

Ist mein Smartphone sicher?

Der einfache 15-Minuten-Sicherheitscheck für iPhone und Android

In Ruhe prüfen - Schritt für Schritt

Diese Checkliste hilft dir, die wichtigsten Sicherheitseinstellungen deines Smartphones zu prüfen. Du musst kein Technikprofi sein. Kreuze ab, was bereits erledigt ist, und markiere, wobei du noch Hilfe möchtest.

So verwendest du die Checkliste

1. Nimm dein eingeschaltetes Smartphone zur Hand.
2. Arbeite die Punkte nacheinander durch. Die Menünamen können je nach Gerät etwas anders heißen.
3. Setze ein Kreuz, wenn alles erledigt ist. Bleibt ein Feld frei, ist das kein Grund zur Sorge.

Wichtig

Gib Passwörter, PIN-Codes oder Bestätigungscodes niemals an andere Personen weiter. Auch seriöse Banken, Behörden und bekannte Firmen fragen nicht danach.

Name: _____

Geprüft am: _____

Kostenloses Freebie von seniorenundtechnik.de

Das Smartphone richtig sperren

1. Smartphone-Sperre

Warum ist das wichtig? Eine Bildschirmsperre schützt Fotos, Nachrichten und persönliche Daten, wenn das Gerät verloren geht.

- Öffne die Einstellungen und suche nach Code, PIN, Face ID, Fingerabdruck oder Displaysperre.
- Verwende mindestens eine sechsstellige PIN. Vermeide Geburtsdaten, 123456 und leicht zu erratende Zahlenfolgen.
- Stelle ein, dass sich das Smartphone nach kurzer Zeit selbst sperrt.

- ☐ Mein Smartphone ist mit PIN oder Code geschützt.
- ☐ Der Code ist nicht leicht zu erraten.
- ☐ Das Gerät sperrt sich spätestens nach wenigen Minuten.

Gut zu wissen

Fingerabdruck oder Gesichtserkennung sind bequem. Eine sichere PIN wird trotzdem als Ersatz benötigt.

2. Updates einschalten

Warum ist das wichtig? Updates sind kostenlose Verbesserungen. Sie schließen bekannte Sicherheitslücken.

- Öffne die Einstellungen. Suche nach Softwareupdate, Systemupdate oder Aktualisierung.
- Aktiviere automatische Updates, wenn diese Möglichkeit angeboten wird.
- Führe größere Updates am besten zu Hause im WLAN durch. Der Akku sollte ausreichend geladen sein.

- ☐ Automatische Systemupdates sind eingeschaltet.
- ☐ Auch meine Apps werden automatisch aktualisiert.

Gut zu wissen

Ein Update kann einige Minuten dauern und das Smartphone dabei neu starten. Das ist normal.

Apps und Passwörter

3. Apps nur aus sicheren Quellen laden

Warum ist das wichtig? Gefälschte Apps können Daten ausspähen oder unerwünschte Kosten verursachen.

- Lade Apps beim iPhone nur aus dem App Store und bei Android nur aus dem Google Play Store.
- Prüfe vor dem Laden den Namen des Anbieters, Bewertungen und die Zahl der Downloads.
- Lösche Apps, die du nicht mehr nutzt oder nicht kennst.

- ☐ Ich lade Apps nur aus dem offiziellen App-Laden.
- ☐ Unbekannte oder ungenutzte Apps habe ich entfernt.

Gut zu wissen

Öffne keine Links, die angeblich eine App direkt installieren. Gehe selbst in den offiziellen App-Laden und suche dort nach der App.

4. Starke und unterschiedliche Passwörter

Warum ist das wichtig? Wird ein Passwort gestohlen, sind sonst gleich mehrere Konten gefährdet.

- Nutze für wichtige Konten jeweils ein eigenes Passwort.
- Ein gutes Passwort ist lang. Eine leicht merkbare Wortgruppe mit Zahlen und Zeichen ist oft besser als ein kurzes, kompliziertes Wort.
- Ein Passwortmanager kann Passwörter sicher speichern. Das ist eine digitale, geschützte Merkhilfe.

- ☐ Meine wichtigsten Konten haben unterschiedliche Passwörter.
- ☐ Meine Passwörter sind lang und nicht leicht zu erraten.
- ☐ Ich gebe Passwörter niemals per Telefon, SMS oder WhatsApp weiter.

Gut zu wissen

Passwörter nicht offen neben das Smartphone legen. Wenn du sie auf Papier notierst, bewahre die Liste an einem geschützten Ort auf.

Konten doppelt schützen

5. Zwei-Faktor-Anmeldung aktivieren

Warum ist das wichtig? Diese zusätzliche Sicherung verlangt neben dem Passwort einen zweiten Nachweis. Ein gestohlenes Passwort allein reicht dann meist nicht aus.

- Aktiviere die Funktion zuerst bei deiner E-Mail-Adresse, danach beim Online-Banking und bei wichtigen Kundenkonten.
- Sie kann auch Zwei-Schritt-Anmeldung oder Bestätigung in zwei Schritten heißen.
- Der zweite Nachweis ist zum Beispiel eine Bestätigung in einer App oder ein einmaliger Zahlencode.

- ☐ Meine E-Mail-Adresse ist doppelt geschützt.
- ☐ Weitere wichtige Konten sind doppelt geschützt.
- ☐ Meine Wiederherstellungsdaten sind aktuell.

Gut zu wissen

Ein unerwarteter Bestätigungscode ist ein Warnzeichen. Gib ihn niemandem weiter und bestätige keine Anmeldung, die du nicht selbst begonnen hast.

6. Betrügerische SMS und WhatsApp erkennen

Warum ist das wichtig? Betrüger erzeugen Zeitdruck oder Angst. Häufig geben sie sich als Paketdienst, Bank, Behörde oder Familienmitglied aus.

- Sei vorsichtig bei unbekannten Nummern, Rechtschreibfehlern und dringenden Geldforderungen.
- Tippe nicht auf Links in überraschenden Nachrichten.
- Meldet sich angeblich ein Angehöriger mit neuer Nummer, rufe ihn über die bisher bekannte Nummer an.

- ☐ Ich öffne keine verdächtigen Links oder Anhänge.
- ☐ Ich prüfe überraschende Bitten über einen zweiten Kontaktweg.
- ☐ Ich blockiere und melde betrügerische Absender.

Gut zu wissen

Lass dich nicht drängen. Eine kurze Pause und ein Rückruf über eine selbst gesuchte Nummer verhindern viele Betrugsfälle.

Anrufe und WLAN unterwegs

7. Verdächtige Anrufe richtig behandeln

Warum ist das wichtig? Die angezeigte Telefonnummer kann gefälscht sein. Eine vertraut wirkende Nummer ist deshalb kein Beweis.

- Beende den Anruf, wenn jemand nach Geld, PIN, Passwort oder einem Bestätigungscode fragt.
 - Rufe Banken, Polizei oder Firmen nur über eine selbst gesuchte offizielle Nummer zurück.
 - Erlaube unbekannten Anrufern keinen Fernzugriff auf dein Smartphone oder deinen Computer.
- ☐ Ich verrate am Telefon keine Zugangsdaten oder Codes.
 - ☐ Ich beende Druckgespräche und prüfe die Behauptung selbst.
 - ☐ Ich installiere auf Zuruf keine Fernwartungs-App.

Gut zu wissen

Die Polizei fordert niemals telefonisch Geld, Schmuck oder Wertsachen zur sicheren Verwahrung.

8. Öffentliches WLAN vorsichtig nutzen

Warum ist das wichtig? Frei zugängliche WLAN-Netze in Cafés, Hotels oder Bahnhöfen können unsicher oder gefälscht sein.

- Nutze für Online-Banking und Einkäufe besser das Mobilfunknetz oder dein vertrautes WLAN zu Hause.
 - Verbinde dich nur mit dem offiziellen WLAN-Namen. Frage im Zweifel das Personal.
 - Schalte die automatische WLAN-Verbindung aus und entferne nicht mehr benötigte öffentliche Netze.
- ☐ Für Bankgeschäfte nutze ich kein öffentliches WLAN.
 - ☐ Mein Smartphone verbindet sich nicht automatisch mit jedem offenen Netz.
 - ☐ Bluetooth schalte ich aus, wenn ich es längere Zeit nicht brauche.

Gut zu wissen

Mobilfunk über 4G oder 5G ist unterwegs meist die einfachere und sicherere Wahl.

Persönliche Daten und Notfälle

9. Datenschutz und App-Berechtigungen

Warum ist das wichtig? Nicht jede App benötigt Zugriff auf Standort, Kontakte, Mikrofon, Kamera oder Fotos.

- Öffne in den Einstellungen den Bereich Datenschutz, Sicherheit oder Berechtigungen.
- Prüfe besonders Standort, Kontakte, Kamera und Mikrofon.
- Erlaube den Zugriff nur, wenn er für die Funktion der App nötig ist. Wähle möglichst Nur beim Verwenden der App.

- ☐ Ich habe die Berechtigungen meiner wichtigsten Apps geprüft.
- ☐ Unnötige Zugriffe sind ausgeschaltet.

Gut zu wissen

Eine Navigations-App benötigt deinen Standort. Eine einfache Taschenlampen-App benötigt normalerweise weder Kontakte noch Mikrofon.

10. Notfallinformationen hinterlegen

Warum ist das wichtig? Helfer können wichtige Angaben im Notfall sehen, ohne das Smartphone vollständig zu entsperren.

- Beim iPhone findest du dies meist in der App Health unter Notfallpass.
- Bei Android suche in den Einstellungen nach Notfallinformationen, Sicherheit und Notfall oder Medizinische Informationen.
- Trage nur Angaben ein, die im Notfall helfen, zum Beispiel Kontaktperson, wichtige Erkrankungen oder Allergien.

- ☐ Eine erreichbare Notfallkontaktperson ist hinterlegt.
- ☐ Wichtige medizinische Angaben sind aktuell.
- ☐ Die Anzeige im Sperrbildschirm ist erlaubt und wurde getestet.

Gut zu wissen

Informiere deine Notfallkontaktperson darüber, dass du sie eingetragen hast.

Warnmeldungen und Hilfe

11. Cell Broadcast und Warnmeldungen

Warum ist das wichtig? Cell Broadcast ist ein Warnsystem. Behörden können damit bei akuter Gefahr eine Meldung direkt an viele Mobiltelefone in einem Gebiet senden.

- Öffne die Einstellungen und suche nach Notfallwarnungen, Warnmeldungen oder Cell Broadcast.
- Lass Warnungen der höchsten Gefahrenstufe eingeschaltet. Manche wichtigen Warnungen lassen sich nicht abschalten.
- Für Warnmeldungen ist keine besondere App nötig. Eine zusätzliche Warn-App kann weitere Informationen liefern.

- ☐ Notfallwarnungen sind auf meinem Smartphone eingeschaltet.
- ☐ Ich weiß, wie sich eine Warnmeldung anhört und was dann zu tun ist.

Gut zu wissen

Bei einer echten Warnung: Ruhe bewahren, den Text vollständig lesen und die genannten Anweisungen befolgen.

12. Was tun bei einem Verdacht?

Warum ist das wichtig? Schnelles, ruhiges Handeln kann Schäden begrenzen.

- Brich den Kontakt ab. Antworte nicht weiter und tippe auf keinen Link.
- Bei Bankdaten oder Zahlungen: Rufe sofort deine Bank über die offizielle Nummer an. Der Sperr-Notruf für Karten in Deutschland ist 116 116.
- Ändere betroffene Passwörter von einem vertrauenswürdigen Gerät aus. Beginne mit dem E-Mail-Konto.
- Sichere Nachrichten, Nummern und Zahlungsbelege als Beweis. Erstatte bei einem Schaden Anzeige bei der Polizei.
- Bitte eine vertraute Person um Hilfe. Scham ist unangebracht - Betrüger gehen sehr geschickt vor.

- ☐ Ich kenne eine Person, die ich im Zweifel fragen kann.
- ☐ Die offizielle Banknummer ist sicher notiert.
- ☐ Ich weiß: Erst stoppen, dann prüfen, dann handeln.

Mein persönlicher Hilfe-Kontakt

Name: _____ Telefon: _____

Mein Ergebnis

Zähle deine Kreuze. Entscheidend ist nicht die Punktzahl, sondern dass du offene Punkte erkennst und in Ruhe erledigst.

Bereich	Erledigt	Noch prüfen
Smartphone-Sperre	☐	☐
Updates	☐	☐
Apps	☐	☐
Passwörter	☐	☐
Zwei-Faktor-Anmeldung	☐	☐
SMS und WhatsApp	☐	☐
Anrufe	☐	☐
WLAN unterwegs	☐	☐
Berechtigungen	☐	☐
Notfallinformationen	☐	☐
Warnmeldungen	☐	☐
Verhalten im Verdachtsfall	☐	☐

Die drei wichtigsten Regeln

1. Keine Passwörter, PINs oder Codes weitergeben.
2. Bei Zeitdruck oder Angst: Gespräch beenden und selbst prüfen.
3. Im Zweifel eine vertraute Person fragen.

Notizen

Hinweis: Diese Checkliste bietet eine allgemeine Orientierung. Menünamen und Einstellungen können sich je nach Smartphone-Modell und Software-Version unterscheiden.

Mehr verständliche Hilfe rund um Smartphone und Internet:
seniorenundtechnik.de