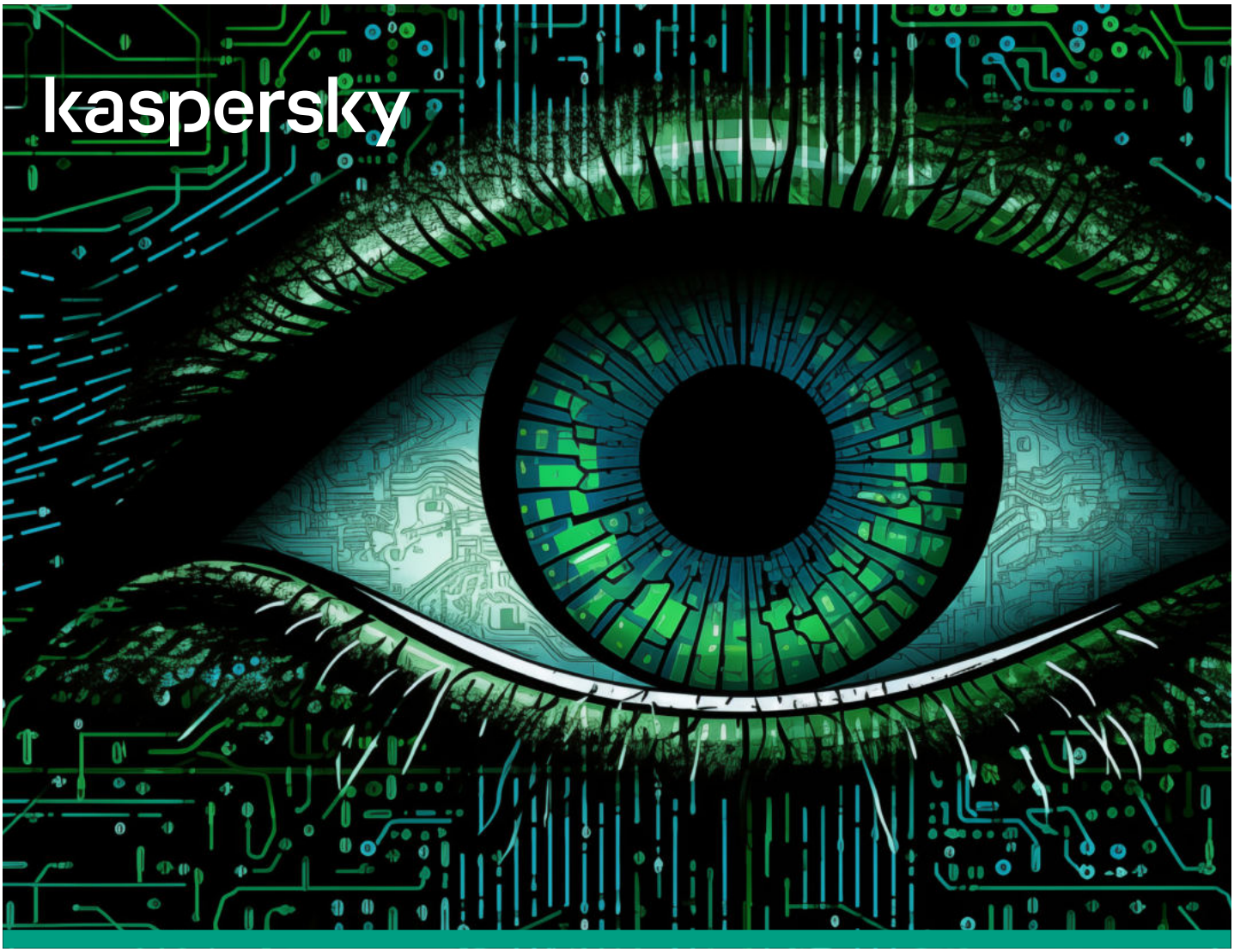
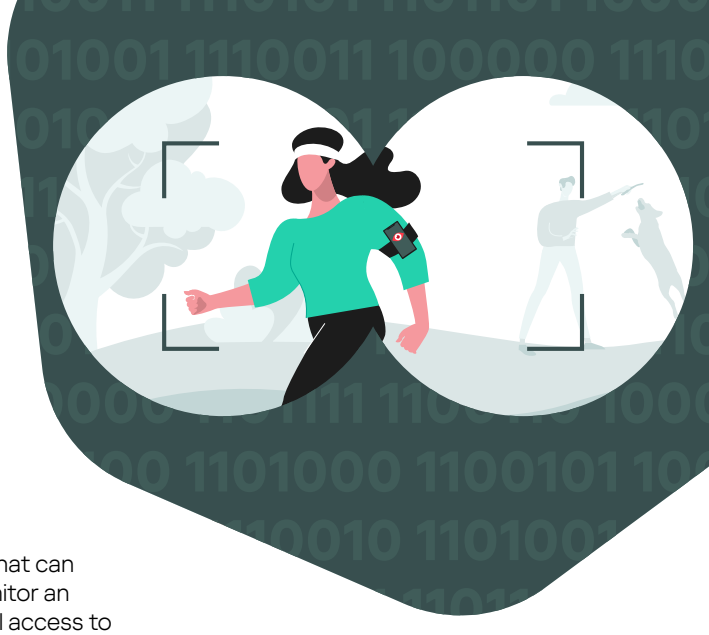


The State of **Stalkerware** in 2023

A Kaspersky Report
February 2024

Contents



2023 main findings

The annual Kaspersky State of Stalkerware report aims to contribute to awareness and a better understanding of how people around the world are impacted by digital stalking. Stalkerware is commercially available software that can be discreetly installed on smartphone devices, enabling perpetrators to monitor an individual's private life without their knowledge. Stalkerware requires physical access to be installed, but our report also notes the range of remote technology that can be used for nefarious purposes.

Easily downloaded and installed by anyone with an internet connection, stalkerware makes access to a smartphone possible from anywhere. Not only can a perpetrator violate their victim's privacy by monitoring their activities, they can also use the software to access huge volumes of personal data. Depending on the software used, everything from device location, text messages, social media chats, photos, browser history and more can be monitored. Since stalkerware works in the background unseen, the majority of victims will be completely unaware that their every step and action is being monitored.

In most countries around the world, use of stalkerware software is currently not prohibited, but installing such an application on another individual's smartphone without their consent is illegal and punishable. However, it is the perpetrator who will be held responsible, not the developer of the application.

Along with other related technologies, stalkerware is one element of tech-enabled abuse and is often used in abusive relationships. As this is a digital aspect of a wider, real-world problem, Kaspersky is working with relevant experts and organizations in the field of domestic violence, ranging from victim support services and perpetrator programs through to research and government agencies, to share knowledge and support professionals and victims alike.

2023 data highlights

- In 2023, a total of 31,031 unique users were affected by stalkerware, an increase compared to 2022 (29,312).
- The Kaspersky Security Network reveals that stalkerware is most commonly used in Russia, Brazil, and India, and continues to be a global issue, with the largest number of affected users in the following countries:
  - Germany, France, and United Kingdom (Europe);
  - Iran, Turkey, and Yemen (Middle East and Africa);
  - India, Indonesia, and Philippines (Asia-Pacific);
  - Brazil, Mexico, and Colombia (Latin America);
  - United States (North America);
  - Russian Federation, Belarus, and Kazakhstan (Eastern Europe (except European Union countries), Russia and Central Asia).
- Worldwide, the most commonly used stalkerware app is TrackView with 4,049 affected users.
- 23 percent of people worldwide revealing they have encountered some form of online stalking from someone they were recently dating.
- 40 percent disclosed they experienced stalking or suspected they were being stalked.

Stalkerware:

Commercially available software used for spying. Stalkerware enables a person to remotely monitor the activities on another user's device without that user's consent and without explicit, persistent notification to that user.

Stalking:

"A pattern of behavior directed at a specific person that would cause a reasonable person to fear for the person's safety or the safety of others; or suffer substantial emotional distress. Stalkers use a variety of tactics, including (but not limited to): unwanted contact including phone calls, texts, and contact via social media, unwanted gifts, showing up/approaching an individual or their family/friends, monitoring, surveillance, property damage, and threats."

2023 trends observed by Kaspersky

Methodology

The data in this report has been taken from aggregated threat statistics obtained from the Kaspersky Security Network, dedicated to processing cybersecurity-related data streams from millions of anonymous volunteer participants around the world. To calculate the statistics, the consumer line of Kaspersky's mobile security solutions has been reviewed according to the Coalition Against Stalkerware's detection criteria on stalkerware. This means that the affected number of users have been targeted by stalkerware only. Other types of monitoring or spyware apps that fall outside of the Coalition's definition are not included in the report statistics.

The statistics reflect unique mobile users affected by stalkerware, which is different from the total number of detections. The number of detections can be higher as stalkerware may have been detected several times on the same device of the same unique user if they decided not to remove the app upon receiving a notification. Often survivors are advised by support organizations not to remove the stalkerware so as not to alert the perpetrator that they have been discovered.

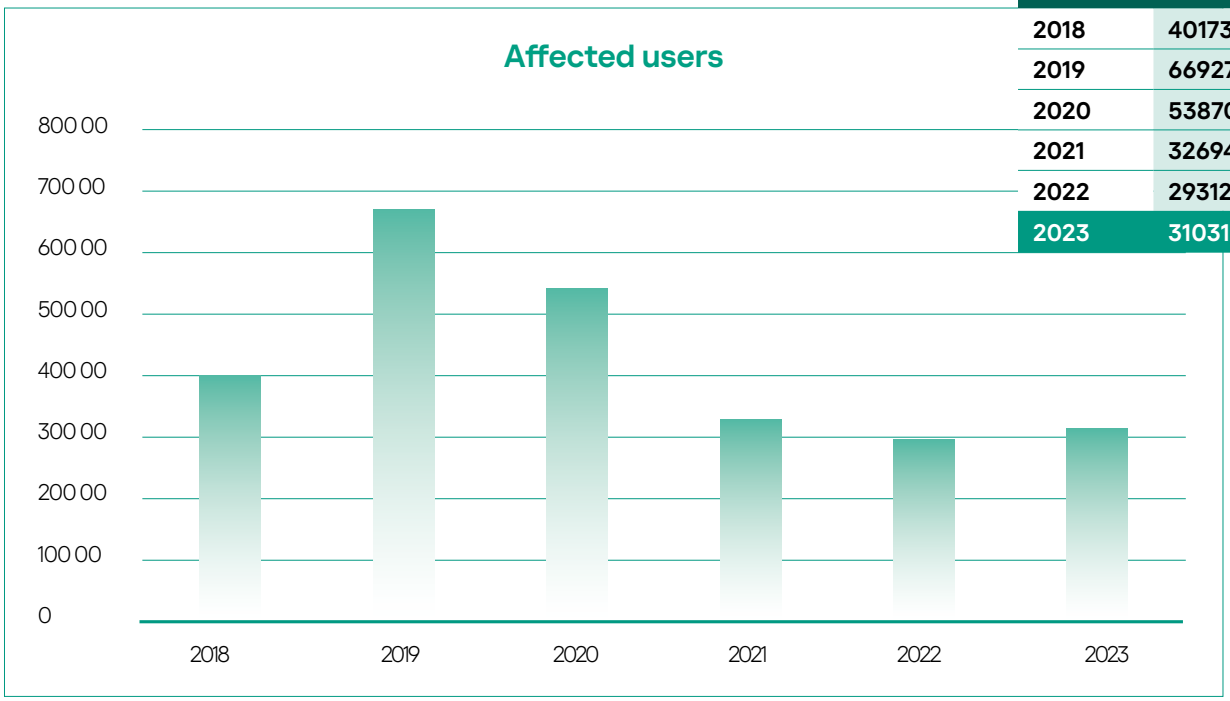
Finally, the statistics reflect only mobile users using Kaspersky's IT security solutions. Some users may use another cybersecurity solution on their devices, while some do not use any solution at all.

> In 2023, a total of **31,031** unique users were affected by stalkerware

Global detection figures: affected users

Using global and regional statistics, Kaspersky has been able to compare data collected in 2023 and the previous four years. In 2023, a total of 31,031 unique users were affected by stalkerware, an increase compared to 2022 (29,312 unique users). Graphic 1, below, shows how this number has varied year-on-year since 2018.

Year	Affected users
2018	40173
2019	66927
2020	53870
2021	32694
2022	29312
2023	31031



Graphic 1: Evolution of affected users year-on-year since 2018

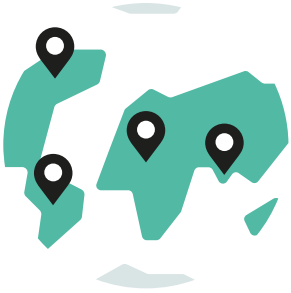
Global and regional detection figures: geography of affected users

> In 2023, Kaspersky detected affected users in 175 countries.

Stalkerware continues to be a global problem. In 2023, Kaspersky detected affected users in 175 countries.

In 2023, Russia (9,890), Brazil (4,186), and India (2,492) were the top three countries with the most affected users. According to Kaspersky statistics, those three countries have held leading positions since 2019, all with an increase in detected stalkerware infections. Iran entered the top five most affected in the previous year and remains there.

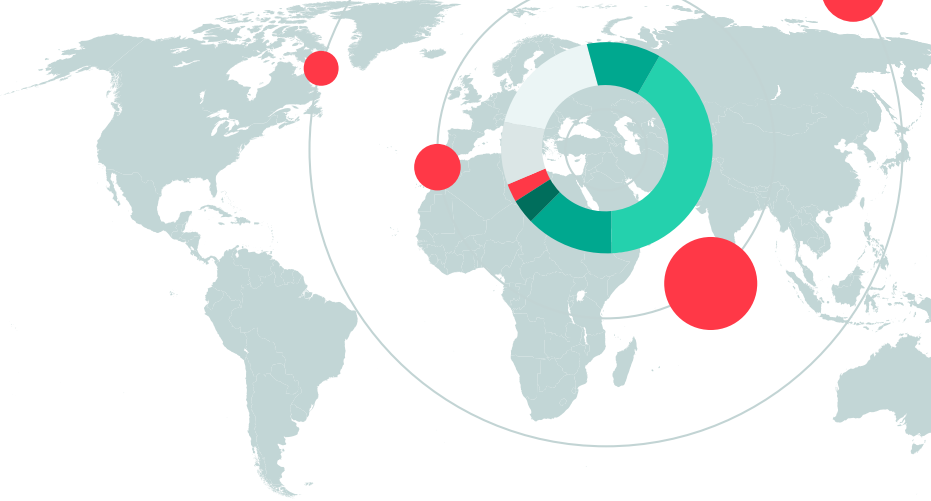
When compared to 2021, there are slight changes to the top 10 affected countries, with most remaining in the same position. While Germany dropped from rank seven to 10, Saudia Arabia (ranked eighth in 2022) is not in the list of most affected countries this year.



	Country	Affected users
1	Russian Federation	9,890
2	Brazil	4,186
3	India	2,492
4	Iran	1,578
5	Turkey	1,063
6	Indonesia	871
7	United States of America	799
8	Yemen	624
9	Mexico	592
10	Germany	577

Table 1: Top 10 countries most affected by stalkerware in the world in 2023

Middle East and Africa region, the total affected users was **6,561**



	Country	Affected users
1	Germany	577
2	France	332
3	United Kingdom	271
4	Spain	257
5	Italy	252
6	Poland	179
7	Netherlands	177
8	Switzerland	116
9	Austria	70
10	Portugal	63

Table 2 - Top 10 countries most affected by stalkerware in Europe in 2023

The total number of unique affected European users in 2023 was 2,645, a significant decrease compared to 2022 (3,158). The three most affected countries in Europe were Germany (577), France (332) and the United Kingdom (271). Compared to 2021, the countries listed continued to feature as the most affected in Europe with the exception of Greece which dropped out of the list. Unfortunately, Portugal entered the list ranked tenth.

	Country	Affected users
1	Russian Federation	9,890
2	Belarus	307
3	Kazakhstan	270
4	Ukraine	268
5	Azerbaijan	243
6	Uzbekistan	100
7	Kyrgyzstan	52
8	Moldova	49
9	Armenia	43
10	Tajikistan	30

Table 3 - Top 10 countries most affected by stalkerware in Eastern Europe (excluding EU countries), Russia and Central Asia in 2023

In Eastern Europe (excluding European Union countries), the Russian Federation and Central Asia, the total number of unique affected users in 2023 was 11,210, also an increase compared to the previous year (9,406). The top three countries were Russia, Kazakhstan, and Belarus.

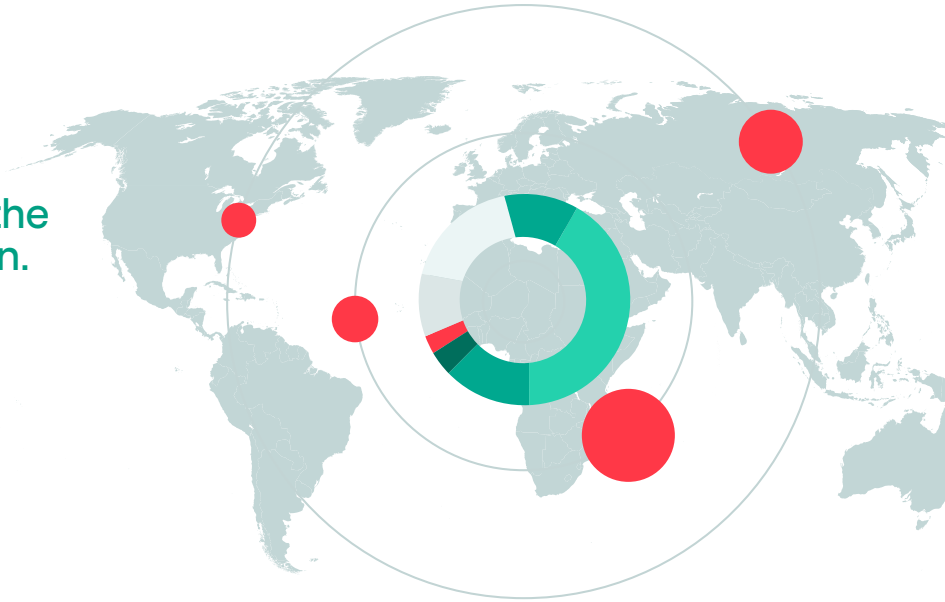
	Country	Affected users
1	Iran	1,578
2	Turkey	1,063
3	Yemen	624
4	Egypt	569
5	Saudi Arabia	511
6	Algeria	495
7	Morocco	215
8	United Arab Emirates	184
9	Iraq	127
10	South Africa	126

Table 4 - Top 10 countries most affected by stalkerware in Middle East & Africa in 2023

Looking at the Middle East and Africa region, the total number of affected users was 6,561, slightly higher than in 2022 (6,330), but there is a small change to the top three most affected this year. While in 2022 Iran, Turkey and Saudi Arabia were the most affected countries, in 2023 it was Iran, Turkey and Yemen.

with **2,492** affected users India remains far ahead of the other countries in the region.

with **4,186** affected users Brazil dominates the Latin America and the Caribbean region.



	Country/Territory	Affected users
1	India	2,492
2	Indonesia	871
3	Philippines	323
4	Australia	168
5	Vietnam	97
6	Malaysia	88
7	Japan	85
8	Bangladesh	66
9	Hong Kong	51
10	Sri Lanka	51

Table 5 - Top 10 countries most affected by stalkerware in Eastern Europe (excluding EU countries), Russia and Central Asia in 2023

The Asia-Pacific region saw an increase in the use of stalkerware compared to the last year, with a total of 4,575 affected users, up from 3,187 in 2022. India remains far ahead of other countries in the region, with 2,492 affected users. Indonesia occupies second place with 871 affected users; Philippines is third with 323 affected users and Australia fourth.

	Country	Affected users
1	Brazil	4,186
2	Mexico	592
3	Colombia	149
4	Peru	138
5	Argentina	95
6	Ecuador	88
7	Chile	63
8	Venezuela	19
9	Bolivia	18
10	Paraguay	17

Table 6 - Top 10 countries most affected by stalkerware in Latin America in 2023

Brazil dominates the Latin America and the Caribbean region with 4,186 affected users, accounting for approximately 76 percent of the region's total number of affected users. Brazil is followed in the list by Mexico and Colombia. A total of 5,478 of affected users were recorded in the region, which is a small decrease compared to 2022 (6,170).

	Country	Affected users
1	United States of America	799
2	Canada	250

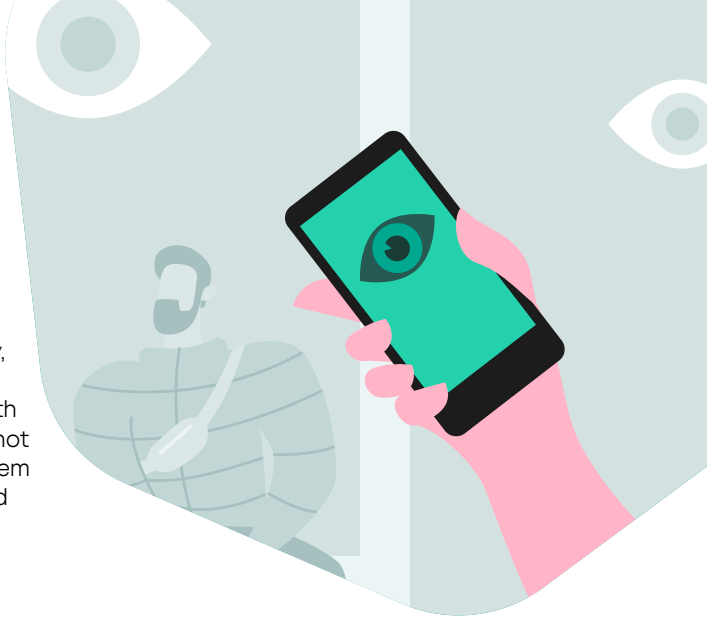
Table 7 - Number of users affected by stalkerware in North America in 2023

Finally, in North America, 77 percent of all affected users were in the United States. This is to be expected given the relative size of the population compared to Canada. Across the North American region, 1,049 users were affected in total.

Global detection figures – stalkerware applications

This year, Kaspersky detected 195 different stalkerware apps. The most commonly used stalkerware application to control smartphones around the world in 2023 was TrackView, affecting 4,049 users.

Stalkerware products are typically marketed as legitimate anti-theft or parental control apps on smartphones, tablets, and computers, but in reality, they are very different. Installed without the knowledge or consent of the person being tracked – they operate stealthily and provide a perpetrator with the means to gain control over a victim's life. Usually, these kind of apps are not shown in the list of installed apps in a phone´s configuration, which makes them hard to spot. Stalkerware capabilities vary depending on the application, and whether they have been paid for or are freely obtained.



	Application name	Affected users
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

Table 8: Top 10 list of stalkerware applications in 2023

> Stalkerware typically masquerades as legitimate anti-theft or parental control apps on smartphones, tablets, and computers

Below are some of the most common functions that may be present in stalkerware applications:

- Hidden app icon
- Reading SMS, MMS and call logs
- Accessing contact lists
- Tracking GPS location
- Tracking calendar events
- Reading messages from popular messenger services and social networks, such as 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 etc.
- Viewing photos and pictures from phones' image galleries
- Taking screenshots
- Taking front (selfie-mode) camera photos

Are Android OS and iOS devices equally affected by stalkerware?

Stalkerware apps are much less frequent on iPhones than on Android devices, because iOS is traditionally a closed system. Moreover, while perpetrators can work around this limitation on 'jailbroken' iPhones, they still require direct physical access to the phone to jailbreak it and install the stalkerware app. Nevertheless, iPhone users fearing surveillance should always keep a close eye on their device.

Alternatively, an abuser can offer their victim an iPhone – or any other device – with pre-installed stalkerware. There are many companies that make these services available online, allowing abusers to have these tools installed on new phones and delivered in factory packaging under the guise of a gift to the intended target.

Digital stalking, trust, and dating

Stalkerware and digital stalking are related but not mutually exclusive. We noted a rise in the use of legitimate technology and apps for illegitimate or nefarious purposes to track and monitor partners in recent years. To get further insights into the wider topic of digital stalking, Kaspersky commissioned Arlington Research to conduct 21,000 online interviews to get insights into digital stalking and stalkerware worldwide. The marketing research company questioned 1,000 people in each of the following countries: The UK, Germany, Spain, Serbia, Portugal, The Netherlands, Italy, France and Greece, The USA, Brazil, Argentina, Chile, Peru, Colombia, Mexico, China, Singapore, Russia, India and Malaysia. Respondents were aged 16 years and over and were either in a long-term relationship (62%), dating someone (16%) or not currently dating/in a relationship but had been in the past (21%). The fieldwork took place between 3-17 January 2024.

7%
have had stalkerware surreptitiously installed on their devices without their knowledge

Overview on stalking and being stalked

23 percent of respondents revealed they have encountered some form of online stalking from someone they were recently dating. It is possible for daters to potentially use publicly available information on dating apps to stalk or abuse. The spectrum of abuse is diverse, with over one-third (39%) of respondents reporting experiences of violence or abuse from a current or previous partner. Notably, 16 percent have received unwanted emails or messages, and –distressingly – 13 percent have been filmed or photographed without their consent. Additionally, 10 percent acknowledged having their location tracked, 10 percent have experienced unauthorized access to their social media accounts or emails, and alarmingly, seven percent have had stalkerware surreptitiously installed on their devices without their knowledge.

The gender disparity in these experiences is evident, with a higher proportion of female respondents (42%) having encountered violence or abuse compared to male respondents (36%). Those presently dating report higher instances of violence or abuse compared to individuals in long-term relationships (48% versus 37%). A notable 34 percent of respondents express concerns about the potential for online stalking, with female respondents showing slightly higher apprehension (36%) than their male counterparts (31%). This disconcerting scenario extends globally, with higher occurrences of online stalking reported in parts of South and Central America, and Asia. For instance, 42 percent of respondents in India, 38 percent in Mexico, and 36 percent in Argentina acknowledge experiencing some form of online stalking.

Additionally, 40 percent disclosed they had experienced stalking or suspected they were being stalked, with a further 14 percent saying they cannot recall or are uncertain such incidents occurred. Less than half (46%) stated they have never been stalked or suspected this had happened to them. Compared to 2021, fewer respondents

confirmed being stalked through technology (24%), but in 2024, a notable 14 percent couldn't recall, representing a concerning increase of 2 percent from 2021. Regional variations show higher incidents/suspicions in Singapore (69%), India (63%), Malaysia (54%), Mexico (53%), Peru (52%), and China (50%); while Portugal (21%), UK, Spain, and Italy (27%) reported lower rates.

Among those reporting incidents/suspicions, stalking through a phone app was the most prevalent (20%), followed by a laptop app (10%) and access via the webcam (10%). While a majority (78%) had never faced pressure to install monitoring apps or set parameters on their phones by their partner, 13 percent reported having a partner install or set parameters (similar to 14% in 2021), and 10 percent felt pressured into installing a monitoring app (15% in 2021). Significantly, in India, 34 percent reported partners installing/setting parameters and 29 percent faced pressure to install monitoring apps.

Worryingly, 12 percent of respondents admitted to installing or setting parameters on their partner's phone, while nine percent acknowledged pressuring their partner to install monitoring apps. In India, one-third did so, and 26 percent pressured their partners into installing monitoring apps.

Awareness of stalkerware varied, with 46 percent having no knowledge, 17 percent being unsure, and only 37 percent feeling confident about knowing what stalkerware is. Among those confident, less than 10 percent could identify all its surveillance capabilities. Notably, in 2021, 40 percent knew about stalkerware, with 19 percent unsure. In 2024, if respondents found stalkerware on their devices, 38 percent would try to identify and speak to the installer, 34 percent would attempt deletion, 20 percent would stop using the device, and 24 percent would involve the police. This is a shift from 2021, when 50 percent sought to identify the installer and 20 percent went to the police.

Shifting perspectives on stalking in modern relationships: privacy, consent, and the reality of stalking

A majority of individuals (54%) do not endorse the idea of monitoring a partner without their knowledge, signaling a prevailing disapproval of such actions. Significantly, the older generations, including Gen X, Baby Boomers, and the Silent Generation, exhibit a stronger inclination against monitoring without consent when compared to their younger counterparts. In comparison, between 2021 and 2024, there has been a noteworthy decrease in the percentage of respondents asserting that monitoring a partner without their knowledge is never acceptable, falling from 70 percent to 54 percent. Interestingly, those endorsing the viewpoint that it is always acceptable also decreased, from 13 percent in 2021 to eight percent in 2024. The nuanced perspective on this matter is evident in the fact that 38 percent in 2024 find monitoring without knowledge acceptable under certain circumstances, a substantial rise from the 17 percent reported in 2021.

Examining attitudes toward consensually monitoring (sharing of information with full knowledge and consent for a purpose such as safety) a partner's online activities, 45 percent of respondents express the belief that it is not acceptable, emphasizing the importance of privacy rights. Meanwhile, 27 percent advocate for full transparency in relationships, deeming consensual monitoring appropriate, and 12 percent find it acceptable only when it's mutual. Additionally, 12 percent concur with such monitoring when it concerns physical safety, while 4 percent reluctantly agree to it due to their partner's insistence. While sentiments this year regarding consensual monitoring of a partner's online activity closely align with those in 2021, a slightly higher percentage is open to the idea in 2024 (27%, compared to 25% in 2021). However, such actions remain unacceptable to the majority (45%), reinforcing the conviction that privacy is a fundamental right within relationships.

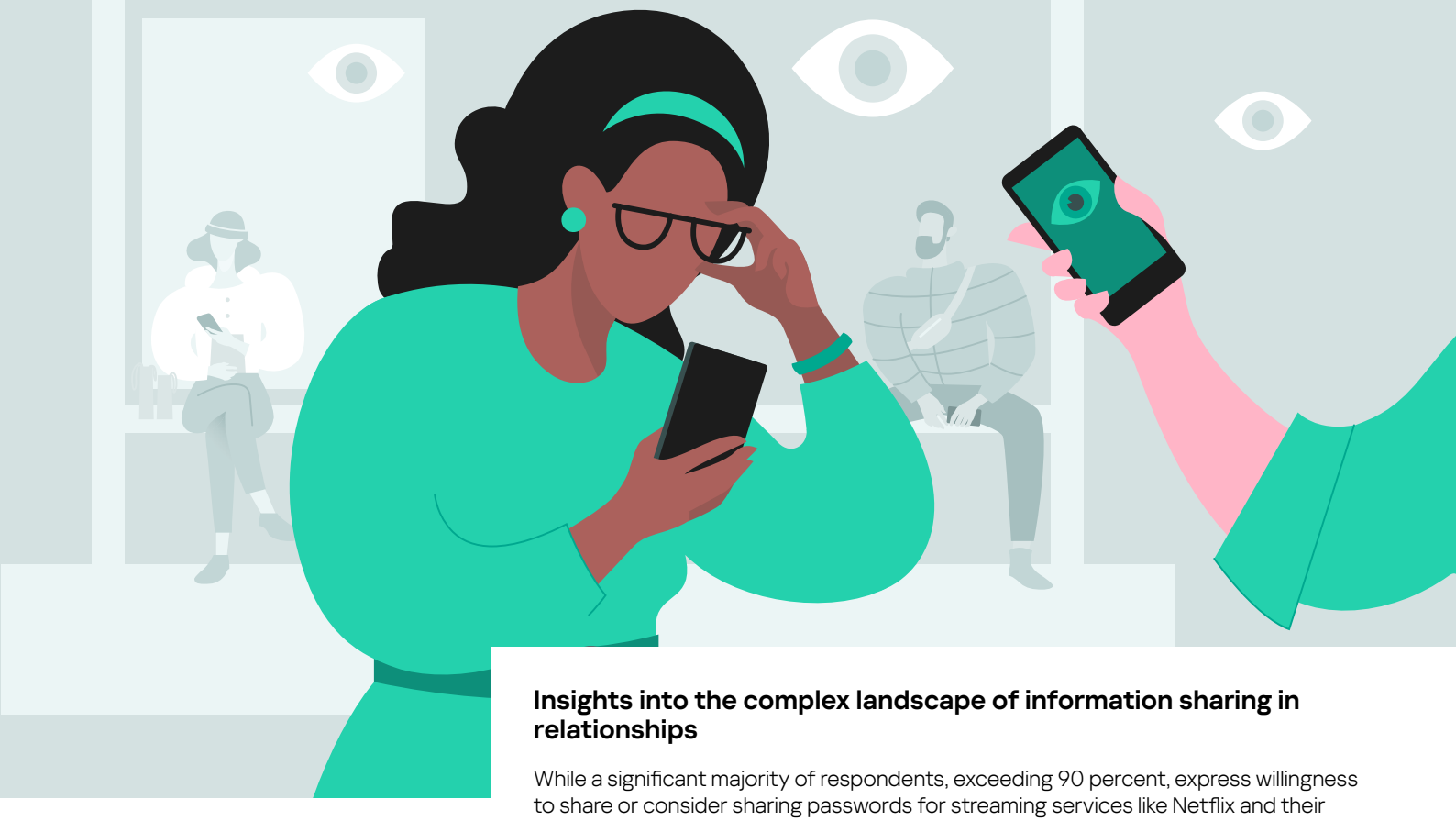
Despite the prevailing sentiments on monitoring, the issue of stalking surfaces prominently in dating scenarios. A substantial 34 percent of respondents view Googling or checking social media accounts of someone they recently started dating as an acceptable form of due diligence. Additionally, less than a quarter (23%) report experiencing some form of online stalking from a new dating prospect, underscoring the prevalence of this concerning phenomenon in contemporary dating landscapes.

Navigating trust and boundaries: A deep dive into digital privacy issues

Nearly half of the respondents (47%) express concerns about their partners violating their digital privacy, marking a notable increase from 2021 when only 37 percent reported these worries. This apprehension is more pronounced in Europe, where 62 percent of respondents share these concerns, contrasting with a lower percentage in the Asia-Pacific region (37%). Across all regions, common sources of worry include the monitoring of text messages (20%) and partners seeking full access to their phones, both physically and remotely (20%). More respondents now fret about partners breaching their privacy by removing passwords from their devices (13% in 2024 compared to 9% in 2021) or consistently requesting geolocation sharing (12% in 2024 compared to 10% in 2021). However, a slightly smaller percentage (15% in 2024 compared to 17% in 2021) worry about partners invading their privacy by reading their emails.

Regarding trust and access to personal devices, half of the respondents (51%) express trust in their partners by granting them full access to their phones. Another 19 percent permit access but with certain apps protected by additional passwords or security measures. One-fifth, while trusting their partners, opt not to provide access to their phones. The remaining respondents are divided, with five percent not trusting their partners with any access and four percent choosing not to answer. Remarkably, individuals in current relationships exhibit more hesitancy, with 40 percent agreeing to grant full access compared to 61 percent among those in long-term relationships.

On the flip side, 52 percent of respondents enjoy full access to their partners' phones, while an additional 23 percent have access but with specific apps shielded by additional passwords or security measures. Conversely, 18 percent report not being granted access to their partners' phones, and seven percent prefer not to disclose this information. These dynamics highlight the intricate interplay of trust and digital boundaries within romantic relationships.



Insights into the complex landscape of information sharing in relationships

While a significant majority of respondents, exceeding 90 percent, express willingness to share or consider sharing passwords for streaming services like Netflix and their photos, a more cautious approach emerges when it comes to certain types of sensitive information. Interestingly, respondents exhibit heightened reluctance to share passwords for security devices, with 18 percent firmly stating they would never share access to these.

> It's positive to observe increased caution, especially regarding sensitive data like security device passwords.

Delving into specifics, the data reveals a nuanced perspective on different types of information sharing. For instance, sharing passwords to streaming services sees 69 percent willing, and only nine percent asserting they would never share. Likewise, for photos, 66 percent are open to sharing, 26 percent might consider it, and eight percent firmly resist the idea. Moving to more personal domains, regarding data such as text messages, 52 percent stated they were willing to share them, while 33 percent might consider it, but 15 percent would never show this data to others.

The same trend holds for passwords to security devices such as Bluetooth enabled video doorbells, where 52 percent are open to sharing, and 30 percent might consider it, 18 percent are adamant they would not disclose them. Similarly, payment information sees 49 percent willing, 30 percent possibly willing, and 21 percent won't share. As the sensitivity of information increases, the willingness to divulge it decreases, as evident in the decreasing percentages of people willing to reveal passwords to other trackable accounts (47% willing, 29% might consider, and 24% unwilling) and browser history (46% willing, 34% might consider, and 20% unwilling). This intricate balance between openness and reservations highlights the complex dynamics surrounding privacy and information sharing within intimate relationships.

***David Emm**, security and data privacy expert at Kaspersky said:*

These findings highlight the delicate balance individuals strike between intimacy and safeguarding personal information. It's positive to observe increased caution, especially regarding sensitive data like security device passwords. The reluctance to share such critical access aligns with cybersecurity principles. The willingness to share streaming service passwords and photos signifies a cultural shift, though individuals should recognize potential risks even in seemingly innocuous information sharing. These insights underscore the importance of fostering open communication within relationships, establishing clear boundaries, and promoting digital literacy. For security professionals, it reinforces the need for ongoing education on cybersecurity best practices and empowering individuals to make informed decisions about sharing personal information within relationships.

Emma Pickering, Head of Technology-Facilitated Abuse and Economic Empowerment Team at Refuge

> Sadly, we recognise that for many survivors setting passwords on devices or not sharing the device or password is not a luxury they are afforded.

The statistics highlighted in this report are really concerning, but we are sadly not surprised. Here at Refuge, we are seeing an alarming increase in survivors reporting concerns relating to stalkerware. As these statistics reveal, the issue of stalkerware is a widespread concern.

It is likely that we are seeing this due to an increase in stalkerware features within parental monitoring Apps making the ability to stalk ever more accessible. While we are actively looking for stalkerware that is intended towards monitoring your ex-partner there are many other forms of stalkerware available that is aimed towards an audience who download the Apps without understanding the full features, or to be used for other nefarious reasons.

It is also very important to note that we rarely see any form of tech abuse used in isolation. Alongside stalkerware, abusers are often misusing other forms of technology to cause harm and distress. This is why we should always ensure, as agencies, we are completing a detailed tech assessment and supporting survivors to regain access to all accounts and devices. For this reason it is imperative that we continue to work together with the wider tech community to understand the technology being used, to try to prevent it being used for harm and to try and build in safety by design collaboratively.

Sadly, we recognise that for many survivors setting passwords on devices or not sharing the device or password is not a luxury they are afforded. We do advise if anyone is concerned, to always use a safe device to make contact with an agency for support, and that for any sensitive conversations, emails or searches, that they do not conduct these on the device that they are worried may being monitored.

> Consent is agreement free of force or coercion.

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

This report highlights both the prevalence of stalking behavior perpetrated with technology and the related perceptions on privacy within intimate partner relationships. The use of stalkerware or any tool to monitor someone else without their consent is a violation of privacy and a common tactic of abuse. This report demonstrates how abusive individuals use a wide range of monitoring tactics, including both stalkerware and other applications that facilitate the sharing of personal information.

The report also explored the norms and perspectives on privacy within intimate partner relationships. A significant portion of respondents reported they would willingly share some information, whether for safety reasons or otherwise. A small percentage, 4%, stated they reluctantly agreed to monitoring at their partner's insistence – this is not the same as consent. It's important to create a clear distinction between consensual sharing and non-consensual monitoring. Consent is agreement free of force or coercion.

Combatting stalkerware together

Stalkerware is foremost not a technical problem, but an expression of a problem within society which therefore requires action from all sections of society. Kaspersky is not only actively committed to protecting users from this threat but also maintaining a multilevel dialogue with non-profit organizations, and industry, research and public agencies around the world to work together on solutions that tackle the issue.

In 2019, Kaspersky was the first cybersecurity company in the industry to develop a new attention-grabbing alert that clearly notifies users if stalkerware is found on their device. While Kaspersky's solutions have been flagging potentially harmful apps that are not malware – including stalkerware – for many years, the new notifications function alerts the user to the fact that an app has been found on their device that may be able to spy on them.

In 2022, as part of Kaspersky's launch of a new consumer product portfolio, the Privacy Alert was expanded and now it informs the user about the presence of stalkerware on the device, and warns them that, if stalkerware is removed, the person who installed the app will also be alerted. This may lead to an escalation of the situation. Moreover, the user risks erasing important data or evidence that could be used in a prosecution. Figure 2, below, shows the new warning in the blue box. Kaspersky's Privacy Alert is included in all of the company's consumer security solutions to protect users against stalkerware.

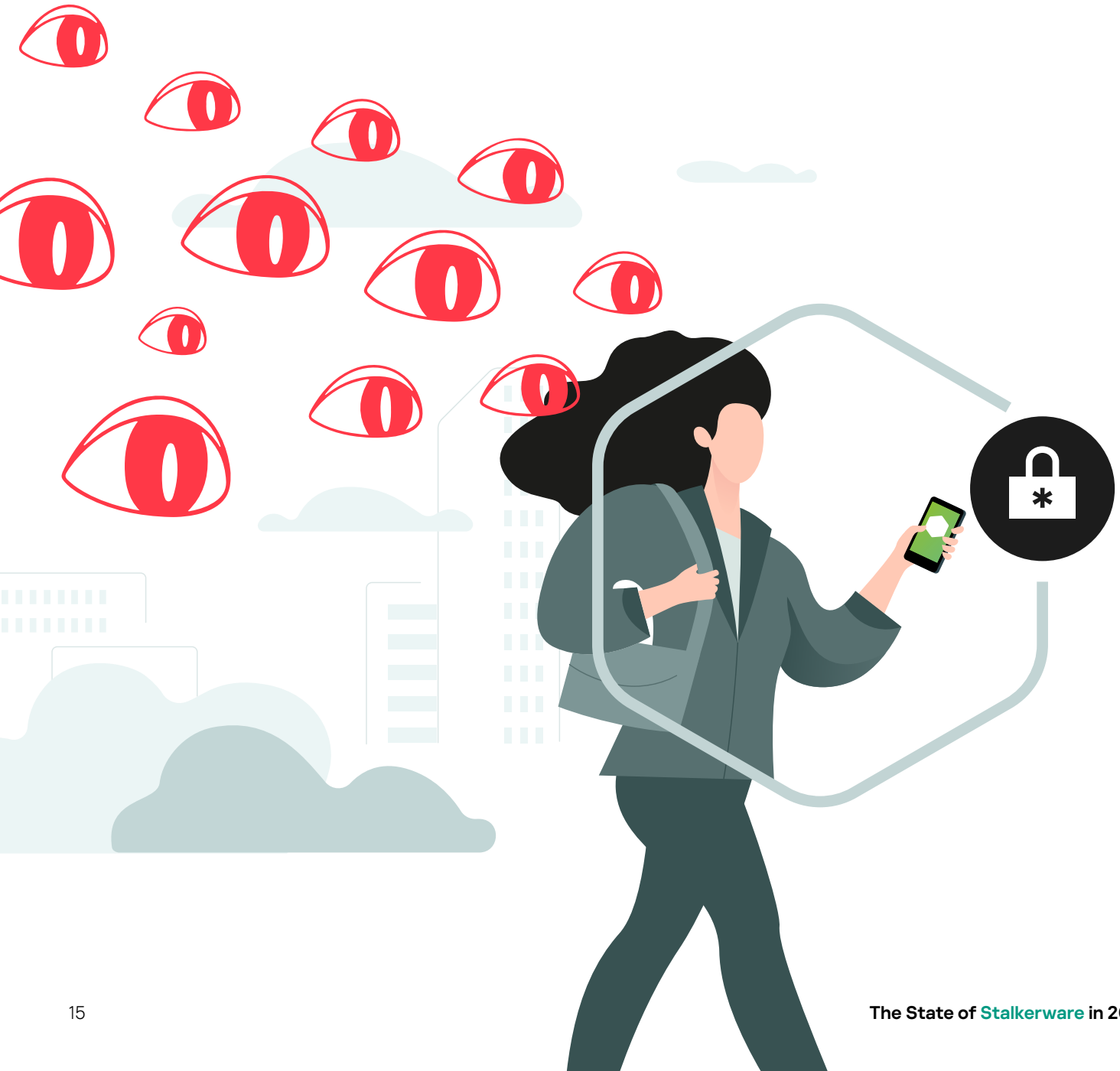
Figure 2 – 2024 update of Kaspersky's privacy alert to warn about removing stalkerware

In 2019, Kaspersky also co-founded the **Coalition Against Stalkerware**, an international working group against stalkerware and domestic violence that brings together private IT companies, NGOs, research institutions, and law enforcement agencies working to combat cyberstalking and help victims of online abuse. Through a consortium of more than 40 organizations, stakeholders can share expertise and work together to solve the problem of online violence. In addition, the Coalition's website, which is available in seven different languages, provides victims with help and guidance in case they may suspect stalkerware is present on their devices.

From 2021-2023, Kaspersky was a consortium partner of the EU project **DeStalk**, co-funded by the Rights, Equality, and Citizenship Program of the European Union. The five project partners that formed the consortium combined the expertise of the IT Security Community, Research, and Civil Society Organizations, and Public Authorities. As a result, the DeStalk project trained a total of 375 professionals directly working in women's support services and perpetrator programs, and officials from public authorities on how to effectively tackle stalkerware and other digital forms of gender-based violence, as well as raising public awareness on digital violence and stalkerware.

As part of the project, Kaspersky developed an e-learning course on cyberviolence and stalkerware within its Kaspersky Automated Security Awareness Platform, a freely available online micro learning training platform which can be accessed in five different languages. To date, more than 210 professionals have completed the e-learning course. Although the DeStalk project has ended, e-learning is still available on the DeStalk project website **https://www.work-with-perpetrators.eu/destalk**.

In June 2022, Kaspersky launched a website dedicated to **TinyCheck** to disseminate further information about the tool. TinyCheck is a free, safe and **open-source tool** that can be used by non-profit organizations and police units to help support victims of digital stalking. In 2020, the tool was created to check devices for stalkerware and monitoring apps without making the perpetrator aware of the check. It does not require installation on a user's device because it works independently to avoid detection by a stalker. TinyCheck scans a device's outgoing traffic using a regular Wi-Fi connection and identifies interactions with known sources such as stalkerware-related servers. TinyCheck can also be used to check any device on any platform, including iOS, Android, or any other OS.



Think you are a victim of stalkerware? Here are a few tips...

Whether you are a victim of stalkerware or not, these tips can help you to better protect yourself:

- Protect your phone with a strong password that you never share with your partner, friends, or colleagues.
- Change passwords for all of your accounts periodically and don't share them with anyone.
- Only download apps from official sources, such as Google Play or the Apple App Store.
- Install a reliable IT security solution like Kaspersky for Android on devices and scan them regularly. However, in cases where stalkerware may have already been installed, the solution should only be uploaded once the risk to the victim has been assessed, as the abuser may notice the use of cybersecurity.

Victims of stalkerware may be victims of a larger cycle of abuse, including physical.

In some cases, the perpetrator is notified if their victim performs a device scan or removes a stalkerware app. If this happens, it can lead to an escalation of the situation and further aggression. This is why it is important to proceed with caution if you think you are being targeted by stalkerware.

- **Reach out to a local support organization:** to find one close to you, check the **Coalition Against Stalkerware website**.
- **Keep an eye out for the following warning signs:** these can include a fast-draining battery due to unknown or suspicious apps using up its charge, and newly installed applications with suspicious access to use and track your location, send, or receive text messages and other personal activities. Also check if your "unknown sources" setting is enabled, it may be a sign that unwanted software has been installed from a third-party source. However, the above indicators are circumstantial and do not indicate the unequivocal presence of stalkerware on the device.
- **Do not try to erase the stalkerware, change any settings or tamper with your phone:** this may alert your potential perpetrator and lead to an escalation of the situation. You also risk erasing important data or evidence that could be used in a prosecution. Take steps to determine what course of action makes the most sense for your current situation prior to making changes that could lead to an escalation in behavior from a potential perpetrator.

For more information about our activities on stalkerware or any other request, please write to us at: ExtR@kaspersky.com

kaspersky