WEISSER RING
Verbrechensopferhilfe

Tag der Kriminalitätsopfer 2019

Cybercrime

22. Februar 2019, 9:00 -13:00 Uhr
Ort: Bundesministerium für Inneres

WEISSER RING Österreich Bundesgeschäftsstelle | 1090 Wien, Alserbachstraße 18 / Tür 6 |
mobil: 0699 / 134 34 017 | Tel.: 01/712 14 05 | E-Mail: office@weisser-ring.at |
www.weisser-ring.at | www.opfernotruf.at | Opfer-Notruf: 0800 112 112
Spendenkonto: BAWAG P.S.K. | IBAN: AT88 6000 0000 0101 6000 | BIC: BAWAATWW
Der WEISSE RING ist mit dem Österreichischen Spendengütesiegel zertifiziert. Spenden sind steuerlich absetzbar.

Was ist der „Tag der Kriminalitätsopfer“?

Der „Tag der Kriminalitätsopfer“ am 22. Februar soll auf die persönliche, wirtschaftliche und rechtliche Situation von durch strafbare Handlungen geschädigten Menschen aufmerksam machen. Initiator dieses mittlerweile in zahlreichen Ländern Europas begangenen Tages war der damalige Leiter der schwedischen Opferhilfe Björn Lagerbag. Er schlug in Erinnerung an die Ermordung von Ministerpräsident Olof Palme den 22. Februar als Tag der Kriminalitätsopfer vor.

Seit 2011 veranstalten das Bundesministerium für Inneres und der WEISSE RING alljährlich an diesem Tag eine gemeinsame Konferenz zu einem aktuellen Thema. Den Vorschlag dazu machte Ende 2010 die damalige Bundesministerin für Inneres, Mag.[a] Dr.[in] Maria Fekter. Die Initiative wurde von den darauf folgenden Innenminister*innen weitergeführt und so findet die Veranstaltung nunmehr zum neunten Mal statt.

Am 22. Februar 2019 steht das Thema **Cybercrime** im Zentrum der Veranstaltung.

Der europäische Dachverband der Opferhilfe-Einrichtungen „Victim Support Europe“ arbeitet in Kooperation mit der EU daran, den Tag der Kriminalitätsopfer europaweit zu institutionalisieren. 2019 geschieht dies mit einer umfassenden Social Media Kampagne unter dem Motto „Making Victims’ Rights a Reality“ (siehe: https://victimsupport.eu/news/press-releasemaking-victims-rights-a-reality-campaign-kicks-off-on-11-february-2019/)

Cybercrime? Cybercrime!

Cybercrime oder Internetkriminalität wird zunehmend als bedrohlich empfunden. Die Fantasien und Vorstellungen zur Thematik sind dabei uferlos wie die Weiten des Internet selbst. Die einen sind überzeugt davon, dass die Bedrohung ausschließlich große Unternehmen betrifft, die anderen befürchten, dass die herkömmliche Strafverfolgung an ihre Grenzen stößt und sich das Internet zunehmend zu einem „Darknet“ entwickelt.

Cybercrime ist ein umfassender Begriff, der sich bislang einer eindeutigen und abschließenden Definition entzieht. Generell werden darunter Straftaten verstanden, die Informations- und Kommunikationstechnik (IKT) nutzen oder durch die Informations- und Kommunikationstechnik vorsätzlich manipuliert / geschädigt wird.

Die Polizei setzt sich mit der Thematik seit Jahren auseinander: Die Website des Bundeskriminalamtes bietet seit 2011 detaillierte Berichte zu Cybercrime an. Dabei wird zwischen Cybercrime im engeren und im weiteren Sinne differenziert:

- Cybercrime im engeren Sinne umfasst jene Straftaten, bei denen Angriffe auf Daten oder Computersysteme unter Ausnutzung der Informations- und Kommunikationstechnik begangen werden (z.B. Datenbeschädigung, Hacking, DDoS - Attacken).
- Unter Cybercrime im weiteren Sinne versteht man Straftaten, bei denen die Informations- und Kommunikationstechnik zur Planung, Vorbereitung und Ausführung für herkömmliche Kriminaldelikte eingesetzt wird, wie z.B. Betrugsdelikte, Kinderpornografie, Cyber-Grooming oder Cyber-Mobbing. Diese Straftaten können praktisch jede Form von Kriminalität annehmen.

Weltweit steigen die Fälle von Cybercrime. Möglichkeiten der Anonymität und Verschlüsselung sowie die unbegrenzte Verfügbarkeit des Internet tragen wesentlich zu diesem Trend bei.

Österreich kann sich gegenüber diesem Trend nicht abschotten. Im Sicherheitsbericht des Bundesministeriums für Inneres werden fünf Bereiche der Kriminalität statistisch ausgewertet und dargestellt. Zu den „Big Five“ zählen Einbrüche in Wohnungen und Wohnräume / KFZ-Diebstahl, Gewaltdelikte, Cybercrime und Wirtschaftskriminalität. In drei der fünf Bereichen gehen die Fallzahlen zurück oder bleiben annähernd gleich.

Lediglich im Bereich Cybercrime zeigt die grafische Darstellung der Statistik einen steilen Anstieg. Ein Gesamtanstieg von 28,2% wird ausgewiesen und eine Gesamtzahl der Delikte von 16.804 im Jahr 2017. Berücksichtigt werden muss dabei, dass in dieser Statistik das erste Mal der relativ neue § 107c Strafgesetzbuch erfasst wird, der die „Fortgesetzte Belästigung im Wege einer Telekommunikation oder eines Computersystems“ unter Strafe stellt.

Auch im Bereich der Wirtschaftskriminalität sind von 2016 bis 2017 die Fallzahlen gestiegen, die Analyse des Bundesministeriums für Inneres verweist aber auch in diesem Zusammenhang auf die Steigerung im Betrugsbereich, die dem „Bestellbetrug“ geschuldet ist (2016: 8.231 Fälle; 2017: 15.386 Fälle=> Steigerung von 86,9%).

Statements der Redner*innen

Cybercrime: auch virtuelle Gewalt hinterlässt reale Verletzungen!

Das Internet entwickelt sich immer mehr zu einem der Hauptschauplätze von Straftaten. Während die Statistik in fast allen Bereichen der Kriminalität rückläufige bzw. gleichbleibende Zahlen aufweist, lassen sich bei Internet-Kriminalität seit Jahren steigende Zahlen beobachten – sowohl wenn es um Straftaten geht, die Informations- und Kommunikationstechnik nutzen, als auch um solche, durch die Informations- und Kommunikationstechnik vorsätzlich manipuliert und geschädigt wird. Die Bandbreite der Delikte reicht von Datenbeschädigung, Datenfälschung und betrügerischem Datenverarbeitungsmissbrauch bis zu Beleidigung, Betrugsdelikten, Cyber-Mobbing oder Cyber-Grooming.

Mit dieser Entwicklung stehen Opferschutz- und Opferhilfe-Einrichtungen ebenso wie Strafverfolgungsbehörden in ihrer täglichen Arbeit vor neuen Herausforderungen. Während es für Strafverfolgungsbehörden darum geht, mit modernster Technik und Ausbildung eine möglichst hohe Aufklärungsquote zu erreichen, sind Opferhilfe-Einrichtungen damit konfrontiert, dass Gewalt im Netz ganz reale Auswirkungen auf die Psyche der Opfer hat. Auch wenn Betroffene körperlich nicht verletzt werden, kommt es dennoch zu Folgewirkungen, die den Traumata von Opfern körperlicher Gewalt gleichen. Und auch beim Betrug im Internet ist das Geld weg und der wirtschaftliche Schaden entstanden.

Manches ist im Internet sogar wesentlich folgenschwerer als in der realen Welt. So erreichen Beleidigungen im Internet zumeist ein wesentlich größeres Publikum. Und die Speicherung führt oft auch zu einer viel langfristigeren Wirkung. Deshalb ist es nicht nur wichtig, selbst respektvoll im Internet aufzutreten. Es macht auch Sinn, diesen Respekt von anderen einzufordern, Fehlverhalten wie Cyber-Mobbing zu benennen und beispielsweise die Löschung zu verlangen.

Der Tag der Kriminalitätsopfer 2019 steht im Zeichen von Cybercrime im weiteren Sinne – also jener Form, bei der das Internet dazu benutzt wird, Straftaten zu begehen. Wir betrachten sowohl das Clear Net als auch das Deep Web und das Darknet.

Wir freuen uns, dass es uns auch heuer wieder gelungen ist kompetente Expert*innen als Vortragende zu gewinnen und hoffen, dass auch diese Tagung, wie alle vorangegangenen, nicht nur das Bewusstsein der Öffentlichkeit für diese neue Form der Kriminalität verstärkt sondern auch Basis für künftige vernetzte Arbeit im Interesse der betroffenen Verbrechensopfer bietet.

Hon. Prof. Dr. Udo Jesionek, Präsident des WEISSEN RINGS

Cybercrime – Täter*innenprofile und typische Tathergänge

Petra und Hannes sind schon seit Jahren ein Paar. Sie trennt sich von ihm, da sie sich in der Beziehung schon länger unglücklich fühlt. Hannes verkraftet den Schicksalsschlag nicht. Er möchte sich an ihr rächen. Da beide einen PC nutzten, kennt er alle Passwörter und Zugangsdaten von Petra. Kurzerhand ändert er alle ihre wichtigen Passwörter von E-Mail und Sozialen Medien. Plötzlich kann Petra weder auf ihr Android-Smartphone, ihre E-Mails noch ihren Facebook-Account zugreifen. In ihrem Namen versendet er nun intime Fotos und stellt persönliche Daten von ihr ins Internet.

Kaum ein Tag vergeht, an dem die Medien nicht über Cyber-Angriffe berichten. Aufgrund der voranschreitenden Digitalisierung kann Internetkriminalität mittlerweile fast jede*n treffen. Opfer können dabei Firmen, Staaten oder Privatpersonen werden. Dabei spannt sich der Bogen von den klassischen Hacking-Delikten bis hin zu Cyberstalking. Aber was genau ist nun Cybercrime konkret und wie sieht die Situation in Österreich aus? Seit 2006 werden in Österreich die Fälle von Computerkriminalität in der amtlichen Kriminalstatistik unter dem Sammelbegriff „Cybercrime“ erfasst. Im Rahmen eines von KIRAS (österreichisches Sicherheitsforschungsförderprogramm) geförderten Forschungsprojekts wurden im Zeitraum von 2006 bis 2016 Akten des Wiener Straflandesgerichts (N=5404 Akten) wissenschaftlich untersucht.

Dabei wurde den Fragen nachgegangen, wie typische Profile der Cyber-Kriminellen in Österreich aussehen und ob sich bestimmte Muster im Tathergang erkennen lassen. In der Analyse lassen sich zwei Tendenzen erkennen, die in den vergangenen Jahren massiv an Zuwachs gewonnen haben. Es handelt sich dabei um Delikte, die aus finanziellem Interesse heraus durchgeführt werden, wie z. B. der Identitätsdiebstahl sowie um Delikte, die aus der Rache motiviert sind.

Der Vortrag zeigt, in welchen Facetten Cybercrime jede*n treffen kann und die daraus gewonnenen Erkenntnisse sollen dazu beitragen, die Viktimisierung zu reduzieren, Ermittlungen zu erleichtern und Opfer besser aufzuklären.

Dr.in Edith Huber
Sicherheitsforscherin und Leitung der
Stabsstelle Forschungsservice und Internationales, Donau-Universität Krems

Follow me – eine Exkursion ins Darknet

Was die Suchmaschinen nicht automatisiert erfassen, bezeichnet man als Deep Web. Als Darknet wird in der Regel jener Teil des Deep Webs bezeichnet, der nur über Anonymisierungstools erreichbar ist (z.B. Tor Browser). Nicht alles, was dort stattfindet, ist illegal. Anonymität im Kontext Darknet, aber auch im Deep Web ist vor allem für zwei Gruppen interessant. Einerseits gibt es Menschen, die den Schutz des Deep Web für ihre Kommunikation benötigen.

Menschen, die den Schutz des Deep Web für ihre Kommunikation benötigen sind beispielsweise Journalist*innen, die ihre Informant*innen und Quellen schützen. Dissident*innen, Oppositionelle aus Diktaturen, Whistleblower teilen sensible Daten und Informationen. Das Deep Web / Darknet bietet die Möglichkeit, auf Inhalte zuzugreifen, die im Clear Web (Internet) zensiert oder politischen Restriktionen unterworfen sind.

Diese erste Gruppe schützt sich durch das Ausweichen ins Deep Web vor den negativen Folgen ihrer Aktivitäten und vor staatlicher Verfolgung.

Die zweite Gruppe nutzt die Anonymität des Deep Web, um sich der Strafverfolgung zu entziehen. Dabei handelt es sich um Personen, deren Handeln - sollte es im Clear Net (Internet) gesetzt werden - sofort zu Anzeigen und strafrechtlicher Verfolgung führen würde. Im Darknet finden sich Foren, in denen sich Pädophile austauschen oder Tauschbörsen, auf denen kinderpornografisches Material, Videos von Morden und Misshandlungen, geteilt werden.

In Webshops und auf Handelsplattformen werden Waren und Dienstleistungen angeboten die verboten, reglementiert, illegal oder Restriktionen unterworfen sind.

Wie ist dieses Paralleluniversum abseits von Suchmaschinen entstanden? Welchen Einfluss hatten Kryptowährungen auf die Entstehung von Darknet-Marktplätzen und wie schwierig ist es, entsprechende Dienste im Darknet aufzusuchen? Mit welchen Bekämpfungsstrategien reagieren die Strafverfolgungsbehörden auf die Verlagerung von strafbaren Handlungen ins Darknet?

ChefInsp. Robert Lakits, Bundeskriminalamt

Prävention ist entscheidender Hebel – auch gegen Internet-Betrug

Der Internet Ombudsmann (www.ombudsmann.at) unterstützt Online-Konsumentinnen und -Konsumenten bei Problemen rund ums Online-Shopping – gefördert vom Sozialministerium und der Arbeiterkammer. Die Statistik des Internet Ombudsmanns für 2018 spricht eine klare Sprache: Zu finanziellen Schäden führen in der Praxis vor allem Internet-Betrug und verwandte Online-Fallen. So waren beispielsweise 44% aller beim Internet Ombudsmann eingegangenen Beschwerden Internet-Betrug zuzuordnen.

Online-Shopping hat sich etabliert und wenn einmal Probleme auftauchen, bietet das Instrument der Streitschlichtung bewährte Unterstützung. Auch der Internet Ombudsmann ist seit 2016 eine staatlich anerkannte Verbraucherschlichtungsstelle. Bei Betrugsfällen hingegen ist die Vermittlung zwischen den Streitparteien naturgemäß wirkungslos. Ebenso ist die Rechtsdurchsetzung bei unbekannter Täterschaft aus dem Ausland meist aussichtslos. Vor diesem Hintergrund kommt der Prävention eine entscheidende Rolle zu. Deshalb startete der Internet Ombudsmann mit den zusätzlichen Unterstützern netidee, Bundeskriminalamt und willhaben die Watchlist Internet (www.watchlist-internet.at), um zeitnah über aktuelle Betrugsfallen im Netz zu informieren.

Ziel der Watchlist Internet ist es, Internetnutzerinnen und -nutzer in der Sekunde des Zweifels zu erreichen. Also genau in dem Moment, wenn sie sich Fragen stellen wie z.B.: Handelt es sich bei diesen günstigen Angeboten um einen Fake-Shop? Ist die Aufforderung zur Passwort-Änderung wirklich von meiner Bank? Kann der Absender der Nachricht tatsächlich eine intime Videoaufnahme von mir besitzen?

Viele Menschen suchen mittlerweile in so einer Situation nach weiteren Informationen mit Hilfe von Google & Co. Genau da setzt die Watchlist Internet an: Sie stellt suchmaschinen-optimierte, niederschwellig aufbereitete Warnmeldungen bereit und beantwortet die drei Fragen:

- Handelt es sich in einem konkreten Fall um Betrug?
- Was kann ich tun, wenn ich in eine Betrugsfalle geraten bin?
- Wie kann ich mich generell vor Internet-Betrug schützen?

Die Warnungen der Watchlist Internet erreichen bereits mehr als 100.000 Personen pro Monat. Damit ist die Watchlist Internet ein lebendiges Beispiel für Cybercrime-Prävention. Diese Methoden der Betrugsprävention im Internet gilt es kontinuierlich zu verbessern. Prävention kann aber auch bei Internet-Betrug die Rechtsdurchsetzung nicht ersetzen. In beiden Handlungsfeldern braucht es gerade beim Ausbau der internationalen Zusammenarbeit große Anstrengungen.

Ing. Mag. Bernhard Jungwirth, M.Ed.
Geschäftsführer Österreichisches Institut für angewandte Telekommunikation (ÖIAT)
Leiter Internet Ombudsmann

Zivilcourage Online: Jugendliche und Gewalt im Internet

Jugendliche werden heute immer häufiger Opfer von Online Übergriffen wie Cyber-Mobbing, übergriffigen Postings, rassistischen oder anzüglichen Beleidigungen, Erpressungen, denunzierenden und herabwürdigenden Fake-Profilen, Schockvideos bis hin zu physischen Gewalt- oder Tötungsandrohungen. Diese Übergriffe fallen online in der Regel noch massiver aus als im realen Alltag, da die virtuelle Distanz und Anonymität zu einer Enthemmung der Täter*innen führt. Für betroffene Cyber-Opfer ist es besonders belastend, dass solche Übergriffe vor einem ungleich größeren, unkontrollierbaren Kreis unbeteiligter Dritter (sog. Online Bystander) öffentlich zur Schau gestellt werden. Online Bystander haben ein hohes Deeskalationspotential und können den weiteren Konfliktverlauf entscheidend beeinflussen. Dennoch ist die Bereitschaft Jugendlicher, im Fall von beobachteten Online Übergriffen Verantwortung zu übernehmen, gering.

Das Projekt „Zivilcourage 2.0“ rückt das Präventionspotential jugendlicher Online Bystander in den Mittelpunkt. Ziel ist es, jene Faktoren zu identifizieren, die zivilcouragiertes Handeln Jugendlicher in Online-Kontexten fördern oder hemmen. Dazu wurden Gruppendiskussionen mit 142 14- bis 19-Jährigen sowie eine Online-Erhebung mit 1.600 Jugendlichen in derselben Altersgruppe durchgeführt.

Erste Ergebnisse zeigen, dass sich Online Zivilcourage aus Sicht von Jugendlichen stark von Offline Zivilcourage unterscheidet: während im Alltagsverständnis Assoziationen wie „Mut“ und „Heldentum“ mit Zivilcourage verknüpft sind, werden Online Interventionen nicht als besonders couragiert betrachtet. Die befragten Jugendlichen betrachten die Opfer als selbstverantwortlich und rechtfertigen ihr Nicht-Eingreifen auf Basis von Schuldzuschreibungen an das Opfer bzw. Verharmlosungen der Situation. Mit steigender Internetnutzungserfahrung eignen sich Jugendliche die Kompetenz an, Online-Übergriffe

nicht ernst zu nehmen, und nutzen das als eine Bewältigungsstrategie, um mit negativen Inhalten umgehen zu können. Selbst wenn das Opfer das Bedürfnis nach Hilfe klar signalisiert, lassen sich Online Bystander nur schwer zum Handeln bewegen, da es als „armselig“, schwach und kontraproduktiv gilt, um Hilfe zu bitten. Für die praktische Präventionsarbeit ist es zentral, ein verändertes Selbstverständnis von Zivilcourage zu fördern, das Bewusstsein für Normverletzungen zu erhöhen, einfache Möglichkeiten im Erkennen und Artikulieren von Hilfebedürfnissen anzubieten, und Handlungskompetenzen gezielt zu erweitern.

Projekt „Zivilcourage 2.0“

- Projektleitung: Ulrike Zartler; Projektmitarbeit: Christiane Atzmüller, Ingrid Kromer
- Institut für Soziologie der Universität Wien in Kooperation mit der Kirchlich-Pädagogischen Hochschule Wien/Krems
- Projektlaufzeit: 2017 - 2019
- Gefördert im Rahmen des Sicherheitsforschungs-Förderprogramms KIRAS des Bundesministeriums für Verkehr, Innovation und Technologie

Assoz. Prof.in Dr.in Ulrike Zartler, PD
Institut für Soziologie, Universität Wien

„Gemüsehass und Identitätstorte“

Alternative Trainingsmethoden gegen Gewalt im Netz

Auf einer einschlägigen Fetisch-Website tauchen Bilder von den eigenen Füßen auf? Mit der Post kommen wöchentlich Playmobil-Figuren, die mit Blut beschmiert sind? Im E-Mail-Posteingang trudelt eine Nachricht herein, dass verfängliche Daten vom eigenen PC veröffentlicht werden, wenn nicht ein gewisser Betrag in Bitcoin bezahlt wird? Das Handy wird vom Ex-Partner gehackt und getrackt?

Die Anfragen an den Opfer-Notruf 0800 112 112 gehen im digitalen Zeitalter weit über die klassischen Anfragen hinaus. Wer vor mehr als zwei Jahren in der Opferhilfe begonnen hat, las sich in gesetzliche Rahmenbedingungen und Auswirkungen von Viktimisierung und Traumatisierung ein. Dieses Basiswissen ist nach wie vor gefragt und muss aktualisiert werden. Doch parallel dazu gibt es in Opferhilfe-Einrichtungen immer mehr Anfragen, die sich nicht mit herkömmlichem Wissen beantworten lassen.

Jede Anfrage an eine Beratungsstelle geschieht aus dem Gefühl heraus, festgefahren zu sein. Betroffene können sich – im Moment – nicht selbst helfen und brauchen für den nächsten Schritt ein unterstützendes Gespräch oder jemanden, der gut und aktiv zuhört. Manchmal geht das Gefühl der Ratlosigkeit bei Betroffenen so weit, dass Expert*innen von einer Krise sprechen. Welche Inhalte auch immer besprochen werden, es ist von entscheidender Bedeutung für den Verlauf einer solchen Beratung, dass Berater*innen Sicherheit geben, Schritte planen und Überblick bewahren können.

Im Jahr 2018 entwickelte der WEISSE RING gemeinsam mit dem Forschungszentrum Menschenrechte der Universität Wien Trainings für Berater*innen von Opferhilfe-Einrichtungen und Frauenberatungsstellen. Finanziert wurden sowohl Konzept als auch über 20 Trainings österreichweit vom Bundesministerium für Frauen und Gesundheit.

Entstanden ist gebündeltes Wissen zu gesetzlichen Rahmenbedingungen und zu Auswirkungen von Gewalt im Netz gegen Mädchen und Frauen. Darüber hinaus wurden Trainingsmethoden entwickelt, die einen vollkommen neuen und unbeschwerten Zugang zur Thematik erlauben. In erster Linie gilt es, Berührungsängste mit „online"-Themen abzubauen und auf bewährte Strategien zu setzen. Stark gegen Gewalt – reloaded!

MMag.ª Dr.in Dina Nachbaur, Geschäftsführerin WEISSER RING
Mag.ª Sabine Weber, WEISSER RING

Zitate

Hon. Prof. Dr. Udo Jesionek, Präsident des WEISSEN RINGS

„Steigende Zahlen in der Internet-Kriminalität stellen Opferhilfe-Einrichtungen vor neue Herausforderungen. Denn virtuelle Gewalt kann genauso reale Traumafolgen nach sich ziehen wie wir sie von Opfern körperlicher Gewalt kennen."

Sektionschefin Bernadett Humer, Msc, Leiterin der Sektion V (Familien und Jugend) im Bundesministerium für Frauen, Familien und Jugend

Rund 30% aller Jugendlichen waren schon einmal von Cyber-Mobbing betroffen. Das Ziel des Bundeskanzleramts – Sektion Familien und Jugend - ist es daher, Eltern, Jugendlichen und Jugendarbeiter/innen sowie anderen pädagogisch Tätigen Medienkompetenz zu vermitteln und diese zu fördern. Denn Medienkompetenz ist in unserer digitalen Gesellschaft eine entscheidende Schlüsselfähigkeit und der beste Weg, um Kinder und Jugendliche nachhaltig zu schützen!

Dr.in Edith Huber, Sicherheitsforscherin und Leitung der Stabsstelle Forschungsservice und Internationales, Donau-Universität Krems

„Schützen Sie Ihre Passwörter auch vor Menschen, die Ihnen nahestehen. Evidenzbasierte Daten haben ergeben, dass Cybercrime-Täter oft aus dem persönlichen Umfeld kommen."

ChefInsp. Robert Lakits, Bundeskriminalamt

"Deep Web und Darknet bieten Schutz vor Verfolgung - leider auch für Menschen, die dort strafbare Handlungen begehen. Cyberkriminelle haben kein Recht auf Nutzung der Anonymität bei ihren kriminellen Geschäften. Neue Fahndungsmethoden und eine bessere Vernetzung der Polizei steigern den Fahndungsdruck im Darknet."

Ing. Mag. Bernhard Jungwirth, M.Ed., Geschäftsführer Österreichisches Institut für angewandte Telekommunikation (ÖIAT), Leiter Internet Ombudsmann

„Prävention ist einer der entscheidenden Hebel im Kampf gegen Internetbetrug. Deshalb ist es so wichtig, dass Prävention nicht zur Alibi-Aktion verkommt. Es braucht ein ständiges Ringen um wirkungsvolle Methoden und ausreichende Ressourcen."

„International agierende Internet-Betrüger können nur gemeinsam über Ländergrenzen hinweg wirkungsvoll bekämpft werden."

Assoz. Prof.in Dr.in Ulrike Zartler, PD, Institut für Soziologie, Universität Wien

„Für die praktische Präventionsarbeit ist es zentral, ein verändertes Selbstverständnis von Zivilcourage zu fördern, das Bewusstsein für Normverletzungen zu erhöhen, einfache Möglichkeiten im Erkennen und Artikulieren von Hilfebedürfnissen anzubieten, und Handlungskompetenzen gezielt zu erweitern."

MMag.a Dr.in Dina Nachbaur, Geschäftsführerin WEISSER RING

„Betroffene von Gewalt im Netz fühlen sich oft hilflos und ausgeliefert. Wir Berater*innen müssen diesem Sog widerstehen können. Auch wenn sich Gewalt im Netz nicht mit einem Knopfdruck ausschalten lässt – Ziel der Beratung wird immer sein, dass sich Betroffene wieder handlungsfähig fühlen. Dazu braucht es kompetente Berater*innen und laufende Fortbildung."

Mag.a Sabine Weber, WEISSER RING

"In der Praxis können wir Berater*innen selten eine schnelle Lösung anbieten, aber Halt und Orientierung. Da hilft eine gute fachliche Grundlage – ganz besonders bei neuen Arbeitsfeldern. Und die erwirbt man am besten, indem man beim Training selbst aktiv ist, sich emotional auf das Thema einlassen kann und das Training zu guter letzt auch noch Spaß macht."

Forderungen des WEISSEN RINGS

Aus Sicht des WEISSEN RINGS ergeben sich aus der Diskussion des Themas Cybercrime folgende zentrale Forderungen:

- Für eine effiziente und kompetente Beratung von Cybercrime Betroffener braucht es laufende Fortbildung für die Berater*innen in Opferhilfe-Einrichtungen.
- Für die strafrechtliche Verfolgung von Cybercrime braucht es entsprechende Ausbildung und Fortbildung für die handelnden Personen und eine personelle Ausstattung von Strafverfolgungsbehörden, die dem Ausmaß der neuen Herausforderungen entspricht.
- Präventiv müssen User*innen über Maßnahmen informiert und beraten werden, die ihre Sicherheit im Internet erhöhen. Zielgruppe dafür müssen Personen jeden Alters sein.
- Es muss erkennbar und fühlbar sein, dass auch das Internet kein rechtsfreier Raum ist. Zu überlegen sind „Online-Streifen" der Polizei und Projekte, welche die digitale Zivilcourage fördern.
- Die Anzeigenerstattung sollte erleichtert werden und auch online möglich sein.
- Initiativen von NGOs, welche Meldungen von Cybercrime und insbesondere von Gewalt im Netz fördern, sollten unterstützt und ausgebaut werden.
- Opfer von Cybercrime brauchen Beratung und Unterstützung. Der WEISSE RING fordert die Unterstützung von Opfern aller Straftaten entsprechend ihren Bedürfnissen.

Themen des Tags der Kriminalitätsopfer im Rückblick

2011	Ehrenamtliche Mitarbeiterinnen und Mitarbeiter von Opferschutz-Organisationen
2012	Die Richtlinie des Europäischen Parlaments und des Rates über die Mindeststandards für die Rechte und den Schutz von Opfern von Straftaten sowie für die Opferhilfe
2013	Seniorinnen und Senioren als Opfer: Besonders betroffen – besonders betreut?
2014	Betroffen sind sie auch: Angehörige – Hinterbliebene – Tatzeug*innen
2015	Jugendliche als Betroffene von Straftaten im öffentlichen Raum
2016	Tatort Arbeitsplatz: Prävention und Opferhilfe im Rahmen von Gewalt im Arbeitsumfeld
2017	Wenn aus Hass Verbrechen werden: Wirksame Maßnahmen gegen Hasskriminalität
2018	Zivilcourage – Chancen und Risken: Wegschauen ist keine Lösung
2019	Cybercrime

Über den WEISSEN RING

Der WEISSE RING ist Österreichs einzige allgemeine Opferhilfeorganisation, die allen Opfern krimineller Handlungen jeglicher Form offensteht.

Rasch, unbürokratisch und kostenlos werden geboten:

- Professionelle Beratung und Betreuung
- Psychosoziale und juristische Prozessbegleitung
- Finanzielle Hilfe im Notfall

Darüber hinaus ist der WEISSE RING Anlaufstelle und Drehscheibe für Informationen über die Angebote anderer Opferhilfe-Einrichtungen.

Im Auftrag des Bundesministeriums für Verfassung, Reformen, Deregulierung und Justiz betreibt der WEISSE RING den aus ganz Österreich gebührenfrei und rund um die Uhr erreichbaren Opfer-Notruf 0800 112 112 als erste, zentrale Anlaufstelle für alle Opfer krimineller Handlungen.