Ihr Schutz- und Notfallplan

Für Soloselbständige und Einzelpersonen — einfach erklärt

Rund um iPhone, Mac · Hamburg · Stand 2026

Dieser Plan zeigt Ihnen in einfachen Worten, wie Sie Ihre Konten und Geräte schützen — und was Sie tun, wenn doch etwas passiert. **Sie brauchen kein Technik-Wissen.** Fachbegriffe stehen kurz erklärt daneben. Arbeiten Sie die Schritte einfach der Reihe nach ab. (Keine Rechtsberatung.)

> **So lesen Sie diesen Plan**
>
> - **Teil 1 (Schutz):** Was Sie vorher einrichten, damit möglichst nichts passiert.
> - **Teil 2 (Notfall):** Was Sie tun, wenn ein Konto gehackt wurde.
> - **Teil 3 (Checkliste):** Eine Seite zum Ausdrucken und Abhaken.
>
> **Tipp:** Drucken Sie den Notfall-Teil aus. Wenn Ihr Handy oder Laptop gesperrt ist, haben Sie die Schritte trotzdem zur Hand.

Zuerst: Womit fange ich an?

Fachleute für Sicherheit gehen immer in einer festen Reihenfolge vor — vom Wichtigsten zum weniger Wichtigen. So stecken Sie Ihre Zeit dahin, wo sie am meisten bringt. Merken Sie sich diese Reihenfolge:

> **Die goldene Reihenfolge**
>
> **1. Zugänge sichern → 2. Sicherungskopien anlegen → 3. Geräte schützen → 4. Für den Notfall vorbereiten → 5. regelmäßig kontrollieren.**
>
> Der Grund: Die häufigste Gefahr ist, dass jemand sich in Ihr Konto einloggt. Deshalb kommt der Schutz Ihrer Zugänge zuerst.

Schritt 1 — Überblick verschaffen (etwa 30 Minuten)

Schreiben Sie auf, was Sie überhaupt schützen müssen:

- **Geräte:** iPhone, iPad, Mac/Laptop.
- **Konten:** E-Mail, Apple-ID, Online-Banking, Cloud-Speicher, Instagram/Facebook, PayPal & Co.
- **Wichtige Daten:** Kundendaten, Rechnungen, Verträge, Fotos.

Zwei Konten sind Ihre **„Generalschlüssel“**: Ihr E-Mail-Postfach und Ihre Apple-ID. Über die E-Mail lassen sich fast alle anderen Passwörter zurücksetzen. Wer dort hereinkommt, kommt oft überall herein. Deshalb bekommen diese beiden den besten Schutz.

Schritt 2 — Größte Gefahren kennen

Für Einzelpersonen gibt es vor allem drei realistische Gefahren. Danach richtet sich der ganze Plan:

Gefahr	Was das bedeutet	Bester Schutz dagegen
Konto-Übernahme	Jemand loggt sich in Ihr Konto ein — meist, weil ein Passwort geklaut wurde.	Passkeys / zusätzliche Bestätigung beim Login; für jedes Konto ein eigenes Passwort
Erpressungs-Software	Ein Schadprogramm sperrt Ihre Dateien und verlangt Geld.	Regelmäßige Sicherungskopien (Backups)
Gerät verloren / gestohlen	Ihr Handy oder Laptop ist weg — samt Daten.	Code-Sperre, Face/Touch ID, „Wo ist?“-Funktion

Schritt 3 bis 5 — der Reihe nach abarbeiten

- **Schritt 3:** Die Schutzmaßnahmen aus Teil 1 einrichten — von oben nach unten.
- **Schritt 4:** Den Notfall-Teil (Teil 2) ausdrucken und eine kurze Telefonliste anlegen (Nummern siehe Teil 2).
- **Schritt 5:** Einmal im Monat kurz kontrollieren (Details am Ende von Teil 1).

Teil 1 · So schützen Sie sich (vorher)

Die Maßnahmen sind nach Wirkung sortiert: **Zuerst-Liste** bringt am meisten, dann geht es abgestuft weiter. Arbeiten Sie oben an.

Hinweis zu Anbietern: Dienste mit **(USA)/(UK) !** sitzen außerhalb der EU. Dabei können Daten ins Ausland fließen. Wo es eine gleich gute europäische Lösung gibt, ist diese vorzuziehen. Die Produktnamen sind nur Beispiele, keine Kaufempfehlung.

> **Kurz erklärt — die wichtigsten Begriffe**
>
> **Passwort-Manager:** Ein Programm, das all Ihre Passwörter sicher speichert. Sie müssen sich nur noch ein einziges Haupt-Passwort merken.
>
> **2FA (Zwei-Faktor):** Eine zweite Bestätigung zusätzlich zum Passwort — z. B. ein Code aus einer App. Selbst wenn jemand Ihr Passwort kennt, kommt er ohne diesen zweiten Schritt nicht hinein.
>
> **Passkey:** Ein moderner Login ganz ohne Passwort. Sie bestätigen mit Face ID, Fingerabdruck oder Geräte-PIN. Kann nicht abgephisht werden.
>
> **Backup:** Eine Sicherungskopie Ihrer Daten, damit nichts verloren geht.
>
> **Schutzsoftware (Virenschutz):** Ein Programm, das Schadprogramme erkennt und blockiert.

Zuerst erledigen (der größte Hebel)

Was	So machen Sie es	Warum es so wichtig ist
Passkeys einschalten	Überall dort, wo es angeboten wird: Login per Face ID, Fingerabdruck oder PIN statt Passwort. Geht u. a. bei Apple, Google, Microsoft (USA) !, PayPal, Amazon, eBay (USA) !. Prüfen Sie ein Konto nach dem anderen.	Das ist der sicherste Login. Selbst bei einem Datenleck ist nichts zu holen.
Zweite Bestätigung (2FA) überall anschalten	Wo es noch keinen Passkey gibt: 2FA einschalten — besonders bei E-Mail, Apple-ID, Banking, Cloud und Instagram/Facebook. Bei Instagram (USA) ! die App-Bestätigung wählen, nicht SMS.	Die allermeisten erfolgreichen Konto-Hacks treffen Konten ganz ohne zweite Bestätigung.
E-Mail-Postfach besonders schützen	Ihr wichtigstes E-Mail-Konto bekommt das stärkste Passwort und die zweite Bestätigung. Prüfen Sie, welche Handynummer/Ersatz-Mail hinterlegt ist.	Über die E-Mail werden fast alle anderen Passwörter zurückgesetzt. Fällt sie, fällt alles.

In der ersten Woche

Was	So machen Sie es	Warum es so wichtig ist
Passwort-Manager einrichten	Für jedes Konto ein eigenes, langes Passwort — der Manager merkt sie sich für Sie. Passwörter nicht mehr regelmäßig „auf Verdacht“ wechseln, sondern nur, wenn es einen Anlass gibt (z. B. ein Datenleck).	So kann ein geklautes Passwort nicht für Ihre anderen Konten benutzt werden.
Stärkere zweite Bestätigung	Am sichersten: ein kleiner Sicherheits-Stick (z. B. YubiKey — EU/Schweden) oder ein Passkey. Gut: eine Code-App (z. B. Aegis). Nur im Notfall: Code per SMS.	SMS-Codes lassen sich leichter abfangen. Stick und Passkey schützen auch gegen trickreiche Betrugsseiten.
Apple-ID absichern	Bei der Apple-ID (USA) !: zweite Bestätigung an, einen Wiederherstellungs-Schlüssel und eine Vertrauensperson hinterlegen, Code-Sperre + Face/Touch ID auf dem Gerät.	Die Apple-ID öffnet all Ihre Apple-Geräte und die iCloud. Ein zentraler Schlüssel.

Was	So machen Sie es	Warum es so wichtig ist
Sicherungskopien anlegen (3-2-1)	Drei Kopien Ihrer Daten, auf zwei verschiedenen Speichern, eine davon außer Haus oder offline (z. B. externe Festplatte im Schrank). iCloud (USA) ! allein reicht nicht.	Der einzige verlässliche Schutz, wenn Erpressungs-Software zuschlägt oder ein Gerät kaputtgeht.

Im ersten Monat

Was	So machen Sie es	Warum es so wichtig ist
Schutzsoftware installieren	Ein modernes Schutzprogramm, z. B. Bitdefender oder ESET (beide EU). Nicht-EU-Alternativen: Sophos (UK) !, Microsoft Defender (USA) !. Kosten meist rund 4–7 € pro Gerät und Monat.	Erkennt und blockt Schadprogramme automatisch. Wichtige Grundschicht — aber nicht der einzige Schutz.
Automatische Updates einschalten	iPhone, iPad, Mac und Apps auf „automatisch aktualisieren“ stellen. Programme nur aus dem offiziellen App Store laden.	Updates schließen Sicherheitslücken. Einer der wirksamsten Schutzschritte überhaupt.
Social Media aufräumen	Bei Instagram/Facebook: zweite Bestätigung an, aktive Anmeldungen und Login-Warnungen prüfen, alte verbundene Apps entfernen, Privates und Geschäftliches trennen.	Weniger Angriffsfläche — und ein Hack springt nicht so leicht auf andere Konten über.
Vorsicht bei E-Mails & Links	Nie über einen zugesandten Link einloggen. Achtung: Betrugs-Mails sehen 2026 oft täuschend echt aus — auf Rechtschreibung ist kein Verlass. Im Zweifel über einen zweiten Weg nachfragen (z. B. anrufen).	Die meisten Angriffe beginnen mit einer gefälschten E-Mail. Der Virenschutz hilft hier nicht.

Immer wieder (kleine Routine)

- **Einmal im Monat:** Prüfen, ob eine Ihrer E-Mail-Adressen in einem Datenleck auftaucht (kostenlos beim HPI Identity Leak Checker — EU/Deutschland). Aktive Anmeldungen bei den wichtigsten Konten durchsehen. Eine Sicherungskopie machen.
- **Alle drei Monate:** Einmal ausprobieren, ob sich die Daten aus dem Backup wirklich zurückholen lassen. Ungenutzte App-Verbindungen entfernen.
- **Bei Anlass:** Nach einem Datenleck das betroffene Passwort wechseln.

> **Ehrlich gesagt: Was Schutzsoftware NICHT kann**
>
> Ein Schutzprogramm ist wichtig, aber kein Wachdienst rund um die Uhr. Es hilft nicht, wenn jemand einfach Ihr Passwort errät oder Sie auf eine Betrugsseite locken — dagegen helfen Passkeys und die zweite Bestätigung. Und: Ein Programm schützt nur, wenn es eingeschaltet ist und Sie auf seine Meldungen reagieren.

Dieses Zusammenfassung wurde mit einem ki-generierten Tool unterstützt und redaktionell von einer IT-Forensik überarbeitet und geprüft. Es können dennoch Fehler enthalten, die Aktualität verändert sein und übernimmt keine Haftung in rechtlicher Form oder zu nicht korrekter Handhabung. (Hamburg, 10.08.2026)

Teil 2 · Notfall: Ein Konto wurde gehackt

Ruhig bleiben — und der Reihe nach vorgehen

Die Reihenfolge ist entscheidend. Fangen Sie immer beim E-Mail-Konto an, denn darüber laufen alle Passwort-Zurücksetzungen. Arbeiten Sie die Schritte von oben nach unten ab.

Was Sie sofort tun

	Schritt	So gehen Sie vor
1	Zuerst wieder Zugang bekommen — beim E-Mail-Konto anfangen	Noch eingeloggt? Passwort ändern, dann alle anderen Geräte/Anmeldungen abmelden, danach die zweite Bestätigung (2FA) oder einen Passkey einschalten. Ausgesperrt? „Passwort vergessen“ nutzen. Klappt das nicht: an den offiziellen Support wenden (z. B. Apple (USA) ! oder das „Konto gehackt“-Formular bei Instagram/Facebook (USA) !).
2	Verhindern, dass es sich ausbreitet	Im Konto nachsehen und Verdächtiges entfernen: heimliche E-Mail-Weiterleitungen, geänderte Ersatz-Adresse oder -Nummer, neu verbundene Apps. Wirkt das Gerät befallen? Erst aktualisieren, unbekannte Apps löschen; im Ernstfall das Gerät zurücksetzen und aus einer sauberen Sicherungskopie neu aufsetzen. Warnen Sie Ihre Kontakte, falls in Ihrem Namen Nachrichten verschickt wurden.
3	Geldschaden begrenzen	Bank oder Zahlungsdienst informieren, unbekannte Abbuchungen reklamieren. Bei Kartenmissbrauch die Karte sperren: Sperr-Notruf 116 116. Hinterlegte Zahlungsmittel aus dem gehackten Konto entfernen.
4	Beweise sichern und Anzeige erstatten (Hamburg)	Machen Sie Screenshots: verdächtige Nachrichten, Zeitpunkte, Abbuchungen, fremde Anmeldungen. Anzeige online über die Onlinewache der Polizei Hamburg (portal.onlinewache.polizei.de/de/hh) — rund um die Uhr, ohne Anmeldung; oft auch für die Versicherung nötig. Bei akuter Bedrohung: Notruf 110.
5	Nur für Selbständige: Meldepflicht prüfen	Sind fremde persönliche Daten betroffen (z. B. Daten Ihrer Kundinnen und Kunden) und besteht für diese ein Risiko? Dann müssen Sie das binnen 72 Stunden nach Bekanntwerden beim Hamburgischen Datenschutzbeauftragten (HmbBfDI) melden — Formular auf datenschutz-hamburg.de. Lieber vorläufig melden, auch wenn noch nicht alles klar ist. Bei hohem Risiko zusätzlich die Betroffenen informieren.
6	Kostenlose, seriöse Hilfe holen	BSI (Bundesamt für Sicherheit in der Informationstechnik): Notfall-Checklisten und Bürger-Hotline zur Orientierung. Verbraucherzentrale Hamburg bei Betrug oder Identitätsdiebstahl. Werden in Ihrem Namen Forderungen gestellt: eventuell eine Anwältin/einen Anwalt hinzuziehen.

Wichtige Nummern (am besten ausdrucken)

Wofür	Kontakt	Erreichbar
Karte/Konto sperren	Sperr-Notruf 116 116	rund um die Uhr
Akute Bedrohung	Polizei-Notruf 110	rund um die Uhr
Anzeige erstatten	Onlinewache Polizei Hamburg	rund um die Uhr, online
Datenpanne melden	HmbBfDI · datenschutz-hamburg.de	werktags / online

Wofür	Kontakt	Erreichbar
Orientierung/Beratung	BSI-Bürgerhotline	werktags
Betrug/Identität	Verbraucherzentrale Hamburg	werktags

Kurz gemerkt: die Notfall-Reihenfolge

E-Mail sichern → Passwörter ändern und überall abmelden → zweite Bestätigung anschalten → Einstellungen säubern → Geld stoppen → Beweise sichern → Anzeige (Onlinewache Hamburg) → als Selbständige/r: 72-Stunden-Meldung prüfen → Hilfe bei BSI oder Verbraucherzentrale.

Teil 3 · Checkliste zum Ausdrucken

Schutz — zum Abhaken

- ☐ Passkeys eingeschaltet, wo möglich
- ☐ Zweite Bestätigung (2FA) überall an: E-Mail, Apple-ID, Banking, Cloud, Social Media
- ☐ E-Mail-Konto besonders geschützt
- ☐ Passwort-Manager: für jedes Konto ein eigenes langes Passwort
- ☐ Apple-ID: Wiederherstellungs-Schlüssel und Vertrauensperson hinterlegt
- ☐ Sicherheits-Stick oder Passkey als stärkste Bestätigung
- ☐ Sicherungskopien (3-2-1) angelegt und einmal getestet
- ☐ Schutzsoftware installiert und aktiv
- ☐ Automatische Updates an, Apps nur aus dem App Store
- ☐ Social Media aufgeräumt: Anmeldungen und verbundene Apps geprüft

Notfall — die Reihenfolge

1. E-Mail zuerst sichern
2. Passwörter ändern und überall abmelden
3. Zweite Bestätigung anschalten
4. Weiterleitungen und verbundene Apps prüfen
5. Geld stoppen (116 116)
6. Beweise sichern (Screenshots)
7. Anzeige bei der Onlinewache Hamburg
8. Als Selbständige/r: 72-Stunden-Meldung prüfen
9. Hilfe bei BSI / Verbraucherzentrale

Hinweis zu Anbietern und Datenschutz: *Dienste mit (USA)/(UK) ! sitzen außerhalb der EU; dabei können Daten ins Ausland übertragen werden. Wo eine gleichwertige EU-Lösung besteht, ist sie vorzuziehen. Produktnamen sind nur Beispiele, keine Kaufempfehlung; Preise und Funktionen können sich ändern. Dieser Plan gibt allgemeine Orientierung und ist keine Rechts- oder Anlageberatung.*