1 WENIGER DATEN HABEN ●●○



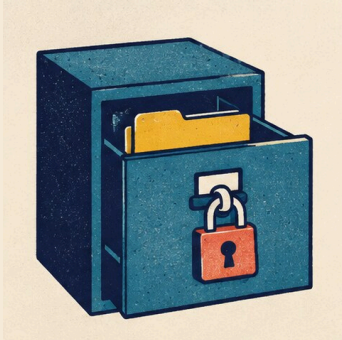
Weniger abfragen

Wir fragen nur ab, was wir wirklich brauchen. Dann gibt es bei einem Angriff weniger zu stehlen.

HABEN WIR DAS SCHON?

Ja, wenn unser wichtigstes Formular nicht nach Gesundheit, Herkunft oder Meinung fragt und kein freies Feld für Bemerkungen zu Personen hat. Auch im zuletzt ausgefüllten Bogen steht nichts davon.

2 WENIGER DATEN HABEN ●●○



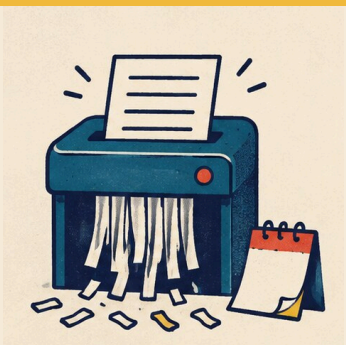
Sicherer Ordner statt Mail

Heikle Daten liegen in einem geschützten Ordner, nicht in Mails oder Chats. So findet ein Angreifer sie nicht in jedem Postfach.

HABEN WIR DAS SCHON?

Ja, wenn bei den letzten 3 Einsätzen oder Veranstaltungen niemand eine Liste mit Namen per Mail oder Chat bekommen hat.

3 WENIGER DATEN HABEN ●●○



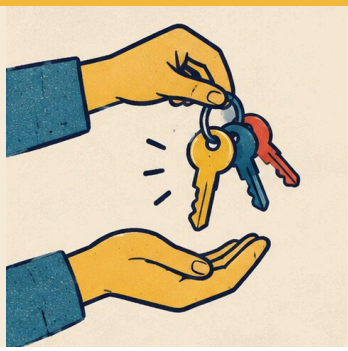
Regelmäßig löschen

Alte Daten löschen wir regelmäßig, im Postfach und bei den Ehrenamtlichen. So gibt es weniger zu stehlen.

HABEN WIR DAS SCHON?

Ja, wenn wir aufgeschrieben haben, wie lange wir Daten aufheben, und keine heikle Mail im Postfach älter ist.

4 WENIGER DATEN HABEN ●●○



Zugriff begrenzen

Jede Person sieht nur die Daten für ihre Aufgabe. Wird ein Konto gehackt, ist weniger betroffen.

HABEN WIR DAS SCHON?

Ja, wenn wir für unsere Kontaktliste von Mitgliedern und Ehrenamtlichen wissen, wer sie öffnen kann. Das sind nur die, die sie brauchen. Es gibt keine Freigabe „Jeder mit dem Link“.

2 Sicherer Ordner statt Mail

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Legt einen Ordner an, den der Verein verwaltet, zum Beispiel in der Vereins-Cloud (Speicher im Internet). Nur wer ihn braucht, bekommt Zugriff.
2. Verschickt Links, die nach ein paar Tagen ablaufen, statt Dateien im Anhang.
3. Regel für alle: Listen mit Namen und Adressen nicht weiterleiten, nicht in Chatgruppen stellen und nicht auf private Geräte laden.
4. Kommt doch etwas Heikles per Mail, legt es ab und löscht die Mail. Sagt dem Absender freundlich den neuen Weg.

1 Weniger abfragen

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Nehmt euer wichtigstes Formular, etwa die Anmeldung oder die Kontaktliste.
2. Fragt bei jedem Feld: Wofür brauchen wir das? Gibt es keinen klaren Grund, streicht das Feld.
3. Ersetzt freie Felder wie „Bemerkungen“ durch Angaben ohne Namen: „1 Kind mit Allergie, die Begleitperson hat das Notfallset.“
4. Schickt das neue Formular an alle Partner. Schreibt dazu: Bitte keine Namen, Diagnosen oder Einschätzungen.
5. Braucht ihr eine heikle Angabe doch, dann gelten dafür die Karten 2, 3 und 4.

VORLAGE DAZU Formular ohne Namen (Vorlage 8)

4 Zugriff begrenzen

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Listet eure geteilten Ordner, Tabellen und Chats auf.
2. Schreibt zu jedem dazu: Wer braucht das wirklich für seine Aufgabe?
3. Nehmt allen anderen den Zugriff weg. Ehrenamtliche sehen nur ihren eigenen Einsatz.
4. Ersetzt „Jeder mit dem Link“ durch Freigaben für einzelne Personen.
5. Prüft die Freigaben zweimal im Jahr.

3 Regelmäßig löschen

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Schreibt für eure heikelsten Daten auf, wie lange ihr sie braucht. Beispiel: Gruppenbögen bis 14 Tage nach dem Termin.
2. Tragt einen festen Löschtermin in den Kalender ein, zum Beispiel jeden ersten Montag im Monat.
3. Löscht dann überall: Posteingang, „Gesendet“, Papierkorb, Cloud und Download-Ordner.
4. Erinnert Ehrenamtliche nach jedem Einsatz daran, ihre Unterlagen zu löschen.
5. Was ihr laut Gesetz aufheben müsst, etwa die Buchhaltung, bleibt. Legt es getrennt ab.

5 WENIGER DATEN HABEN ●○○



Zugänge beim Austritt sperren

Wer geht, verliert in derselben Woche alle Zugänge. Kein altes Konto bleibt offen.

HABEN WIR DAS SCHON?

Ja, wenn es eine Austrittsliste mit zuständiger Person gibt und beim letzten Austritt in einer Woche alles gesperrt war.

6 WENIGER DATEN HABEN ●●○



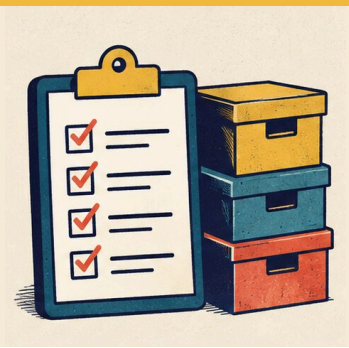
Wohnadressen schützen

Wohnadressen unserer Leute stehen in keiner geteilten Liste. Wer bedroht wird, lässt die Adresse beim Meldeamt sperren.

HABEN WIR DAS SCHON?

Ja, wenn keine geteilte Liste Wohnadressen von Ehrenamtlichen oder Mitgliedern enthält.

7 WENIGER DATEN HABEN ●●○



Wissen, welche Daten wir haben

Eine Seite zeigt, welche Daten wir wo haben. Nach einem Angriff sehen wir schnell, wen es betrifft.

HABEN WIR DAS SCHON?

Ja, wenn die Liste höchstens ein Jahr alt ist und für alle Daten nennt, wo sie liegen und wann wir sie löschen.

8 GUT ABSICHERN ●●○



Passkey fürs Postfach

Wir melden uns im Postfach mit einem Passkey an, also mit Handy oder Laptop statt Passwort. Ein gestohlenes Passwort reicht dann nicht.

HABEN WIR DAS SCHON?

Ja, wenn man ins Postfach mit den heikelsten Daten nur mit Passkey oder Sicherheitsschlüssel kommt, nicht mit dem Passwort allein.

6 Wohnadressen schützen

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Löscht Wohnadressen aus geteilten Tabellen. Braucht ihr sie für Fahrtkosten, speichert sie getrennt, nur für die Kasse.
2. Sucht Wohnadressen auf eurer Website, in alten Flyern und im Impressum. Nehmt dort, wo es geht, die Adresse des Vereins.
3. Wer bedroht wird, kann beim Meldeamt eine Auskunftssperre beantragen. Dann gibt das Amt die Adresse nicht heraus. Der Verein bestätigt die Bedrohung schriftlich.
4. Veröffentlicht Namen und Fotos von Ehrenamtlichen nur, wenn sie zugestimmt haben.

5 Zugänge beim Austritt sperren

SO SETZT IHR ES UM · ●○○ UNTER EINER STUNDE

1. Schreibt auf, was jemand bei euch bekommt: Postfach, Cloud, Chatgruppen, geteilte Passwörter, Schlüssel.
2. Geht jemand, hakt die Liste ab: Zugänge sperren, geteilte Passwörter ändern.
3. Bittet darum, Vereinsdaten auf privaten Geräten zu löschen. Lasst euch das bestätigen.
4. Benennt eine Person, die sich darum kümmert.

VORLAGE DAZU Austrittsliste (Vorlage 6)

8 Passkey fürs Postfach

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Sucht in den Einstellungen des Postfachs „Passkey“ oder „Sicherheitsschlüssel“. Oder fragt euren Anbieter nach FIDO2.
2. Richtet für jedes Postfach mit Personendaten einen Passkey auf Handy oder Laptop ein. Oder nutzt einen Sicherheitsschlüssel, einen Stick. Legt einen zweiten als Reserve an.
3. Schaltet unsichere Wege ab, wo es geht: Code per SMS, Sicherheitsfragen.
4. Fragt euren Anbieter, ob der Schutz auch in Mail-Programmen gilt (Abruf per IMAP). Wenn nicht, lest Mails nur im Browser oder in der Anbieter-App.
5. Gibt es keinen Passkey, nehmt Karte 9. Achtet beim nächsten Anbieterwechsel darauf.

7 Wissen, welche Daten wir haben

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Nehmt ein Blatt mit 4 Spalten: Welche Daten? Wozu? Wo liegen sie? Wann löschen wir sie?
2. Geht eure Aufgaben durch: Mitglieder, Ehrenamtliche, Anmeldungen, Spenden, Rundbrief.
3. Markiert, was heikel ist: Kinder, Gesundheit, Herkunft, Meinungen, Wohnadressen.
4. Legt die Liste zur Notfallkarte. Im Ernstfall seht ihr dann schnell, wen es betrifft.
5. Seht sie einmal im Jahr durch.

VORLAGE DAZU Datenliste (Vorlage 2)

9 GUT ABSICHERN ●○○



Anmelde-Code per App

Zum Passwort kommt ein Code aus einer Handy-App. Das schützt vor gestohlenen Passwörtern, aber nicht immer vor gefälschten Seiten.

HABEN WIR DAS SCHON?

Ja, wenn alle Postfächer mit Personendaten beim Anmelden einen Code oder Passkey verlangen.

10 GUT ABSICHERN ●●○



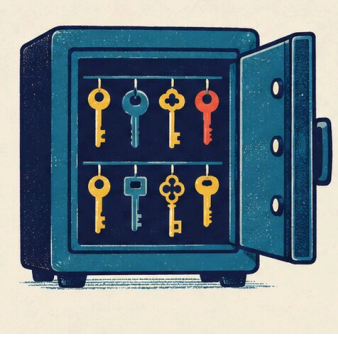
Anmelde-Code für alle Konten

Auch Cloud, Website und soziale Medien verlangen einen App-Code. Wer unser Postfach hat, kommt so nicht überall hinein.

HABEN WIR DAS SCHON?

Ja, wenn jedes Konto mit Personendaten einen Code oder Passkey verlangt, der nicht per Mail kommt.

11 GUT ABSICHERN ●●○



Passwort-Manager

Ein Programm merkt sich für jedes Konto ein eigenes Passwort. Wird eines gestohlen, sind die anderen sicher.

HABEN WIR DAS SCHON?

Ja, wenn alle im Team einen Passwort-Manager nutzen und kein Passwort doppelt vorkommt.

12 GUT ABSICHERN ●○○



Postfach-Einstellungen prüfen

Das Postfach warnt uns bei fremden Anmeldungen. Einmal im Monat prüfen wir, ob Mails heimlich weitergeleitet werden.

HABEN WIR DAS SCHON?

Ja, wenn wir in den letzten 30 Tagen Weiterleitungen und Filter unserer Postfächer geprüft haben.

10 Anmelde-Code für alle Konten

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Nehmt die Kontoliste (Karte 13) zur Hand.
2. Schaltet den Anmelde-Code bei jedem Konto mit Personendaten ein. Auch bei Website und sozialen Medien.
3. Ein Code per Mail hilft wenig. Wer das Postfach hat, bekommt ihn auch. Nutzt Passkey oder App-Code.
4. Gebt bei sozialen Medien besser jeder Person einen eigenen Zugang. Sonst legt den Code im gemeinsamen Passwort-Manager ab.

9 Anmelde-Code per App

SO SETZT IHR ES UM · ●○○ UNTER EINER STUNDE

1. Ladet eine Code-App (Authenticator) aufs Handy.
2. Schaltet im Postfach die „Zwei-Faktor-Anmeldung“ ein. Scannt den QR-Code mit der App.
3. Druckt die Ersatzcodes aus und legt sie verschlossen ab.
4. Macht das für alle, die an Personendaten kommen.
5. Gebt den Code nur auf Seiten ein, die ihr selbst aufgerufen habt. Nie nach einem Klick in einer Mail.

12 Postfach-Einstellungen prüfen

SO SETZT IHR ES UM · ●○○ UNTER EINER STUNDE

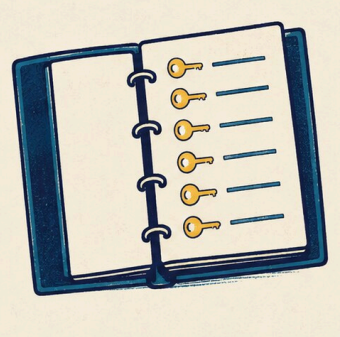
1. Schaltet in den Sicherheitseinstellungen die Warnung bei Anmeldung von neuen Geräten ein, falls es sie gibt.
2. Öffnet die Einstellungen „Weiterleitung“ und „Filter“ oder „Regeln“. Steht dort etwas, das keiner von euch angelegt hat?
3. Seht euch die Liste der angemeldeten Geräte an und meldet unbekannte ab.
4. Macht daraus einen festen Termin: einmal im Monat, 5 Minuten.

11 Passwort-Manager

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Wählt einen Passwort-Manager für das Team. Es gibt gute kostenlose und Rabatte für Vereine.
2. Sichert ihn mit einem langen Hauptpasswort und einem Anmelde-Code.
3. Lasst für jedes Konto ein neues Passwort erzeugen. Fangt beim Postfach an.
4. Lasst den Manager die Passwörter ausfüllen. Auf einer gefälschten Seite tut er das nicht. Dann solltet ihr misstrauisch werden.
5. Teilt gemeinsame Zugänge im Manager und nie im Chat.

13 GUT ABSICHERN ●○○



Liste aller Konten

Eine Liste zeigt alle Konten des Vereins und wer sie verwaltet. So vergessen wir keines, wenn wir etwas sperren müssen.

HABEN WIR DAS SCHON?

Ja, wenn die Liste zu jedem Konto die Verwalter und die Adresse für „Passwort vergessen“ nennt.

14 GUT ABSICHERN ●●○



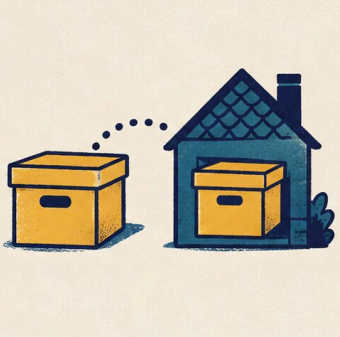
Handys und Laptops sichern

Alle Geräte mit Vereinsdaten haben Sperre, Updates und Verschlüsselung, auch private. Geht eins verloren, kommt keiner an die Daten.

HABEN WIR DAS SCHON?

Ja, wenn alle im Kernteam die 4 Punkte für ihre Geräte bestätigen und die Ehrenamtlichen sie schriftlich haben.

15 GUT ABSICHERN ●●○



Sicherungskopie

Von wichtigen Daten gibt es eine Kopie, an die ein Angreifer nicht herankommt. So holen wir verlorene Daten zurück.

HABEN WIR DAS SCHON?

Ja, wenn unsere letzte Kopie höchstens einen Monat alt ist und wir das Zurückholen einmal geübt haben.

16 GUT ABSICHERN ●●○



Echte Mails von uns erkennen

Unsere Leute wissen, wie echte Mails von uns aussehen. Bei Zweifeln rufen sie an, auch wenn die Mail von unserer Adresse kommt.

HABEN WIR DAS SCHON?

Ja, wenn Ehrenamtliche und Partner im letzten Jahr schriftlich erfahren haben, wie wir Unterlagen schicken und wen sie im Zweifel anrufen.

14 Handys und Laptops sichern

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Bildschirmsperre mit Code oder Fingerabdruck, die nach wenigen Minuten von selbst angeht.
2. Automatische Updates für Betriebssystem, Browser und Apps einschalten.
3. Speicher verschlüsseln. Neue Handys tun das von selbst. Am Laptop schaltet ihr es in den Einstellungen ein.
4. Auf geteilten Familiengeräten ein eigenes Benutzerkonto anlegen.
5. Gebt die 4 Punkte allen Ehrenamtlichen als Liste zum Abhaken mit. Ihr kontrolliert ihre Geräte nicht.

VORLAGE DAZU Vier Punkte für private Geräte (Vorlage 5)

13 Liste aller Konten

SO SETZT IHR ES UM · ●○○ UNTER EINER STUNDE

1. Sammelt alle Konten: Mail, Cloud, Chat, Website, Rundbrief, Bank, soziale Medien, Internetadresse.
2. Notiert zu jedem: Wem gehört es? Wer verwaltet es? An welche Adresse geht „Passwort vergessen“?
3. Jedes Konto braucht 2 Verwalter und läuft auf eine Mailadresse des Vereins.
4. „Passwort vergessen“ sollte an euer am besten geschütztes Postfach gehen.
5. Legt die Liste zur Notfallkarte und prüft sie zweimal im Jahr.

VORLAGE DAZU Kontoliste (Vorlage 3)

16 Echte Mails von uns erkennen

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Sagt allen: Wir fragen nie per Mail nach Passwörtern. Unterlagen schicken wir immer auf demselben Weg.
2. Nennt eine Telefonnummer für Rückfragen. Wer zweifelt, ruft an und klickt nicht.
3. Sagt es bei jeder Einweisung und einmal im Jahr im Rundbrief.
4. Fragt euren Anbieter nach SPF, DKIM und DMARC für eure Internetadresse. Das erschwert gefälschte Absender. Es hilft nicht, wenn jemand euer echtes Postfach übernommen hat.

15 Sicherungskopie

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Fragt euch: Was brauchen wir, um nächste Woche weiterzuarbeiten? Kontakte, Termine, Finanzen, Website.
2. Kopiert das regelmäßig an einen zweiten Ort: externe Festplatte oder zweiter Cloud-Dienst.
3. Verschlüsselt die Kopie, gebt ihr ein eigenes Passwort und trennt sie danach.
4. Probiert einmal aus, eine Datei zurückzuholen.
5. Auch in der Kopie löscht ihr alte Daten.

17 VORBEREITET SEIN ●●○



Betrugs-Mails erkennen

Alle kennen typische Tricks wie Zeitdruck und gefälschte Anmeldeseiten. Im Zweifel rufen wir an und fragen nach.

HABEN WIR DAS SCHON?

Ja, wenn Team und Ehrenamtliche im letzten Jahr dazu eine Übung hatten.

18 VORBEREITET SEIN ●○○



Probleme sofort melden

Wer etwas Seltsames bemerkt oder falsch klickt, sagt es sofort einer festen Person. Dafür gibt es keinen Ärger.

HABEN WIR DAS SCHON?

Ja, wenn 3 Leute aus Team und Ehrenamt auf die Frage, wem sie einen Verdacht melden, dieselbe Person nennen.

19 VORBEREITET SEIN ●○○



Notfallkarte

Eine Seite an der Wand sagt, wer im Notfall entscheidet, wen wir anrufen und was wir zuerst tun.

HABEN WIR DAS SCHON?

Ja, wenn sie ausgefüllt aushängt und eine Vertretung nennt.

20 VORBEREITET SEIN ●○○



Eine Person spricht für uns

Im Ernstfall spricht eine Person für uns. Ein erster Text für Betroffene und Presse liegt schon bereit.

HABEN WIR DAS SCHON?

Ja, wenn Sprecher:in und Vertretung feststehen und der Text bereitliegt.

18 Probleme sofort melden

SO SETZT IHR ES UM · ●○○ UNTER EINER STUNDE

1. Benennt eine Notfallperson und eine Vertretung.
2. Sagt allen, auch den Ehrenamtlichen: Bei Verdacht, verlorenem Gerät oder falschem Klick sofort anrufen oder schreiben.
3. Versprecht: Wer etwas meldet, bekommt keinen Ärger. Schnelles Melden hilft allen.
4. Schreibt Namen und Nummer auf die Notfallkarte.

17 Betrugs-Mails erkennen

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Nehmt euch im nächsten Teamtreffen 20 Minuten. Zeigt eine Betrugs-Mail und sucht gemeinsam die Warnzeichen.
2. 3 Fragen bei Mails mit Link oder Anhang: Erwarte ich das? Stimmt die Adresse hinter dem Namen? Wohin führt der Link?
3. Meldet euch nie über einen Link aus einer Mail an. Ruft die Seite selbst auf.
4. Ruft im Zweifel an, unter der Nummer, die ihr schon kennt.
5. Wiederholt es jährlich, auch mit den Ehrenamtlichen.

20 Eine Person spricht für uns

SO SETZT IHR ES UM · ●○○ UNTER EINER STUNDE

1. Legt fest, wer für euch spricht und wer sie vertritt. Alle anderen schicken Fragen an diese Person.
2. Nutzt die Vorlage „Text für den Ernstfall“. 3 Absätze reichen.
3. Legt die Reihenfolge fest: erst die Betroffenen und Partner, dann die Öffentlichkeit.
4. Beschönigt nichts und vermutet nichts. Sagt ruhig: „Das wissen wir noch nicht.“
5. Notiert Beratungsstellen, falls danach Hetze gegen euch beginnt.

VORLAGE DAZU Text für den Ernstfall (Vorlage 7)

19 Notfallkarte

SO SETZT IHR ES UM · ●○○ UNTER EINER STUNDE

1. Füllt die Vorlage aus, die dem Spiel beiliegt: Notfallperson, Vertretung, Telefonnummern.
2. Tragt ein: Mail-Anbieter, Datenschutzbehörde eures Bundeslands, Polizei, Beratungsstellen.
3. Klärt, wer für euch spricht und wer der Datenschutzbehörde meldet.
4. Druckt sie aus: fürs Büro, für zu Hause, für den Geldbeutel. Im Ernstfall kommt ihr vielleicht nicht an eure Dateien.
5. Einmal im Jahr prüfen.

VORLAGE DAZU Notfallkarte (Vorlage 1)

21 VORBEREITET SEIN ●●○



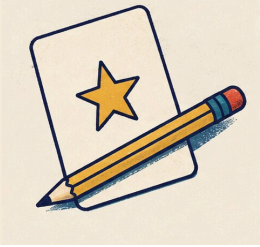
Ehrenamtliche einweisen

Neue Ehrenamtliche lernen unsere Regeln für Daten und unterschreiben, dass sie sich daran halten.

HABEN WIR DAS SCHON?

Ja, wenn alle aktiven Ehrenamtlichen, die Personendaten sehen, die Erklärung unterschrieben haben.

★ JOKER 1 VON 2



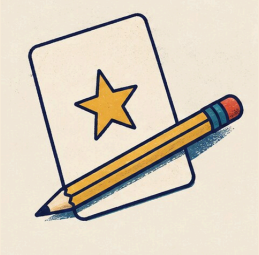
Joker

Mit dem Joker bringt ihr eigenen Schutz ins Spiel, der auf keiner Karte steht.

UNSER SCHUTZ

DARAN SIEHT MAN ES HEUTE

★ JOKER 2 VON 2



Joker

Mit dem Joker bringt ihr eigenen Schutz ins Spiel, der auf keiner Karte steht.

UNSER SCHUTZ

DARAN SIEHT MAN ES HEUTE

? ÜBERSICHT · LIEGT IN DER MITTE

Eine Runde

1. **Vorlesen** 2 Min.
   Halte das Szenenblatt hoch, mit dem Bild zum Team. Lies die Rückseite vor. Dann stell dem Team die Frage.
2. **Beraten** 4 Min.
   Leg das Blatt mit dem Bild nach oben in die Mitte. Darauf stehen die Frage und 3 Fragen fürs Gespräch. Das Team sucht im Stapel „Haben wir“ Karten, die jetzt helfen. Es legt sie neben das Blatt.
3. **Auflösen** 3 Min.
   Nimm das Blatt auf. Lies vor, welche Karten den Angriff stoppen und welche den Schaden kleiner machen.
4. **Schaden** 1 Min.
   Das Team legt Marken auf die Schadensleiste.
5. **Plan** 1 Min.
   Karten aus der Auflösung, die im Stapel „Noch nicht“ liegen, kommen auf das Feld „Plan“.
6. **Logbuch** 1 Min.
   Leo notiert den Schaden und einen Satz: Was nehmen wir aus dieser Runde mit?

★ Joker

SO SPIELT IHR IHN

1. Sagt, was ihr schon tut, das in dieser Runde hilft.
2. Sagt, woran man heute sieht, dass ihr das wirklich tut.
3. Glaubt euch die Spielleitung, gibt es in dieser Runde 1 Schaden weniger. Es bleibt aber mindestens 1.
4. Schreibt beides auf die Vorderseite. Danach könnt ihr den Joker nicht mehr nutzen.

Es gibt 2 Joker. Halb gemacht zählt nicht.

21 Ehrenamtliche einweisen

SO SETZT IHR ES UM · ●●○ EIN NACHMITTAG

1. Nutzt die Vorlage „Vertraulichkeitserklärung“: eine Seite, verständlich geschrieben.
2. Erklärt bei der Einweisung 3 Regeln: nichts weiterleiten, nach dem Einsatz löschen, Verdacht sofort melden.
3. Gebt die 4 Punkte für private Geräte mit (Karte 14).
4. Bewahrt die unterschriebenen Erklärungen geordnet auf.
5. Wiederholt die Einweisung einmal im Jahr.

VORLAGE DAZU Vertraulichkeitserklärung (Vorlage 4)

? Schaden

Der Schaden ist euer Punktestand. Je weniger, desto besser.

- Jede Runde bringt erst einmal **3 Schaden**.
- Für jede Karte im Stapel „Haben wir“, die den Schaden **kleiner macht**: 1 Schaden weniger, aber nie unter 1.
- Habt ihr eine Karte, die den Angriff **stoppt**, ist der Schaden **0**.
- Jede passende Karte im Stapel „Haben wir“ zählt, auch wenn niemand sie gelegt hat.

0–6	**Leicht.** Der Angriff macht Arbeit. Aber kaum jemand wird geschädigt. Bleibt dran und erledigt, was noch fehlt.
7–12	**Mittel.** Menschen, die euch vertrauen, sind betroffen. Ihr habt einiges richtig gemacht. Euer Plan zeigt, was ihr jetzt tut.
13–18	**Schwer.** Der Angreifer kommt an fast alle Daten. So ginge es heute den meisten Vereinen. Euer Plan ändert das.

★ Joker

SO SPIELT IHR IHN

1. Sagt, was ihr schon tut, das in dieser Runde hilft.
2. Sagt, woran man heute sieht, dass ihr das wirklich tut.
3. Glaubt euch die Spielleitung, gibt es in dieser Runde 1 Schaden weniger. Es bleibt aber mindestens 1.
4. Schreibt beides auf die Vorderseite. Danach könnt ihr den Joker nicht mehr nutzen.

Es gibt 2 Joker. Halb gemacht zählt nicht.