SICHER SOCIAL

SICHERER UMGANG MIT SOZIALEN MEDIEN

Ratgeber

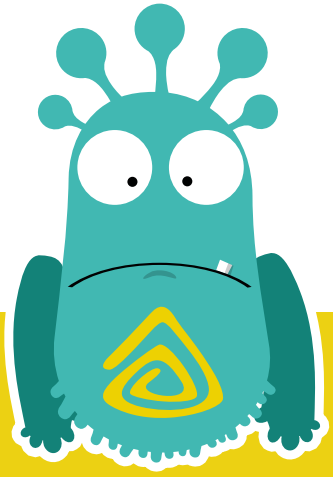
SYNYO

netidee
powerful innovations

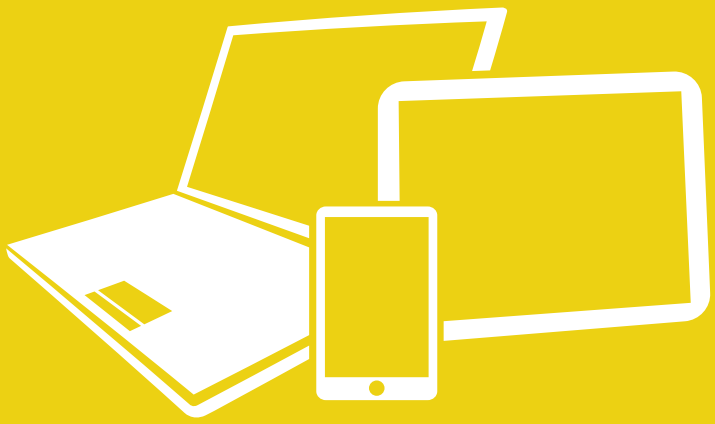
Vorwort

Mit zunehmender Zahl an NutzerInnen von Facebook, Twitter und Co steigt auch die Kriminalität in Sozialen Medien rasant an. Der Mangel an Wissen über diese Phänomene gefährdet speziell jüngere UserInnen. Um die Sicherheit in Sozialen Netzwerken zu erhöhen, entwickelt das Projekt SicherSocial verschiedene Lern- und Arbeitsmaterialien zu diesem Thema. Diese zielen darauf ab, Kinder und jugendliche NutzerInnen zu sensibilisieren sowie Wissen für LehrerInnen und Eltern bereitzustellen.

Die vorliegende Broschüre bietet Eltern einen Überblick über die wesentlichen Phänomene von Kriminalität in Sozialen Medien. Dadurch sollen sie die Gefahren, denen ihre Kinder im Internet womöglich ausgesetzt sind, frühzeitig erkennen und ihnen dadurch entgegenwirken können.



Inhaltsangabe



KAPITEL 1

Social Hacking und Datenschutz in Sozialen Medien

Soziale Medien erlauben es TäterInnen, sehr einfach an öffentlich zugängliche Informationen zu gelangen (Social Hacking). So können sie persönliche oder personenbezogene Informationen oder Daten über Aufenthaltsort, Freundeskreis oder Vorlieben sammeln, die für die Ausführung einer Straftat hilfreich sein können. Das Vorgehen wird durch den Umstand erleichtert, dass es in Sozialen Netzwerken relativ einfach ist, sich über falsche Profile als vertrauenswürdige Person auszugeben. Durch Freundschaftsanfragen, die aus Unwissenheit oder Vertrauenswürdigkeit angenommen werden, können von TäterInnen auch nicht-öffentliche Informationen ausgelesen werden. Außerdem können Daten mit Hilfe von gefälschten Apps gesammelt und missbräuchlich verwendet werden.

Diese gesammelten Informationen können in weiterer Folge für vielerlei Zwecke genutzt werden. Planung von Einbrüchen, Erpressung und Nötigung oder der Missbrauch persönlicher Daten für Spam sind nur einige der unzähligen Möglichkeiten.

Gefahren

Vor allem Kinder und jugendliche NutzerInnen von Sozialen Medien erkennen oft nicht, welche persönlichen Informationen, die zum Beispiel in einem Profil eingebettet und gespeichert sind, eigentlich für fremde NutzerInnen sichtbar oder auffindbar sind. Da die Identität in Sozialen Medien nicht belegt werden muss, ist es außerdem nahezu unmöglich zu erkennen, wer sich tatsächlich hinter einem vermeintlich vertrauenswürdigen Profil verbirgt. Informationen, die durch Social Hacking gesammelt werden, können jedoch eine Straftat oder Erpessung ermöglichen. Daher ist es wichtig, Kindern und Jugendlichen zu vermitteln, dass sie mit Inhalten, die sie posten, und Apps, die sie verwenden, vorsichtig umgehen, und sie mit grundlegenden Fragen des Datenschutzes vertraut zu machen.

FALLBEISPIEL

In einem Fall aus den USA hackte eine Gruppe von TäterInnen alle wichtigen Internet-Konten eines Jugendlichen. Die TäterInnen gaben sich als Mitarbeiter des technischen Supports der jeweiligen Internetdienste aus und erhielten so die Passwörter. Sie griffen auf einzelne Seiten zu und erhielten dadurch die Zugangsdaten zu weiteren Accounts. Innerhalb kurzer Zeit wurde das Google-Konto des Opfers übernommen und gelöscht. Von seinem gekaperten Facebook-Account wurden rassistische Nachrichten abgesetzt. Schließlich wurde seine Apple-ID genutzt, um alle Daten auf seinem iPhone, iPad und MacBook zu löschen.

§

Das Sammeln von öffentlich zugänglichen Daten gilt als Vorbereitungshandlung und ist daher nicht strafbar. Die Verwendung der Daten zur Erpressung oder Nötigung ist jedoch strafbar. Ebenso kann gegen das Veröffentlichen von personenbezogenen Daten im Internet und gegen das Einhacken in Accounts zivil- und strafrechtlich vorgegangen werden.

TIPP

Es gibt mehrere Möglichkeiten, die Gefahr von Social Hacking abzuwenden oder zumindest zu minimieren. Eine relativ einfache Möglichkeit besteht darin, die Sichtbarkeit des persönlichen Profils in einem Sozialen Netzwerk einzuschränken. Außerdem kann das automatische Teilen des aktuellen Standortes bei Postings abgestellt werden. Ebenso sollten persönliche Informationen wie etwa Adresse oder Telefonnummer von Profilen gelöscht werden. Eine regelmäßige online Suche nach dem eigenen Namen kann dazu führen, dass eine missbräuchliche Verwendung persönlicher Daten frühzeitig erkannt wird. In diesem Fall können Löschungsanträge gestellt werden. Weiters sollten wichtige Daten immer mehrfach abgespeichert werden und dasselbe Passwort nicht für unterschiedliche Accounts verwendet werden. Passwörter sollten außerdem regelmäßig erneuert und vermeintlich bekannten Apps nicht blind vertraut werden. Mit offenen WLAN-Netzen und öffentlichen Computern sollte ebenfalls vorsichtig umgegangen werden.

KAPITEL 2

Betrug und Erpressung in Sozialen Medien

Ebenso wie bei „offline" Betrugsfällen wird auch in Fällen von Online-Betrug eine Person unter Vorspiegelung falscher Tatsachen zu einer willentlichen Geldtransaktion bewegt. Sie erhält jedoch nie eine Gegenleistung. Eine verbreitete Variante besteht darin, ein Opfer mit Gutscheinen, Gewinnspielen oder Ähnlichem zu locken. Das Opfer navigiert durch verschiedene Webseiten und soll immer wieder personenbezogene Daten preisgegeben. Ähnlich sind sogenannte „Abo-Fallen", bei denen (oft auch unwissentlich) Abonnements mit versteckten Kosten abgeschlossen werden. Eine andere Variante besteht darin, dass Personen über Soziale Netzwerke für Geldtransfers rekrutiert werden, häufig durch Jobangebote mit Aussicht auf hohe Löhne. Sie überweisen gegen ein Honorar Gelder zwischen verschiedenen Ländern und betreiben dadurch Geldwäsche. Eine dritte Variante ist der sogenannte „Klickbetrug", bei dem Users über das Anklicken von Werbebannern Umsatz für Klickbetrüger generieren. Ziel der Betrüger ist es, so viele Klicks und Reichweite wie möglich zu erhalten. Dadurch tragen User auch zur Verbreitung dieser Betrugsfälle bei.

Soziale Netzwerke werden außerdem immer wieder für Erpressungsversuche genutzt, wenn beispielsweise ein/e TäterIn ein Opfer zu einem Webcam-Chat einlädt und sich so anzügliche Aufnahmen erschleichen. Der/die TäterIn erpresst das Opfer danach mit der Drohung der Veröffentlichung dieser Bilder.

Gefahren

Im Fall von Betrug über Soziale Medien besteht die große Gefahr, dass Kinder und Jugendliche einen Betrugsversuch nicht erkennen und diesen durch „Teilen" und „Liken" verbreiten. Neben klassischen Betrugsmethoden werden zunehmend auch fiktive Währungen in Online-Spielen oder virtuelle Währungen wie BitCoin für Betrugsversuche verwendet. Da Eltern meistens keinen Überblick haben, welchen Aktivitäten Kinder oder Jugendlichen im Internet nachgehen, sind solche Betrugsfälle nur schwer zu kontrollieren – umso wichtiger ist daher die Aufkärung über Gefahren und Risiken.

Bei Erpressungsfällen kommt erschwerend hinzu, dass falsche Profile oft nur schwer zu erkennen sind und Kinder oder Jugendliche dadurch häufig Vertrauen zu TäterInnen aufbauen.

FALLBEISPIEL BETRUG

Auf Facebook wird ein 200 Euro Gutschein für ein bekanntes Bekleidungsgeschäft beworben. Es wird darauf hingewiesen, dass die Anzahl streng limitiert ist und dass das Teilen, Liken und Kommentieren des Gutscheins die Chancen eines Gewinns erhöhen. Außerdem werden zusätzlich persönliche Daten abgefragt, die in weiterer Folge unbefugt weiterverwendet werden.

TIPP

Als erster Schritt, um Betrugsversuchen zu entgegen, sollten Internet-Aktionen genau überprüft werden. Falls sich herausstellt, dass es sich um einen Betrugsversuch handelt, sollte die Information dokumentiert (z.B. durch ein Bildschirmfoto, engl.: *Screenshot*) und in Sozialen Netzwerken über Meldefunktionen gemeldet sowie per E-Mail oder Instant Messaging verbreitet werden, um andere NutzerInnen darauf aufmerksam zu machen.

Weitere Tipps und Informationen unter: www.saferinternet.at/internet-betrug

FALLBEISPIEL ERPRESSUNG

Ein Täter (31) gibt sich in einem Sozialen Netzwerk als Jugendlicher aus und überredet ein Mädchen im Alter von 14 Jahren, ihm Nacktfotos zu senden. Das Opfer wägt sich in Sicherheit, da sich der Chatpartner ebenfalls intim zeigt. Es handelt sich jedoch um ein vorab aufgenommenes Video, das während des Chats abgespielt wird. Mit den Fotos, die der Täter bekommt, erpresst er das Opfer.

Im Fall von Erpressungsversuchen sollte man rechtliche Schritte einleiten und keinesfalls bezahlen. Es widerspricht Nutzungsbedingungen der meisten Sozialen Netzwerke, Nacktfotos zu veröffentlichen – dennoch kann es zuminest kurzfristig zu einer Veröffentlichung kommen. In diesem Fall können die Betroffenen bei den Betreibenden eines Sozialen Netzwerks die Löschung der Bilder beantragen.

TIPP

„Klickbetrug" und das Herauslocken personenbezogener Daten sind strafbare Handlungen, wobei hier auch sogenannte „Abo-Fallen" und allgemein „Online-Betrug" zugeordnet werden. Falls Bilder im Internet veröffentlicht und Dritten zugänglich gemacht werden, wird das Recht auf Datenschutz verletzt. Ebenso strafbar sind das Verschaffen und der Besitz sexueller Darstellungen minderjähriger Personen, wobei auch die Erpressung mit Hilfe von intimen Bildern als Straftatbestand gilt.

KAPITEL 3

Beleidigung und Bedrohung in Sozialen Medien

3A Cybermobbing

Cybermobbing bezeichnet das Beleidigen, Bedrohen, Bloßstellen oder Belästigen eines Opfers mit Hilfe moderner Kommunikationsmittel und Sozialer Medien. Es findet oft in Kombination mit klassischem Mobbing und häufig über einen lägeren Zeitraum hinweg statt.

Es sind unterschiedliche Formen und Kanäle des Mobbings möglich: Von beleidigenden Nachrichten via E-Mail, Instant Messenger, Chat, Forum oder Gästebuch bis hin zu diffamierenden bzw. verunstalteten Fotos oder Filmen, die im Netz verbreitet werden.

TäterInnen nutzen aus, dass sie im Internet relativ anonym agieren können. Gemobbt wird beispielsweise über Aussehen, Gewicht, Religion, Kleidung, Nationalität etc. der Opfer.

Gefahren

Cybermobbing richtet sich meist gegen Kinder und Jugendliche, aber auch Erwachsene können betroffen sein. Durch gruppendynamische Prozesse werden häufig unbeteiligte Personen zu TäterInnen, um nicht selbst zum Opfer zu werden. Im Gegensatz zum klassischen Mobbing tritt Cybermobbing in Sozialen Medien rund um die Uhr auf und erreicht auch ein deutlich größeres Publikum, was den Druck auf das Opfer zusätzlich erhöht.

FALLBEISPIEL

Ein 13-jähriger Schüler findet auf einer Webseite, die auf Facebook verlinkt ist, eine Fotomontage, in der er in einer sexuellen Darstellung gezeigt wird. Der Link wird in Sozialen Netzwerken geteilt und es wird behauptet, er wäre homosexuell. Auch in der Schule wird er täglich deswegen gemobbt. Da er selbst keinen Ausweg aus der Situation sieht, nimmt er sich schließlich das Leben.

Cybermobbing ist ein eigener Strafbestand: Das Mobben eines Opfers, dessen Lebensführung dadurch unzumutbar beeinträchtigt wird, ist strafbar, vor allem, wenn dem Opfer gegenüber „intensives Verfolgungsverhalten" gezeigt wird.

Wichtig ist ein Bewusstsein über Cybermobbing und dessen Anzeichen. Eltern sollten deshalb Beratungs- und Aufklärungsmaßnahmen wie Workshops wahrnehmen.

Im Fall von Cybermobbing sollten Eltern Ruhe bewahren, mit dem Kind darüber reden und dafür sorgen, dass belastende Inhalte im Internet gelöscht werden.

Hilfe, Informationen und Tipps gibt es unter: 147 Rat auf Draht und www.saferinternet.at/fuer-eltern

TIPP

Happy Slapping

„Happy Slapping" ist die Bezeichnung für selbstgefilmte Gewaltvideos, in denen ein grundloser Angriff auf eine meist unbekannte Person gefilmt und über Soziale Netzwerke verbreitet wird. Es findet häufig (aber nicht immer) im öffentlichen Raum statt und geht von überfallsartigen Schlägen auf ein Opfer bis hin zu sexueller Nötigung oder Vergewaltigung. Die Gewaltvideos verbreiten die Vorstellung, dass Gewalt ein Mittel zur Konfliktlösung ist. Opfer werden als schwach dargestellt und es wird angedeutet, dass sie es verdient hätten, geschlagen und erniedrigt zu werden.

FALLBEISPIEL

Zwei Mädchen (13) verprügeln ein anderes, gleichaltriges Mädchen auf einem Spielplatz. Die Tat wird dabei von anwesenden Burschen mitgefilmt. Die Videoaufnahmen werden danach zur Belustigung in unterschiedlichen Sozialen Netzwerken veröffentlicht.

3B Cyberstalking

Als Cyberstalking wird das Nachspionieren, Belästigen, Ausspähen, Verfolgen und Bedrohen von Einzelpersonen über Soziale Medien bezeichnet. Der Täter oder die Täterin setzt sein/ihr Opfer dadurch massiv und dauerhaft psychisch unter Druck. Oft stellt der/die TäterIn dem Opfer schließlich auch im „echten Leben" nach.

Gefahren

Der psychische Druck, der durch ständige und dauerhafte Kontaktierung aufgebaut wird, führt zu einer massiven Beeinträchtigung der Lebensqualität des Opfers. Außerdem verwendet der/die TäterIn oft persönliche Daten des Opfers, um etwa Waren im Internet in seinem Namen zu bestellen. Durch die Lieferung von „Geschenken" an die Privatadresse des Opfers möchte der/die TäterIn dem Opfer noch näher sein. Cyberstalking kann sich schließlich auch verlagern, indem die räumliche Nähe aktiv gesucht wird.

Die Gefahren von Cyberstalking reichten von der Verbreitung von Lügen, Gerüchten oder Verleumdungen über die Veröffentlichung intimer Details bis hin zu Identitätsdiebstahl und Kriminalisierung, etwa durch Begehen von Straftaten im Internet unter dem Namen des Opfers.

FALLBEISPIEL

Ein Täter (33) findet zufällig über einen Blog ein Opfer. Zuerst schreibt er harmlose Nachrichten und möchte eine Chat-Freundschaft eingehen, auf die sich das Opfer zunächst einlässt. Dabei realisiert es nicht, dass es laufend persönliche Daten wie Mobiltelefonnummer, Wohnadresse und Ähnliches preisgibt.

Mit der Zeit wird der Täter zum Stalker und seine Nachrichten im Ton aggressiver – zum Beispiel, wenn das Opfer keine Zeit für ihn hat. Das Opfer möchte schließlich den Kontakt abbrechen, doch der Täter schreibt trotzdem E-Mails, kommentiert Blogeinträge und schickt Text-Nachrichten, in denen er dem Opfer letztlich sogar droht, es umzubringen.

§

Sowohl die beharrliche Verfolgung als auch Nötigung und gefährliche Drohung können als Straftatbestände angesehen werden.

TIPP

Die Maßnahmen gegen StalkerInnen können von Anzeigen über Wegweisung und Betretungsverbote bis hin zur Festnahme reichen. Im Fall von Cyberstalking ist es wichtig, eine detaillierte Dokumentation der Handlungen zu erstellen und alle Nachrichten etc. zu sammeln.

3C Sexting

Sexting setzt sich aus den beiden englischen Wörtern „sex“ und „texting“ zusammen und bezeichnet den Austausch intimer Fotos und/oder Videos über Soziale Medien. Der Austausch der Inhalte findet fast immer freiwillig statt. Problematisch wird Sexting meist dann, wenn diese Inhalte anderen Personen oder Personengruppen zugänglich gemacht werden oder wenn intime Bilder mit unbekannten oder kaum bekannten Personen ausgetauscht werden.

Gefahren

Sexting findet häufig über Apps statt, die Bilder automatisch nach einer gewissen Zeit löschen. Diese Funktion kann jedoch relativ leicht umgangen werden, wenn beispielsweise Screenshots angefertigt werden. Dadurch können Fotos dauerhaft gespeichert werden. Natürlich werden aber auch andere Kanäle und Apps für Sexting verwendet.

Intime Fotos werden häufig aus Rache, Eifersucht oder in Fällen von Cybermobbing verbreitet oder zur Erpressung verwendet.

FALLBEISPIEL

Ein 15-jähriges Mädchen verliebt sich in einen 18-Jährigen und beide schreiben sich häufig Nachrichten über unterschiedliche Apps. Nach einer Weile bittet er sie um intime Fotos, die sie ihm bereitwillig schickt. Einige Tage später wird in der Schule über das Mädchen getuschelt: Ein Mitschüler hat die freizügigen Fotos von ihr im Internet entdeckt und den Link an seine KlassenkollegInnen weitergeschickt. Der Freund des Mädchens hat die Nacktfotos ins Internet gestellt, ohne es ihr zu sagen.

§

Erpressung, Nötigung und gefährliche Drohung stellen Straftatbestände dar, die verfolgt werden können.

Sowohl das Verschaffen als auch der Besitz sexueller Darstellungen minderjähriger Personen ist strafbar.

Neben Aufklärung in Schulen sollten auch Eltern über die Gefahren Bescheid wissen, um ihre Kinder entsprechend unterstützen zu können. Der Umgang mit Bildmaterial sollte mit Kindern und Jugendlichen geklärt werden und anhand von Fallbeispielen aufgeklärt werden, welche Gefahren bestehen. Weiterbildungsangebote wie Elternabende können das Bewusstsein steigern.

Weitere Tipps: www.schau-hin.info

TIPP

KAPITEL 4

Online-Radikalisierung und Hass im Internet

Der Begriff Online-Radikalisierung bezeichnet die Verbreitung von radikalen politischen oder religiösen Botschaften über Soziale Medien. Es reicht von Verhetzung, Mobilisierung und Rekrutierung von Personen über Aufrufe zu Gewalt gegen Angehörige anderer Glaubensgemeinschaften bis hin zu Attentate und Waffengewalt.

Auch die Koordinierung von Aktionen und Angriffen wird über Soziale Medien durchgeführt. NutzerInnen können zur Verbreitung von radikalen Botschaften beitragen und/oder durch die Aufnahme dieser Botschaften radikalisiert werden. Die Radikalisierung erfolgt dabei nicht nach dem Ansehen eines einzelnen Videos oder Lesen eines einzelnen Beitrages, sondern über die Dauer, Häufigkeit und Intensität des Nachrichtenflusses.

Hass im Internet (Hate Speech) durch sogenannte „Hasspostings" oder „Hasskommentare" richtet sich meist gegen bestimmte Menschengruppen und zeichnet sich durch Fremdenfeindlichkeit, Rassismus, Sexismus oder sonstige Formen der Diskriminierung aus.

Gefahren

Die Verbreitung von links- bzw. rechtsradikalem oder radikalem religiösen Gedankengut dient in erster Linie zur Rekrutierung neuer Mitglieder durch radikale Gruppierungen. Personen werden dazu aufgerufen, die Gruppierung zu unterstützen und weitere Mitglieder zu rekrutieren. Soziale Medien sind dafür insofern interessant, als zielgerichtet eine große Menge an Personen erreicht werden kann. Dabei werden in Kombination mit Sozialen Medien auch klassische Webseiten oder Podcats eingesetzt.

Durch Hate Speech werden Personen oder Personengruppe diskriminiert. Dieses Phänomen geht über Mobbing hinaus, denn es ordnet sich in Diskriminierung und Machtverhältnisse in der Gesellschaft ein.

FALLBEISPIEL

Ein 17-Jähriger fühlt sich ausgeschlossen und ist schon seit längerem unglücklich, er sieht keinen Sinn in seinem Leben. Im Internet stößt er auf YouTube-Kanal eines Salafisten-Predigers, der seine Fragen zu beantworten scheint. Er lernt online Personen kennen, die ihm das Gefühl geben, akzeptiert zu werden und die regelmääßig mit ihm chatten. Durch die Chats auf verschiedenen Kanälen gerät er in einen Sog: Die Gespräche werden immer intensiver, er erhält mit der Zeit Gewaltvideos und sonstige Propaganda und wird schließlich auch aufgefordert, nach Syrien zu reisen.

TIPP

Für Eltern ist es wichtig, Kindern eine grundlegende Medienkompetenz sowie ein Gespür für Ironie und Sarkasmus im Internet zu vermitteln, um das Erkennen von falschen oder nicht ernstgemeinten Informationen zu ermöglichen. Außerdem sollten radikale Kommentare direkt in Sozialen Netzwerken sowie an Meldestellen gemeldet werden, z.B. unter www.ombudsmann.at.

Mehr Informationen unter: hass-im-netz.info

Rechtsradikale Aktivitäten sind als Nationalsozialistische Wiederbetätigung strafbar, wenn eindeutige Symbole wie etwa das Hakenkreuz verwendet werden. Der öffentliche Friede wird gefährdet, wenn eine breite Öffentlichkeit (ab ca. 150 Personen) zu Gewalttaten gegen eine bestimmte Gruppe oder deren Mitglieder aufgefordert wird. Für Online-Radikalisierung wie auch für Hasspostings können die Delikte Beleidigung, üble Nachrede, Verleumdung oder Verhetzung herangezogen werden.

Allgemeine Informationen zu den gängigsten Sozialen Netzwerken






ALTERSBEGRENZUNG

Für die Nutzung aller gängigen und hier vorgestellten Sozialen Netzwerke müssen die NutzerInnen 14 Jahre oder älter sein, da sie einen rechtmäßig gültigen Vertrag mit dem jeweiligen Dienst abschließen. Für WhatsApp ist die Nutzung unter 14 Jahren mit Zustimmung der Eltern möglich.

DATENSCHUTZ

Alle der gängigen Sozialen Netzwerke erfassen sämtliche bereitgestellte personenbezogene Daten, außerdem alle Aktivitäten und alle Daten, die von den Kontakten des bzw. der NutzerIn bereitgestellt werden. Zudem werden von allen Dienste Geräteinformationen und Verbindungsdaten, Zahlungsinformationen, Cookies, Standortdaten und, sofern der Zugriff von dem/der NutzerIn erlaubt wird, Kontaktdaten z.B. aus dem Adressbuch des Mobiltelefons gespeichert.

WERBUNG

Alle der gängisten sozialen Netzwerke platzieren personalisierte Werbeeinschaltungen, die anhand der gesammelten Informationen ausgewählt werden. Werbung wird nicht immer als solche gekennzeichnet, etwa bei Facebook und Instagram.

VERBOTENE INHALTE

In allen der hier vorgestellten Sozialen Netzwerke sind pornografische und gewalthaltige Inhalte, Hassreden, Einschüchtern, Mobben und Beleidigen verboten. Inhalte, die gegen die Öffentlichkeits-, Datenschutz-, Urheber-, Marken- oder sonstige geistige Eigentumsrechte anderer verstoßen oder diese verletzen, dürfen ebenfalls nicht veröffentlicht werden.

FACEBOOK, FACEBOOK-APP UND MESSENGER

- Ein Profil muss mit dem richtigen Namen und korrekten Daten des/der NutzerIn erstellt werden. Name, Profilbild, Coverbild, angegebenes Geschlecht, Netzwerke, Username und User-ID sind öffentlich sowohl für Facebook als auch für alle verbundenen Apps und Dienste.
- Wenn Facebook als Login-Account für Spiele verwendet wird und in diesen Spielen Käufe getätigt werden, speichert Facebook – zusätzlich zu den sonstigen Daten – sämtliche Zahlungsinformationen.

INSTAGRAM

- Die App kann auf die Informationen von Drittanbietern (z.B. verbundene Soziale Netzwerke wie Facebook) zugreifen. Erfasst werden außerdem Metadaten wie Hashtags, Geotags, Kommentare und sonstige Daten.
- Nach dem Löschen eines Instagram-Accounts können Daten und Bilder dennoch nach wie vor verfügbar sein, wenn sie von Dritten geteilt wurden.
- Nackt- und Teilnacktfotos dürfen nicht auf Instagram veröffentlicht werden. Fotos von nackten oder teilnackten Kindern werden entfernt.

SNAPCHAT

- Snapchat bietet zusätzliche Dienste an, für die man älter als 14 Jahre sein muss, um sie nutzen zu dürfen.
- Sobald dem Archivierungsservice Memorys einmal zugestimmt wurde, wird es automatisch aktiviert, solange der Snapchat-Account existiert.

- Snapcode und Profilbilder sind in Snapchat öffentliche Daten, eventuell auch Inhalte, die an ein Live-, Lokal- oder ein sonstiges Crowdsourcing-Service geschickt werden.

TWITTER

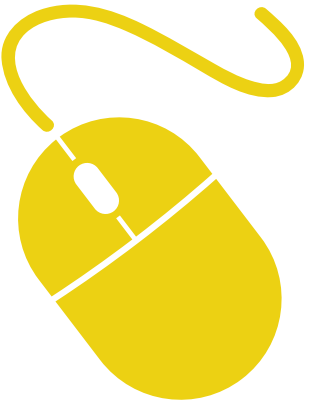
- Was auf Twitter mitgeteilt wird, kann von allen NutzerInnen auf der ganzen Welt unmittelbar angesehen werden.
- Unter gewissen Umstände und wenn sie als sensible Medien gekennzeichnet sind, können bestimmte Inhalte wie gewalthaltige oder pornografische Darstellungen erlaubt sein.
- Accounts, die länger als sechs Monate inaktiv sind, können gelöscht werden.

WHATSAPP

- WhatsApp ist kein Ersatz für einen Telefon- und/oder SMS-Dienst, da es keinen Zugriff auf Notdienste (inklusive Polizei, Feuerwehr und Rettung) anbietet!
- WhatsApp verwendet eine Ende-zu-Ende-Verschlüsselung, sodass nur SenderInnen und EmpfäntgerInnen einer Nachricht diese Nachricht lesen können.
- WhatsApp greift regelmäßig auf die Telefonnummern des Adressbuches eines bzw. einer NutzerIn zu.

YOUTUBE

- Wenn ein/e NutzerIn wiederholt, d.h. mehr als zwei Mal, wegen Copyrightverletzungen identifiziert wird, wird sein/ihr Konto gesperrt.
- Inhalte wie etwa Nacktheit oder Darstellungen realer Gewalt, die grundsätzlich nicht erlaubt sind, können unter gewissen Umständen (etwa bei pädagogischer, dokumentarischer, wissenschaftlicher oder künstlerischer Aufbereitung) mit einer Altersbeschränkung belegt sein und werden daher nicht entfernt.
- Die Verwendung von Spam oder von irreführenden Meta-Daten bzw. Thumbnails können dazu führen, dass Videos entfernt oder das Konto gesperrt werden.



Links

www.saferinternet.at

www.rataufdraht.at

www.jugendschutz.net

www.chatten-ohne-risiko.net

www.ombudsmann.at

www.gemeinsamspielen.at

www.schau-hin.info

www.mobbing-schluss-damit.de

www.cybermobbing-hilfe.de

www.elterngesundheit.at

www. stopline.at

www.klicksafe.de

www.no-hate-speech.de

www.sichersocial.com

facebook.com/sichersocial
twitter.com/sichersocial

SICHER SOCIAL

SYNYO