

Sicherheit von Amts- und Mandatsträgern

VERHALTENS-
EMPFEHLUNGEN



RheinlandPfalz

LANDESKRIMINALAMT

Wir möchten, dass Sie
sicher leben.



Inhalt

Vorwort	04
Allgemeine Verhaltensempfehlungen	06
Sicherheit im häuslichen Bereich	09
Post- und Warensendungen	10
Sicherheit zwischen Wohnung und Arbeitsplatz	11
Sicherheit am Arbeitsplatz	12
Sicherheit bei Veranstaltungen	13
Sicherheit im Netz und beim Umgang mit sozialen Medien	15
Hotline für Amts- und Mandatsträger	19
Weiterführende Informationen	20

Vorwort

Übergriffe auf Repräsentanten des Staates, sogenannte Amts- und Mandatsträger, häufen sich. Politiker und Personen des öffentlichen Lebens sehen sich aufgrund ihres Einsatzes für demokratische Werte, Ansichten oder Entscheidungen zunehmend Anfeindungen ausgesetzt. In der überwiegenden Mehrheit der Fälle geht es um schriftliche Drohungen und Hassmails. Doch auch tätliche Angriffe sind mittlerweile keine Seltenheit mehr, Autos werden angezündet, Partei- und Wahlkampfbüros beschmiert oder verwüstet.



Die folgenden Verhaltens-empfehlungen dienen der Sensibilisierung des Sicherheits- und Gefahrenbewusstseins. Sie sollen dem betroffenen Personenkreis dabei helfen, auf verschiedene Situationen, wie z.B. Bedrohungen und Übergriffe, gut vorbereitet zu sein und sicher handeln zu können. Die Empfehlungen richten sich an Amts- und Mandatsträger sowie weitere Personen, die aufgrund ihrer beruflichen oder ehrenamtlichen Tätigkeit im Fokus der Öffentlichkeit stehen.

Sollten Sie unsicher sein, wie Sie sich in konkreten Situationen zu verhalten haben, zögern Sie nicht und informieren Sie die Polizei unter der Notrufnummer 110.

Allgemeine Verhaltensempfehlungen

Seien Sie aufmerksam und nehmen Sie Ihre Umgebung bewusst wahr.

Halten Sie sich in der Öffentlichkeit nur an belebten Orten auf. Denken Sie an eine Begleitperson und begeben Sie sich nicht allein in kritische Situationen.

Führen Sie stets ein Mobiltelefon mit sich, um im Notfall Hilfe holen zu können.

Ihr analoger und digitaler Terminkalender sollte nicht öffentlich zugänglich sein. Dies gilt sowohl für Ihren persönlichen, dienstlichen

wie auch den sensiblen Bereich Ihrer öffentlichen Termine.

Melden Sie mögliche Gefahren bzw. verdächtige Wahrnehmungen und Straftaten (z.B. Beleidigungen, Bedrohungen, Sachbeschädigungen, etc.) unverzüglich der Polizei, damit diese schnell Hilfe leisten und mögliche weitere Gefahren und Straftaten abwenden kann. Wählen Sie im Zweifel den Polizeinotruf 110.

Leiten Sie Drohungen, die Sie elektronisch erhalten, nicht weiter, sondern warten Sie bis die Polizei die Nachricht gesichert hat.

Dokumentieren Sie das Gespräch detailliert (Inhalt des Gespräches / der Drohung oder Beleidigung, Ort bzw. Anschluss, Stimme des Anrufers, Datum, Uhrzeit, etc.).

Informieren Sie Angehörige oder auch Ihre Arbeitsstätte über Ihren Aufenthaltsort und Ihre voraussichtliche Rückkehrzeit.

Sie können beim Einwohnermeldeamt eine Auskunftssperre und bei der Zulassungsbehörde eine Übermittlungssperre für Ihr Kfz-Kennzeichen beantragen.





Sicherheit im häuslichen Bereich

Beratungsangebote

Ergreifen Sie technische Sicherungsmaßnahmen in Ihrer Wohnung / Ihrem Haus. Hierzu können Sie die kostenlose und herstellerneutrale kriminalpolizeiliche Beratung in Anspruch nehmen.

Vorsorgemaßnahmen

Schützen Sie Ihre Privatsphäre vor neugierigen Blicken durch Gardinen, Rollläden, Vorhänge, Plissees, etc.

Halten Sie Außentüren und Fenster bei Abwesenheit verschlossen und schalten Sie die Türklingel aus, um eine Anwesenheitskontrolle zu erschweren.

Umgang mit Fremden

Lassen Sie sich von unbekannten Personen den Ausweis zeigen. Verweigern Sie im Zweifel den Zutritt und informieren Sie die Polizei.

Nutzen Sie Türsprechanlagen und Türsicherungen (z.B. Kastenschloss

mit Sperrbügel) und gewähren Sie fremden Personen keinen Zutritt zu Ihrem Wohnobjekt.

Nutzen Sie - wenn möglich - nachbarschaftliche Hilfe.

Überprüfen Sie Ihr Wohnobjekt bei der Rückkehr nach einer längeren Abwesenheit auf Veränderungen.

Teilen Sie bei Gesprächen mit Fremden keine Informationen über Reisepläne oder zukünftige Vorhaben mit.



Post- und Warensendungen

Öffnen Sie keine verdächtigen Postsendungen und nehmen Sie keine unbestellten Warensendungen von Unbekannten entgegen.

Verdachtsmomente könnten sein:

- Übergewicht
- ungewöhnliches Format
- unbekannter oder fehlender Absender
- persönliche Zustellvermerke (eigenhändig, persönlich, nur durch zu öffnen)
- ausgetretene Inhaltsstoffe (z.B. Flüssigkeit oder Pulver).

Verdächtige Sendungen bitte nicht anfassen, sie könnten Spurenträger sein.

Bei einem begründeten Verdachtsfall:

- Sendung nicht berühren
- Fundort / Übergabeort verlassen
- andere Personen informieren und fernhalten
- Polizei verständigen.

Halten Sie für den Notfall Feuerlöscher und Löschdecke bereit und machen Sie sich im Vorfeld mit der Bedienung vertraut.

Sicherheit zwischen Wohnung und Arbeitsplatz

Parken Sie Ihr Kraftfahrzeug zu Hause möglichst in der Garage.

Überprüfen Sie in regelmäßigen Abständen die technische Sicherheit Ihres Fahrzeuges, insbesondere das Bremssystem, Radmuttern, Lenkung und Bereifung.

Halten Sie verdächtige Wahrnehmungen fest (Ort, Zeit, Fahrzeugtyp mit Kennzeichen, Personenbeschreibung).

Nutzen Sie ausschließlich vertrauenswürdige Kfz-Werkstätten.

Halten Sie sich bei Bahnreisen nach Möglichkeit in belebten Abteilen auf.

Steigen Sie nicht in Ihr Fahrzeug, wenn sich unbekannte Personen ohne eindeutig erkennbare Gründe oder in verdächtiger Weise in Fahrzeugnähe aufhalten oder das sofortige und zügige Abfahren durch parkende Fahrzeuge oder durch Gegenstände verhindert oder wesentlich erschwert wird.

Beobachten Sie vor der Abfahrt Ihre Umgebung hinsichtlich möglicher Auffälligkeiten. Variieren Sie nach Möglichkeit Ihre Fahrtstrecken und fahren Sie alternative Routen. Sollten Sie verfolgt werden, suchen Sie einen sicheren Ort, wie z.B. eine Polizeidienststelle oder einen belebten Platz, auf.





Sicherheit am Arbeitsplatz

Parken Sie Ihr Kraftfahrzeug auch am Arbeitsplatz möglichst in einer Garage oder in einem anderen gesicherten Bereich.

Veranlassen Sie nach Möglichkeit eine Zutrittskontrolle im Geschäftsbereich.

Richten Sie Ihr Büro so ein, dass Sie anderen Personen gegenüber sitzen und diese gut im Blick haben. Sie sollten im Notfall den kürzesten Weg zur Tür als Fluchtpunkt nutzen können. Der Fluchtweg sollte gut erreichbar und frei von Möbeln oder anderen Gegenständen sein.

Bewahren Sie keine Gegenstände auf dem Schreibtisch auf, die durch andere Personen als Angriffsmittel / Waffe verwendet werden können. Dazu zählen beispielsweise Scheren, Locher, Tacker und Brieföffner. Planen Sie den Ablauf für den Fall eines Angriffs. Auf Familienfotos sollte möglichst verzichtet werden.

Fremden gegenüber sollten Sie und auch Ihre Mitarbeitenden keine Auskünfte zu Ihrer Tätigkeit, Ihren Terminen, An- und Abwesenheitszeiten sowie persönlichen Verhältnissen erteilen; dies gilt insbesondere für telefonische Anfragen.

Sicherheit bei Veranstaltungen

Achten Sie bei der Wahl des Parkplatzes auf ausreichende Beleuchtung und stellen Sie Ihr Fahrzeug in Veranstaltungsnähe ab.

Besuchen Sie Veranstaltungen mit Zugang für jedermann nach Möglichkeit mit mindestens einer Begleitperson.

Informieren Sie sich beim Veranstalter über den geplanten Ablauf der Veranstaltung und die zu erwartende Teilnehmerzahl. Fragen Sie auch nach getroffenen

Sicherheitsmaßnahmen und nach den möglichen Fluchtwegen.

Melden Sie dem Veranstalter oder dem Sicherheitspersonal auffällige oder verdächtige Personen, damit ggf. eine Überprüfung erfolgen kann.

Halten Sie bei Gesprächen mit Fremden einen angemessenen Abstand. Lassen Sie sich nicht provozieren, brechen Sie bei einer sich andeutenden Eskalation das Gespräch ab und ziehen Sie sich zurück.





Sicherheit im Netz und beim Umgang mit sozialen Medien

Seien Sie bei der Nutzung des Internets und beim Umgang mit sozialen Medien wachsam und lassen Sie ein gesundes Misstrauen walten.

Datenspuren im Netz

Die Veröffentlichung persönlicher und sensibler Daten im Internet kann es Dritten ermöglichen, u.a. umfangreiche Verhaltensmuster oder Bewegungsprofile von Ihnen zu erstellen sowie Angehörige, Freunde oder sonstige Bezugspersonen zu identifizieren.

Insbesondere in sozialen Netzwerken und über andere Kommunikations-

medien sollten Sie mit dem Teilen von persönlichen Informationen vorsichtig sein. Teilen Sie nur solche Informationen, die Sie auch in der realen Welt einer beliebigen anderen Person mitteilen würden.

Dies gilt auch für Aussagen gegenüber Medienvertretern.

Beschränken Sie den Zugang zu Ihrem Profil und beachten Sie beim Anlegen Ihres Profils die Sicherheitseinstellungen für den privaten Bereich.

Prüfen Sie kritisch, welche Rechte Sie den Betreibern sozialer Netzwerke an den von Ihnen eingestellten Bildern, Texten und Informationen einräumen.

Urlaubs- und Reisepläne, hochgeladene Bilder oder Posts, die Rückschlüsse auf Ihre Abwesenheit oder Ihren Aufenthaltsort zulassen, sollten nicht veröffentlicht werden. Hier besteht die Gefahr, dass Ihre Abwesenheit von Dritten gezielt zum Einbruch in Ihre Wohn- oder Büroräume genutzt wird und dort Manipulationen jeglicher Art vorgenommen werden können. Darüber hinaus besteht die Gefahr, dass Ihnen Personen an den anderen Aufenthaltsort folgen.

Orientieren Sie sich gegebenenfalls am Social Media Leitfaden Ihrer Behörde.

Sicherheitseinstellungen im Netzwerk

Neben der freiwilligen Preisgabe von persönlichen Informationen im Internet besteht weiterhin die Gefahr, dass Dritte gegen Ihren Willen durch die Nutzung technischer Mittel auf Ihre Daten zugreifen. Dritte können auf vielfache Weise Schadsoftware auf Ihre elektronischen Geräte einspielen, über die beispielsweise Zugriff auf die gespeicherten Daten erlangt werden oder eine umfangreiche Überwachung Ihrer sämtlichen Aktivitäten mit den Geräten möglich sein kann.

Stellen Sie daher sicher, dass bei Ihrem Heimnetzwerk (Router) alle notwendigen Sicherheitsvorkehrungen (z.B. Änderung der voreingestellten

Passwörter) getroffen wurden, um den Zugriff auf und Manipulationen an diesem Netzwerk durch Unberechtigte zu verhindern. Achten Sie bei all Ihren elektronischen Geräten darauf, dass Sie die aktuellste Software und einen aktuellen Virenschutz nutzen sowie die Firewall aktiviert ist.

Sicheres Passwort

Wählen Sie ein Passwort, das mindestens zwölf Zeichen lang ist und nicht im Wörterbuch vorkommt. Es sollte aus Groß- und Kleinbuchstaben in Kombination mit Zahlen und Sonderzeichen bestehen und auf den ersten Blick sinnlos zusammengesetzt sein (Ausnahme: Bei WPA3, dem empfohlenen Verschlüsselungsverfahren für WLAN, sollte das Passwort mindestens

20 Zeichen lang sein). Sofern der Dienst-anbieter eine Multifaktor-Authentifizierung (z.B. Handy, Dongle, etc.) zulässt, sollte diese genutzt werden. Nähere Infos gibt es auf der Internetseite des Bundesamts für Sicherheit in der Informationstechnik.

Vermeiden Sie den Besuch von verdächtigen Webseiten und gehen Sie vorsichtig mit Nachrichten von unbekannten Absendern um (z. B. keine Anhänge öffnen, nicht auf mitgeschickte Links klicken). Geben Sie keine Passwörter oder Codes an Dritte weiter.

Achten Sie bei der Eingabe persönlicher Daten grundsätzlich auf eine verschlüsselte, sichere Verbindung (erkennbar an dem Kürzel "https" in der Browserleiste).



Verstöße melden

Melden Sie "Cyberstalker", die Sie unaufgefordert und dauerhaft über das soziale Netzwerk kontaktieren, an den Betreiber des jeweiligen sozialen Netzwerkes. In schwerwiegenden Fällen sollten Sie auch die Polizei informieren, damit ggf. strafverfolgende Maßnahmen eingeleitet werden können.

Leiten Sie Drohungen oder Beleidigungen, die Sie per E-Mail erhalten, nicht weiter, sondern warten Sie, bis die Polizei die Nachricht gesichert hat.

Dokumentieren und sichern Sie Bedrohungen und Beleidigungen, die Sie über soziale Netzwerke oder Messengerdienste erhalten, per

Screenshot oder fotografisch per Kamera, um der Polizei diese zur Verfügung stellen zu können.

Beachten Sie auch, dass einige Messengerdienste das Versenden elektronischer Nachrichten ermöglichen, die nicht automatisch auf unbestimmte Zeit gespeichert werden, weil sie z. B. mit einem Timer versehen sind, bei dessen Ablauf die Nachricht automatisch gelöscht wird. Besonders bei diesen „flüchtigen“ Nachrichtenformen ist eine Sicherung mittels Screenshot oder Kamera essenziell.

Dokumentieren Sie generell bei der Sicherung von Nachrichten in Messengern und sozialen Netzwerken den Namen des genutzten Dienstes, Festsellungsdatum und -uhrzeit sowie

(sofern verfügbar) den vollständigen Link des Nutzerprofils, von dem Sie die Nachricht erhalten haben (inklusive Username / Userkennung oder UserID).

Hotline für Amts- und Mandatsträger

Über die Hotline **06131 65-65250** erreichen Sie rund um die Uhr einen polizeilichen Ansprechpartner des Landeskriminalamtes, der den Sachverhalt entgegennimmt, erste Verhaltenshinweise gibt und bei Bedarf weitere Ansprechpartner vermittelt.

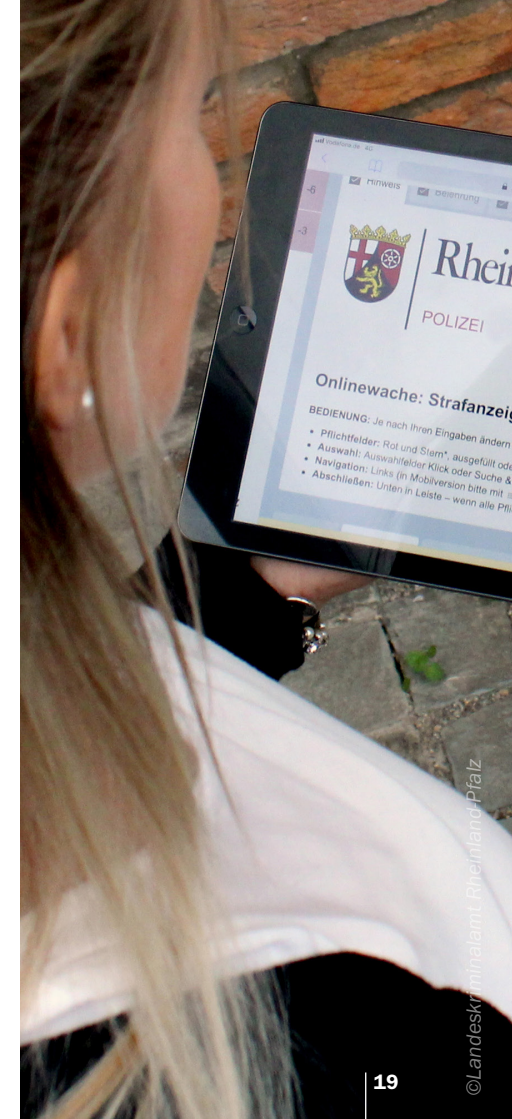
Unabhängig davon können Sie auf jeder Polizeidienststelle Strafanzeige erstatten oder gefährdungsrelevante Sachverhalte melden.

Bringen Sie konsequent und umgehend jedes strafbare Verhalten zur Anzeige, um eine Erforschung des Sachverhalts durch die Strafverfolgungsbehörde zu gewährleisten.

Unter www.polizei.rlp.de/de/onlinewache/ können Sie Ihre Strafanzeige auch online erstatten oder der Polizei einen Hinweis geben.

In akuten Bedrohungssituationen, die ein sofortiges polizeiliches Eingreifen erfordern, wählen Sie bitte direkt den Notruf **110**.

Für Rückfragen und weitere Informationen steht Ihnen das Präventionsteam des Landeskriminalamtes Rheinland-Pfalz gerne zur Verfügung.



Weiterführende Informationen

Sie sind beim Thema "Einbruchschutz" nicht auf sich allein gestellt. Ihre Polizei hilft Ihnen bei der Suche nach Schwachstellen am Haus. Die Fachberater/-innen erklären Ihnen, wie Sie diese beheben können, worauf Sie achten sollten und welche Handwerksbetriebe in Ihrer Nähe die polizeilichen Standards beim Einbau von Sicherheitstechnik erfüllen.

Je nach Umfang werden die Einbruchschutzberatungen in den zentralen Präventionsstellen der Polizeipräsidien, am Telefon oder bei Ihnen Zuhause am Wohnobjekt durchgeführt.

Ihre persönliche Beratungsstelle bei der Polizei finden Sie auf der Homepage www.polizei.rlp.de in der Rubrik „Aufgaben“, „Prävention“, „Kriminalprävention“, „Ansprechpartner“.

Informationen zur Sicherung Ihres Wohnobjektes erhalten Sie auch in der Broschüre „Sicher Wohnen“ aus dem Programm „Polizeiliche Kriminalprävention“ (ProPK) oder auf der Homepage www.polizei.rlp.de in der Rubrik „Aufgaben“, „Prävention“, „Kriminalprävention“, „Einbruchschutz“.

Weitergehende Informationen zum Thema "Nachbarschaftshilfe" finden Sie im Faltblatt „Ganze Sicherheit für unser Viertel“ aus dem Programm „Polizeiliche Kriminalprävention“ (ProPK).

Tipps und Tricks zum Thema "Internetgefahren" und "Mediensicherheit" gibt es unter www.cybersicherheit-rlp.de und www.bsi-fuer-buerger.de.

Auch die Broschüre „Klicksmomente - Informationen für Internetnutzer" aus dem Programm „Polizeiliche Kriminalprävention“ (ProPK) hält weitere Informationen für Sie bereit.

Auf der Internetseite der Initiative ContraHassRLP (www.kriminalpraevention.rlp.de/de/unsere-themen/contra-hass) finden Sie wichtige Infos rund um das Thema Hass und Hetze im Netz; beispielsweise wie man beweissichere Screenshots fertigt.

Alle aufgeführten Faltblätter und Broschüren erhalten Sie kostenlos bei jeder Polizeidienststelle oder online unter www.polizei-beratung.de in der Rubrik „Medienangebot" zum Download.



Ihre Notizen



RheinlandPfalz

LANDESKRIMINALAMT

Landeskriminalamt Rheinland-Pfalz
Valenciaplatz 1-7
55118 Mainz

