Nicht erstarren, sondern handeln!

Was können Sie tun, um in einer Krisensituation handlungsfähig zu bleiben und sich sicher zu fühlen? Und wer übernimmt welche Aufgaben?

Analoge Sicherheit

Was sollten Sie tun?	Was erreichen Sie damit und wer ist verantwortlich?
Polizeistation vor Ort kontaktieren und ein Sicherheitsgespräch verlangen	Einschätzung der Gefahrensituation durch Expert*innen gibt Ihnen Kontrolle und Handlungsfähigkeit. **Sicherheitsbeauftragte*r:** **In Absprache mit Beobachter*in der Angriffe:**
Rechtssichere Screenshots erstellen	Rechtssichere Screenshots dokumentieren den Verlauf und die Inhalte dauerhaft. Dies ist wichtig, wenn Sie sich auch rechtlich zur Wehr setzen wollen, z. B. durch eine Anzeige bei der Polizei. Weitere Informationen und Anleitungen finden Sie auf unserer Webseite. **Community Manager*in:**
Melderegisteraus-kunftssperre beantragen	Mehr Informationen hierzu finden Sie im Hauptteil des Krisenplans. Bedenken Sie, dass Ihre Adresse eventuell an weiteren Stellen leicht in Erfahrung gebracht werden kann und informieren Sie sich frühzeitig über Schutzmöglichkeiten. **Privatsphäre-Hüter*in:**
Routinen verändern und Alleinsein vermeiden	Variieren Sie Ihre täglichen Abläufe, um schwerer auffindbar zu sein und bleiben Sie möglichst in Begleitung, besonders an öffentlichen Orten. **Selbstständig organisieren**
Übernachtungsort kurz-fristig wechseln	So können Sie vorübergehend Schutz und Distanz bei akuten Drohungen schaffen und analoge Angriffe vermeiden. Erstellen Sie präventiv eine Liste an Menschen, die Ihnen nahestehen und bei denen Sie für eine Übergangszeit unterkommen können. **Selbstständig organisieren**
Soziales Umfeld infor-mieren und sensibili-sieren	Sie sensibilisieren Ihr soziales Umfeld, z. B. Familie, Bekannte und Nachbar*innen, für Ihre Situation und bekommen ggf. emotionale Unterstützung. Sensibilisieren Sie auch Bildungseinrichtungen Ihrer Familienmitglieder, besonders vorsichtig mit Ihren personenbezogenen Daten umzugehen. **Eigene Nachbar*innen selbstständig informieren.** **Büronachbar*innen übernimmt die*der Krisenkoordinator*in:**
Bei Veranstaltungen, auf denen Sie als Gast eingeladen sind: Anmeldeliste verlangen, Sicherheitspersonal organisieren und Hausregeln aufstellen lassen.	Sie erhalten einen Überblick, wer an Veranstaltungen teilnimmt und können sich vorbereiten und ggf. Gefahren abwenden. **Selbstständig in Absprache mit Safeguard für Netiquette:**
Konsequent Strafanzeige erstatten	Durch Anzeigen wird die Polizei über Ihre Situation informiert und kann ggf. Sicherheitsmaßnahmen ergreifen. Darüber hinaus können unbekannte Täter*innen durch geeignete Ermittlungsmaßnahmen ggf. identifiziert und in der Folge zur Rechenschaft gezogen werden. **Sicherheitsbeauftragte*r ggf. zusammen mit der Person, gegen die sich die Angriffe richten:**

Ihren Standpunkt vertreten

Was sollten Sie tun?	Was erreichen Sie damit und wer ist verantwortlich?
Statement veröffentlichen	Sie können Ihre eigene Position klar darstellen. **Pressesprecher*in:**
Lokalzeitung kontaktieren	Sie können Ihre eigene Position in unterschiedlichen Zielgruppen verbreiten und dem Thema mehr Glaubhaftigkeit und Wichtigkeit verleihen. **Pressesprecher*in:**

Digitale Sicherheit

Was sollten Sie tun?	Was erreichen Sie damit und wer ist verantwortlich?
Passwörter ändern	Starke Passwörter verringern das Hacking-Risiko. Ein Passwort-Manager kann Sie dabei unterstützen. Dabei handelt es sich um ein Tool, das sichere Passwörter generiert und diese in einer Datenbank für Sie speichert. **Selbstständig in Absprache mit IT-Sicherheitsbeauftragter*m:**
Zwei-Faktor-Authentifizierung einstellen	Die Zwei-Faktor-Authentifizierung erschwert Hacking-Angriffe, weil Sie sich nicht nur mit Ihrem Passwort, sondern mit einer zusätzlichen Information einloggen. Die Authentifizierung kann z. B. über einen Code erfolgen, der Ihnen per Mail zugesendet wird. **Selbstständig mit Unterstützung von IT-Sicherheitsbeauftragter*m:**
Sensible Informationen im Netz suchen und ggf. löschen	Sie schützen die eigene Privatsphäre. **Privatsphärehüter*in:** (ggf. HateAid zur Unterstützung kontaktieren)
Bei Hacking-Verdacht externe IT-Expertise einbeziehen	Hacking-Angriffe können unterschiedlich gefährlich sein. Mit externer Unterstützung können Sie die eigene IT-Sicherheit wiederherstellen und die Aufklärung des Vorfalls vorantreiben. **IT-Sicherheitsbeauftragte*r:**

Social-Media-Kommunikation

Was sollten Sie tun?	Was erreichen Sie damit und wer ist verantwortlich?
Kommentarfunktion auf den eigenen Social-Media-Kanälen einschränken	Passen Sie die Kommentareinstellungen in der Kommentarfunktion an (z.B.„öffentlich“ → „privat“, oder Blockliste für bestimmte Begriffe). **Community Manager*in:**
Bei Bedarf Social-Media-Konten für eine kurze Zeit deaktivieren	Ihr Konto wird nicht gelöscht, sondern für eine Zeit unsichtbar geschaltet. Wenn Sie Ihr Konto nach der Krise wieder verwenden wollen, müssen Sie sich in der Regel nur erneut einloggen. Damit endet die Deaktivierung. Das Konto zeitweise zu deaktivieren, kann zu mehr Entlastung und Abgrenzung beitragen. **Community Manager*in:**
Inhalte auf Social-Media-Plattformen melden	Wenn bereits rechtssichere Screenshots (siehe links) erstellt wurden, können Sie die Inhalte melden. Gemeldete Inhalte werden im besten Fall von den Plattformen gelöscht. **Community Manager*in:**
Angreifer*innen auf Social-Media-Plattformen blockieren	Wenn Sie die Profile der Angreifenden „melden“ und für sich „blockieren“, sehen diese Personen nicht, was Sie zukünftig veröffentlichen, und können Sie nicht kontaktieren. **Community Manager*in:**
Kommentare, die der Netiquette widersprechen, konsequent löschen	Sie zeigen Grenzen auf und schaffen einen sicheren Ort, für Menschen, die respektvoll mit Ihnen und mit anderen interagieren wollen. **Community Manager*in:** **in Absprache mit Safeguard für Netiquette:** gut
Unterstützer*innen aktivieren	Auf diese Weise können Sie auf Ihren Kanälen Unterstützung und Solidarität suchen und aktivieren, z. B. in Form von öffentlichem Zuspruch durch Kooperationspartner*innen oder Gegenrede. **Krisenkoordinator*in:** das funktioniert

Hate Aid