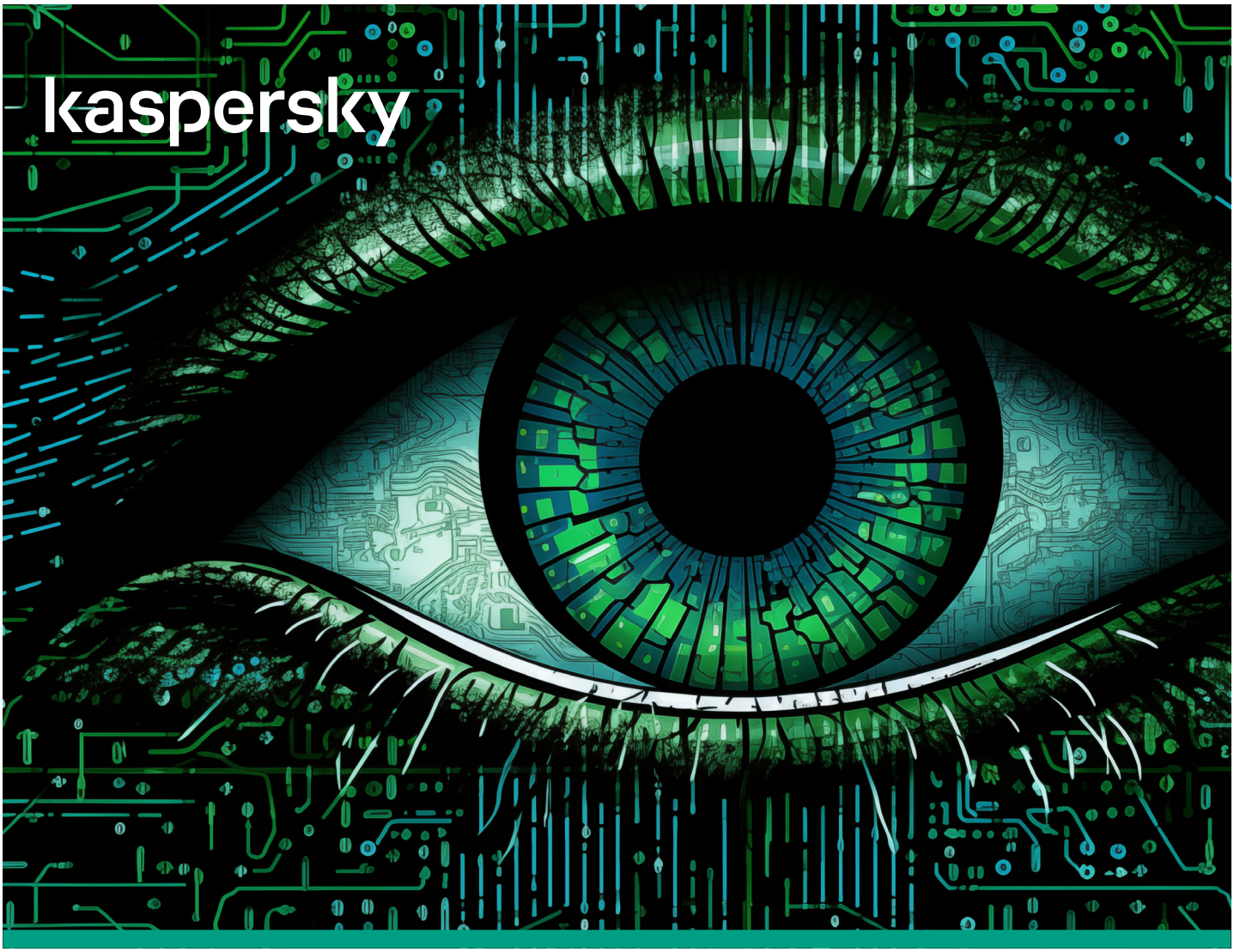


Stalkerware im Jahr 2023

Kaspersky Report
Februar 2024

Inhalt

Die wichtigsten Ergebnisse für 2023

Der jährlich erscheinende ‚State of Stalkerware Report' von Kaspersky soll dazu beitragen, das Bewusstsein und Verständnis für Menschen auf der ganzen zu Welt schärfen, die von digitalem Stalking betroffen sind. Bei Stalkerware handelt es sich um eine legal erhältliche Software, die unauffällig auf Smartphones installiert werden kann und es den Tätern ermöglicht, das Privatleben einer Person, ohne deren Wissen, auszuspionieren. Auch wenn Stalkerware meist über direkten physischen Zugang auf einem Gerät installiert wird, soll im Rahmen unserer Studie auch auf die Bandbreite von Remote-Technologien eingegangen werden, mit denen Stalkerware aus der Ferne installiert werden kann.

Stalkerware kann von jedem Nutzer, der über eine Internetverbindung verfügt, heruntergeladen und installiert werden. Diese Art von Schadsoftware ermöglicht einen ortsunabhängigen Zugriff auf Smartphones; dadurch verletzt der Täter nicht nur die Privatsphäre der anvisierten Zielperson, sondern kann auch mittels der Software auf weitere persönliche Daten des Betroffenen zugreifen. Je nach verwendeter Software kann alles – vom Gerätestandort über Textnachrichten, Chats in sozialen Medien und Fotos bis hin zum Browserverlauf – eingesehen und überwacht werden. Da Stalkerware unbemerkt im Hintergrund arbeitet, sind sich die meisten Betroffenen nicht darüber bewusst, dass jeder ihrer Schritte und sämtliche Online-Aktivitäten ausgekundschaftet werden.

In den meisten Ländern der Welt ist die Verwendung von Stalkerware-Software derzeit nicht verboten, aber die Installation einer solchen Anwendung auf dem Smartphone einer anderen Person ohne deren Zustimmung illegal und strafbar. Allerdings wird nur der Täter zur Verantwortung gezogen, nicht der Entwickler der Anwendung.

Zusammen mit anderen verwandten Technologien ist Stalkerware ein Element technologiegestützten Missbrauchs und wird häufig in zwischenmenschlichen Beziehungen eingesetzt. Da es sich hierbei um einen digitalen Aspekt eines umfassenderen, realen Problems handelt, arbeitet Kaspersky mit einschlägigen Experten und Organisationen auf dem Gebiet der häuslichen Gewalt zusammen – von Hilfsdiensten für Betroffene und Täterprogrammen bis hin zu Forschungseinrichtungen und Behörden. Übergeordnetes Ziel ist es, Wissen auszutauschen sowie Fachleute und Betroffene gleichermaßen zu unterstützen.

Top-Erkenntnisse 2023

- 2023 waren weltweit insgesamt 31.031 einzelne Nutzer von Stalkerware betroffen. Dies entspricht einem Anstieg gegenüber 2022 (29.312) von 5,86 Prozent.
- Das Kaspersky Security Network (KSN) zeigt, dass Stalkerware am häufigsten in Russland, Brasilien und Indien eingesetzt wird und ein globales Problem darstellt, wobei die meisten Nutzer in den folgenden Ländern betroffen sind:
  - In Europa: Deutschland, Frankreich und Vereinigtes Königreich
  - Im Nahen Osten und Afrika: Iran, Türkei und Jemen
  - Im asiatisch-pazifischen Raum: Indien, Indonesien und Philippinen
  - In Lateinamerika: Brasilien, Mexiko und Kolumbien
  - In Nordamerika: USA
  - In Osteuropa (ohne die Länder der Europäischen Union), Russland und Zentralasien: Russland, Weißrussland und Kasachstan
- Die weltweit am häufigsten verwendete Stalkerware-App ist TrackView mit 4.049 betroffenen Personen.
- Knapp ein Viertel (23 Prozent) der von Kaspersky befragten Anwender weltweit geben an, dass sie in irgendeiner Form Online-Stalking durch eine Person erlebt haben, mit der sie kürzlich zusammen waren.
- 40 Prozent gaben an, von Stalking betroffen zu sein oder den Verdacht zu haben, ihnen werde nachgestellt.

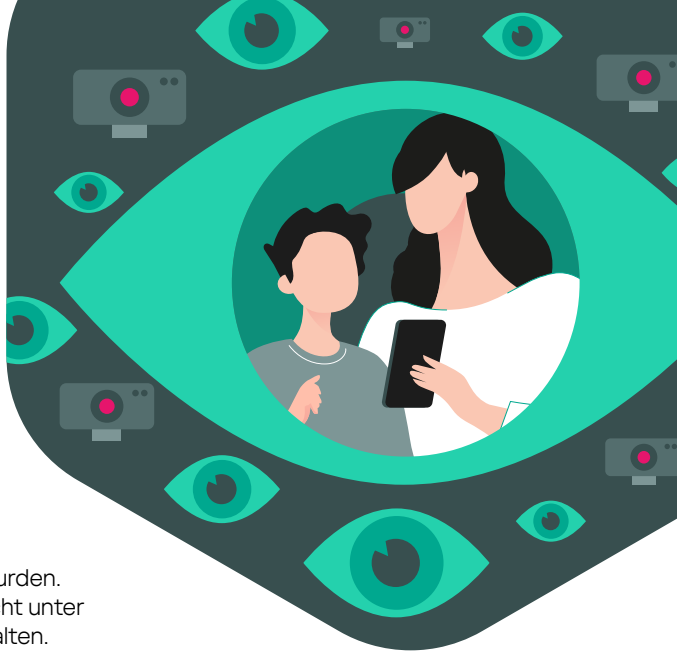
Stalkerware:

Kommerziell erhältliche Software, die zum Ausspionieren verwendet wird. Stalkerware ermöglicht es einer Person, die Aktivitäten auf dem Gerät eines anderen Menschen aus der Ferne zu überwachen, ohne dass dieser zugestimmt hat oder darüber klar und dauerhaft benachrichtigt wird.

Stalking:

Ein auf eine bestimmte Person ausgerichtetes Verhaltensmuster, das Dritte dazu veranlassen würde, sich um die Sicherheit der gestalkten Person zu sorgen. Stalker verwenden verschiedene Taktiken, unter anderen: unerwünschte Kontaktaufnahme durch Telefonanrufe, Textnachrichten, Soziale Medien, unerwünschte Geschenke, Treffen oder Annähern, Beobachtung, Überwachung, Sachbeschädigung und Drohungen.

Trends, die Kaspersky im Jahr 2023 festgestellt hat



Methodik

Die Daten in diesem Bericht stammen aus aggregierten Bedrohungsstatistiken des Kaspersky Security Network, das die Cybersecurity-bezogenen Datenströme von Millionen anonymer und freiwilliger Teilnehmer aus aller Welt verarbeitet. Zur Berechnung der Statistik wurden die Heimanwenderprodukte für mobile Sicherheitslösungen von Kaspersky herangezogen – gemäß den Erkennungskriterien der Koalition gegen Stalkerware. Das bedeutet, dass ausschließlich die von Stalkerware betroffenen Nutzer in die Analyse einbezogen wurden. Andere Arten potenzieller Überwachungs- oder Spyware-Anwendungen, die nicht unter die Definition der Koalition fallen, sind in den Statistiken des Berichts nicht enthalten.

Die Statistiken spiegeln nur die von Stalkerware betroffenen Mobilfunknutzer wider, deren Anzahl sich von der Gesamtsumme an Entdeckungen unterscheidet. Die Zahl der identifizierten Fälle kann theoretisch höher sein, da Stalkerware möglicherweise mehrmals auf demselben Gerät desselben Nutzers entdeckt wurde, falls dieser nach Erhalt einer Benachrichtigung die Malware nicht entfernt hat. Hilfsorganisationen raten oftmals dazu, Stalker-Software nicht zu eliminieren, um Täter nicht darauf aufmerksam zu machen, dass sie entdeckt worden sind.

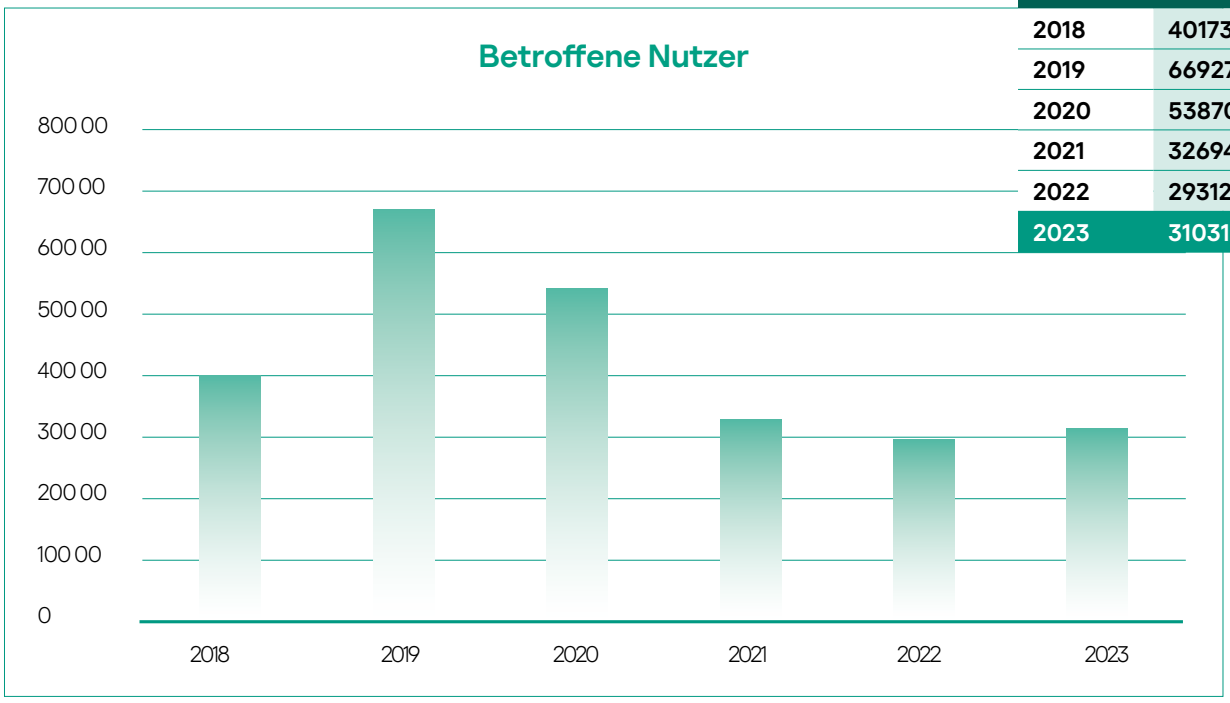
Schließlich spiegeln die Statistiken nur jene mobilen Nutzer wider, die IT-Sicherheitslösungen von Kaspersky einsetzen. Einige Anwender nutzen andere Cybersicherheitslösungen auf ihren Geräten, manche wiederum überhaupt keine.

2023 waren insgesamt 31.031 einzelne Nutzer von Stalkerware betroffen

Globale Erkennungszahlen: Betroffene Nutzer

Anhand globaler und regionaler Statistiken konnte Kaspersky die im Jahr 2023 erhobenen Daten, mit denen der vergangenen vier Jahre vergleichen. Im Jahr 2023 waren insgesamt 31.031 einzelne Nutzer von Stalkerware betroffen, ein leichter Anstieg gegenüber 2022 (29.312 einzelne Nutzer). Die folgende Grafik 1 zeigt, wie sich diese Zahl seit 2018 von Jahr zu Jahr verändert hat.

Jahr	Betroffene Nutzer
2018	40173
2019	66927
2020	53870
2021	32694
2022	29312
2023	31031



Grafik 1: Entwicklung der betroffenen Nutzer im Jahresvergleich seit 2018

Globale und regionale Erkennungszahlen: Geografie der betroffenen Nutzer

Stalkerware ist nach wie vor ein weltweites Problem. Im Jahr 2023 entdeckte Kaspersky betroffene Nutzer in 175 Ländern.

Im Jahr 2023 waren Russland (9.890), Brasilien (4.186) und Indien (2.492) die drei Länder mit den meisten betroffenen Nutzern. Laut Kaspersky-Statistiken haben diese drei Länder seit 2019 die Spitzenposition inne und verzeichnen alle einen Anstieg entdeckter Stalkerware-Infektionen. Der Iran war im vergangenen Jahr in die Reihe der fünf am stärksten betroffenen Länder aufgestiegen und verbleibt dort weiterhin.

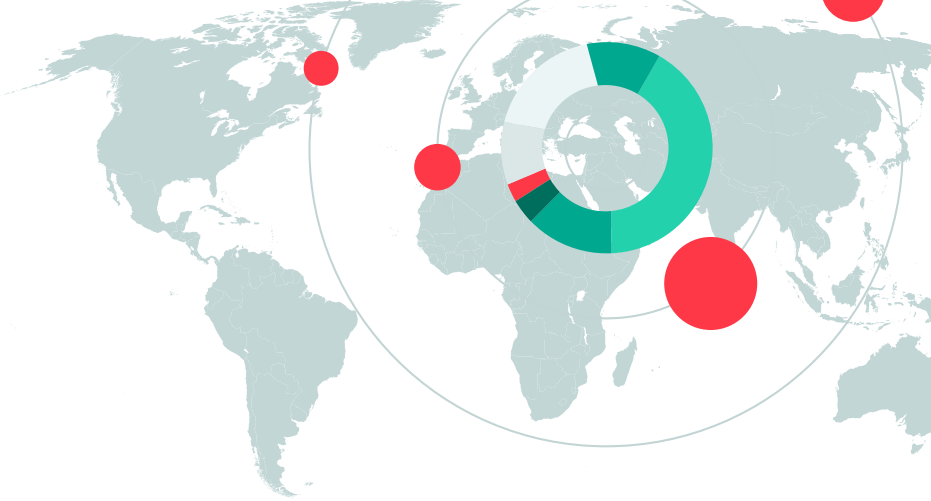
Im Vergleich zu 2021 gibt es leichte Veränderungen bei den Top-10 der betroffenen Länder, wobei die meisten ihre Position beibehalten haben. Während Deutschland vom siebten auf den zehnten Platz zurückfiel, ist Saudi-Arabien (2022 auf Platz acht) in diesem Jahr nicht auf der Liste der am stärksten betroffenen Länder.

2023 entdeckte Kaspersky in 175 Ländern betroffene Nutzer.

	Land	Betroffene Nutzer
1	Russische Föderation	9.890
2	Brasilien	4.186
3	Indien	2.492
4	Iran	1.578
5	Türkei	1.063
6	Indonesien	871
7	USA	799
8	Jemen	624
9	Mexiko	592
10	Deutschland	577

Tabelle 1 – Die zehn am stärksten von Stalkerware betroffenen Länder weltweit im Jahr 2023

In Deutschland waren insgesamt **577** Nutzer betroffen.



	Land	Betroffene Nutzer
1	Deutschland	577
2	Frankreich	332
3	Vereinigtes Königreich	271
4	Spanien	257
5	Italien	252
6	Polen	179
7	Niederlande	177
8	Schweiz	116
9	Österreich	70
10	Portugal	63

Tabelle 2 – Die zehn am stärksten von Stalkerware betroffenen Länder in Europa im Jahr 2023

Die Gesamtzahl der betroffenen europäischen Nutzer lag im Jahr 2023 bei 2.645, ein deutlicher Rückgang gegenüber 2022 (zuvor 3.158). Die drei am stärksten betroffenen Länder in Europa waren Deutschland (577), Frankreich (332) und das Vereinigte Königreich (271). Im Vergleich zu 2021 sind die aufgeführten Länder weiterhin die am stärksten betroffenen in Europa, mit Ausnahme von Griechenland, das aus der Liste herausfiel. Dafür wird Portugal nun auf Platz zehn neu auf der Liste geführt.

	Land	Betroffene Nutzer
1	Russische Föderation	9.890
2	Weißrussland	307
3	Kasachstan	270
4	Ukraine	268
5	Aserbaidschan	243
6	Usbekistan	100
7	Kirgisistan	52
8	Moldawien	49
9	Armenien	43
10	Tadschikistan	30

Tabelle 3 – Die zehn am stärksten von Stalkerware betroffenen Länder in Osteuropa (ohne EU-Länder), Russland und Zentralasien im Jahr 2023

In Osteuropa (ohne die Länder der Europäischen Union), der Russischen Föderation und Zentralasien lag die Gesamtzahl der betroffenen Nutzer im Jahr 2023 bei 11.210; dies bedeutet ebenfalls einen Anstieg gegenüber dem Vorjahr (9.406). Die drei führenden Länder waren Russland, Kasachstan und Weißrussland.

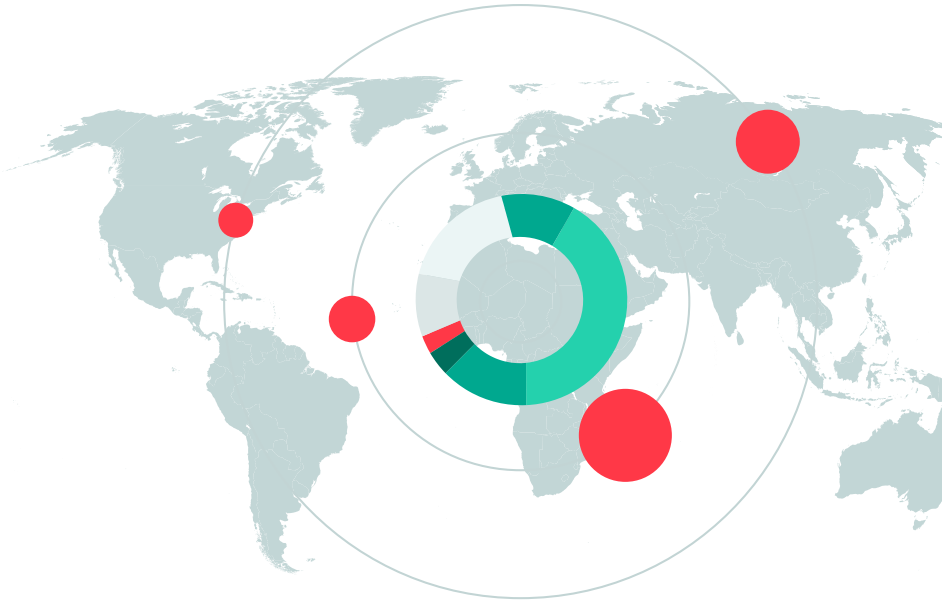
	Land	Betroffene Nutzer
1	Iran	1.578
2	Türkei	1.063
3	Jemen	624
4	Ägypten	569
5	Saudi-Arabien	511
6	Algerien	495
7	Marokko	215
8	Vereinigte Arabische Emirate	184
9	Irak	127
10	Südafrika	126

Tabelle 4 – Die zehn am stärksten von Stalkerware betroffenen Länder im Nahen Osten und Afrika im Jahr 2023

Im Nahen Osten und Afrika lag die Gesamtzahl der kompromittierten Anwender bei 6.561 und damit etwas höher als im Jahr 2022 (6.330), allerdings gab es in diesem Jahr eine kleine Veränderung bei den drei am stärksten betroffenen Ländern. Während 2022 der Iran, die Türkei und Saudi-Arabien am stärksten betroffenen waren, sind es 2023 der Iran, die Türkei und der Jemen gewesen.

Indien liegt mit **2.492** betroffenen Nutzern weiterhin weit vor anderen Ländern der Region.

Brasilien führt mit **4.186** betroffenen Nutzern in der Region Lateinamerika und Karibik.



	Land	Betroffene Nutzer
1	Indien	2.492
2	Indonesien	871
3	Philippinen	323
4	Australien	168
5	Vietnam	97
6	Malaysia	88
7	Japan	85
8	Bangladesch	66
9	Hongkong	51
10	Sri Lanka	51

Tabelle 5 – Die zehn am stärksten von Stalkerware betroffenen Länder im asiatisch-pazifischen Raum im Jahr 2023

In der asiatisch-pazifischen Region ist die Nutzung von Stalkerware im Vergleich zum Vorjahr gestiegen: 4.575 Nutzer waren betroffen, im Jahr 2022 waren es noch 3.187. Indien liegt mit 2.492 betroffenen Nutzern weit vor den anderen Ländern der Region. An zweiter Stelle steht Indonesien mit 871, an dritter Stelle die Philippinen mit 323 und an vierter Stelle Australien mit 168 Betroffenen.

	Land	Betroffene Nutzer
1	Brasilien	4.186
2	Mexiko	592
3	Kolumbien	149
4	Peru	138
5	Argentinien	95
6	Ecuador	88
7	Chile	63
8	Venezuela	19
9	Bolivien	18
10	Paraguay	17

Tabelle 6 – Die zehn am stärksten von Stalkerware betroffenen Länder in Lateinamerika im Jahr 2023

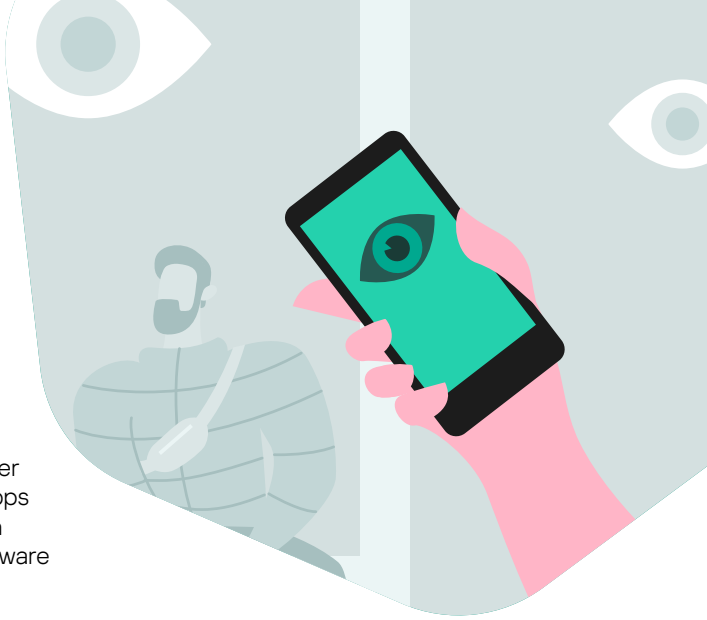
In der Region Lateinamerika und Karibik dominiert Brasilien mit 4.186 Betroffenen Personen; dies macht etwa 76 Prozent der Gesamtzahl der betroffenen Nutzer in der Region aus. Auf Brasilien folgen Mexiko und Kolumbien. Insgesamt wurden 5.478 kompromittierte Anwender in der Region gezählt und bedeutet einen leichten Rückgang gegenüber 2022 (6.170).

	Land	Betroffene Nutzer
1	USA	799
2	Kanada	250

Tabelle 7 – Anzahl der von Stalkerware betroffenen Nutzer in Nordamerika im Jahr 2023

In Nordamerika schließlich befanden sich 77 Prozent aller betroffenen Nutzer in den Vereinigten Staaten. Dies ist angesichts der relativen Größe der Bevölkerung im Vergleich zu Kanada zu erwarten. In der gesamten nordamerikanischen Region waren insgesamt 1.049 Nutzer betroffen.

Globale Erkennungszahlen: Stalkerware-Anwendungen



In diesem Jahr hat Kaspersky 195 verschiedene Stalkerware-Anwendungen entdeckt. Die weltweit am häufigsten für Smartphones verwendete Stalkerware-Anwendung im Jahr 2023 war TrackView, von der 4.049 Nutzer betroffen waren.

Stalkerware-Produkte werden in der Regel als legitime Anti-Diebstahl- oder Kindersicherungs-Apps für Smartphones, Tablets und Computer vermarktet, werden aber in Wirklichkeit zu anderen Zwecken missbraucht. Ohne das Wissen oder die Zustimmung der verfolgten Person installiert, arbeiten sie im Verborgenen und geben dem Täter die Möglichkeit, umfassende Kontrolle über das Leben des Betroffenen zu erlangen. In der Regel werden diese Art von Apps innerhalb der Telefonkonfiguration nicht in der Liste installierter Applikationen angezeigt, sodass sie schwer zu erkennen sind. Die Funktionalität von Stalkerware variiert je nach Anwendung und ob sie kostenpflichtig oder frei erhältlich ist.

	Name der Anwendung	Betroffene Nutzer
1	TrackView	4.049
2	Reptilic	3.089
3	SpyPhone	2.126
4	MobileTracker	2.099
5	Cerberus	1.816
6	Wspy	1.254
7	Unisafe	981
8	Mspy	899
9	MonitorMinor	863
10	KeyLog	852

Tabelle 8 – Top-10 der Stalkerware-Anwendungen im Jahr 2023

> Stalkerware tarnt sich in der Regel als legitime Anti-Diebstahl- oder Kindersicherungs-App auf Smartphones, Tablets und Computern.

Im Folgenden sind einige der häufigsten Funktionen aufgeführt, die in Stalkerware-Anwendungen vorhanden sein können:

- App-Symbol ausblenden
- Lesen von SMS, MMS und Anrufprotokollen
- Zugriff auf Kontakte
- Verfolgung des GPS-Standorts
- Tracking von Kalenderereignissen
- Lesen von Nachrichten in beliebten Messenger-Diensten und sozialen Netzwerken wie Facebook, WhatsApp, Signal, Telegram, Viber, Instagram, Skype, Hangouts, Line, Kik, WeChat, Tinder, IMO, Gmail, Tango, SnapChat, Hike, TikTok, Kwai, Badoo, BBM, TextMe, Tumblr, Weico, Reddit usw.
- Anzeigen von Fotos und Bildern aus den Fotogalerien des Telefons
- Screenshots aufnehmen
- Aufnehmen von Fotos mit der Frontkamera (Selfie-Modus)

Sind Android OS- und iOS-Geräte gleichermaßen von Stalkerware betroffen?

Auf iPhones finden sich viel seltener Stalkerware-Apps als auf Android-Geräten, da iOS traditionell ein geschlosseneres System darstellt. Allerdings können Täter diesen iPhone-Schutz umgehen, wenn sie direkten physischen Zugang zum Telefon haben, um es zu „jailbreaken“ und die Stalkerware-App zu installieren. In jedem Fall sollten iPhone-Nutzer, die ein Stalking befürchten, ihr Gerät immer gut im Auge behalten.

Alternativ dazu kann ein Täter der Zielperson ein iPhone – oder ein anderes Gerät – mit vorinstallierter Stalker-Software anbieten. Es gibt diverse Unternehmen, die diese Dienste online zur Verfügung stellen und es den Tätern ermöglichen, diese Tools auf neuen Telefonen zu installieren und Betroffenen in einer Fabrikverpackung als Geschenk getarnt zukommen zu lassen.

Digitales Stalking, Vertrauen und Dating

Stalkerware und digitales Stalking sind miteinander verwandt und schließen sich gegenseitig nicht aus. Wir haben festgestellt, dass in den vergangenen Jahren vermehrt legitime Technologien und Anwendungen für illegale oder schädliche Zwecke eingesetzt werden – etwa um Partner zu verfolgen und zu überwachen. Um weltweit Einblicke in das umfassendere Thema digitales Stalking und Stalkerware zu erhalten, hat Kaspersky zusammen mit dem Forschungsinstitut Arlington Research insgesamt 21.000 Online-Interviews beauftragt. Hierfür wurden 1.000 Personen in jedem der folgenden Länder befragt: Vereinigtes Königreich, Deutschland, Spanien, Serbien, Portugal, Niederlande, Italien, Frankreich, Griechenland, USA, Brasilien, Argentinien, Chile, Peru, Kolumbien, Mexiko, China, Singapur, Russland, Indien und Malaysia. Die Befragten waren 16 Jahre und älter und befanden sich entweder in einer langfristigen Beziehung (62 Prozent), waren mit jemandem seit Kurzem zusammen (16 Prozent) oder waren zum Zeitpunkt der Befragung nicht liiert, hatten aber in der Vergangenheit eine Beziehung (21 Prozent) gehabt. Die Befragung fand zwischen dem 3. und 17. Januar 2024 statt.

Bei **7 %** wurde heimlich Stalkerware auf deren Geräten installiert

Überblick: Stalking und Betroffene

23 Prozent der Befragten gaben an, dass sie in irgendeiner Form Online-Stalking durch eine Person erlebt haben, mit der sie kürzlich zusammen waren. Es ist auch möglich, dass Dating-Willige öffentlich zugängliche Informationen auf Dating-Apps nutzen, um Stalking oder Missbrauch zu betreiben. Das Spektrum des Missbrauchs ist vielfältig: Mehr als ein Drittel (39 Prozent) der Befragten berichtete über Erfahrungen mit Gewalt oder Missbrauch durch einen aktuellen oder früheren Partner. Insbesondere haben 16 Prozent unerwünschte E-Mails oder Nachrichten erhalten, und 13 Prozent wurden ohne ihre Zustimmung gefilmt oder fotografiert. Darüber hinaus gaben zehn Prozent der Umfrageteilnehmer an, dass ihr Standort verfolgt wurde, weitere zehn Prozent stellten bereits unbefugten Zugriff auf ihre Social-Media-Konten oder E-Mails fest, und bei sieben Prozent der Befragten wurde schon Stalker-Software ohne ihr Wissen auf ihrem Gerät installiert.

Die geschlechtsspezifischen Unterschiede bei diesen Erfahrungen sind offensichtlich: Der Anteil der weiblichen Befragten (42 Prozent), die Gewalt oder Missbrauch erlebt haben, ist höher als bei den männlichen Umfrageteilnehmern (36 Prozent). Personen in erst kurz andauernden Beziehungen berichten häufiger über Gewalt oder Missbrauch als solche in langfristigen Partnerschaften (48 Prozent gegenüber 37 Prozent). Bemerkenswerte 34 Prozent der Befragten äußern sich besorgt über das Potenzial von Online-Stalking, wobei die Besorgnis bei den weiblichen Befragten (36 Prozent) etwas größer ist als bei den männlichen (31 Prozent). Dieses beunruhigende Szenario erstreckt sich auf die ganze Welt, wobei in Teilen Süd- und Mittelamerikas und Asiens mehr Fälle von

Online-Stalking gemeldet werden. So geben beispielsweise 42 Prozent der Befragten in Indien, 38 Prozent in Mexiko und 36 Prozent in Argentinien an, in irgendeiner Form von Online-Stalking betroffen zu sein.

Darüber hinaus gaben 40 Prozent der Befragten an, Stalking erlebt zu haben oder vermuten, dass sie bereits verfolgt wurden. Weitere 14 Prozent konstatierten, dass sie sich nicht an solche Vorfälle erinnern können oder sich nicht sicher sind. Weniger als die Hälfte (46 Prozent) gab an, noch nie gestalkt worden zu sein oder den Verdacht zu haben, dass dies bei ihnen der Fall gewesen sei. Im Vergleich zu 2021 bestätigten weniger Befragte, dass sie durch Technologie belästigt wurden (24 Prozent), aber 2024 konnten sich bemerkenswerte 14 Prozent nicht daran erinnern, dies entspricht einem besorgniserregenden Anstieg von zwei Prozent gegenüber 2021. Regionale Unterschiede zeigen eine höhere Anzahl an Vor-/Verdachtsfällen in Singapur (69 Prozent), Indien (63 Prozent), Malaysia (54 Prozent), Mexiko (53 Prozent), Peru (52 Prozent) und China (50 Prozent), während Portugal (21 Prozent), das Vereinigte Königreich sowie Spanien und Italien (27 Prozent) niedrigere Werte melden.

Unter denjenigen, die Angaben über Vor-/Verdachtsfälle machten, war Stalking über eine Telefon-App am häufigsten (20 Prozent), gefolgt von einer Laptop-App (10 Prozent) und dem Zugriff über eine Webcam (10 Prozent). Während die Mehrheit (78 Prozent) noch nie von ihrem Partner unter Druck gesetzt wurde, Überwachungs-Apps zu installieren oder sich Parameter auf ihrem Telefon vom Partner einstellen zu lassen, berichteten 13 Prozent, dass ein Partner Parameter installiert oder eingestellt hat (14 Prozent im Jahr 2021), und 10 Prozent fühlten sich unter Druck gesetzt, eine Überwachungs-App zu installieren (15 Prozent im Jahr 2021). Bezeichnenderweise berichteten in Indien 34 Prozent der Befragten, dass ihre Partner Parameter installieren bzw. festlegen, und 29 Prozent sahen sich dem Druck ausgesetzt, Überwachungsanwendungen zu installieren.

Besorgniserregend ist, dass 12 Prozent der Befragten zugaben, selbst Parameter auf dem Telefon ihres Partners zu installieren oder einzustellen, während neun Prozent einräumten, ihren Partner unter Druck gesetzt zu haben, selbst Überwachungs-Apps zu installieren. In Indien tat dies ein Drittel und 26 Prozent drängten dort ihre Partner zur Installation von Überwachungs-Apps.

Das Wissen über Stalkerware war unterschiedlich: 46 Prozent der Befragten wussten nichts darüber, 17 Prozent waren sich unsicher und nur 37 Prozent waren überzeugt zu wissen, was Stalkerware ist. Von denjenigen, die sich sicher waren, konnten jedoch weniger als zehn Prozent alle Überwachungsmöglichkeiten benennen. Zum Vergleich: Im Jahr 2021 wussten 40 Prozent über Stalkerware Bescheid, 19 Prozent waren sich nicht sicher. Falls Befragte im Jahr 2024 Stalker-Software auf ihren Geräten auffinden, würden 38 Prozent versuchen, die für diese Installation verantwortliche Person zu identifizieren und mit ihr zu sprechen, 34 Prozent würden versuchen, die App zu löschen, 20 Prozent das Gerät nicht mehr benutzen und 24 Prozent die Polizei einschalten. Dies ist eine Veränderung gegenüber 2021, wo 50 Prozent versuchten, die installierende Person zu ermitteln, und 20 Prozent sich an die Polizei wandten.

Wechselnde Perspektiven auf Stalking in modernen Beziehungen: Privatsphäre, Einverständnis und die Realität von Verfolgung

Eine Mehrheit der Befragten (54 Prozent) lehnt die Überwachung eines Partners ohne dessen Wissen ab. Es ist bezeichnend, dass die älteren Generationen, darunter die Generation X, die Babyboomer und die Silent Generation, im Vergleich zu jüngeren

Befragten eine stärkere Abneigung gegenüber einer Überwachung ohne Zustimmung zeigen. Im Vergleich dazu ist zwischen 2021 und 2024 ein bemerkenswerter Rückgang des Prozentsatzes an Befragten zu verzeichnen, die die Überwachung eines Partners ohne dessen Wissen für völlig inakzeptabel erachten – von

70 Prozent auf 54 Prozent. Interessanterweise sank auch der Anteil derjenigen, die ein solches Vorgehen stets für akzeptabel halten von 13 Prozent im Jahr 2021 auf acht Prozent im Jahr 2024. Die differenzierte Sichtweise innerhalb dieser Frage zeigt sich darin, dass 38 Prozent der Umfrageteilnehmer im Jahr 2024 eine Überwachung ohne Wissen unter bestimmten Umständen für akzeptabel halten – ein deutlicher Anstieg gegenüber 17 Prozent im Jahr 2021.

Bei der Untersuchung der Einstellung zur einvernehmlichen Überwachung der Online-Aktivitäten eines Partners (Weitergabe von Informationen mit vollem Wissen und Einverständnis zu einem bestimmten Zweck, etwa aus Sicherheitsgründen) sind 45 Prozent der Befragten der Meinung, dass dies inakzeptabel sei, und betonen damit die Bedeutung des Rechts auf Privatsphäre. 27 Prozent der Befragten befürworten eine vollständige Transparenz in Beziehungen und halten eine Überwachung im gegenseitigen Einvernehmen für angemessen, während 12 Prozent sie nur dann für akzeptabel halten, wenn sie auf Gegenseitigkeit beruhe. Darüber hinaus sind 12 Prozent mit einer solchen Überwachung einverstanden, wenn es um die körperliche Sicherheit geht, wohingegen 4 Prozent nur widerwillig zustimmen, weil ihr Partner darauf besteht. Während in diesem Jahr die Einstellung zur einvernehmlichen Überwachung der Online-Aktivitäten des Partners weitgehend mit der von 2021 übereinstimmt, steht 2024 ein etwas höherer Prozentsatz der Befragten dieser Idee offen gegenüber (27 Prozent im Vergleich zu 25 Prozent im Jahr 2021). Für fast die Hälfte der Befragten (45 Prozent) sind solche Handlungen jedoch nach wie vor inakzeptabel. Dies zeigt, dass sehr viele Menschen die Überzeugung vertreten, die Privatsphäre sei in Beziehungen ein absolutes Grundrecht.

Trotz der vorherrschenden Meinung im Hinblick auf Überwachung taucht das Thema Stalking in Dating-Szenarien immer wieder auf. Beachtliche 34 Prozent der Befragten betrachten das Googeln oder Überprüfen von Konten in den sozialen Medien einer Person, mit der sie seit kurzem zusammen sind, als eine akzeptable Form der Sorgfaltsprüfung. Darüber hinaus berichtet weniger als ein Viertel (23 Prozent), in irgendeiner Form Online-Stalking durch einen neuen Partner erlebt zu haben. Dies unterstreicht, wie verbreitet dieses besorgniserregende Phänomen in der heutigen Dating-Landschaft ist.

Vertrauen und Grenzen überwinden: Ein tiefer Einblick in die Problematik des digitalen Datenschutzes

Fast die Hälfte der Befragten (47 Prozent) macht sich Sorgen darüber, dass der eigene Partner ihre digitale Privatsphäre verletzen könnte. Dies ist ein deutlicher Anstieg gegenüber 2021, als nur 37 Prozent diese Sorge äußerten. In Europa ist diese Befürchtung ausgeprägter, wo 62 Prozent der Umfrageteilnehmer diese Bedenken teilen, während der Prozentsatz in der asiatisch-pazifischen Region (37 Prozent) geringer ist. In allen Regionen ist die Überwachung von Textnachrichten (20 Prozent) und der Wunsch des Partners nach uneingeschränktem Zugriff auf das Telefon, sowohl physisch als auch aus der Ferne (20 Prozent), ein häufiger Anlass zur Sorge. Mehr Befragte befürchten nun, ihr Partner könnte ihre Privatsphäre verletzen, indem dieser Passwörter von Geräten entfernt (13 Prozent im Jahr 2024 im Vergleich zu 9 Prozent im Jahr 2021) oder ständig die Freigabe von Geolokalisierungsdaten verlangt (12 Prozent im Jahr 2024 im Vergleich zu 10 Prozent im Jahr 2021). Ein etwas geringerer Prozentsatz (15 Prozent im Jahr 2024 gegenüber 17 Prozent im Jahr 2021) befürchtet jedoch, dass der Partner durch das Mitlesen von E-Mails in die eigene Privatsphäre eindringt.

Was das Vertrauen und den Zugang zu persönlichen Geräten angeht, so drückt die Hälfte der Befragten (51 Prozent) ihr Vertrauen in den eigenen Partner durch die Gewährung des vollständigen Zugriffs auf das eigene Telefon aus. Weitere 19 Prozent erlauben auch einen Zugriff, wobei bestimmte Anwendungen durch zusätzliche Passwörter oder Sicherheitsmaßnahmen geschützt sind. Ein Fünftel vertraut seinem Partner zwar, entscheidet sich aber dafür, keinen Zugang zum eigenen Telefon zu gewähren. Die übrigen Umfrageteilnehmer sind geteilter Meinung: 5 Prozent erlauben ihren Partnern keinen Zugang und 4 Prozent machen keine Angaben. Bemerkenswerterweise sind Personen in langfristigen Beziehungen eher dazu bereit (61 Prozent), während in „frischen Beziehungen" lediglich 40 Prozent offen dafür wären.

Auf der anderen Seite haben 52 Prozent der Befragten vollen Zugriff auf die Telefone ihrer Partner, während weitere 23 Prozent zwar Zugriff haben, aber nur auf bestimmte Apps, die durch zusätzliche Passwörter oder Sicherheitsmaßnahmen geschützt sind. Umgekehrt geben 18 Prozent an, dass sie keinen Zugang zu den Telefonen ihrer Partner haben, und sieben Prozent ziehen es vor, diese Informationen nicht preiszugeben. Diese Dynamik verdeutlicht das komplizierte Zusammenspiel von Vertrauen und digitalen Grenzen in partnerschaftlichen Beziehungen.

Einblicke in die komplexe Landschaft des Informationsaustauschs in Beziehungen

Während mit 90 Prozent eine deutliche Mehrheit der Befragten bereit ist, Passwörter für Streaming-Dienste wie Netflix oder eigene Fotos zu teilen oder dies zumindest in Erwägung zieht, ist man bei bestimmten Arten von sensiblen Informationen vorsichtiger. Interessanterweise zeigen sich die Befragten sehr zurückhaltend, wenn es um die Weitergabe von Passwörtern für Sicherheitsgeräte (etwa videoüberwachte Türklingeln) geht. 18 Prozent der Befragten gaben an, dass sie niemals Zugang zu diesen Geräten gewähren würden.

Bei genauerer Betrachtung zeigen die Daten eine differenzierte Sichtweise auf die verschiedenen Arten des Informationsaustauschs. Bei der Weitergabe von Passwörtern für Streaming-Dienste beispielsweise sind 69 Prozent dazu bereit, und nur neun Prozent geben an, dass sie diese Zugangsdaten niemals weitergeben würden. Bei Fotos sind 66 Prozent offen für eine gemeinsame Nutzung, 26 Prozent könnten es sich vorstellen, und acht Prozent lehnen die Idee entschieden ab. Wenn es um persönlichere Daten wie Textnachrichten geht, gaben 52 Prozent an, dass sie bereit wären, diese weiterzugeben, 33 Prozent würden es in Erwägung ziehen und für 15 Prozent wäre eine Weitergabe solcher Daten niemals eine Option.

Derselbe Trend gilt bei Passwörtern für Sicherheitsgeräte wie Bluetooth-fähige und videoüberwachte Türklingeln, bei denen 52 Prozent offen für eine Weitergabe sind und 30 Prozent es in Erwägung ziehen. 18 Prozent würden diese hingegen auf keinen Fall preisgeben. Ähnlich verhält es sich mit der Weitergabe von Zahlungsinformationen: 49 Prozent sind dazu bereit, 30 Prozent sind möglicherweise bereit und 21 Prozent wollen derartige Informationen nicht weitergeben. Je sensibler die Informationen sind, desto geringer ist die Bereitschaft, sie preiszugeben. Dies zeigt sich an der sinkenden Zahl von Personen, die bereit sind, Passwörter für Konten (47 Prozent bereit, 29 Prozent könnten es in Erwägung ziehen und 24 Prozent wollen es nicht) und den Browserverlauf (46 Prozent bereit, 34 Prozent könnten es in Erwägung ziehen und 20 Prozent wollen es nicht) preiszugeben. Dieses schwierige Gleichgewicht zwischen Offenheit und Vorbehalten verdeutlicht die komplexe Dynamik im Zusammenhang mit der Privatsphäre und dem Informationsaustausch in intimen Beziehungen.

David Emm, Sicherheits- und Datenschutzexperte bei Kaspersky:

„Die Studienergebnisse verdeutlichen, wie schwierig es ist, ein Gleichgewicht zwischen Intimität und dem Schutz persönlicher Daten zu finden. Es ist gut, erhöhte Vorsicht walten zu lassen, insbesondere bei sensiblen Daten wie Passwörtern für Sicherheitsgeräte. Die Zurückhaltung bei der Freigabe solcher kritischen Zugänge steht im Einklang mit den Grundsätzen der Cybersicherheit. Die Bereitschaft zur Weitergabe von Passwörtern für Streaming-Dienste oder Bildergalerien zeigt einen Kulturwandel, auch wenn jeder die potenziellen Risiken – selbst bei der scheinbar harmlosen Weitergabe von Informationen – zwischenzeitlich kennen sollte. Die Ergebnisse unserer Studie zeigen deutlich, wie wichtig es ist, in Beziehungen eine offene Kommunikation zu pflegen, klare Grenzen zu setzen und digitale Kompetenz zu fördern. Für Sicherheitsexperten unterstreicht dies die Notwendigkeit, sich kontinuierlich über bewährte Verfahren der Cybersicherheit zu informieren und Einzelpersonen in die Lage zu versetzen, sachkundige Entscheidungen über die Weitergabe persönlicher Daten innerhalb von Beziehungen zu treffen."

Emma Pickering, Leiterin des Teams für technologiegestützte Missbrauchsbekämpfung und wirtschaftliche Stärkung bei Refuge

> Für viele Betroffene sind gemeinsame Passwörter oder eben das Nichtteilen von Passwörtern ein Luxus, den sie sich nicht leisten können.

„Die in diesem Bericht ermittelten Statistiken sind besorgniserregend, wobei wir über die Ergebnisse leider nicht überrascht sind. Hier bei Refuge stellen wir eine alarmierende Zunahme von Betroffenen fest, die über Stalker-Software berichten. Wie die Kaspersky-Studie zeigt, ist das Thema Stalkerware ein weit verbreitetes Problem.

Es ist wahrscheinlich, dass dies auf die Zunahme von Stalkerware-Funktionen in Apps zur elterlichen Überwachung von Kindern zurückzuführen ist, weil dadurch das Stalken immer leichter gemacht wird. Während wir aktiv nach Stalkerware suchen, die darauf abzielt, beispielsweise Ex-Partner zu überwachen, gibt es viele andere Formen von Stalkerware, die sich auf eine Nutzergruppe fokussiert, der die vollständigen Funktionen der Apps nicht bekannt sind oder die für andere schädliche Zwecke verwendet werden.

Wichtig ist auch, dass wir in der Regel feststellen müssen, dass die Technik nicht isoliert missbraucht wird. Neben Stalkerware setzen Täter häufig auch andere Formen von Technologie ein, um Menschen zu schädigen und Leid zu verursachen. Deshalb müssen wir als Hilfsorganisation durch detaillierte technische Bewertungen dauerhaft sicherstellen, Betroffene bei der Wiedererlangung aller Zugänge zu Konten und Geräten bestmöglich unterstützen zu können. Deshalb ist auch in Zukunft eine umfassende Zusammenarbeit mit der ganzen Bandbreite der Tech-Community für uns unerlässlich. Nur so erhalten wir ein tieferes Verständnis über für Missbrauchszwecke eingesetzte Technologien und können verhindern, dass diese Schaden verursachen können. Gemeinsames Ziel muss es sein, Security by Design so stark wie möglich zu etablieren.

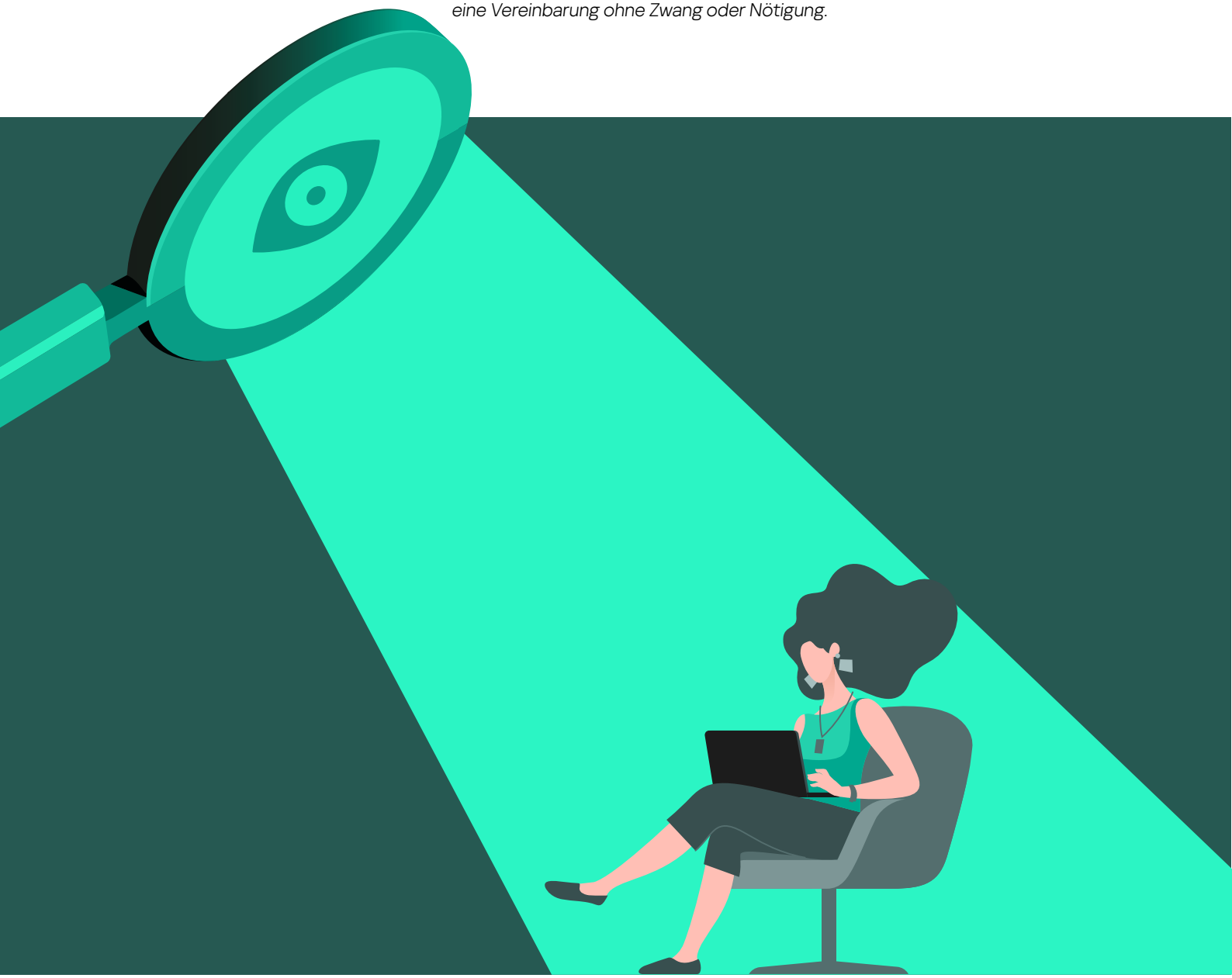
Leider müssen wir feststellen, dass für viele Betroffene das Festlegen von Passwörtern auf Geräten oder die Nichtweitergabe des Geräts oder des Passworts keine Option darstellt. Wir raten allen, die eine Überwachung befürchten, immer ein sicheres Gerät zu nutzen, um mit einer Hilfsorganisation in Kontakt zu treten. Auch im Falle anderer sensibler Gespräche, aber auch bei E-Mails oder Suchanfragen sollte niemals das Gerät verwendet werden, das möglicherweise überwacht werden könnte.

Zustimmung ist eine Vereinbarung, ohne Zwang oder Nötigung

Erica Olsen, Senior Director, Safety Net Project, National Network to End Domestic Violence (NNEDV)

Dieser Bericht beleuchtet sowohl die Häufigkeit von Stalking-Verhalten mit Hilfe von Technologie als auch die damit verbundenen Auffassungen über Privatsphäre in intimen Partnerbeziehungen. Der Einsatz von Stalkerware oder anderer Tools zur Überwachung von Personen ohne deren Zustimmung ist eine Verletzung der Privatsphäre und ein gängiges Vorgehen bei Missbrauch. Dieser Bericht zeigt, wie missbräuchlich handelnde Personen eine breite Palette von Überwachungstaktiken einsetzen, darunter Stalkerware und andere Anwendungen, die den Zugang zu persönlichen Informationen ermöglichen.

Der Bericht untersuchte auch die vorherrschenden Regeln und Auffassungen über Privatsphäre in intimen Partnerbeziehungen. Ein erheblicher Teil der Befragten gab an, bereit zu sein, einige sensible Informationen weiterzugeben – sei es aufgrund von Sicherheitsbedenken oder aus anderen Gründen. Ein kleiner Anteil (4 Prozent) gab an, dass sie der Überwachung auf Drängen ihres Partners nur widerwillig zugestimmt haben – dies ist nicht gleichbedeutend mit einer Zustimmung aus freien Stücken oder eigener Überzeugung. Es ist wichtig, eine klare Unterscheidung zwischen einvernehmlicher Weitergabe und nicht einvernehmlicher Überwachung zu treffen. Die Zustimmung ist eine Vereinbarung ohne Zwang oder Nötigung.



Gemeinsamer Kampf gegen Stalkerware

Stalkerware ist in erster Linie kein technisches Problem, sondern Ausdruck einer gesellschaftlichen Problematik. Diese erfordert daher Maßnahmen aus allen Bereichen der Gesellschaft. Kaspersky setzt sich nicht nur aktiv für den Schutz vor dieser Art von Bedrohung ein, sondern pflegt auch einen mehrstufigen Dialog mit gemeinnützigen Organisationen, der Industrie, der Forschung sowie öffentlichen Einrichtungen auf der ganzen Welt, um gemeinsam an Lösungen zu arbeiten, mit denen diesem Problem begegnet werden kann.

Kaspersky war 2019 das erste Cybersicherheitsunternehmen, das eine neue, aufmerksamkeitsstarke Warnmeldung entwickelt hat, die Nutzer deutlich benachrichtigt, wenn Stalkerware auf deren Gerät gefunden wird. Während die Lösungen von Kaspersky schon seit vielen Jahren potenziell schädliche Apps, die nicht als Malware zu qualifizieren sind – darunter auch Stalkerware – anzeigen, macht die neue Benachrichtigungsfunktion den Nutzer darauf aufmerksam, dass eine App, die ihn ausspionieren könnte, auf seinem Gerät gefunden wurde.

Im Jahr 2022 wurde der „Privacy Alert" im Rahmen der Einführung des neuen Produktportfolios von Kaspersky für Privatanwender erweitert. Er informiert nun über das Vorhandensein von Stalkerware auf einem Gerät und weist darauf hin, dass bei Entfernung der Stalkerware auch die Person alarmiert wird, die die App ursprünglich installiert hat. Denn dies kann zu einer Eskalation der Situation führen. Außerdem riskiert der Nutzer, dass wichtige Daten oder Beweise, die bei einer Strafverfolgung verwendet werden könnten, gelöscht werden. Abbildung 2 unten zeigt die neue Warnung im blauen Kasten. Der Privacy Alert von Kaspersky ist in alle Sicherheitslösungen des Unternehmens integriert, um Nutzer vor Stalkerware zu schützen.

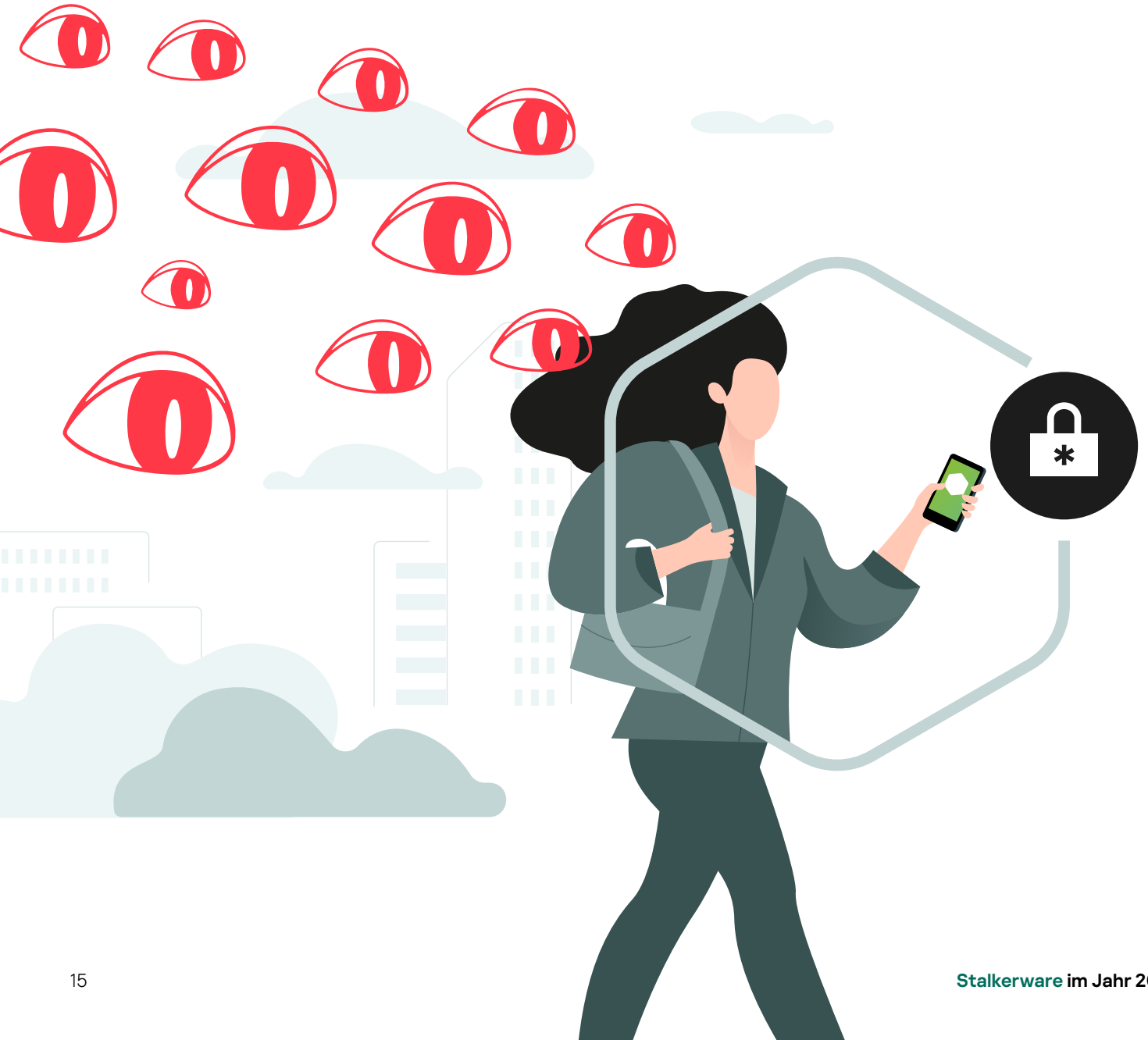
Abbildung 2 – Update 2024 des Kaspersky-Privacy-Alert, der darauf hinweist, eine gefundene Stalkerware nicht zu entfernen

Im Jahr 2019 gründete Kaspersky außerdem die Koalition gegen Stalkerware, eine internationale Arbeitsgruppe gegen Stalkerware und häusliche Gewalt, die private IT-Unternehmen, Nichtregierungsorganisationen, Forschungseinrichtungen und Strafverfolgungsbehörden zusammenbringt, um Cyberstalking zu bekämpfen und Betroffenen von Online-Missbrauch zu helfen. Im Rahmen eines aus mehr als 40 Organisationen bestehenden Konsortiums können alle Beteiligten ihr Fachwissen austauschen und gemeinsam an der Lösung des Problems der Online-Gewalt arbeiten. Darüber hinaus bietet die in sieben Sprachen verfügbare Website der Koalition Betroffenen Hilfe und Anleitung, falls sie den Verdacht hegen, dass auf ihren Geräten Stalkerware installiert ist.

Von 2021 bis 2023 war Kaspersky im Rahmen ein Konsortiums-partner des EU-Projekts DeStalk, welches durch das Rights-, Equality-, and Citizenship-Programm der Europäischen Union kofinanziert wurde. Die insgesamt fünf Projektpartner vereinten das Fachwissen der IT-Sicherheitsgemeinschaft, der Forschung, von Organisationen der Zivilgesellschaft und von Behörden. Im Rahmen des DeStalk-Projekts wurden insgesamt 375 Fachleute, die direkt in Frauen-Unterstützungsdiensten und Täterprogrammen arbeiten, sowie Beamte von Behörden darin geschult, wie Stalker-ware und andere digitale Formen geschlechtsspezifischer Gewalt wirksam bekämpft und die Öffentlichkeit für digitale Gewalt und Stalkerware sensibilisiert werden können.

Im Rahmen des Projekts entwickelte Kaspersky einen E-Learning-Kurs zum Thema Cybergewalt und Stalkerware auf der Kaspersky Automated Security Awareness Platform, einer frei zugänglichen Online-Mikro-Lernplattform, die in fünf verschiedenen Sprachen zur Verfügung steht. Bis heute haben mehr als 130 Fachleute den E-Learning-Kurs erfolgreich absolviert, weitere 80 nehmen derzeit daran teil. Obwohl das DeStalk-Projekt inzwischen abgeschlossen wurde, ist der Kurs auf der DeStalk-Projekt-Website weiterhin verfügbar https://www.work-with-perpetrators.eu/destalk.

Im Juni 2022 startete Kaspersky Webseite für TinyCheck. TinyCheck ist ein kostenloses, sicheres Open-Source-Tool, das von gemeinnützigen Organisationen und Polizeieinheiten genutzt werden kann, um von digitalem Stalking Betroffene zu unterstützen. Das 2020 entwickelte Tool überprüft Geräte auf Stalkerware und Überwachungsanwendungen, ohne dass der Täter über die Überprüfung informiert wird. Das Open-Source-Tool muss nicht auf dem Gerät installiert werden, da es unabhängig arbeitet, um eine Entdeckung durch einen Stalker zu vermeiden. TinyCheck scannt den ausgehenden Datenverkehr eines Geräts über eine normale WLAN-Verbindung und identifiziert Interaktionen mit bekannten Quellen wie Stalkerware-Servern. TinyCheck kann jedes Gerät auf jeder Plattform überprüfen – einschließlich iOS, Android und andere Betriebssysteme.



Möglicherweise von Stalkerware betroffen? Top-Tipps zur Erkennung

Unabhängig davon, ob Sie von Stalkerware betroffen sind oder nicht, können diese Tipps Ihnen helfen, sich besser zu schützen:

- Schützen Sie Ihr Telefon mit einem sicheren Passwort, das Sie niemals Ihrem Partner, Freunden oder Kollegen mitteilen.
- Nutzen Sie starke Passwörter für alle Ihre Konten und geben Sie diese nicht an Dritte weiter.
- Laden Sie nur Apps aus offiziellen Quellen herunter, etwa aus Google Play oder dem App Store von Apple.
- Installieren Sie eine zuverlässige IT-Sicherheitslösung wie **Kaspersky Premium** auf den Geräten und scannen Sie diese regelmäßig. Wurde bereits Stalkerware installiert, sollte die Sicherheitslösung jedoch erst heruntergeladen und aktiviert werden, wenn das Risiko für den Betroffenen abgeschätzt werden kann, da der Täter den Einsatz von Cybersicherheits-Tools bemerken könnte.

Betroffene von Stalkerware können zu Leidtragenden eines umfassenderen Kreislaufs von Missbrauch, einschließlich körperlicher Gewalt, werden.

In einigen Fällen wird der Täter benachrichtigt, wenn seine Zielperson einen Gerätescan durchführt oder eine Stalkerware-App entfernt. Wenn dies geschieht, kann es zu einer Eskalation der Situation und zu weiterer Gewalt führen. Deshalb ist es wichtig, Vorsicht walten zu lassen, wenn der Verdacht besteht, von Stalkerware betroffen zu sein.

- **Wenden Sie sich an eine lokale Hilfsorganisation** Um eine in Ihrer Nähe zu finden, besuchen Sie die **Website der Koalition gegen Stalkerware**.
- Achten Sie auf **folgende Warnsignale**: Ein sich schnell entladender Akku aufgrund unbekannter oder verdächtiger Apps, neu installierte Anwendungen mit verdächtigem Zugriff auf die Nutzung und Verfolgung Ihres Standorts oder das Senden oder Empfangen von Textnachrichten und andere persönliche, nicht autorisierte Aktivitäten, sind kritisch zu betrachtende Anzeichen. Überprüfen Sie auch, ob die Einstellung „Unbekannte Quellen“ aktiviert ist. Dies kann ein Hinweis darauf sein, dass unerwünschte Software aus einer Drittquelle installiert wurde. Die oben genannten Punkte sind jedoch nur Indizien und deuten nicht eindeutig auf das Vorhandensein von Stalkerware auf dem Gerät hin.
- **Versuchen Sie nicht, die Stalker-Software zu löschen, Einstellungen zu ändern oder Ihr Telefon zu manipulieren, bevor Sie einen Sicherheitsplan in der Tasche haben:** Dies könnte Ihren potenziellen Täter alarmieren und zu einer Verschärfung der Situation führen. Sie riskieren zudem, wichtige Daten oder Beweise zu löschen, die bei einer Strafverfolgung verwendet werden könnten. Ermitteln Sie, welches Vorgehen in Ihrer aktuellen Situation am sinnvollsten ist, bevor Sie Änderungen am Telefon vornehmen, die eine Eskalation des Verhaltens eines potenziellen Täters provozieren könnten.

Für weitere Informationen über unsere Aktivitäten gegen Stalkerware oder für andere Anfragen schreiben Sie uns bitte unter: ExtR@kaspersky.com.

kaspersky