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

(03V)30.2024.07 OSCAR CHARLIE / H2F

Informationen Ihrer Polizei

SICHERHEIT IM MEDIENALLTAG

KLICKS-MOMENTE FÜR INTERNETNUTZER

Wir wollen, dass Sie sicher leben.
Ihre Polizei

Ihr Ansprechpartner vor Ort:

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 40

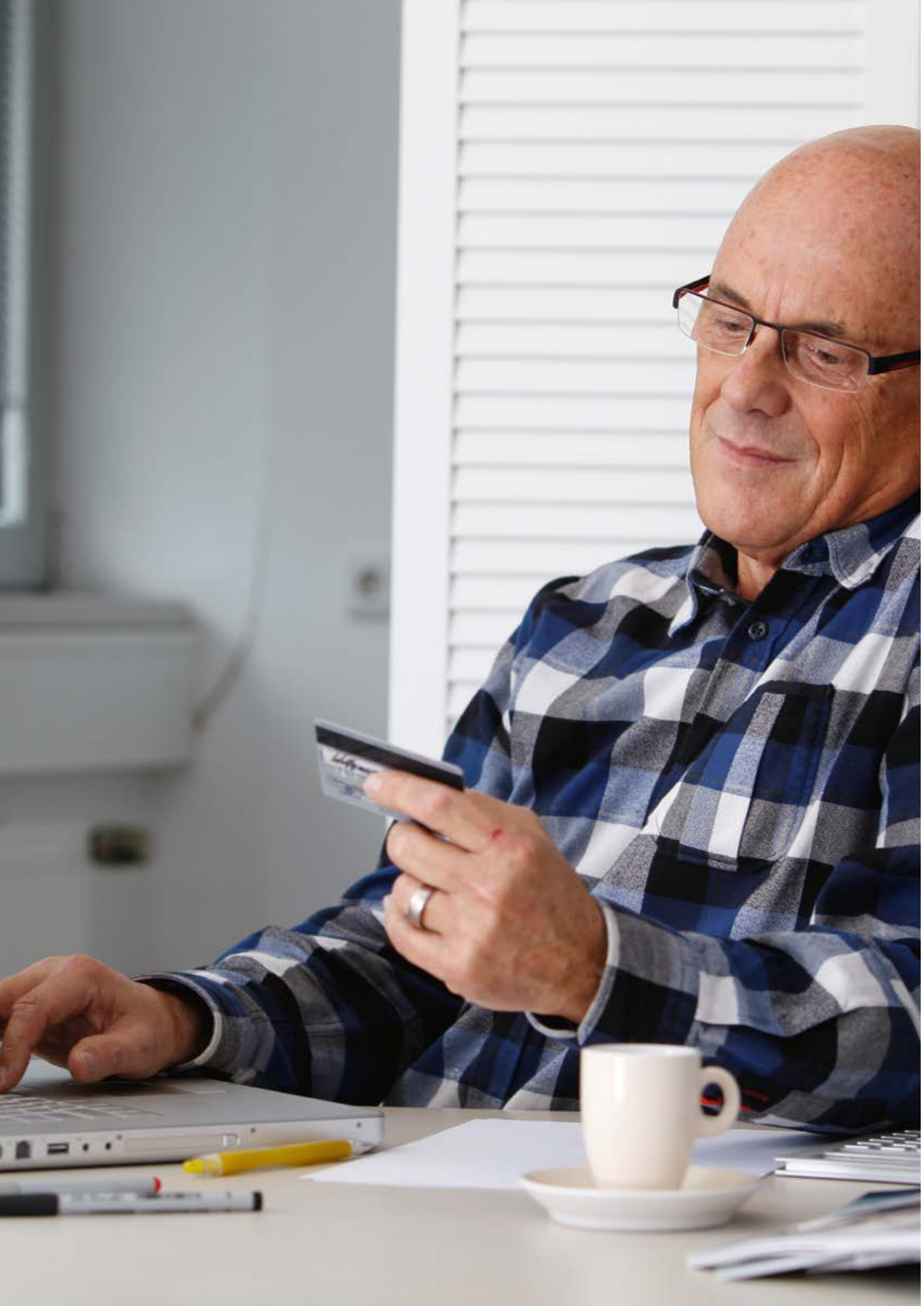
Impressum 43

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 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 Cyberkriminelle 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 Kfz-Verkauf. Die Täter geben sich dabei als Kaufinteressenten aus. Scheinbar versehentlich überweisen sie meist für nicht persönlich begutachtete Fahrzeuge einen höheren Kaufpreis als vereinbart. Danach bitten sie die Verkäufer, den Differenzbetrag zurückzubuchen. Geht der Verkäufer darauf ein, ziehen die Betrüger ihre Überweisung komplett zurück. Eine ähnliche Vorgehensweise gibt es auch mit zu hoch dotierten Schecks.

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. Wer auf solche Angebote eingeht, kann sich wegen Geldwäsche strafbar machen. Durch ihre Überweisungen unterstützen Finanzagenten die Betrüger dabei, die Wege von Geldbeträgen zu verschleiern, die bei anderen Straftaten erbeutet wurden.

TIPPS

Grundsätzliche Verhaltenstipps der Polizei gegen Betrug im Internet:

- Schützen Sie Ihre internetfähigen Geräte, insbesondere Smartphones, durch Antiviren-Programme und regelmäßige System-Updates.
- Schützen Sie Ihre privaten Daten: Veröffentlichen Sie keine persönlichen Daten wie Anschrift, Geburtsdatum oder Arbeitgeber in sozialen Netzwerken und anderen Internetportalen. Betrüger nutzen jede Information, um ihre Opfer zu täuschen und z. B. Geld zu fordern.
- Sichern Sie Online-Accounts in sozialen Netzwerken und in Messenger-Diensten: Nutzen Sie möglichst eine Zwei-Faktor-Authentisierung, um den Account vor Angriffen zu schützen. Verwenden Sie dafür sichere Passwörter. Mehr Tipp dazu finden Sie auf Seite 24.
- Achten Sie auf Ihre Kommunikation in Netzwerken und über Messenger: Werden Sie misstrauisch, wenn Unbekannte Sie anschreiben. Hinterfragen Sie insbesondere Geldforderungen von vermeintlichen Freunden und Verwandten, die sich unter einer fremden Telefonnummer melden. Rufen Sie diese unter einer Ihnen bekannten Nummer an oder bitten Sie um eine Sprachnachricht.
- Nutzen Sie beim Online-Shopping möglichst den Kauf auf Rechnung, um sich vor Fake-Shops zu schützen. Bargeld-Transferdienstleister (z. B. Western Union) sollten Sie nur für Überweisungen an Personen nutzen, die Sie persönlich aus dem realen Leben kennen.
- Achten Sie auf die Kosten: Deutsche Anbieter von Internetseiten müssen Bezahlinhalte mittels eines deutlich erkennbaren Buttons kennzeichnen. Bei einem Abonnement muss neben dem Preis auch die Mindestlaufzeit genannt werden – dies gilt nicht für Angebote auf ausländischen Servern.

TIPPS

Empfehlungen für den Ernstfall:

- Werden Sie misstrauisch bei Angeboten, bei denen viele persönliche Daten benötigt werden und Sie mindestens 18 Jahre alt sein müssen.
- Melden Sie unseriöse Angebote dem Portalbetreiber oder dem Original-Hersteller oder Vertrieb.
- Erste Hilfe bei Betrugsverdacht: Speichern Sie alle E-Mails als Beweis. Fertigen Sie Screenshots von Internetseiten an. Heben Sie auch Überweisungsbelege auf. Machen Sie, wenn möglich, geleistete Zahlungen rückgängig.
- Wenden Sie sich an Ihre örtliche Polizeidienststelle, wenn Sie vermuten, Opfer eines Betrugs im Internet geworden zu sein.

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

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 rechtswidrigen Tat herrührt,
1. verbirgt,
2. in der Absicht, dessen Auffinden, dessen Einziehung oder die Ermittlung von dessen Herkunft zu vereiteln, umtauscht, überträgt oder verbringt,
3. sich oder einem Dritten verschafft oder
4. verwahrt oder für sich oder einen Dritten verwendet […] wird mit Freiheitsstrafe bis zu fünf Jahren oder mit Geldstrafe bestraft.“

2. VERBREITUNG VERBOTENER INHALTE

Gewaltverherrlichende oder pornografische Inhalte sind aufgrund ihrer jugendgefährdenden Wirkung meist verboten. Auch die Herstellung und Verbreitung von solchen Inhalten ist strafbar. 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.

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.

Kinderpornografische Inhalte

Unter Kinderpornografie (Missbrauchsdarstellungen) werden Bilder und Videos verstanden, die den Missbrauch von Kindern unter 14 Jahren zeigen. Gemeint sind damit auch Aufnahmen, die Kinder in unnatürlich geschlechtsbetonter Körperhaltung wiedergeben. oder ihre unbekleideten Geschlechtsteile in sexuell aufreizender Art zur Schau stellen. Strafbar ist der Besitz, das Sich-Verschaffen, das Herstellen oder Verbreiten von Bildern, Filmen, aber auch von Zeichnungen oder Schriften.

Kampagne gegen Missbrauchsdarstellungen

Die polizeiliche Kampagne unter www.soundswrong.de klärt Erwachsene und Kinder über die strafbare Verbreitung von Missbrauchsdarstellungen auf.

SOUNDS WRONG

Linkempfehlungen

www.soundswrong.de
www.polizei-beratung.de
www.jugendschutz.net
www.internet-beschwerdestelle.de
www.polizeifuerdich.de

Rechtliche Aspekte

§ 130 Strafgesetzbuch (StGB)
Volksverhetzung

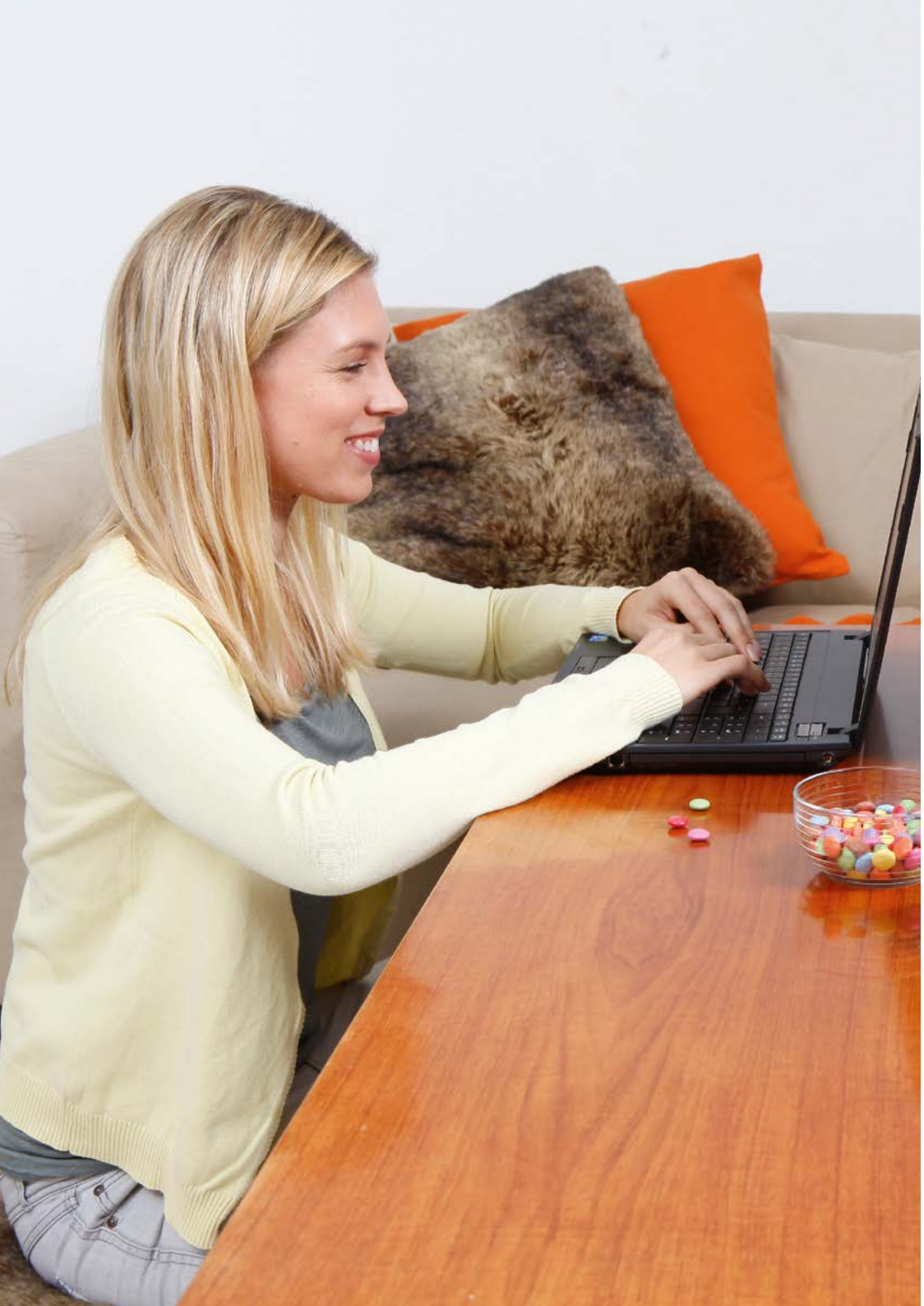
„(1) Wer in einer Weise, die geeignet ist, den öffentlichen Frieden zu stören,
1. gegen eine nationale, rassische, religiöse oder durch ihre ethnische Herkunft bestimmte Gruppe, gegen Teile der Bevölkerung oder gegen einen Einzelnen wegen seiner Zugehörigkeit zu einer vorbezeichneten Gruppe oder zu einem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

§ 131 Strafgesetzbuch (StGB)
Gewaltdarstellung

„Mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe wird bestraft, wer
1. einen Inhalt (§ 11 Absatz 3), der 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 […].“

§ 184 Strafgesetzbuch (StGB)
Verbreitung pornographischer Inhalte

„(1) Wer einen pornographischen Inhalt (§ 11 Absatz 3)
1. einer Person unter achtzehn Jahren anbietet, überlässt oder zugänglich macht,
2. an einem Ort, der Personen unter achtzehn Jahren zugänglich ist oder von ihnen eingesehen werden kann, zugänglich macht […]
wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft […].“



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 – Nutzerinnen und Nutzer haben 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. Vielen ist kaum bewusst, dass sie beispielsweise Aufnahmen von Dritten nicht einfach weiterverwenden dürfen.

Wenn auf den Aufnahmen Bekannte, Familienmitglieder oder Kolleginnen und Kollegen zu sehen sind, dürfen sie nicht ohne deren Erlaubnis im Internet verbreitet werden. 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**).

TIPPS

- Heimliche Film- und Bildaufnahmen von Dritten sind nicht erlaubt – deren Veröffentlichung im Internet ist strafbar.
- Nutzen Sie Inhalte von Dritten ausschließlich in der zugelassen Form. Beachten Sie dabei, dass Veränderungen der Inhalte ausgeschlossen sind.
- Setzen Sie Verlinkungen zu den Webseiten anderer, statt Inhalte zu kopieren. Holen Sie dazu die Zustimmung des Seitenbetreibers ein und geben Sie eine Quelle an.
- 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.
- 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 Seitenbetreiber sind die Voraussetzungen dafür unterschiedlich. Wenden Sie sich bei Verdacht auf eine Straftat an die Polizei.

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

Rechtliche Aspekte

§ 201a Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten 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 Bildaufnahme, die in grob anstößiger Weise eine verstorbene Person zur Schau stellt, unbefugt herstellt oder überträgt […].“

§ 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.bund.de
www.irights.info
www.internet-guetesiegel.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 Nutzerinnen und Nutzer leichtfertig mit ihren Daten umgehen und allgemeine Sicherheitsempfehlungen ignorieren. 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. Auch Erwachsene können wie Kinder und Jugendliche in den sozialen Netzwerken gezielten Anfeindungen ausgesetzt sein. Neben dem unbedachten Umgang mit den eigenen Daten sind 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 um 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

- 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 eine Äußerung.
- 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.

Mehr Informationen über Zivilcourage im Netz finden unter:
www.zivile-helden.de

zivile helden
FÜR MEHR ZIVILCOURAGE

So sichern Sie Online-Accounts

- Bevor Sie ein Profil bei einem Dienst einrichten: Achten Sie auf die AGB und den Datenschutz.
- Nutzen Sie wenn möglich die 2-Faktor-Authentisierung für die Account-Anmeldung, auch bei Messenger-Diensten oder Netzwerk-Konten. Dabei wird neben dem Passwort zusätzlich z. B. die Eingabe eines Codes (verschickt auf ein anderes Gerät in Ihrem Besitz), ein Fingerabdruckscan oder ein USB-Token zur Identifikation gefordert.
- Wählen Sie sichere Passwörter. Nutzen Sie einen Passwort-Manager, damit Sie Passwörter für viele Accounts verwalten können.
- Teilen Sie nie Ihre Login-Daten mit Dritten.
- Überprüfen Sie regelmäßig die Sicherheitseinstellungen Ihrer Netzwerk-Accounts: Machen Sie so viele Bereiche wie möglich ausschließlich für Ihre Freunde sichtbar, z. B. Daten wie Telefonnummer, E-Mail oder auch die Chronik.
- Geben Sie nie Ihre Ausweis- oder Kontodaten in sozialen Netzwerken an.
- Beschränken Sie den Zugriff von anderen Apps z. B. auf Ihr Facebook-Konto. Sie können App-Verknüpfungen nur auf Kontodaten zulassen.
- Klicken Sie nicht auf verdächtige Links.
- Melden Sie Personen, die Sie andauernd unaufgefordert kontaktieren, dem Netzwerkbetreiber. Erstatten Sie Anzeige bei der Polizei in schweren Fällen.
- Melden Sie Personen, die Sie oder andere beleidigen oder bedrohen dem Netzwerkbetreiber oder unter **www.internet-beschwerdestelle.de**
- Melden Sie sich von einem Account nach der Nutzung immer ab. Dies ist besonders wichtig, wenn Sie über fremde Geräte bei Ihrem Account angemeldet waren.

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 öffentlich […] oder mittels einer Tätlichkeit begangen wird, mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bestraft."

Linkempfehlungen

www.bsi.bund.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, Haustechnik 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 Nutzerinnen und Nutzer Cloud-Dienstanbietern, 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.

Linkempfehlungen

www.polizei-beratung.de/gefahren-im-internet
www.bsi-fuer-buerger.de
www.klicksafe.de
www.polizei-praevention.de
www.sicher-im-netz.de

TIPPS

- Nutzen Sie den Gerätesperrcode, die automatische Displaysperre und aktivieren Sie stets die SIM/USIM-PIN.
- Nutzen Sie nur App-Stores seriöser Anbieter. Bei Android: Verbieten Sie in den Einstellungen, dass Apps aus unbekannten 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.
- Richten Sie Drittanbietersperren beim Provider ein, um sich vor Abofallen zu schützen.
- Nutzen Sie, Antivirenprogramme und Überwachungs-Apps, die Ihnen die Berechtigungen von Apps (z. B. Zugriff auf das Telefonbuch) anzeigen.
- Deaktivieren Sie bei Smartphones oder Tablets die automatische Speicherung der Daten in der Cloud. So vermeiden Sie, dass Daten wie Kontoverbindungen usw. unwissentlich dort 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.
- Löschen Sie alle sensiblen Daten, wenn Sie das Gerät verkaufen. Stellen Sie das Gerät dafür auf Werkseinstellungen zurück.

Tipps gegen Betrug bei Whatsapp:

- Code checken: Teilen Sie niemals den sechsstelligen Code zur Verifizierung des Accounts, den Sie bei der Registrierung per SMS erhalten haben.
- PIN checken: Richten Sie eine persönliche PIN für Ihren Account ein, auch bekannt als Verifizierung in zwei Schritten.
- Bild checken: Schützen Sie Ihr Profilbild, damit es nur Ihre Kontakte sehen können.
- Kontakte checken: Wenn vermeintliche Kontakte Sie um einen Gefallen bitten, z. B. um Geld oder andere finanzielle Leistungen, überprüfen Sie ihre Identität, indem Sie um eine Sprachnachricht bitten oder unter der Ihnen bekannten Nummer anrufen.

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 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 einer Kryptowährung. Wenn Betroffene nicht zahlen wollen, drohen die Täter alle Daten zu löschen. Die Varianten dieser betrügerischen Masche sind vielfältig und immer werden die Betroffenen immens unter Druck gesetzt. Viele zahlen, statt sich direkt an die Polizei zu wenden.

Eine andere Gefahr geht von Bot-Netzen aus. Diese Bots genannten Schadprogramme 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.

TIPPS

- Schützen Sie Ihren PC durch einen Virenscanner. Halten Sie alle Programme und das Betriebssystem aktuell. Eine Firewall ist in modernen Betriebssystemen vorhanden oder wird oft durch Antivirensoftware bereitgestellt.
- Gehen Sie nie mit Administrator-Rechten online. Legen Sie für die Internetnutzung ein Benutzerkonto mit eingeschränkten Rechten an.
- Öffnen Sie niemals ungeprüft Dateianhänge. Löschen Sie verdächtige E-Mails im Posteingang, ohne sie zu öffnen.
- 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-Explorer unter „Extras – Ordneroptionen – Ansicht – Erweiterte Einstellungen – Dateien und Ordner" das Häkchen vor „Erweiterungen bei bekannten Dateitypen ausblenden" entfernen).

Erste Hilfe bei Schadsoftware: Die Checkliste von Polizei und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) hilft bei einer Infektion.
www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/ransomware/

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.bund.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 Nutzerinnen und 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 Cyberkriminelle 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, Identifikations-nummer, 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

- Antworten Sie niemals auf verdächtige E-Mails, Tweets oder Beiträge, in denen Sie persönliche Daten preisgeben 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 dann 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.
- Erstatten Sie in jedem Fall von Identitätsdiebstahl Strafanzeige. Melden Sie verdächtige E-Mails Ihrem E-Mail-Provider.

Erste Hilfe bei Phishing finden Sie in der Checkliste von Polizei und dem Bundesamt für Sicherheit in der Informationstechnik (BSI) unter:
www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/phishing/

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 beweiserheblicher Daten
„(1) Wer zur Täuschung im Rechtsverkehr beweiserhebliche 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 […].“

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.bund.de
www.polizei-praevention.de

NOTIZEN

NOTIZEN

ANSPRECHPARTNER DER POLIZEILICHEN KRIMINALPRÄVENTION

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

Bayerisches Landeskriminalamt
Polizeiliche Kriminalprävention
Maillingerstraße 15
80636 München
Tel.: 0 89/12 12-0, -41 44
E-Mail: blka.sg513@polizei.bayern.de
www.polizei.bayern.de

Polizei Berlin Landeskriminalamt
Zentralstelle für Prävention
Columbiadamm 4
10965 Berlin
Tel.: 0 30/46 64 -97 91 14
E-Mail: lkapraev@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
E-Mail: polizeiliche.praevention@polizei.brandenburg.de
www.polizei.brandenburg.de

Polizei Bremen
Zentrale Polizeiliche Prävention
Am Wall 195
28195 Bremen
Tel.: 04 21/3 62 -1 90 03
E-Mail: praeventionszentrum@polizei.bremen.de
www.polizei.bremen.de

Landeskriminalamt Hamburg
Polizeiliche Kriminalprävention
Postfach 60 02 80
22202 Hamburg
Tel.: 0 40/42 86 -7 07 07
E-Mail: kriminalpraevention@polizei.hamburg.de
www.polizei.hamburg

Hessisches Landeskriminalamt
Prävention
Hölderlinstraße 1–5
65187 Wiesbaden
Tel.: 06 11/83-0, -84 85
E-Mail: 0E40.hlka@polizei.hessen.de
www.polizei.hessen.de

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

Landeskriminalamt Niedersachsen
Dezernat FPJ – Zentralstellen
Forschung, Prävention, Jugend
Am Waterlooplatz 11
30169 Hannover
Tel.: 05 11/2 62 62-0, -12 03
E-Mail: fpj@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 08
E-Mail: vorbeugung@polizei.nrw.de
https://lka.polizei.nrw

Landeskriminalamt Rheinland-Pfalz
Polizeiliche Prävention
Valenciaplatz 1–7
55118 Mainz
Tel.: 0 61 31/65-0
E-Mail: LKA.LS3.MA@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
E-Mail: lpp20-kriminalpraevention@polizei.slpol.de
www.saarland.de/polizei.htm

Landeskriminalamt Sachsen
Polizeiliche Kriminalprävention
Neuländer Straße 60
01129 Dresden
Tel.: 0351/855-0, -2309
E-Mail: praevention.lka@polizei.sachsen.de
www.polizei.sachsen.de

Landeskriminalamt Sachsen-Anhalt
Polizeiliche Kriminalprävention
Lübecker Straße 53–63
39124 Magdeburg
Tel.: 0391/250-0, -2440
E-Mail: praevention.lka@polizei.sachsen-anhalt.de
www.polizei.sachsen-anhalt.de

Landespolizeiamt Schleswig-Holstein
Polizeiliche Kriminalprävention
Mühlenweg 166
24116 Kiel
Tel.: 0431/160-0, -65555
E-Mail: kiel.lpa132@polizei.landsh.de
www.polizei.schleswig-holstein.de

Landespolizeidirektion Thüringen
Polizeiliche Kriminalprävention
Melchior-Bauer-Straße 5
99092 Erfurt
Tel.: 0361/5743-16218
E-Mail: praevention.lpd@polizei.thueringen.de
www.thueringen.de/th3/polizei

Bundespolizeipräsidium
Polizeiliche Kriminalprävention
Heinrich-Mann-Allee 103
14473 Potsdam
Tel.: 0331/97997-0
E-Mail: kriminalpraevention@polizei.bund.de
www.bundespolizei.de

Bundeskriminalamt
Polizeiliche Kriminalprävention (IZ 34)
65173 Wiesbaden
Tel.: 0611/55-18034, -18068
E-Mail: iz34-propk@bka.bund.de
www.bka.de

IMPRESSUM

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

Redaktion
Martina Plackmann
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
Bonifatius GmbH
Druck Buch Verlag
Karl-Schurz-Str. 26
33100 Paderborn

Stand
07/2024