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.“

OSCAR CHARLIE

(01V)200.2014.04

Wir wollen, dass Sie sicher leben. Ihre Polizei

www.polizei-beratung.de

Betrug im Internet

Klicks-Momente

Wir wollen, dass Sie sicher leben. Ihre Polizei

Kompetent. Kostenlos. Neutral.

Problematik

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 Internetnutzer Opfer geworden sind. 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 Käufer 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 so genannte Fake-Shops zu, fälschen also Verkaufsplattformen. Eine weitere Variante ist das Anbieten vermeintlicher Gratisleistungen hinter denen sich so genannte Abofallen verbergen. Hier ist die Gratisleistung an den Abschluss eines Abonnements gebunden.

Besonders perfide gehen Betrüger beim Romance-Scamming vor. In Online-Partnerbörsen, Sozialen Netzwerken oder Online-Chats suchen sie Kontakt zu ihren Opfern, erschleichen sich Schritt für Schritt deren Vertrauen und täuschen diesen oft über Wochen eine Liebesbeziehung vor. Dann geben sie vor, in Geldnot geraten zu sein und bitten ihre neue Liebe, ihnen auszuhelfen. Wenn das Opfer nicht mehr zahlen kann oder will, wird der Kontakt abgebrochen.
Was mit Liebesbeziehungen funktioniert, gelingt auch beim Auto- und Immobilienkauf. Dabei wird für ein zum Verkauf angebotenes Auto oder eine Wohnung vom angeblichen Käufer eine versehentlich höhere Summe überwiesen oder per Scheck übergeben. Der Differenzbetrag soll dem Käufer entweder bar ausgehändigt oder zurück überwiesen werden. Damit rechnet der Täter: Er holt seine Überweisung zurück oder der Scheck stellt sich als Fälschung heraus. Damit betreiben Täter aktiv Geldwäsche.

Tipps

- Grundsätzlich gilt: Je verlockender ein Angebot ist, desto misstrauischer sollten Sie sein!
- Zur Überprüfung eines Online-Shops hilft ein Blick in Diskussionsforen im Internet oder auf die Internetseite des Original-Herstellers, der vor Fake-Shops warnt.
- 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 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.
- Nutzen Sie zusätzliche Software gegen Fake-Shops oder Abofallen-Websites (z. B. Abzockschutz der Computerbild oder WOT (Web Of Trust) als warnendes Add-On für Browser).

Linkempfehlungen

www.kaufenmitverstand.de
www.polizei-beratung.de/abofallen
www.polizei-beratung.de/scamming
www.polizei-beratung.de/fake-shops
www.sicherer-autokauf.de
www.mywot.com *(Add-On für Browser gegen als schädlich gemeldete Internetseiten)*
www.verbraucherzentrale.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. […]“

§ 184b Strafgesetzbuch (StGB)
Verbreitung, Erwerb und Besitz kinderpornographischer 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

„Wer Schriften (§ 11 Abs. 3), die grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen oder menschenähnliche Wesen in einer Art schildern, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt,
1. verbreitet,
2. öffentlich ausstellt, anschlägt, vorführt oder sonst zugänglich macht,
3. einer Person unter achtzehn Jahren anbietet, überlässt oder zugänglich macht oder
4. herstellt, bezieht, liefert, vorrätig hält, anbietet, ankündigt, anpreist, einzuführen oder auszuführen unternimmt, um sie oder aus ihnen gewonnene Stücke im Sinne der Nummern 1 bis 3 zu verwenden oder einem anderen eine solche Verwendung zu ermöglichen, wird mit Freiheitsstrafe bis zu einem Jahr oder mit Geldstrafe bestraft.“

Wir wollen, dass Sie sicher leben. Ihre Polizei

www.polizei-beratung.de

OSCAR CHARLIE

(01V)200.2014.04

Verbotene Inhalte im Internet

Klicks-Momente

Wir wollen, dass Sie sicher leben. Ihre Polizei

Kompetent. Kostenlos. Neutral.

Problematik

Nach deutschem Recht stellt die Veröffentlichung und damit auch das Verfügbarmachen bestimmter Inhalte im Internet eine Straftat dar. Diese Inhalte sind, soweit sie auf Servern bereitgestellt werden, die im Geltungsbereich des deutschen Strafgesetzbuchs beheimatet sind, meist wegen der von ihnen ausgehenden Jugendgefährdung 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 eine Entfernung der Inhalte bewirken, ist die Polizei auch für die Strafverfolgung der Verfasser verbotener Inhalte zuständig.

Tipps

» Sichern Sie Beweise für strafbare Inhalte im Internet ausschließlich in Form eines Screenshots und wenden Sie sich damit an die Polizei oder die Meldestellen unter www.jugendschutz.net oder www.internet-beschwerdestelle.de

» 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

Verbotene Inhalte

Verbotene Inhalte im Internet

Verboten sind

Extremistische Inhalte

Extremistische Gruppen und Personen (Rechtsextreme, Linksautonome oder Islamisten) nutzen das Internet, um Propaganda zu verbreiten und insbesondere um junge 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. Darunter fallen Bilder oder Videos von toten, teilweise entstellten Personen, realen Hinrichtungen und anderen gewaltsamen Tötungen.

Linkempfehlungen

www.polizei-beratung.de
www.jugendschutz.net
www.internet-beschwerdestelle.de
www.irights.info
www.klicksafe.de

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.“

Wir wollen, dass Sie sicher leben. Ihre Polizei
www.polizei-beratung.de

OSCAR CHARLIE
(02V)130.2015.03

Persönlichkeits- und Urheberrechte im Internet

Klicks-Momente

Achtung: Aktualisierte Fassung!
Bitte in Mappe austauschen.

Wir wollen, dass Sie sicher leben. Ihre Polizei
Kompetent. Kostenlos. Neutral.

Problematik

Schnell ein Bild aus dem Netz gezogen, das Lieblingslied heruntergeladen oder das selbstgedrehte Video ins eigene Facebook-Profil eingestellt – durch das Mitmach-Web haben 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 Arbeitskollegen 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.

Urheber-rechte

Persönlichkeitsrechte

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 beinhalten die Gefahr von Schadsoftware und zivilrechtlichen Forderungen der Rechteinhaber.

» 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 Faltblatt „Soziale Netzwerke“.

Linkempfehlungen

www.polizei-beratung.de
www.klicksafe.de
www.bsi-fuer-buerger.de
www.irights.info

Rechtliche Aspekte

In Sozialen Netzwerken besteht unter anderem die Gefahr, Opfer von Betrugs- oder Beleidigungsstraftaten zu werden:

§ 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. […]“

§ 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.“

§ 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.“

Wir wollen, dass Sie sicher leben. Ihre Polizei
www.polizei-beratung.de

OSCAR CHARLIE
(01V)200.2014.04

Soziale Netzwerke

Klicks-Momente

Wir wollen, dass Sie sicher leben. Ihre Polizei
Kompetent. Kostenlos. Neutral.

Problematik

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. Da diese praktisch vor den Augen aller Netzwerk-Mitglieder geschehen, wirken sie sich auch auf das reale Leben des Opfers aus. Neben falschen Freunden nutzen Kriminelle die Sozialen Netzwerke für Betrug, beispielsweise indem sie Profile übernehmen, um von Freunden der realen Person Geld zu erpressen oder Daten auszuspähen.

Soziale Netzwerke

Soziale Netzwerke

Tipps

» Achten Sie auch bei der Nutzung Sozialer Netzwerke grundsätzlich auf den Schutz Ihres PCs oder Ihres Smartphones: Nutzen Sie dazu beispielsweise aktuelle Software und Virenscanner.

» Informieren Sie sich über die Allgemeinen Geschäftsbedingungen und die Bestimmungen zum Datenschutz des gewählten Sozialen Netzwerks, bevor Sie dort ein Profil einrichten.

» Nutzen Sie ein sicheres Passwort für Ihren Account, das zum Beispiel aus den Anfangsbuchstaben der Wörter einer Textzeile besteht, mit Zahlen kombiniert wird und für Fremde kein sinnvolles Wort ergibt. Fremde Personen können sonst Ihr Profil und damit Ihre Identität in einem Sozialen Netzwerk übernehmen und Ihren guten Namen missbräuchlich verwenden oder Straftaten begehen.

» Seien Sie zurückhaltend mit der Veröffentlichung persönlicher Daten wie Ihrer Anschrift oder dem Geburtsdatum – und mit Auskünften über Ihren Arbeitgeber. Fragen Sie sich immer, bevor Sie Informationen von sich online verbreiten, ob andere dies wirklich über Sie wissen sollen. Denn der Kreis der Personen, dem Sie Zugang zu Ihren Informationen gewähren, ist nicht statisch – weitere Personen können ebenfalls an diese Informationen gelangen. Geben Sie auch nicht an, dass Sie sich im Urlaub befinden – Einbrecher nutzen dies aus.

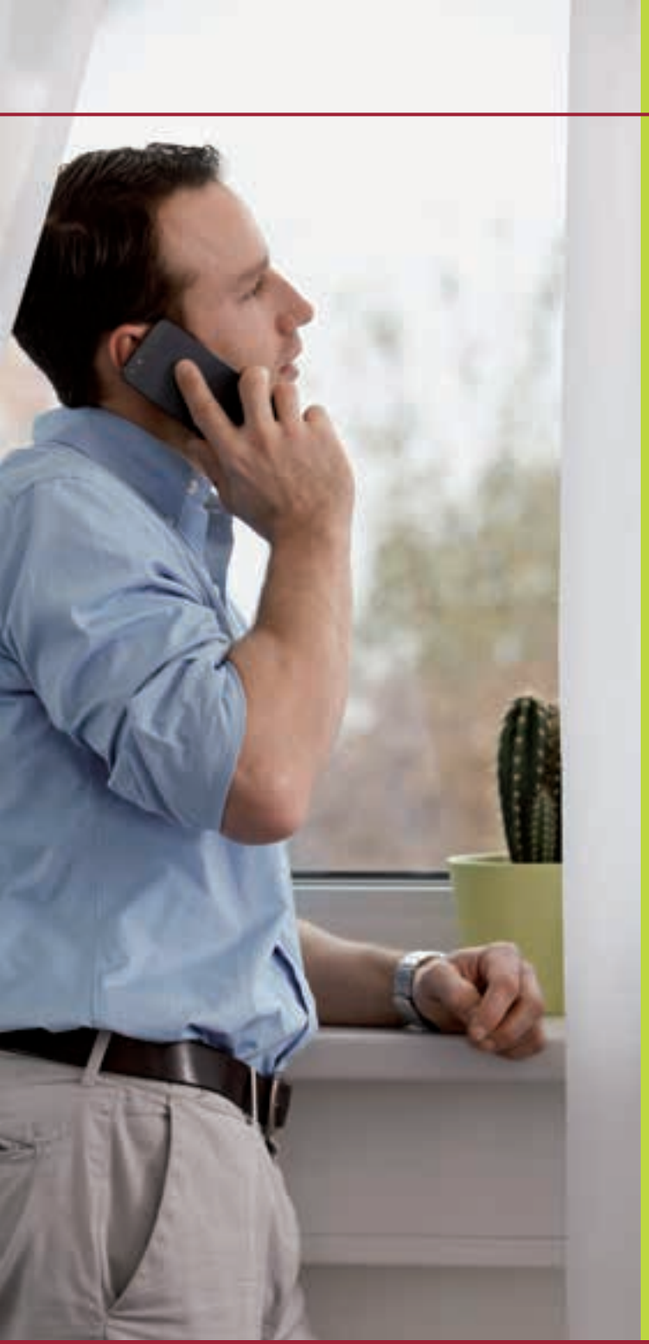
» Ausweis- oder Kontodaten sollten in Sozialen Netzwerken niemals angegeben werden.

» 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.

Linkempfehlungen

www.bsi-fuer-buerger.de
www.sicher-im-netz.de
www.klicksafe.de



Weitere Infos: www.polizei-beratung.de

OSCAR CHARLIE

(01V)200.2014.04

Wir wollen, dass Sie sicher leben.
Ihre Polizei
www.polizei-beratung.de

Smartphone und Tablet-PC

Klicks-Momente

Wir wollen, dass Sie sicher leben.
Ihre Polizei
Kompetent. Kostenlos. Neutral.

Problematik

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. Die Angriffsmöglichkeiten unterscheiden sich bei Smartphones und Tablet-PC und auch je nach verwendetem Betriebssystem. Die Arbeitsweisen der Täter verändern sich ebenso rasant wie die technische Entwicklung dieser Geräte.

Smartphone Tablet-PC

Smartphone und Tablet-PC

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. Passwörter sollten getrennt vom Gerät aufbewahrt werden. Achten Sie bei der PIN-Eingabe darauf, dass niemand Ihr Passwort ausspähen kann.
- Löschen Sie alle sensiblen Daten, wenn Sie das Gerät verkaufen. Stellen Sie das Gerät dafür auf Werkeinstellungen zurück.
- Laden Sie keine Dateien aus unsicheren Quellen herunter. Nutzen Sie nur App-Stores seriöser Anbieter.
- Aktivieren Sie drahtlose Schnittstellen nur bei Bedarf. Tauschen Sie Daten nur mit vertrauenswürdigen Partnern aus.
- 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 (z. B. teure SMS/MMS-Dienste) über die Telefonrechnung verhindern.
- Nutzen Sie, wenn verfügbar, Antivirenprogramme und Überwachungs-Apps, die Ihnen die Berechtigungen von anderen Apps (z. B. Zugriff auf das Telefonbuch) anzeigen.
- Verwenden Sie Online-Banking-Apps nicht auf dem gleichen Gerät, auf dem Sie auch die mobilen TAN empfangen.
- Hinterfragen Sie Provider-Updates, die Sie per SMS, MMS oder als Link erhalten – es kann sich um Schadsoftware handeln.

Linkempfehlungen

www.polizei-beratung.de/gefahren-im-internet
www.bsi-fuer-buerger.de
www.mjv.rlp.de/smartphones
www.klicksafe.de

Weitere Infos: www.polizei-beratung.de

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. […]“

Wir wollen, dass Sie sicher leben.
Ihre Polizei
www.polizei-beratung.de

OSCAR CHARLIE

(01V)200.2014.04

Schadsoftware und Bot-Netze

Klicks-Momente

Wir wollen, dass Sie sicher leben.
Ihre Polizei
Kompetent. Kostenlos. Neutral.

Problematik

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.

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. Der Bot-Netz-Betreiber ist in der Lage den Rechner vollständig und für den Computerbesitzer nahezu unerkannt fern zu steuern.

Schad-
software

Schadsoftware und Bot-Netze

Tipps

» Schützen Sie Ihren PC durch einen Virenscanner. Halten Sie alle Programme und das Betriebssystem aktuell. Nutzen Sie auch automatische Updatefunktionen. Eine Firewall ist in den modernen Betriebssystemen vorhanden oder wird oft durch Antivirensoftware zusätzlich 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. Viele Antivirenprogramme kontrollieren ein- und ausgehende Mails ebenfalls.

» 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).

» 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 so genannte Ransomware. Informieren Sie sich darüber auf www.botfrei.de bei Ihrer Polizei und erstatten gegebenenfalls Strafanzeige.

» Überprüfen Sie Ihren Computer regelmäßig auf Schadsoftware. Nicht jede Schadsoftware wird sofort durch die Scanner erkannt und beseitigt. Nutzen Sie dazu zusätzlich zu Ihrer Anti-Viren-Software beispielsweise ein Programm unter https://www.botfrei.de/decleaner.html

Linkempfehlungen

www.polizei-beratung.de/viren-und-trojaner
www.polizei-beratung.de/bot-netze
www.botfrei.de
www.bsi-fuer-buerger.de
www.verbraucher-sicher-online.de

Rechtliche Aspekte

Phishing oder das Ausspähen von Daten ist unter anderem eine Straftat entsprechend:

§ 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. […]“

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.

Wir wollen, dass Sie sicher leben.
Ihre Polizei
www.polizei-beratung.de

OSCAR CHARLIE

(01V)200.2014.04

Identitätsdiebstahl und Phishing

Klicks-Momente

Wir wollen, dass Sie sicher leben.
Ihre Polizei
Kompetent. Kostenlos. Neutral.

Problematik

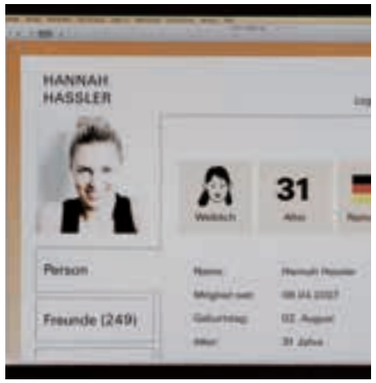
Identitätsdiebstahl liegt vor, wenn jemand persönliche Informationen einer anderen Person ausspäht und diese Daten zur Vorspiegelung einer falschen Identität nutzt. An persönliche Daten gelangen die Betrüger durch Phishing. Dieses geschieht oft durch so genannte drive-by-downloads: Besucht ein Nutzer infizierte Websites, wird im Hintergrund unbemerkt Schadsoftware auf seinem 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. Beim so genannten 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 zum Nachteil Dritter.

Identitäts-
Phishing
diebstahl

Identitätsdiebstahl und Phishing

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 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 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.
- Erstatten Sie in jedem Fall von Identitätsdiebstahl Strafanzeige, auch wenn der Täter nicht bekannt ist. Melden Sie verdächtige E-Mails Ihrem E-Mail-Provider.

Linkempfehlungen

www.polizei-beratung.de/gefahren-im-internet
www.bsi-fuer-buerger.de