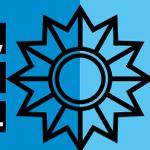


SICHERHEIT IM MEDIENALLTAG

KLICKS-MOMENTE FÜR INTERNETNUTZER



**Wir wollen,
dass Sie
sicher leben.**



Ihre Polizei



Ihr Ansprechpartner vor Ort:

A large, empty rectangular box with a thin green border, intended for providing contact information for the local contact person.

	Einleitung	5
1.	Betrug im Internet	7
2.	Verbreitung verbotener Inhalte	13
3.	Verletzung von Persönlichkeits- und Urheberrechten	17
4.	Straftaten in sozialen Netzwerken	21
5.	Mangelnder Schutz von Smartphone und Tablet-PC	27
6.	Folgen von Schadsoftware	31
7.	Identitätsdiebstahl und Phishing	35
	Ansprechpartner der Polizeilichen Kriminalprävention	38
	Impressum	39



LIEBE LESERIN, LIEBER LESER,

moderne Kommunikationsmittel bestimmen unser Leben. Und sie machen unseren Alltag oft ein wenig leichter. Schnelle Kommunikation, einfache Bedienung und kinderleichte Datenverwaltung sind nur einige Vorteile der digitalisierten Gesellschaft. Doch der digitale Alltag birgt Risiken und Gefahren, die auch durch die intensive Vernetzung aller Bereiche und aller Geräte – vom Saugroboter bis zum Kinderspielzeug – entstehen. Datenklau, beinahe täglich neue Betrugsvarianten, digitale Erpressung und Schadprogramme betreffen nicht nur exzessive Internetnutzer, sondern können ein Problem für alle werden.

Diese Broschüre informiert Sie über mögliche Risiken der digitalen Welt. Sie zeigt Probleme, Gefahren aber auch Straftaten im Zusammenhang mit dem Internet auf. Zugleich vermittelt sie Sicherheitstipps, die jeder einfach in

seinem Alltag umsetzen kann. Diese polizeilichen Empfehlungen sollen Ihnen aufzeigen, wie Sie sich selbst vor den aktuellen Kriminalitätsformen im Internet schützen können.

Der erste Schritt zu mehr Sicherheit im Internet: Sorgen Sie für einen guten Basisschutz Ihrer Geräte und Ihres Heimnetzwerks. Der Sicherheitskompass von Polizei und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zeigt, wie Sie sich in Ihrem digitalen Alltag einfach und schnell schützen können.





1. BETRUG IM INTERNET

Das Internet eröffnet Kriminellen viele Möglichkeiten, Menschen zu betrügen: Vorauszahlungsbetrug, Warenbetrug oder Romance-Scamming (eine Variante des Heiratsschwindels) sind nur einige Betrugsformen, bei denen schon viele Opfer geworden sind.

Online-Shopping

Besonders aktiv sind Betrüger im Bereich des Online-Shoppings. Sie bieten oft zu sehr niedrigen Preisen Waren zum Verkauf an. Bei solchen Schnäppchen greifen viele internetaffine Menschen zu. Doch nachdem das Bestellte, wie oft gefordert, im Voraus bezahlt wurde, bleibt die Lieferung aus. Oder es wird mangelhafte Ware geliefert. Was viele Nutzer nicht wissen: Betrüger legen sich sogenannte Fake-Shops zu,

fälschen also Verkaufsplattformen. Eine weitere Variante ist das Anbieten vermeintlicher Gratisleistungen hinter denen sich sogenannte Abofallen verbergen. Hier ist die Gratisleistung an den Abschluss eines Abonnements gebunden.

Betrug beim Dating

Vor allem in sozialen Netzwerken suchen Täter nach Frauen und Männern, die sie beim Romance Scamming um ihr Geld betrügen können. Sie täuschen Liebesbeziehungen vor, um Geld und andere Gefälligkeiten zu erschleichen (Näheres dazu unter „Straftaten in sozialen Netzwerken“).

Online-Kauf von Kfz

Was mit Liebesbeziehungen funktioniert, gelingt auch beim Auto- und Immobilienkauf. Dabei wird für ein zum Verkauf angebotenes Auto oder eine Wohnung angeblichen Käufern versehentlich eine höhere Summe überwiesen oder per Scheck übergeben. Den Differenzbetrag sollen nichts ahnende Verkäufer entweder bar aushändigen oder zurücküberweisen. Doch ist der Differenzbetrag beglichen, holen sich die Täter ihre Überweisung zurück oder der Scheck stellt sich als Fälschung heraus. Die Verkäufer verlieren also sowohl das Geld aus dem Verkauf als auch das verkaufte Gut.

Finanzagenten

Eine andere weitverbreitete Betrugsmasche sind dubiose Stellenangebote und Nebenverdienstmöglichkeiten. Dabei locken als Unternehmen getarnte Kriminelle mit lukrativen Jobs. Oft geben sie sich als Finanzmanagementunternehmen und Ähnliches aus und suchen Personen mit einem Konto in Deutschland. Dieses soll nur für Überweisungen zur Verfügung gestellt werden - die Inhaber sollen dafür gute Provisionen erhalten. Viele ahnungslose Opfer haben sich auf diese Weise schon strafbar gemacht, weil sie Betrüger unterstützt haben. Denn das Geld stammt oft aus Phishing-Aktionen.

TIPPS

- › Grundsätzlich gilt: Je verlockender ein Angebot ist, desto misstrauischer sollten Sie sein!
- › Überprüfen Sie einen Online-Shop, indem Sie in Diskussionsforen schauen und Erfahrungen aus dem persönlichen Umfeld beachten.
- › Achten Sie auf die Kosten: Deutsche Anbieter von Internetseiten müssen Bezahlinhalte mittels eines deutlich erkennbaren Buttons kennzeichnen. Bei einem Abonnement muss auf der Internetseite neben dem Preis deutlich auch die Mindestlaufzeit genannt werden. Dies gilt jedoch nicht für Angebote auf ausländischen Servern. Seien Sie vorsichtig, wenn für kostenlose Dienste persönliche Daten benötigt werden und Sie mindestens 18 Jahre alt sein müssen.
- › Zahlen Sie niemals per Vorkasse Geld an Anbieter.
- › Nutzen Sie sichere Zahlungswege z. B. Überweisungen auf Girokonten. Seriöse Internetportale stellen Bezahlmöglichkeiten zur Verfügung, die Ihr Geld schützen.
- › Nutzen Sie Bargeldtransfer-Dienstleister (z. B. Western Union) nur für Überweisungen an Personen, die Sie aus Ihrem realen Leben kennen.
- › Melden Sie dubiose Angebote dem Portalbetreiber oder dem Original-Hersteller/-Vertrieb.
- › Erste Hilfe bei Betrugsverdacht: Speichern Sie alle E-Mails als Beweis. Fertigen Sie von der Internetseite einen Screenshot an. Heben Sie Überweisungsbelege usw. auf. Machen Sie, wenn noch möglich, bereits geleistete Zahlungen rückgängig und erstatten Sie Anzeige bei der Polizei.
- › Prüfen Sie in Online-Shops u. a. Impressum, AGB und Verlinkungen zu Zahlungsdiensten. Nutzen Sie öffentliche Telefonbücher oder Gütesiegelbetreiber zur Gegenkontrolle.

Rechtliche Aspekte

Warenbetrug ist eine Straftat entsprechend:

§ 263 Strafgesetzbuch (StGB)

Betrug

„(1) Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er durch Vorspiegelung falscher oder durch Entstellung oder Unterdrückung wahrer Tatsachen einen Irrtum erregt oder unterhält, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.

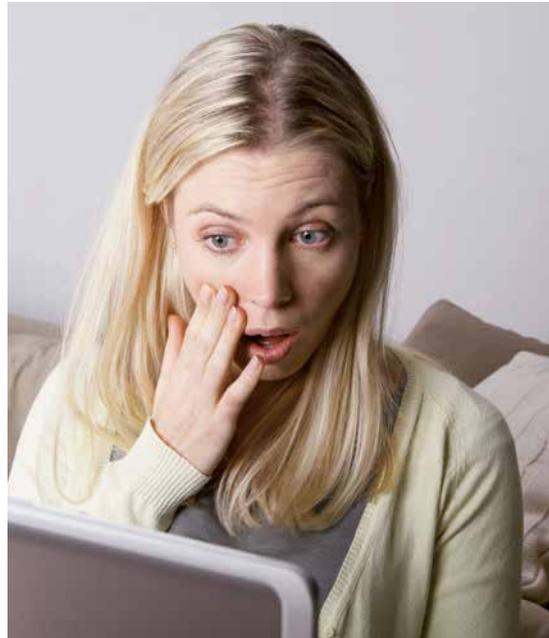
(3) In besonders schweren Fällen ist die Strafe Freiheitsstrafe von sechs Monaten bis zu zehn Jahren. [...]“

§ 261 Strafgesetzbuch (StGB)

Geldwäsche; Verschleierung unrechtmäßig erlangter Vermögenswerte

„(1) Wer einen Gegenstand, der aus einer in Satz 2 genannten rechtswidrigen Tat herrührt, verbirgt, dessen Herkunft verschleiert oder die Ermittlung der Herkunft, das Auffinden, den Verfall, die Einziehung oder die Sicherstellung eines solchen Gegenstandes vereitelt oder

gefährdet, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft.“



Linkempfehlungen

www.polizei-beratung.de/abofallen

www.polizei-beratung.de/scamming

www.polizei-beratung.de/fake-shops

www.sicherer-autokauf.de

www.verbraucherzentrale.de

www.polizei-praevention.de

www.computerbetrug.de

www.internet-guetesiegel.de

www.safer-shopping.de



2. VERBREITUNG VERBOTENER INHALTE

Wer im Internet bestimmte Inhalte veröffentlicht und anderen verfügbar macht, begeht nach deutschem Recht eine Straftat. Denn gewaltverherrlichende oder pornografische Inhalte sind aufgrund ihrer jugendgefährdenden Wirkung meist verboten. Zuständig für die Verfolgung solcher Verstöße sind – neben den Polizeibehörden – zwei im staatlichen Auftrag handelnde Institutionen: die Internet-Beschwerdestelle sowie www.jugendschutz.net.

Während die Meldestellen mit Abmahnungen und Bußgeldern beim Seitenbetreiber die Inhalte löschen lassen können, verfolgt die Polizei die Verfasser verbotener Inhalte. Verbotene Inhalte werden nicht nur über Internetforen, Chats oder soziale Netzwerke verbreitet, sondern auch über Messengerdienste wie WhatsApp.

TIPPS

- › Sichern Sie Beweise für strafbare Inhalte im Internet oder in Messengerdiensten und wenden Sie sich damit an die Polizei oder die Meldestellen unter www.jugendschutz.net oder www.internet-beschwerdestelle.de.
Wichtig: Notieren Sie sich den Fundort der verbotenen Inhalte (z. B. Facebook, Youtube) sowie die dazugehörige URL. Diese Quellenangaben sind wichtige Informationen für die Meldestellen.
- › Im Falle von Kinderpornografie im Netz dürfen Sie nicht selbst nach einschlägigen Seiten suchen und diese sichern, dadurch können Sie sich strafbar machen. Wenn Sie zufällig einen solchen Inhalt entdecken, melden Sie diesen sofort der Polizei oder weisen die Internet-Beschwerdestelle darauf hin unter www.internet-beschwerdestelle.de.

VERBOTEN SIND

Extremistische Inhalte

Extremistische Gruppen und Personen nutzen das Internet, um Propaganda zu verbreiten und Menschen für ihre Ideen einzunehmen.

Verboten ist u. a.

- › gegen Minderheiten zu hetzen, zum Hass gegen sie aufzustacheln oder zur Gewalt gegen sie aufzufordern,
- › Kennzeichen und Symbole verfassungswidriger Organisationen zu verwenden,
- › den Holocaust zu leugnen und das Nazi-Regime zu verherrlichen,
- › den Staat, seine Symbole oder seine Verfassungsorgane zu verunglimpfen.

Pornografische Inhalte (insbesondere Kinderpornografie)

Als pornografisch ist laut Bundesgerichtshof (BGH) eine Darstellung

anzusehen, „wenn sie unter Ausklammerung aller sonstigen menschlichen Bezüge sexuelle Vorgänge in grob aufdringlicher, anreißerischer Weise in den Vordergrund rückt und in ihrer Gesamttendenz ausschließlich oder überwiegend auf das lüsterne Interesse des Betrachters an sexuellen Dingen abzielt“. Unter Kinderpornografie versteht man pornografische Darstellungen, die den sexuellen Missbrauch von unter 14-Jährigen zeigen.

Gewaltverherrlichende Inhalte

Die Herstellung und Verbreitung von Medien, die grausame oder unmenschliche Gewalttätigkeiten gegen Menschen zeigen, sind verboten. Dieses Verbot beinhaltet unter anderem die Verherrlichung von Gewalt und Krieg sowie die Verletzung der Menschenwürde.

Linkempfehlungen

www.polizei-beratung.de

www.jugendschutz.net

www.internet-beschwerdestelle.de

www.irights.info

www.klicksafe.de

www.polizeifürdich.de

Rechtliche Aspekte

§ 130 Strafgesetzbuch (StGB)

Volksverhetzung

„(1) Wer in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören,
1. gegen eine nationale, rassische, religiöse oder durch ihre ethnische Herkunft bestimmte Gruppe, gegen Teile der Bevölkerung oder gegen einen Einzelnen wegen seiner Zugehörigkeit zu einer vorbezeichneten Gruppe oder zu einem Teil der Bevölkerung zum Hass aufstachelt, zu Gewalt- oder Willkürmaßnahmen auffordert oder
2. die Menschenwürde anderer dadurch angreift, dass er ... [sie] ... beschimpft, böswillig verächtlich macht oder verleumdet, wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft. [...]“

§ 182b Strafgesetzbuch (StGB)

Verbreitung, Erwerb und Besitz kinderpornografischer Schriften

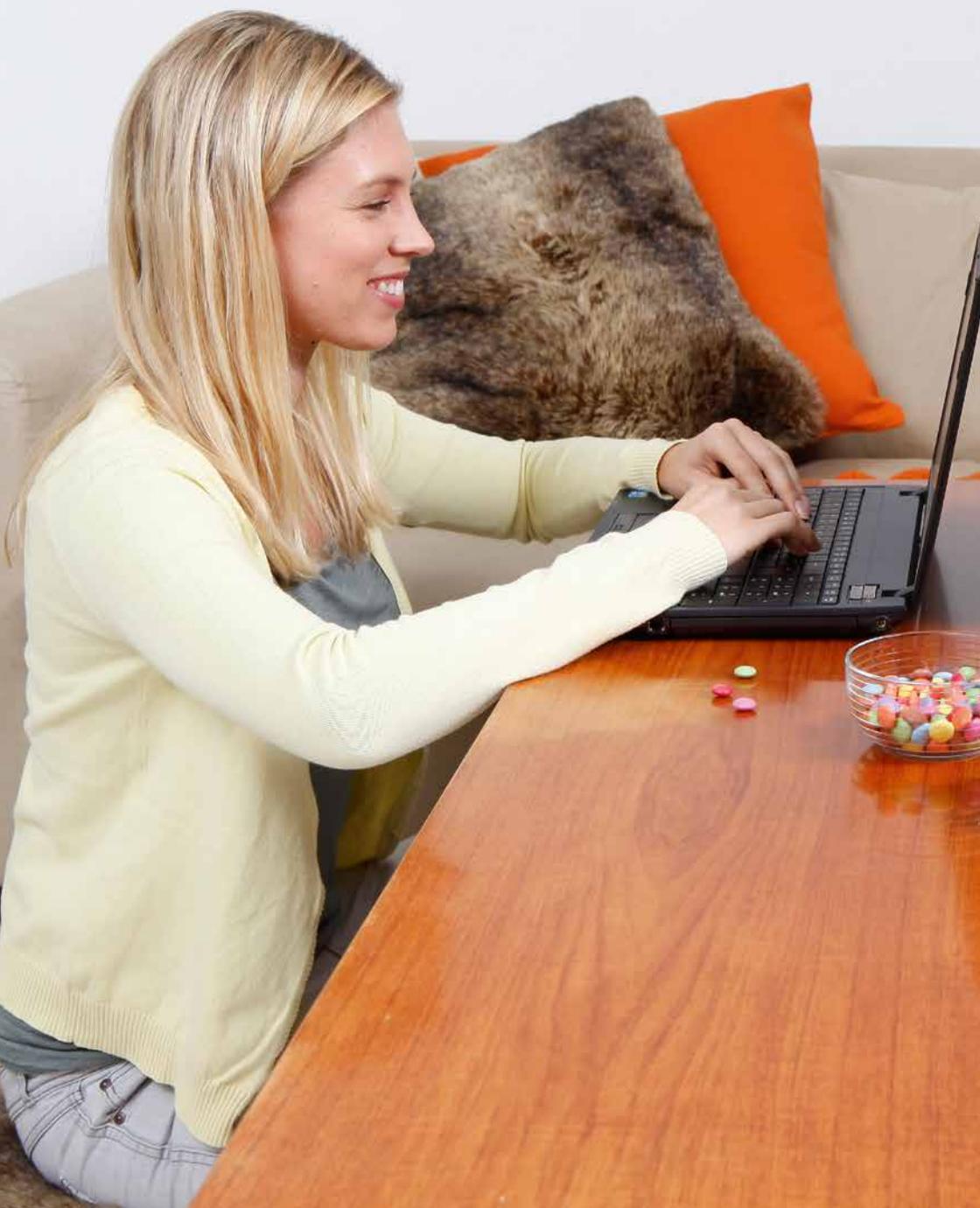
„(1) Wer pornographische Schriften (§ 11 Abs. 3), die sexuelle Handlungen von, an oder vor Kindern (§ 176 Abs. 1) zum Gegenstand haben (kinderpornographische Schriften),
1. verbreitet,
2. öffentlich ausstellt, [...], oder
3. herstellt, [...], anbietet,

wird mit Freiheitsstrafe von drei Monaten bis zu fünf Jahren bestraft. [...]“

§ 131 Strafgesetzbuch (StGB)

Gewaltdarstellung

„(1) Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer
1. eine Schrift (§ 11 Absatz 3), die grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen oder menschenähnliche Wesen in einer Art schildert, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt,
a) verbreitet oder der Öffentlichkeit zugänglich macht,
b) einer Person unter achtzehn Jahren anbietet, überlässt oder zugänglich macht oder
2. einen in Nummer 1 bezeichneten Inhalt mittels Rundfunk oder Telemedien
a) einer Person unter achtzehn Jahren oder
b) der Öffentlichkeit zugänglich macht oder
3. eine Schrift (§ 11 Absatz 3) des in Nummer 1 bezeichneten Inhalts herstellt [...]“



3. VERLETZUNG VON PERSÖNLICHKEITS- UND URHEBERRECHTEN

Schnell ein Bild aus dem Netz gezogen, das Lieblingslied heruntergeladen oder das selbstgedrehte Video ins eigene Profil bei Facebook, Instagram und Co. eingestellt – durch das Mitmach-Web haben alle Nutzer viele Möglichkeiten, Inhalte zu generieren. Diese Freiheit hat jedoch Grenzen: Nicht alle Daten dürfen von jedem in jeder Form genutzt und verbreitet werden. Problematisch ist neben illegalen Downloads von Bildern, Videos, Software oder Musik vor allem auch der Umgang mit selbst erstellten Inhalten.

Das ist der Fall, wenn auf den Aufnahmen Bekannte, Familienmitglieder oder Kolleginnen und Kollegen zu sehen sind. Vielen ist nicht bewusst, dass sie diese Inhalte nicht einfach ohne die Erlaubnis der darin Gezeigten im Internet verbreiten dürfen. Gerade wenn Dritte in peinlichen oder erniedrigenden Situationen gezeigt werden, wird aus dem scheinbar harmlosen Spaß schnell strafbares Verhalten. Auch wer Aufnahmen von Verkehrsunfällen mit Verletzten oder Toten erstellt, macht sich strafbar.

(Mehr Informationen über das Thema Persönlichkeitsrechte und digitale Verwertung finden Sie unter www.polizei-beratung.de/gefahren-im-internet).

TIPPS

- › Heimliche Film- und Bildaufnahmen von Dritten sind nicht erlaubt – deren Veröffentlichung im Internet ist strafbar.
- › Achten Sie darauf, für welche Nutzung Inhalte Dritter freigegeben sind und nutzen Sie diese ausschließlich in der zugelassenen Form. Beachten Sie dabei, dass Veränderungen der Inhalte ausgeschlossen sind.
- › Statt Inhalte von anderen Websites zu kopieren, können Sie Verlinkungen setzen. Aber immer mit Zustimmung des Betreibers und mit Quellenangabe.
- › Nutzen Sie ausschließlich legale Musik- und Videoportale, um Filme im Internet anzuschauen oder um Musik zu hören. Illegale Downloads können Schadsoftware enthalten oder zivilrechtliche Forderungen der Rechteinhaber nach sich ziehen.
- › Auch das Online-Streaming von illegalen Inhalten kann strafbar sein.
- › Wenn Ihre persönlichen Daten, Bilder oder Texte unerlaubt verbreitet werden: Sichern Sie alle Seiten durch Screenshots und machen Sie den Einsteller auf die Verletzung Ihrer Rechte aufmerksam. Setzen Sie ihm Fristen, innerhalb derer die Inhalte entfernt werden sollen. Beantragen Sie dann eine Löschung der Daten beim Provider der Website. Je nach Betreiber sind die Voraussetzungen dafür allerdings unterschiedlich. Wenden Sie sich bei Verdacht auf eine Straftat an die Polizei.

HINWEIS

Beachten Sie dazu auch die Tipps im Kapitel „Straftaten in sozialen Netzwerken“.

Rechtliche Aspekte

§ 201a Strafgesetzbuch (StGB)

[1] Verletzung des höchstpersönlichen Lebensbereichs durch Bildaufnahmen

„**(1)** Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer

- 1.** von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,
- 2.** eine Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt, unbefugt herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,
- 3.** eine durch eine Tat nach den Nummern 1 oder 2 hergestellte Bildaufnahme gebraucht oder einer dritten Person zugänglich macht oder
- 4.** eine befugt hergestellte Bildaufnahme der in den Nummern 1 oder 2 bezeichneten Art wissentlich unbefugt einer dritten Person zugänglich macht und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt.[...]“

§ 33 Kunsturheberrechtsgesetz

(KunstUrhG)

„**(1)** Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer entgegen den §§ 22, 23 ein Bildnis verbreitet oder öffentlich zur Schau stellt.

(2) Die Tat wird nur auf Antrag verfolgt.“

§ 106 Urheberrechtsgesetz (UrhG)

Unerlaubte Verwertung urheberrechtlich geschützter Werke

„**(1)** Wer in anderen als den gesetzlich zugelassenen Fällen ohne Einwilligung des Berechtigten ein Werk oder eine Bearbeitung oder Umgestaltung eines Werkes vervielfältigt, verbreitet oder öffentlich wiedergibt, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar.“

Linkempfehlungen

www.polizei-beratung.de

www.klicksafe.de

www.bsi-fuer-buerger.de

www.irights.info

www.gvu.de

www.computerbetrug.de

www.internet-guetesiegel.de

www.safer-shopping.de



4. STRAFTATEN IN SOZIALEN NETZWERKEN

Das Risiko in einem sozialen Netzwerk Opfer einer Straftat zu werden, steigt mit jeder persönlichen Information im eigenen Profil. Betrug, Cybermobbing oder Phishing sind Straftaten, die meist erst möglich werden, weil Nutzer leichtsinnig mit ihren Daten umgehen und allgemeine Sicherheitsempfehlungen ignorieren – oft mit fatalen Folgen. Während ein materieller Schaden beispielsweise durch einen Betrug meist noch zu verkraften ist, sind die Folgen von Beleidigungen, übler Nachrede oder Verleumdungen gravierender. Solche Straftaten tauchen oft in Verbindung mit (Cyber)Mobbing oder Cyberstalking (Nachstellung mittels moderner Kommunikationsmittel) auf. Denn auch Erwachsene können wie Kinder und Jugendliche in den sozialen Netzwerken gezielten Anfeindungen ausgesetzt sein. Neben dem unbedachten Umgang mit den eigenen Daten sind auch mangelnde Schutzeinstellungen der jeweiligen Profile ein Anreiz für Täter.

Kriminelle nutzen die sozialen Netzwerke für Betrug, beispielsweise indem sie Profile übernehmen, um von Freunden der realen Person Geld zu erpressen oder Daten auszuspähen. Beim sogenannten Doxing, dem Sammeln von Daten einer Person über das Internet, eröffnen sich Tätern viele Möglichkeiten. Sie können diese Daten beispielsweise für Identitätsdiebstahl oder zum Stalking nutzen.

Romance Scamming

Besonders perfide gehen Betrüger beim Romance Scamming vor. Sie täuschen ihren Opfern über Wochen und Monate eine Online-Beziehung vor und bitten diese um Geld und andere Gefälligkeiten. Dabei üben sie nicht selten immensen Druck aus, damit Betroffenen weiter zahlen. Auf diese Weise haben viele Geschädigte bereits ihre gesamten Ersparnisse an die Kriminellen verloren.

Gegen Hate Speech

Beleidigung, Bedrohung, Verfolgung: Im Internet nimmt Hass auf Menschen oder ganze Menschengruppen oft grausame Formen an. Ein vermeintlich klischeehafter Spruch kann ausreichen, damit andere daraufhin Hassbotschaften, extremistische Parolen oder Beschimpfungen verbreiten.

Hass im Netz zielt auf ganze Gruppen, beleidigt, bedroht und verachtet auch einzelne Personen aufgrund ihrer Herkunft, ihrer Religion, ihres Geschlechtes oder ihrer sexuellen Orientierung. Die verbreiteten Inhalte, auch Hate Speech genannt, können extremistisch, rassistisch, sexistisch, homophob, holocaustverleugnend oder gewaltverherrlichend sein. Sie erscheinen in sozialen Netzwerken in Form von Bildern und Kommentaren oder werden über Fake-Accounts verbreitet.

Hasserfüllte Äußerungen sind strafbar, wenn die Grenze der freien Meinungsäußerung überschritten und die Rechte anderer verletzt werden.

Oft stacheln sich einzelnen Hassredner gegenseitig an und rufen nicht selten auch zur Gewalt gegen die von ihnen verachteten Menschen auf.

TIPPS GEGEN HASS IM NETZ

- › Hassreden sollten nicht toleriert oder ignoriert werden. Eine Gegenreaktion ist ein wichtiges Zeichen für Täter und andere Nutzerinnen und Nutzer, dass solches Verhalten nicht hinnehmbar ist.
- › Sprechen Sie denjenigen direkt an, der den Kommentar gepostet hat. Fragen Sie nach, warum solche Kommentare sein müssen. Verlangen Sie gegebenenfalls nach Beispielen und Fakten für Äußerungen.
- › Beleidigen Sie selbst nicht, das aktiviert und provoziert.
- › Argumentieren Sie sinnvoll gegen die Hasskommentare. Sie können auch Quellen für Ihre Argumente anführen.
- › Wenn Sie unsicher sind, ob die Kommentare nicht bereits strafbar sind, können Sie diese dem Portalbetreiber, Internetbeschwerdestellen oder der Polizei melden.
- › Wer gezielt Hassreden im Internet verbreitet, um anderen zu schaden, macht sich strafbar. Solche Personen sollten den genannten Stellen immer wieder gemeldet werden.

TIPPS

- › Achten Sie auch in sozialen Netzwerken grundsätzlich auf Schutzeinstellungen. Machen Sie Profile nicht für jeden zugänglich.
- › Informieren Sie sich über die AGB und die Bestimmungen zum Datenschutz, bevor Sie ein Profil einrichten.
- › Nutzen Sie ein sicheres Passwort, das zum Beispiel aus den Anfangsbuchstaben der Wörter einer Textzeile besteht, mit Zahlen kombiniert wird und kein sinnvolles Wort ergibt.
- › Seien Sie zurückhaltend mit der Veröffentlichung persönlicher Daten wie Ihrer Anschrift, dem Geburtsdatum und mit Auskünften über Ihren Arbeitgeber. Andere können ebenfalls an diese Informationen gelangen.
- › Ausweis- oder Kontodaten sollten in sozialen Netzwerken niemals angegeben werden.
- › Seien Sie misstrauisch bei der Kontaktaufnahme mit Personen, die Sie nur aus dem Internet und nicht aus Ihrem realen Leben kennen. Es kann sich dabei um Kriminelle wie Betrüger, Heiratsschwindler oder Sexualstraftäter handeln.
- › Melden Sie Personen, die Sie dauerhaft und unaufgefordert kontaktieren, dem Netzwerkbetreiber. In schweren Fällen erstatten Sie Strafanzeige bei der Polizei.
- › Melden Sie Personen, die andere beleidigen oder bedrohen dem Netzwerkbetreiber oder unter www.internet-beschwerdestelle.de.
- › Prüfen Sie regelmäßig Ihre Account- und Privatsphäre-Einstellungen.
- › Achten Sie auch auf die Sicherheit Ihrer mobilen Endgeräte (Mehr dazu unter „Mangelnder Schutz von Smartphone und Tablet-PC“).

Rechtliche Aspekte

§ 186 Strafgesetzbuch (StGB)

Üble Nachrede

„Wer in Beziehung auf einen anderen eine Tatsache behauptet oder verbreitet, welche denselben verächtlich zu machen oder in der öffentlichen Meinung herabzuwürdigen geeignet ist, wird, wenn nicht diese Tatsache erweislich wahr ist, mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Tat öffentlich oder durch Verbreiten von Schriften (§ 11 Abs. 3) begangen ist, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“

§ 111 Öffentliche Aufforderung zu Straftaten (StGB)

„(1) Wer öffentlich, in einer Versammlung oder durch Verbreiten von Schriften (§ 11 Abs. 3) zu einer rechtswidrigen Tat auffordert, wird wie ein Anstifter (§ 26) bestraft. [...]“

§ 185 Strafgesetzbuch (StGB)

Beleidigung

„Die Beleidigung wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe und, wenn die Beleidigung mittels einer Tätlichkeit begangen wird, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft.“



Linkempfehlungen

www.bsi-fuer-buerger.de

www.sicher-im-netz.de

www.klicksafe.de

www.mimikama.at

www.polizei-praevention.de

www.zivile-helden.de

www.internet-beschwerdestelle.de



5. MANGELNDER SCHUTZ VON SMARTPHONE UND TABLET-PC

Die Sicherheitsanforderungen an mobile Geräte haben sich verändert. Mit ihrer zunehmenden Verbreitung muss auch verstärkt auf die Sicherheit der Daten, die auf solchen Geräten gespeichert sind, geachtet werden. Hinzu kommt, dass darauf inzwischen nicht nur private Daten, sondern auch immer mehr geschäftliche Informationen abgelegt werden. Damit sind Smartphones und Tablets denselben Risiken ausgesetzt wie stationäre und tragbare PCs.

Gerade weil man mit Smartphones und Tablets kinderleicht im Internet surfen kann, bieten sie Angriffspunkte für Schadsoftware oder Phishing. Hinzu kommt, dass viele Menschen Smartphones und Tablets dazu nutzen, Haus-technik und andere vernetzte Geräte zu steuern. Auf dem Vormarsch ist auch das Bezahlen per Smartphone – eine bequeme Anwendung, die immer mehr Menschen für sich entdecken. Je mehr

Funktionen ein Smartphone im Alltag übernimmt, umso größer die Gefahr für Zugriffe von außen und Datenmissbrauch.



Auch aus diesen Gründen vertrauen viele Nutzer Cloud-Diensteanbietern, die Sicherheit bei der Datenverwaltung versprechen. Nutzer einer Cloud sind in der Lage, von jedem Endgerät mit einem Passwort auf die Inhalte und die Dienste der Cloud zurückgreifen zu können. Doch auch dabei können vertrauliche Daten schnell in falsche Hände geraten.

TIPPS

- › Lassen Sie Ihr Smartphone oder Tablet nie unbeaufsichtigt liegen. Geben Sie es auch kurzzeitig nur in Ihrem Beisein an Dritte weiter.
- › Nutzen Sie den Gerätesperrcode, die automatische Displaysperre und aktivieren Sie stets die SIM/USIM-PIN. Ein Wischcode schützt nicht ausreichend. Nutzen Sie möglichst einen Fingerabdruckscanner.
- › Löschen Sie alle sensiblen Daten, wenn Sie das Gerät verkaufen. Stellen Sie das Gerät dafür auf Werkseinstellungen zurück.
- › Laden Sie keine Dateien aus unsicheren Quellen herunter. Nutzen Sie nur App-Stores seriöser Anbieter. Bei Android: Verbieten Sie in den Einstellungen, dass Apps aus unbekanntem Quellen auf Ihrem Gerät installiert werden können.
- › Aktivieren Sie drahtlose Schnittstellen nur bei Bedarf. Tauschen Sie Daten nur mit vertrauenswürdigen Partnern aus.
- › Öffnen Sie keine Links oder Dateien, die Sie von Unbekannten über Messenger erhalten haben.
- › Nutzen Sie fremde WLANs, z. B. öffentliche Hotspots an Flughäfen oder in Cafés, nur mit einem VPN (Virtuelles privates Netzwerk). Übermitteln Sie aber auch dann keine vertraulichen Daten.
- › Nutzen Sie bei Verlust oder Diebstahl mögliche Ortungs-, Fernsperr- oder Löschdienste.
- › Drittanbietersperren, die Sie beim Provider einrichten, können Missbrauch durch Abofallen verhindern.
- › Nutzen Sie, wenn verfügbar, Antivirenprogramme und Überwachungs-Apps, die Ihnen die Berechtigungen von anderen Apps (z. B. Zugriff auf das Telefonbuch) anzeigen.

- › Hinterfragen Sie Provider-Updates, die Sie per SMS, MMS oder als Link erhalten – es kann sich um Schadsoftware handeln.
- › Deaktivieren Sie bei Smartphones oder Tablets die automatische Speicherung der Daten in der Cloud. So vermeiden Sie, dass Daten wie Kontoverbindungen usw. unwissentlich in der Cloud gespeichert werden.
- › Überlegen Sie grundsätzlich, welche Daten Sie in der Cloud ablegen. Je vertraulicher die Information, umso weniger sollte sie in Anwendungen gespeichert werden.
- › Achten Sie bei smarten Geräten auch auf Sicherheitskonfiguration und Datenschutz. Verbinden Sie die Geräte, z.B. nur mit einem Gastzugang mit dem heimischen Router.



Linkempfehlungen

www.polizei-beratung.de/gefahren-

[im-internet](http://www.polizei-beratung.de/gefahren-im-internet)

www.bsi-fuer-buerger.de

www.klicksafe.de

www.polizei-praevention.de

www.sicher-im-netz.de



6. FOLGEN VON SCHADSOFTWARE

Schadsoftware (Malware) zielt darauf ab, auf einem fremden Computersystem unerwünschte Aktionen auszuführen und dadurch Schaden anzurichten. Grundsätzlich kann sich diese Software in jeder Art von Datei- oder Programmbestandteilen verbergen und sich sozusagen im Vorbei-Surfen auf einem fremden System einnisten. Schadprogramme können auch mit jedem Download, jedem Dateianhang aus einer E-Mail oder schlicht über E-Mails auf das System gelangen.

Kriminelle nutzen sogenannte Ransomware, um Nutzerinnen und Nutzer digital zu erpressen. Solche Schadprogramme verschlüsseln Daten und Dateien auf Computern und/oder angeschlossenen Datenträgern. Die Besitzer des PCs können danach nicht mehr auf diese Daten zugreifen. Für das Entschlüsseln verlangen die Kriminellen ein Lösegeld (ransom) häufig in der Kryptowährung Bitcoin. Wenn Betroffene nicht zahlen wollen, drohen die Täter alle Daten zu löschen. Die Varianten dieser betrügerischen Masche sind vielfältig und immer werden die Betroffenen extrem unter Druck gesetzt. Viele zahlen, statt sich direkt an die Polizei zu wenden.

Eine andere Gefahr geht von Bot-Netzen aus. Sogenannte Bots installieren sich auf einem Rechner meist so, dass es dem PC-Besitzer nicht auffällt. Betrüger schließen „befallene“ Rechner später zu Bot-Netzen zusammen und nutzen sie zum Beispiel für den massenhaften Versand von Spam-Mails. Der Rechner ist mit dem Anschluss an ein Bot-Netz nicht mehr nur geschädigt, sondern führt auch gleichzeitig Straftaten aus. Bot-Netz-Betreiber sind in der Lage den Rechner vollständig und für den Computerbesitzer nahezu unerkannt fern zu steuern.



The image shows a social media profile for Hannah Hassler. The profile includes a name, a profile picture, and several key details:

- Name:** Hannah Hassler
- Mitglied seit:** 06.04.2007
- Geburstag:** 02. August
- Alter:** 31 Jahre

Additional information shown includes the gender (Weiblich) and nationality (German flag). The profile also indicates that she has 249 friends.

TIPPS

- › Schützen Sie Ihren PC durch einen Virenschanner. Halten Sie alle Programme und das Betriebssystem aktuell. Nutzen Sie auch automatische Updatefunktionen. Eine Firewall ist in modernen Betriebssystemen vorhanden oder wird oft durch Antivirensoftware bereitgestellt.
- › Gehen Sie nie mit Administrator-Rechten online. Da ein Angreifer über dieselben Rechte verfügt, wie Sie als angemeldeter Benutzer, kann er das System übernehmen – und Sie selbst von der Nutzung ausschließen. Legen Sie für die Internetnutzung ein Benutzerkonto mit eingeschränkten Rechten an.
- › Öffnen Sie niemals ungeprüft Dateianhänge. Löschen Sie verdächtige E-Mails schon im Posteingang, ohne sie zu öffnen. Lassen Sie sich nicht verunsichern, wenn Sie in der E-Mail mit vollständigem Namen und Adresse angesprochen werden. Cyberkriminelle nutzen diese Daten, um Schadsoftware zu verbreiten.
- › Machen Sie regelmäßig Backups Ihrer Daten auf externen und entfernbaren Datenträgern. Beachten Sie dabei, dass Schadsoftware auch externe Datenträger befallen kann.
- › Stellen Sie Ihren E-Mail-Account auf das „Nur-Text“-Format um, denn E-Mails im HTML-Format können Schadsoftware enthalten.
- › Seien Sie kritisch bei ausführbaren Programm-Dateien mit den Endungen .exe, aber auch .bat, .com oder .vbs. Ändern Sie die Standardkonfiguration Ihres Rechners, um den Dateityp sehen zu können (im Windows-Explo-

rer unter „Extras – Ordneroptionen – Ansicht – Erweiterte Einstellungen – Dateien und Ordner“ das Häkchen vor „Erweiterungen bei bekannten Dateitypen ausblenden“ entfernen).

- › Wird Ihr PC gesperrt und Sie am Monitor aufgrund angeblich strafbarer Handlungen Ihrerseits zu Zahlungen aufgefordert, kommen Sie dieser Aufforderung nicht nach – dabei handelt es sich um Ransomware. Informieren Sie sich darüber auf www.botfrei.de bei Ihrer Polizei und erstatten gegebenenfalls Strafanzeige.
- › Lassen Sie keine Fremden an Ihren PC – auch nicht, wenn sich diese Personen als Support-Mitarbeiter o. Ä. ausgeben und behaupten, Ihr Computer sei mit Viren verseucht.

Rechtliche Aspekte

§ 202a Strafgesetzbuch (StGB)

Ausspähen von Daten

„(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. [...]“

Linkempfehlungen

www.polizei-beratung.de/viren-und-trojaner

www.polizei-beratung.de/bot-netze

www.botfrei.de

www.bsi-fuer-buerger.de

www.sicher-im-netz.de

www.polizei-praevention.de



7. IDENTITÄTSDIEBSTAHL UND PHISHING

Identitätsdiebstahl liegt vor, wenn jemand persönliche Informationen einer anderen Person ausspäht und diese Daten zur Vorspiegelung einer falschen Identität nutzt.

An persönliche Daten gelangen die Betrüger durch Phishing. Dieses geschieht oft durch drive-by-downloads: Besuchen Nutzer infizierte Websites, wird im Hintergrund unbemerkt Schadsoftware auf ihrem Rechner installiert, die Daten abfängt. Betrüger fragen auch in E-Mails sensible Daten ab, indem sie sich als vertrauenswürdige Personen oder Institutionen ausgeben.

Auch soziale Netzwerke werden genutzt, um Nutzer geschickt auf Seiten mit falschen Gewinnspiel- und Gratisaktionen zu locken – ihren Opfern gaukeln Betrüger vor, ein seriöses Unternehmen zu sein (mehr dazu unter „Straftaten in sozialen Netzwerken“).

Beim sogenannten Spear-Phishing versuchen sie zielgerichtet, Vertrauen zu ihrem Opfer aufzubauen und nutzen dafür Informationen aus sozialen Netzwerken, aus Blogs oder von Websites. Dann werden die Opfer gebeten, einen Link in einer E-Mail anzuklicken, der sie auf gefälschte Websites führt. Dort werden bestimmte persönliche Daten wie Bankverbindung, Identifikationsnummer, Zugangscodes und andere sicherheitsrelevante Informationen abgefragt.

Beim Identitätsdiebstahl haben es Kriminelle nicht nur auf das Geld abgesehen – sie begehen im Namen ihrer ahnungslosen Opfer auch Straftaten.

TIPPS

- › Sichern Sie Ihren E-Mail-Account mit einem sicheren Passwort, das zum Beispiel aus den Anfangsbuchstaben der Wörter einer Textzeile besteht, mit Zahlen kombiniert wird und für Fremde kein sinnvolles Wort ergibt. Verwenden Sie keine Kose- oder Tiernamen und Namen von Angehörigen, die sich in sozialen Netzwerken erkennen lassen.
- › Antworten Sie niemals auf verdächtige E-Mails, Tweets oder Beiträge, in denen Sie persönliche Daten preisgegeben sollen. Füllen Sie keine Formulare oder Anmeldeseiten aus, auf die in diesen E-Mails verwiesen wird.
- › Versenden Sie Passwörter grundsätzlich niemals per E-Mail.
- › Nutzen Sie Ihren E-Mail-Account nicht auf öffentlich zugänglichen Rechnern. Ihr Passwort kann dort von Unberechtigten unbemerkt gespeichert werden.
- › Nutzen Sie fremde WLANs, z. B. öffentliche Hotspots an Flughäfen oder in Cafés, nur mit einem VPN (Virtuelles privates Netzwerk). Übermitteln Sie aber auch dann keine vertraulichen Daten.
- › Melden Sie sich beim Online-Banking nur bei Ihrem Konto an, wenn Sie sicher sind, dass Sie sich auf der richtigen Website befinden. Tippen Sie die Internetadresse Ihrer Bank am besten immer direkt in die Adresszeile ein.
- › Banken oder Bezahldienste fordern Sie nie per E-Mail zur Eingabe Ihrer Kundendaten sowie Zugangs- und Bankdaten auf.
- › Erstaten Sie in jedem Fall von Identitätsdiebstahl Strafanzeige, auch wenn der Täter nicht bekannt ist. Melden Sie verdächtige E-Mails Ihrem E-Mail-Provider.

Rechtliche Aspekte

§ 202a Strafgesetzbuch (StGB)

Ausspähen von Daten

„(1) Wer unbefugt sich oder einem anderen Zugang zu Daten, die nicht für ihn bestimmt und die gegen unberechtigten Zugang besonders gesichert sind, unter Überwindung der Zugangssicherung verschafft, wird mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bestraft. [...]“

§ 269 Strafgesetzbuch (StGB)

Fälschung beweisheblicher Daten

„(1) Wer zur Täuschung im Rechtsverkehr beweishebliche Daten so speichert oder verändert, dass bei ihrer Wahrnehmung eine unechte oder verfälschte Urkunde vorliegen würde, oder derart gespeicherte oder veränderte Daten gebraucht, wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.

(2) Der Versuch ist strafbar. [...]“

HINWEIS

Neben der strafrechtlichen Verfolgung können Opfer von Identitätsdiebstahl auch zivilrechtlich gegen den oder die Täter vorgehen, etwa durch Abmahnung, Unterlassungsklage, Forderung von Schadensersatz oder Schmerzensgeld.

Linkempfehlungen

www.polizei-beratung.de/gefahren-im-internet

www.bsi-fuer-buerger.de

www.polizei-praevention.de

ANSPRECHPARTNER DER POLIZEILICHEN KRIMINALPRÄVENTION

Landeskriminalamt

Baden-Württemberg

Polizeiliche Kriminalprävention
Taubenheimstraße 85,
70372 Stuttgart
Tel.: 07 11/54 01-0, -34 58
Fax: 07 11/54 01-1010
E-Mail: praevention@polizei.bwl.de
www.polizei-bw.de

Bayerisches Landeskriminalamt

Polizeiliche Kriminalprävention
Maillingerstraße 15,
80636 München
Tel.: 089/12 12-0, -41 44
Fax: 089/12 12-21 34
E-Mail: blka.sg513@
polizei.bayern.de
www.polizei.bayern.de

Polizei Berlin Landeskriminalamt

Zentralstelle für Prävention
Columbiadamm 4, 10965 Berlin
Tel.: 030/46 64-0, -97 91 13
Fax: 030/46 64-83 97 93 99
E-Mail: lkpraev@polizei.berlin.de
www.polizei.berlin.de

Polizeipräsidium Land Brandenburg

Polizeiliche Kriminalprävention
Kaiser-Friedrich-Str. 143,
14469 Potsdam
Tel.: 03 31/2 83-42 60
Fax: 03 31/2 83-31 52
E-Mail: polizeiliche.praevention@
polizei.brandenburg.de
www.polizei.brandenburg.de

Polizei Bremen

Präventionszentrum
Am Wall 195, 28195 Bremen
Tel.: 04 21/3 62-19 00 3
Fax: 04 21/3 62-1 90 09
E-Mail: praeventionszentrum@
polizei.bremen.de
www.polizei.bremen.de

Landeskriminalamt Hamburg

Polizeiliche Kriminalprävention
Caffamacherreihe 4,
20355 Hamburg
Tel.: 0 40/42 86-50, -7 07 77
Fax: 0 40/42 86-7 03 79
E-Mail: kriminalberatung@
polizei.hamburg.de
www.polizei.hamburg.de

Hessisches Landeskriminalamt

Zentralstelle Kriminal- und
Verkehrsprävention
Hölderlinstraße 1-5,
65187 Wiesbaden
Tel.: 06 11/83-0, - 84 85
Fax: 06 11/83-84 88
E-Mail: beratungsstelle.hlka@
polizei.hessen.de
www.polizei.hessen.de

Landeskriminalamt Mecklenburg-Vorpommern

Polizeiliche Kriminalprävention
Retgendorfer Straße 9,
19067 Rame
Tel.: 0 38 66/64-0, -61 11
Fax: 0 38 66/64-61 02
E-Mail: praevention@lka-mv.de
www.polizei.mvnet.de

Landeskriminalamt

Niedersachsen

Polizeiliche Kriminalprävention
Am Waterlooplatz 11,
30169 Hannover
Tel.: 05 11/2 62 62-0, -32 03
Fax: 05 11/2 62 62-32 50
E-Mail: d32@lka.polizei.
niedersachsen.de
www.polizei.niedersachsen.de

Landeskriminalamt

Nordrhein-Westfalen

Polizeiliche Kriminalprävention
Völklinger Straße 49,
40221 Düsseldorf
Tel.: 02 11/9 39-0, -32 05
Fax: 02 11/9 39-32 09
E-Mail: vorbeugung@polizei.nrw.de
<https://lka.polizei.nrw>

Landeskriminalamt

Rheinland-Pfalz

Polizeiliche Kriminalprävention
Valenciaplatz 1-7, 55118 Mainz
Tel.: 0 61 31/65-0
Fax: 0 61 31/65-24 80
E-Mail: LKA.LS3.L@polizei.rlp.de
www.polizei.rlp.de

Landespolizeipräsidium Saarland

Polizeiliche Kriminalprävention
Graf-Johann-Straße 25-29,
66121 Saarbrücken
Tel.: 06 81/9 62-0, - 28 68
Fax: 06 81/9 62-28 65
E-Mail: lpp246@polizei.slpol.de
www.saarland.de/polizei.htm

Landeskriminalamt Sachsen

Zentralstelle für polizeiliche
Prävention
Neuländer Straße 60,
01129 Dresden
Tel.: 03 51/8 55-0, -23 09
Fax: 03 51/8 55-23 90
E-Mail: praevention.lka@
polizei.sachsen.de
www.polizei.sachsen.de

Landeskriminalamt

Sachsen-Anhalt

Polizeiliche Kriminalprävention
Lübecker Straße 53-63,
39124 Magdeburg
Tel.: 03 91/2 50-0, -24 40
Fax: 03 91/2 50-30 20
E-Mail: praevention.lka@
polizei.sachsen-anhalt.de
www.polizei.sachsen-anhalt.de

Landespolizeiamt

Schleswig-Holstein

Polizeiliche Kriminalprävention
Mühlenweg 166, 24116 Kiel
Tel.: 04 31/1 60-0, -6 55 55
Fax: 04 31/1 60-6 14 19
E-Mail: kiel.lpa132@
polizei.landsh.de
www.polizei.schleswig-holstein.de

Landespolizeidirektion

Thüringen

Polizeiliche Kriminalprävention
Andreasstraße 38, 99084 Erfurt
Tel.: 03 61/6 62-0, -31 71
Fax: 03 61/6 62-31 09
E-Mail: praevention.lpd@
polizei.thueringen.de
www.thueringen.de/th3/polizei

Bundespolizeipräsidium

Polizeiliche Kriminalprävention
Heinrich-Mann-Allee 103,
14473 Potsdam
Tel.: 03 31/9 79 97-0
Fax: 03 31/9 79 97-10 10
E-Mail: kriminalpraevention@
polizei.bund.de
www.bundespolizei.de

IMPRESSUM

Das Werk und seine Teile sind urheberrechtlich geschützt. Jede Verwertung, insbesondere eine Reproduktion oder Vervielfältigung – auch in den elektronischen Medien – bedarf der vorherigen schriftlichen Einwilligung des Herausgebers.

Herausgeber

Polizeiliche Kriminalprävention
der Länder und des Bundes
Zentrale Geschäftsstelle
Taubenheimstraße 85
70372 Stuttgart
www.polizei-beratung.de

Redaktion

Viktoria Jerke
Polizeiliche Kriminalprävention
der Länder und des Bundes

Bildnachweis

Fotos:

Wolfgang Schmidberger (Titel; S. 4;
6; 11; 12; 16; 20; 25; 26; 29; 30; 34)

Abbildungen:

Polizeiliche Kriminalprävention
(S. 5; 27; 31)

Gestaltung

Oscar Charlie GmbH, Stuttgart

Druck

Pfitzer GmbH & Co. KG
Benzstraße 39
71272 Renningen

Stand

08/2019

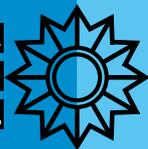


EINE PUBLIKATION IHRER POLIZEI.

Weitere Infos finden Sie unter
www.polizei-beratung.de

Herausgeber:
Polizeiliche Kriminalprävention
der Länder und des Bundes
Zentrale Geschäftsstelle
Taubenheimstraße 85
70372 Stuttgart

**Wir wollen,
dass Sie
sicher leben.**



Ihre Polizei