlich und ändern sich mit jeder größeren Version. Diese Broschüre nennt deshalb, wonach Sie in den Einstellungen suchen – nicht jeden Klickpfad.

Warum das Handy der Hauptschlüssel ist

Auf kaum einem anderen Gerät liegt so viel nebeneinander: E-Mail, Bank, Fotos, Chats, Bezahlfunktion — und oft der zweite Faktor für alle anderen Konten. Wer das Handy hat, hat damit häufig auch den Weg zurück in Konten, die gar nicht auf dem Gerät liegen.

Schlüssel und Schloss zugleich

Das Gerät empfängt den SMS-Code, trägt die Authenticator-App und speichert Passkeys. Es ist damit selbst das Ziel.

Immer dabei

Ein Handy geht schneller verloren als ein Rechner. Der Schutz muss deshalb ohne Ihr Zutun greifen.

Viele Ohren und Augen

Mikrofon, Kamera, Standort und Kontakte sind für jede App nur eine Freigabe entfernt.

Begrenzte Lebensdauer

Ohne Sicherheitsupdates wird auch ein funktionierendes Gerät zum Risiko — anders als ein Toaster.

DREI DINGE, DIE ALLES ANDERE TRAGEN

Eine **Bildschirmsperre**, die man nicht erraten kann. **Automatische Updates**. Und ein **Backup**, das ohne das Gerät funktioniert. Alles Weitere in dieser Broschüre baut darauf auf.

Passend dazu

Wie Sie den zweiten Faktor überhaupt einrichten und welche Verfahren wie stark sind, steht in „Cybersecurity im Alltag“, Kapitel „2FA, Passkeys und Hardwarekeys“.

Bildschirmsperre und Biometrie

Die Sperre ist die einzige Hürde zwischen einem gefundenen Gerät und allem darauf. Sie muss deshalb nicht bequem, sondern wirksam sein.

VERFAHREN	BEWERTUNG	HINWEIS
Wischmuster	✗ schwach	Bleibt als Fettspur auf dem Display sichtbar und lässt sich über die Schulter mitlesen.
Vierstellige PIN	~ Minimum	Besser als nichts. Keine Geburtsdaten, keine Muster wie 1234 oder 2580.
Sechsstellige PIN	✓ gut	Der sinnvolle Standard. Der Aufwand im Alltag ist derselbe.
Passwort	✓✓ am stärksten	Für Geräte mit beruflichen oder besonders sensiblen Daten.

Fingerabdruck und Gesicht

Biometrie ist bequem und im Alltag sicher genug — sie ersetzt aber nie den Code, sondern liegt davor. Nach einem Neustart verlangt das Gerät immer wieder den Code.

- ✓ Sperrzeit kurz halten: 30 Sekunden bis eine Minute. Eine Sperre, die erst nach 15 Minuten greift, ist im Café wirkungslos.
- ✓ Auf dem Sperrbildschirm nur anzeigen, was nicht privat ist. Nachrichtenvorschauen verraten sonst genau die Codes, die sie schützen sollen.
- ✓ Schnelleinstellungen im gesperrten Zustand einschränken — sonst lässt sich das Gerät ohne Code in den Flugmodus schalten und ist nicht mehr ortbar.
- ✓ Bei Reisen und Kontrollen: Gerät vorher neu starten, damit nur der Code entsperrt.



Der Code am Bahnsteig

Eine verbreitete Masche: Jemand beobachtet die Eingabe der PIN und entwendet das Gerät kurz darauf. Mit Code und Gerät lassen sich dann Konten übernehmen, weil der zweite Faktor mitgeliefert wird. Deshalb den Code verdeckt eingeben — genau wie am Geldautomaten.

App-Berechtigungen verstehen

Eine App darf nur, was Sie erlauben. Der Haken: Gefragt wird im Moment der Nutzung, wenn man ohnehin gerade weiterkommen will. Ein Blick in die Liste nach ein paar Wochen zeigt oft Überraschendes.

Standort

„Beim Verwenden der App“ statt „immer“.
Dauerhafter Zugriff ergibt nur bei Navigation oder Notfall-Apps Sinn.

Mikrofon und Kamera

Beide Systeme zeigen einen Punkt oder ein Symbol, wenn etwas aktiv ist. Erscheint er unerwartet, lohnt die Prüfung.

Kontakte

Wer sein Adressbuch freigibt, gibt fremde Daten weiter — Namen, Nummern und Adressen anderer Menschen.

Benachrichtigungszugriff

Eine App mit dieser Berechtigung liest alle Nachrichten mit, auch Bestätigungscode. Sehr sparsam vergeben.

Aufräumen in fünf Minuten

- 1 In den Einstellungen nach **Berechtigungen** oder **Datenschutz** suchen — beide Systeme zeigen die Liste nach Berechtigung sortiert.
- 2 Bei Standort, Mikrofon und Kamera durchgehen: Braucht diese App das wirklich, um ihren Zweck zu erfüllen?
- 3 Alles entziehen, was nicht einleuchtet. Wird es doch gebraucht, fragt die App beim nächsten Mal erneut.
- 4 Apps, die Sie ein Jahr nicht geöffnet haben, ganz entfernen. Nicht genutzte Apps bekommen keine Updates und sammeln trotzdem.

i Was Anbieter darüber hinaus erfahren

Berechtigungen regeln den Zugriff auf das Gerät — nicht, was ein Dienst aus Ihrem Verhalten ableitet. Dazu „Social Media Sicherheit“, Kapitel „Was Plattformen über Sie sammeln“.

Woher Apps kommen dürfen

Die offiziellen Stores prüfen Apps nicht perfekt, aber sie prüfen. Wer daran vorbei installiert, verliert genau diese Kontrolle — und liefert oft freiwillig Rechte mit, die eine App aus dem Store nie bekäme.

✓ VERLÄSSLICH

Der vorinstallierte Store des Systems. Bei Android zusätzlich seriöse Alternativen wie F-Droid für quelloffene Software — bewusst ausgewählt, nicht beiläufig.

✗ RISKANT

APK-Dateien aus Foren, Chat-Nachrichten oder Werbeanzeigen. „Premium gratis“-Versionen bekannter Apps sind fast immer manipuliert.

- ✓ Vor der Installation den Anbieternamen prüfen. Gefälschte Apps kopieren Symbol und Namen, nicht aber den Entwicklereintrag.
- ✓ Bewertungen skeptisch lesen: viele kurze Fünf-Sterne-Texte in kurzer Zeit sind ein Warnzeichen.
- ✓ Stutzig werden, wenn eine Taschenlampe Kontakte will oder ein Spiel Zugriff auf Nachrichten verlangt.
- ✓ Nie eine App installieren, weil ein Anrufer oder eine Nachricht dazu auffordert — das ist der Einstieg in die Fernwartung.

! **Bedienungshilfen und Geräteverwaltung**

Zwei Berechtigungen sind besonders mächtig: **Bedienungshilfen** (die App darf den Bildschirm lesen und für Sie tippen) und **Geräteverwaltung**. Schadsoftware fragt genau danach, oft mit der Begründung, sie werde „für die Einrichtung benötigt“. Eine normale App braucht beides nicht.

i **Wenn jemand Sie zur Installation drängt**

Das Muster und die passende Reaktion stehen in „Cybersecurity im Alltag“, Kapitel „Erpressung, Schockanrufe und falscher Support“.

Updates und die Lebensdauer des Geräts

Bei Smartphones gibt es eine Grenze, die es beim Rechner so nicht gibt: Der Hersteller stellt irgendwann die Sicherheitsupdates ein. Danach bleibt das Gerät benutzbar, aber bekannte Lücken werden nie wieder geschlossen.

Systemupdates

Automatisch einschalten und nicht dauerhaft verschieben. Die meisten Updates schließen Lücken, die bereits ausgenutzt werden.

App-Updates

Ebenfalls automatisch. Browser und Messenger sind dabei am wichtigsten, weil sie fremde Inhalte verarbeiten.

Supportzeitraum

Wie lange ein Modell Updates bekommt, steht auf der Herstellerseite. Beim Kauf ein Kriterium — und oft ein größeres als die Kamera.

Danach

Ein Gerät ohne Updates gehört nicht mehr fürs Banking oder als zweiter Faktor genutzt. Als Musikspieler oder Wecker ist es weiter brauchbar.

BEIM NÄCHSTEN KAUF

Fragen Sie nicht nur, was das Gerät kann, sondern **wie lange es Sicherheitsupdates bekommt**. Hersteller nennen diesen Zeitraum inzwischen offen. Zwei Jahre Support bei einem Gerät, das fünf Jahre halten soll, sind ein schlechtes Geschäft.

Verlust und Diebstahl

Die Weichen dafür stellen Sie vorher. Danach zählt nur noch die Reihenfolge.

Einmal vorbereiten

- ✓ Gerätesuche aktivieren („Mein Gerät finden“ bzw. „Wo ist?“) und einmal ausprobieren, damit Sie den Weg im Ernstfall kennen.
- ✓ Die IMEI notieren und außerhalb des Geräts aufbewahren — sie steht auf der Verpackung und lässt sich über die Telefontastatur mit *#06# abfragen.
- ✓ SIM-PIN aktivieren. Ohne sie steckt die Karte in Minuten in einem fremden Gerät und empfängt Ihre Codes.
- ✓ Notfallnummern und ein aktuelles Backup bereithalten (siehe folgendes Kapitel).

Wenn es passiert ist

- 1 **Orten und sperren.** Über die Gerätesuche aus dem Browser eines anderen Geräts. Die Sperre zeigt auf Wunsch eine Kontaktnachricht an.
- 2 **SIM sperren lassen.** Beim Mobilfunkanbieter, damit niemand auf Ihre Kosten telefoniert und keine Codes empfängt.
- 3 **Konten schützen.** Von einem anderen Gerät aus Passwörter ändern und alle Sitzungen beenden — besonders E-Mail.
- 4 **Zweiten Faktor umziehen.** Ersatzcodes nutzen oder das neue Gerät registrieren, siehe folgendes Kapitel.
- 5 **Anzeige erstatten** und die IMEI angeben. Für Versicherung und Ermittlung.
- 6 **Erst zuletzt löschen.** Ein Fernlöschen beendet auch die Ortung — also nur, wenn die Daten wichtiger sind als das Wiederfinden.

! Die Nachricht danach

Nach einem Verlust kommen häufig Nachrichten, das Gerät sei gefunden worden — mit einem Link zur „Bestätigung Ihrer Konto-Daten“. Das ist Phishing, das gezielt auf Ihre Lage zielt. Melden Sie sich nur über die selbst eingetippte Adresse an.

Gerätewechsel mit zweitem Faktor

Der häufigste Weg, sich selbst auszusperren: Das alte Handy ist weg oder zurückgesetzt, und die Authenticator-App war nur dort. Ohne Vorbereitung hilft dann nur der langwierige Weg über den Support jedes einzelnen Dienstes.

DIE REGEL

Ein zweiter Faktor braucht immer einen **zweiten Weg hinein**: Ersatzcodes, ein zweites Gerät oder einen zweiten Schlüssel. Wer nur eine Möglichkeit hat, hat keine.

Vor dem Wechsel

- ✓ Recovery-Codes aller wichtigen Konten hervorholen und auf Gültigkeit prüfen. Wo sie hingehören, steht im Spickzettel-Kapitel von „Cybersecurity im Alltag“.
- ✓ Prüfen, ob Ihre Authenticator-App einen Export oder eine verschlüsselte Sicherung anbietet — viele können das inzwischen.
- ✓ Passkeys sind meist an das Konto des Systems gebunden und wandern beim Einrichten mit. Kontrollieren Sie das trotzdem, bevor das alte Gerät weg ist.
- ✓ Bei Hardwarekeys den zweiten Schlüssel bereitlegen. Genau dafür gibt es ihn.

Nach dem Wechsel

- ✓ Erst prüfen, ob Sie sich mit dem neuen Gerät bei allen wichtigen Konten anmelden können.
- ✓ Danach das alte Gerät in den Konten als Sitzung beenden und aus der Geräteliste entfernen.
- ✓ Erst ganz zum Schluss das alte Gerät zurücksetzen.

Backups, die im Ernstfall taugen

Ein Backup ist erst dann eines, wenn es ohne das Gerät funktioniert, das kaputt oder weg ist — und wenn Sie es einmal ausprobiert haben.

Systembackup

Beide Systeme sichern Einstellungen, Apps und Daten in die Cloud des Herstellers. Einschalten und gelegentlich das Datum prüfen.

Fotos

Der wertvollste und unwiederbringlichste Teil. Zusätzlich zur Cloud gelegentlich auf eine Festplatte kopieren.

Chatverläufe

Messenger sichern getrennt vom System und oft nur mit eigenem Kennwort. Dieses Kennwort separat notieren.

Der Test

Einmal eine einzelne Datei zurückholen. Ein Backup, aus dem nie etwas wiederhergestellt wurde, ist eine Vermutung.

Cloud-Sync ist kein Backup

Was synchronisiert wird, wird überall gelöscht, sobald es an einer Stelle gelöscht wird. Die 3-2-1-Regel und der Unterschied zur Sicherung stehen in „Cybersecurity im Alltag“, Kapitel „Geräte, Updates, WLAN und Backups“.

Unterwegs: fremde Netze und Ladepunkte

Die meisten Verbindungen sind heute verschlüsselt, deshalb ist ein offenes WLAN weniger gefährlich als sein Ruf. Wichtig ist, was das Gerät nebenbei tut.

- ✓ Automatisches Verbinden mit offenen Netzen abschalten. Sonst hängt das Gerät an Hotspots, die Sie nie bewusst gewählt haben.
- ✓ Gespeicherte Netze gelegentlich aufräumen — Hotelnamen von vor drei Jahren braucht niemand.
- ✓ Bluetooth und Dateifreigabe aus, wenn Sie sie nicht brauchen. Die Freigabefunktionen beider Systeme sind in Zügen ein beliebter Weg für unerwünschte Bilder.
- ✓ An fremden USB-Buchsen nur laden. Fragt das Gerät nach Datenübertragung, ablehnen — besser ist das eigene Netzteil oder eine Powerbank.
- ✓ Der eigene Hotspot ist meist die einfachere Lösung als ein fremdes WLAN.



Zum Thema VPN

Was ein VPN in fremden Netzen leistet und was nicht — samt der Warnung vor kostenlosen Anbietern — steht ausführlich in „Cybersecurity im Alltag“, Kapitel „Öffentliche WLANs und unterwegs“.

Gerät weitergeben, verkaufen, entsorgen

Ein zurückgesetztes Gerät ist nur dann leer, wenn vorher die richtigen Schritte in der richtigen Reihenfolge passiert sind. „Alle Fotos gelöscht“ reicht nicht.

- 1 **Backup anlegen** und prüfen, dass es vollständig ist.
- 2 **Zweiten Faktor umziehen** — vor allem Authenticator-App und Passkeys.
- 3 **Vom Konto abmelden.** Bei iPhones „Wo ist?“ deaktivieren und sich aus der Apple-ID abmelden, bei Android das Google-Konto entfernen. Sonst bleibt das Gerät für den nächsten Besitzer gesperrt.
- 4 **SIM- und Speicherkarte entnehmen.**
- 5 **Auf Werkseinstellungen zurücksetzen.** Moderne Geräte sind standardmäßig verschlüsselt; das Zurücksetzen macht die Daten damit unlesbar.
- 6 **Bei Entsorgung:** Altgeräte gehören in die Sammlung des Handels oder des Wertstoffhofs, nicht in den Restmüll.

! **Gebraucht gekauft**

Umgekehrt gilt dasselbe: Ein gebrauchtes Gerät gehört vor der ersten Nutzung zurückgesetzt, auch wenn der Verkäufer das versichert. Prüfen Sie zudem, ob es noch Sicherheitsupdates erhält — bei sehr günstigen Angeboten ist genau das oft der Grund für den Preis.

Spickzettel zum Ausdrucken

Diese Seite lässt sich einzeln ausdrucken. Sie enthält bewusst keine Zugangsdaten — warum, steht im Spickzettel von „Cybersecurity im Alltag“.

EINMAL EINRICHTEN

-  Sechsstellige PIN oder Passwort
-  Gerätesuche aktiv und getestet
-  SIM-PIN aktiv
-  Automatische Updates an

REGELMÄSSIG

-  Berechtigungen durchgesehen
-  Ungenutzte Apps entfernt
-  Backup-Datum geprüft
-  Gespeicherte WLANs aufgeräumt

BEI VERLUST — IN DIESER REIHENFOLGE

-  Orten und sperren
-  SIM sperren lassen
-  Passwörter, Sitzungen beenden
-  Anzeige mit IMEI

MEINE ANGABEN

IMEI:

Mobilfunkanbieter:

Sperrdienst im eigenen Land:

Versicherung:

WENN SIE NUR EINE SACHE TUN

Gerätesuche aktivieren und einmal ausprobieren. Sie ist im Ernstfall der Unterschied zwischen „gesperrt in fünf Minuten“ und „gar nichts“.

Quellen und weiterführende Hinweise

BSI: Smartphones und Tablets sicher nutzen

bsi.bund.de → Verbraucher → Smartphone und Tablet

BSI: Sicherheitsupdates und Supportzeitraum

bsi.bund.de → Verbraucher → Updates

Google: Mein Gerät finden

support.google.com → Android → Verlorenes Gerät finden

Apple: Wo ist? und Aktivierungssperre

support.apple.com → Wo ist

Verbraucherzentrale: Handy verloren oder gestohlen

verbraucherzentrale.de → Digitale Welt → Mobilfunk

Polizeiliche Kriminalprävention: Diebstahl von Mobilgeräten

polizei-beratung.de → Themen → Diebstahl

Sperr-Notruf 116 116 (Deutschland)

sperr-notruf.de

F-Droid: quelloffener App-Katalog für Android

f-droid.org

**Hinweis**

Diese Broschüre ersetzt keine individuelle IT-Beratung. Menüpfade und Funktionsnamen ändern sich mit jeder Systemversion. Prüfen Sie im Zweifel die aktuelle Dokumentation Ihres Herstellers.

Weitere Broschüren dieser Reihe

- Cybersecurity im Alltag** — Links, Phishing, Passwörter, 2FA, DNS, öffentliche WLANs und Notfälle.
- Social Media Sicherheit** — Konten, Privatsphäre-Einstellungen, Fake-Profile, Datenweitergabe.
- Smartphone absichern** — diese Broschüre
- Heimnetz und Smart Home** — Router, WLAN, Gastnetz, vernetzte Geräte, Kameras, Portfreigaben.
- Kinder online begleiten** — Für Eltern: Altersgrenzen, Regeln, Mobbing, Grooming, Anlaufstellen.
- Deine Rechte an deinen Daten** — DSGVO praktisch: Auskunft, Löschung, Übertragbarkeit, Musterschreiben.
- Gruppen sicher organisieren** — Rollen, Regeln, Störer, Treffen, Voice, Minderjährige in der Gruppe.
- Allergene und Kennzeichnung** — Die 14 Pflichtangaben, Zutatenlisten lesen, „kann Spuren enthalten“.
- Erste Schritte** — Zweiseitiges Merkblatt zum Einstieg — kein Heft.

Weitergabe und Lizenz

Herausgeber

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
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 übrigen Hefte sind Ergänzung, keine Voraussetzung.