The State of **Stalkerware** in 2022

Coalition Against Stalkerware

kaspersky

Contents

Main findings of 2022

The State of Stalkerware is an annual report by Kaspersky which contributes to a better understanding of how many people in the world are affected by digital stalking. Stalkerware is a commercially available software that can be discretely installed on smartphone devices, enabling perpetrators to monitor an individual's private life without their knowledge.

Stalkerware can be downloaded and easily installed by anyone with an Internet connection and physical access to a smartphone. A perpetrator violates the victim's privacy as they can then use the software to monitor huge volumes of personal data. Depending on the type of software, it is usually possible to check device location, text messages, social media chats, photos, browser history and more. Stalkerware works in the background, meaning that most victims will unaware that their every step and action is being monitored.

In most countries around the world, the 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 part of tech-enabled abuse and often used in abusive relationships. As this is part of a wider 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.

2022 data highlights

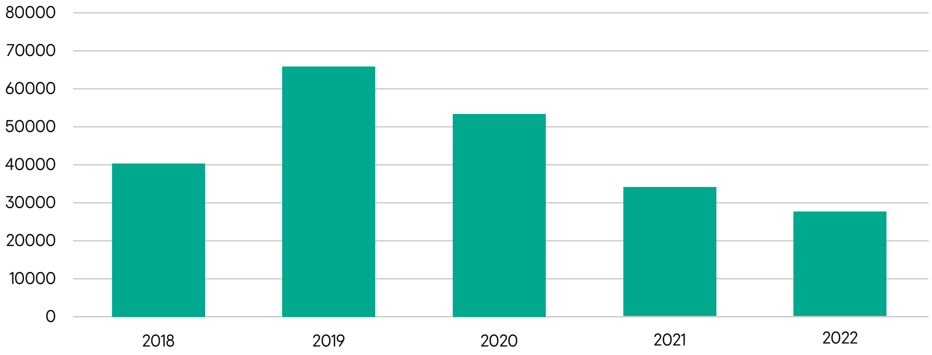
- **In 2022, Kaspersky data shows that 29,312 unique individuals around the world were affected by stalkerware.** Compared to the downwards trend that has been recorded in previous years, this is similar to the total number of affected users in 2021. Taking into account the developments in digital stalking software over the past few years, the data suggests there is a trend towards stabilization. More broadly, it is important to note that the data covers the affected number of Kaspersky users, with the global number of affected individuals likely to be much higher. Some affected users may use another cybersecurity solution on their devices, while some do not use any solution at all.
- **In addition, the data reveals a stable proliferation of stalkerware over the 12 months of 2022.** On average, 3333 users each month were newly affected by stalkerware. The stable detection rate indicates that digital stalking has become a persistent problem that warrants wider societal attention. Members from the Coalition Against Stalkerware estimate that there could be close to one million victims globally affected by stalkerware every year.
- According to the Kaspersky Security Network**, stalkerware is most commonly used in Russia, Brazil, and India,** but continues to be a global phenomenon affecting all countries. Regionally, the data reveals that the largest number of affected users can be found in the following countries:
  - Germany, Italy, and France (Europe);
  - Iran, Turkey, and Saudi Arabia (Middle East and Africa);
  - India, Indonesia, and Australia (Asia-Pacific);
  - Brazil, Mexico, and Ecuador (Latin America);
  - United States (North America);
  - Russian Federation, Kazakhstan and Belarus (Eastern Europe (except European Union countries), Russia and Central Asia).
- Globally, the most commonly used stalkerware app is Reptilicus with 4,065 affected users.

2022 trends observed by Kaspersky

Global detection figures: affected users

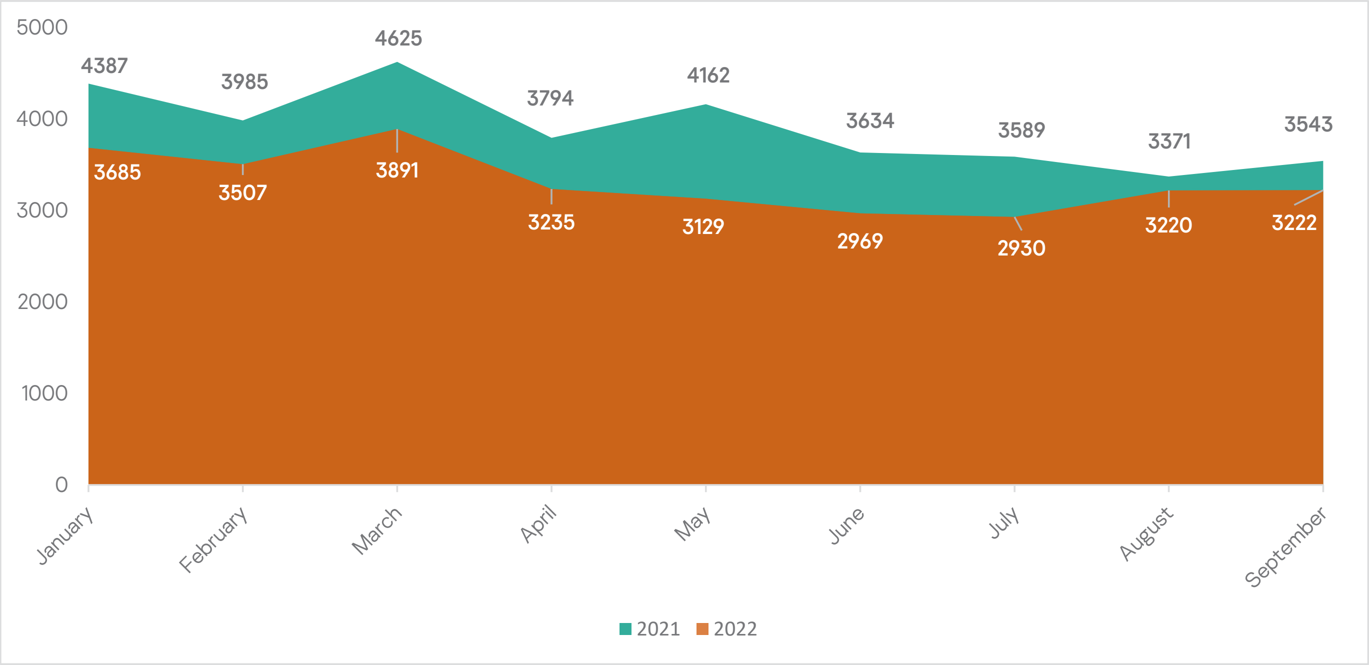
In 2022, a total of 29,312 single users were affected by stalkerware

This section compares the global and regional statistics collected by Kaspersky in 2022 with statistics from previous years. In 2022, a total number of 29,312 unique users were affected by stalkerware. Graphic 1, below, shows how this number has varied from year to year since 2018.



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

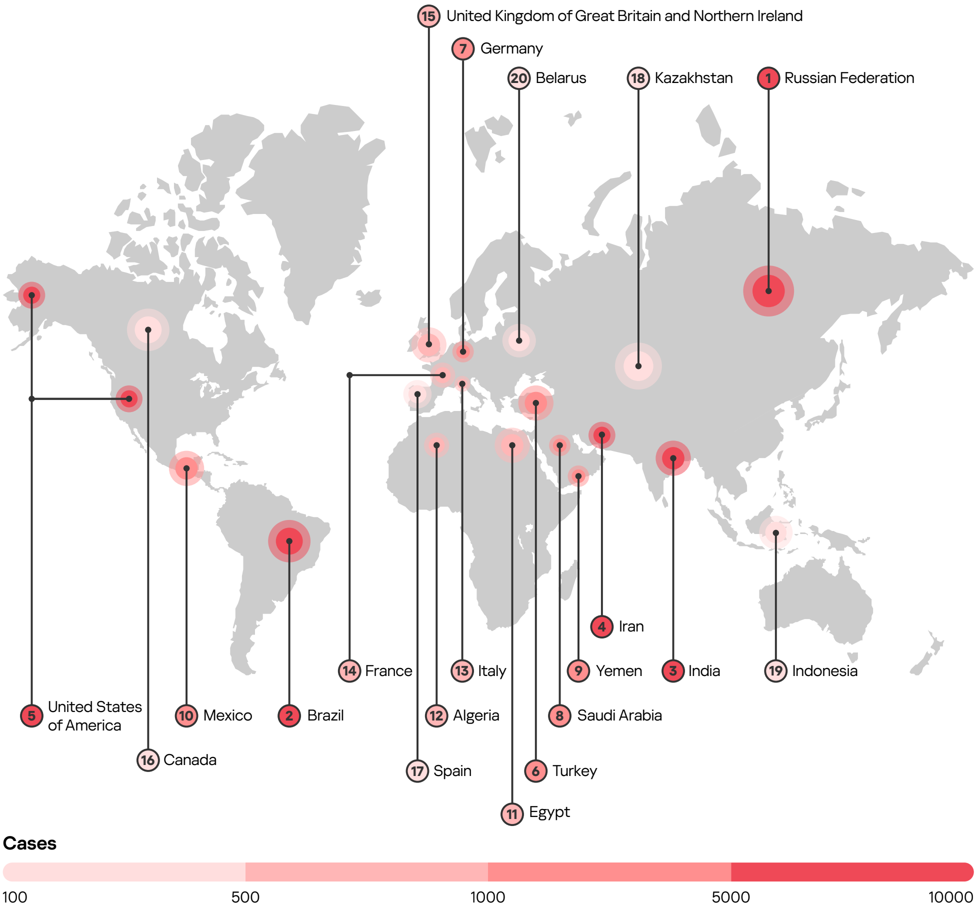
Graphic 2, below, shows the number of unique affected users per month from 2021 to 2022. In 2022, the situation is almost identical to 2021, indicating that the rate of stalkerware proliferation has stabilized. On average, 3333 users were newly affected by stalkerware every month.



Graphic 2 – Unique affected users per month over the 2021-2022 period

Global and regional detection figures: geography of affected users

Stalkerware continues to be a global problem. In 2022, Kaspersky detected affected users in 176 countries.



Map 1 – Countries most affected by stalkerware in 2022

Methodology

The data in this report has been taken from aggregated threat statistics obtained from the Kaspersky Security Network. The Kaspersky Security Network is dedicated to processing cybersecurity-related data streams from millions of volunteer participants around the world. All received data is anonymized. 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.

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 2022, Russia (8,281), Brazil (4,969), and India (1,807) were the top 3 countries with the most affected users. Those three countries remain in leading positions according to Kaspersky statistics since 2019. Compared to previous years, it is noteworthy that the number of affected users in the U.S. has dropped down the ranking and now features in fifth place with 1,295 affected users. Conversely, there has been an increase noted in Iran which has moved up to fourth place with 1,754 affected users.

Compared to 2021, however, only Iran features as a new entrant in the top 5 most affected countries. The other four countries – Russia, Brazil, India, and the U.S. – have traditionally featured at the top of the list. Looking at the other half of the top 10 most affected countries, Turkey, Germany, and Mexico have remained among the countries most affected compared to last year. New entrants into the top 10 most affected countries in 2022 are Saudi Arabia and Yemen.

	Country	Affected users
1	Russian Federation	8,281
2	Brazil	4,969
3	India	1,807
4	Iran	1,754
5	United States of America	1,295
6	Turkey	755
7	Germany	736
8	Saudi Arabia	612
9	Yemen	527
10	Mexico	474

Table 1 – Top 10 countries most affected by stalkerware in the world in 2022

In Europe, the total number of unique affected users in 2022 was 3,158. The three most affected countries in Europe were Germany (737), Italy (405) and France (365). Compared to 2021, all countries up to including seventh place in the list (the Netherlands) continue to feature as the most affected countries in Europe. New entrants in the list are Switzerland, Austria, and Greece.

	Country	Affected users
1	Germany	736
2	Italy	405
3	France	365
4	United Kingdom	313
5	Spain	296
6	Poland	220
7	Netherlands	154
8	Switzerland	123
9	Austria	71
10	Greece	70

Table 2 - Top 10 countries most affected by stalkerware in Europe in 2022

In Eastern Europe (excluding European Union countries), Russia, and Central Asia, the total number of unique affected users in 2022 was 9,406. The top three countries were Russia, Kazakhstan, and Belarus.

	Country	Affected users
1	Russian Federation	8,281
2	Kazakhstan	296
3	Belarus	267
4	Ukraine	258
5	Azerbaijan	130
6	Uzbekistan	76
7	Moldova	34
8	Tajikistan	32
9	Kyrgyzstan	31
10	Armenia	27

Table 3 - Top 10 countries most affected by stalkerware in Eastern Europe (excluding EU countries), Russia and Central Asia in 2022

In the Middle East and Africa region, the total number of affected users was 6,330, slightly higher than in 2021. While Iran with 1,754 affected users features at the top of this list in 2022, Turkey's 755 affected users has seen the country move up to second in the region, followed closely by Saudi Arabia with 612 affected users.

	Country	Affected users
1	Iran	1,754
2	Turkey	755
3	Saudi Arabia	612
4	Yemen	527
5	Egypt	469
6	Algeria	407
7	Morocco	168
8	United Arab Emirates	155
9	South Africa	145
10	Kenya	123

Table 4 - Top 10 countries most affected by stalkerware in Middle East & Africa in 2022

In the Asia-Pacific region, the total number of affected users was 3,187. India remains far ahead of the other countries in the region, with 1,807 affected users. Indonesia occupies second place with 269 affected users, while Australia is third with 190 affected users.

	Country	Affected users
1	India	1,807
2	Indonesia	269
3	Australia	190
4	Philippines	134
5	Malaysia	129
6	Vietnam	109
7	Bangladesh	105
8	Japan	95
9	Thailand	52
10	Pakistan	48

Table 5 - Top 10 countries most affected by stalkerware in Asia-Pacific region in 2022

The Latin America and the Caribbean region is dominated by Brazil with 4,969 affected users. This accounts for approximately 32% of the region's total number of affected users. Brazil is followed by Mexico and Ecuador in the list, while Colombia has moved into fourth place. A total number of 6,170 affected users were recorded in the region.

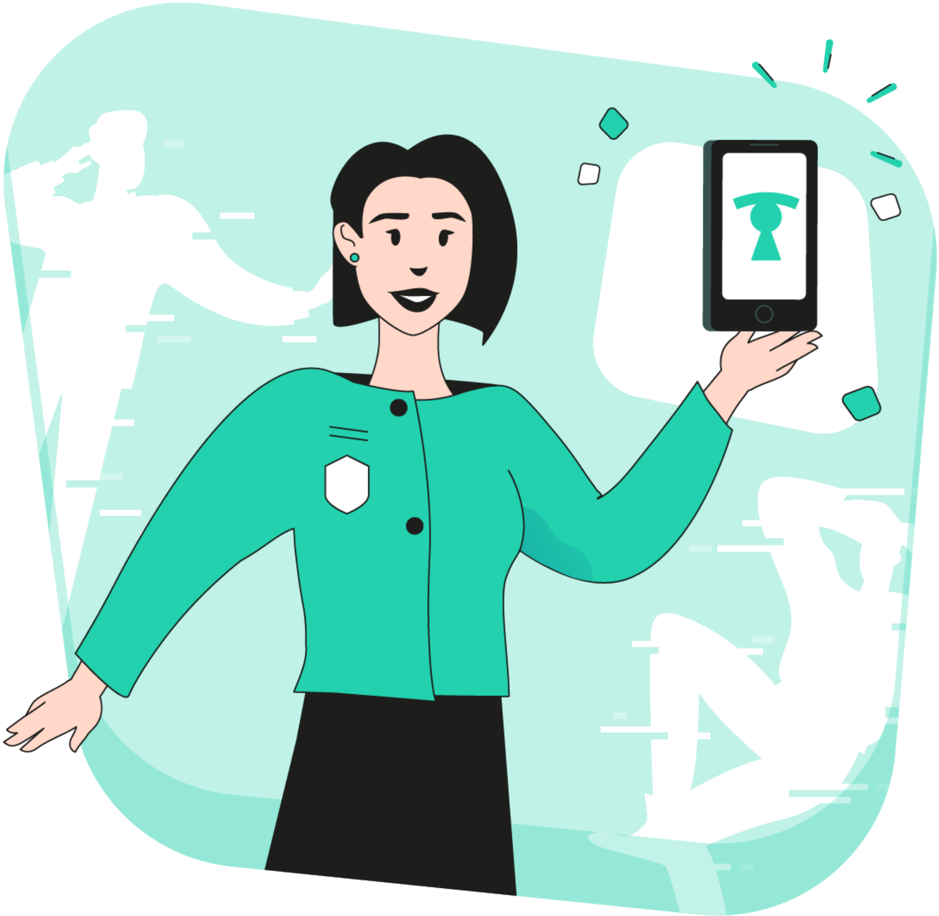
	Country	Affected users
1	Brazil	4,969
2	Mexico	474
3	Ecuador	146
4	Colombia	120
5	Peru	111
6	Argentina	85
7	Chile	49
8	Bolivia	32
9	Venezuela	30
10	Dominican Republic	24

Table 6 - Top 10 countries most affected by stalkerware in Latin America in 2022

Finally, in North America, 87% of all affected users in the region are found in the United States. This is to be expected given the relative size of the population in the United Sates compared to Canada. Across the North America region, 1,585 users were affected in total.

	Country	Affected users
1	United States of America	1,295
2	Canada	299

Table 7 - Number of users affected by stalkerware in North America in 2022



Global detection figures – stalkerware applications

This section lists the stalkerware applications most commonly used to control smartphones around the world. In 2022, the most popular app was Reptilicus (4,065 affected users). This year, Kaspersky detected 182 different stalkerware apps.

	Application name	Affected users
1	Reptilicus (aka Vkurse)	4,065
2	Cerberus	2,407
3	KeyLog	1,721
4	MobileTracker	1,633
5	wSpy	1,342
6	SpyPhone	1,211
7	Anlost	1,189
8	Track My Phones	1,137
9	MonitorMinor	864
10	Hovermon	827

Table 8 - Top 10 list of stalkerware applications in 2022

Stalkerware provides a means to gain control over a victim's life. Their capabilities vary depending on the type of application and whether it has been paid for or obtained freely. Typically, stalkerware masquerades as legitimate anti-theft or parental control apps, when in reality they are very different - most notably due to their installation without consent and notification of the person being tracked, and their operation in stealth mode on smartphone devices.

Are Android OS and iOS devices equally affected by stalkerware?

Stalkerware tools are less frequent on iPhones than on Android devices because iOS is traditionally a closed system. However, perpetrators can work around this limitation on 'jailbroken' iPhones, but they still require direct physical access to the phone to jailbreak it. iPhone users fearing surveillance should always keep an 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, which can then be delivered in factory packaging under the guise of a gift to the intended victim.

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

- Hiding app icon
- Reading SMS, MMS and call logs
- Getting lists of contacts
- 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

Digital stalking and gender-based violence

Stalkerware is a method of cyber stalking which is part of digital violence

Both women and men can be victims of digital violence, but research shows that in the overwhelming majority of cases, women are the target because of their gender. It is important to remember that digital violence is another dimension of violence. It needs to be understood as a continuum of offline violence as it has real and negative effects on the victims. For more information, please read the fact sheet "Cyber Violence against Women and Girls: Key Terms and Concepts" (2022) published by the European Institute for Gender Equality.

Experts from academia and civil society organisations working with victim support services and perpetrator programs share with us their experience and views on digital gender-based violence and on tech abuse in general.

The importance of data to understand the scope of digital violence – Dr Leonie Maria Tanczer, Associate Professor at University College London and head of UCL's Gender and Tech Research Group

Past research on technology-enabled forms of stalking and gender-based violence has focused on a range of "everyday" digital systems that can coerce, control, and harm a person or groups of individuals. Whilst the current report and data are restricted to mobile devices, digital stalking can be facilitated through various devices, including GPS trackers or the so-called "Internet of Things" (IoT). The latter includes smart, Internet-enabled products such as smart doorbells, CCTV cameras or speakers.

The evidence-based on tech-enabled abuse is also still very restricted. Current research hubs are prevalent in Australia, the UK and the USA. Most studies are consequently focused on data deriving from these countries, which creates blind spots. Data such as the one offered in this report contributes to a broader understanding of the tech-enabled abuse landscape, which is urgently needed.

Victim support services have also been shown to struggle with the increasing requirements to keep up-to-date with technological developments. They have called for add-ons to existing risk assessment and safety practices, including "cyberstalking action plans" and dedicated training to increase the capabilities and responsiveness of the sector. Indeed, increasingly specialised service offers are being made available, as Refuge's Tech Safety team, the Safety Net Project by the National Network to End Domestic Violence (NNEDV) or the Clinic to End Tech Abuse (CETA) showcase.

The University College London's (UCL) Gender and Tech Research Group investigates the intersection points of technology, security, and gender to make digital systems work for everyone. Find out more:

https://www.ucl.ac.uk/computer-science/research/research-groups/gender-and-tech

Pay more attention to the suffering from digital violence – Elena Gajotto, Vice President at Una Casa Per L'Uomo

Cyberstalking has a concrete impact in the real lives of those who suffer it. There are medium- to long-term psychological, physical and social effects that we see daily in our anti-violence centers. As the European Parliament Research Service underlined in their study (2021), all women can be potential victims of cyberstalking, whether they are public figures, ex-partners, or simply social media users. Cyberstalking encompasses different types of behaviours such as persistent messaging, monitoring a victim's activity, or other forms of online pursuit, and as the same study states, "it may be that cyber stalking is simply an additional tool in the stalker's toolkit".

When working on digital violence, the following characteristics need to be considered:

- Digital violence can be perpetrated together with other forms of violence (physical, sexual, psychological, economical, etc.).
- Violence can start online and then carry on offline, or, vice versa, it can start in the offline world and then continue in the digital sphere.
- It is not simple to remove - permanently - offensive, violent, or triggering contents published online.
- Perpetrators of digital violence can be individuals or groups, and can be both known and unknown to the victim.
- Digital violence can be acted through a wide range of devices (PCs, smartphones, smart home devices, etc.) and on many different platforms (websites, instant messaging apps, online chats, social media, etc.).

As mentioned above, despite being carried out in the cyber sphere, these forms of violence have a deep and tangible impact on the real lives of victims. Studies show that women are mainly victims of cyberstalking or other forms of digital violence. They experience many of the same symptoms like victims of offline violence, such as for example, anxiety, panic attacks, PTSD, suicidal thoughts, anger, lack of self-confidence, and difficulties concentrating. There may be also negative economic effects (extortion, loss of income, etc.) and relational (loss of family and friends' network, social isolation, etc). Moreover, digital violence also has a collective impact, both on the economic and political level, with an increase of public legal, administrative and health costs on one side, and a lower participation to public discourse by women.

It is therefore important to emphasize the danger of this phenomenon. The society needs to pay more attention to the suffering from digital violence. To this end, we are working with our members as well collaborate with Kaspersky and all Coalition Against Stalkerware partners to support victims and to better train professionals working in the field of domestic violence.

Una Casa Per L'Uomo is an Italian civil society organization managing victim support services. Una Casa Per L'Uomo has been a consortium partner of the DeStalk project (2021-2023), co-funded by the Rights, Equality, and Citizenship Program of the European Union, and is a member of the Coalition Against Stalkerware.

Addressing social attitudes that support technology-facilitated abuse — Anna McKenzie, Communications Manager at WWP EN

Technology-facilitated abuse such as stalkerware is a growing concern for our member organisations working on behavioural change with domestic violence perpetrators.

Digital violence continues to be on the rise: digital devices, secret surveillance software and online spaces offer the perfect environment for abusive partners to extend control over their partners' lives. However, checking a partner's phone, reading their e-mails, being aware of their location and knowing their passwords is now so commonplace that individuals often do not even realise they are displaying abusive behaviours.

How is it that these apparent breaches of privacy are not perceived as such?

In 2021, Kaspersky published the "Digital Stalking in Relationships Report", highlighting some worrying trends. According to the data, behaviors such as monitoring a partner's digital activities with their consent was largely considered acceptable to ensure transparency within a relationship. Concerningly, however, almost a third of respondents were ok with monitoring a partner's activities without their consent, especially if they believed their partner was being unfaithful.

These attitudes speak directly to issues our members regularly encounter in their work with domestic violence perpetrators. It is highly problematic to assume that a person not consenting to control means they are hiding a possible infidelity. In abusive relationships, consent is tenuous at best: How can they say yes, if they can't say no, after all? Likewise, the acceptance of suspicion of infidelity as an e xcuse for spying on a partner is a golden opportunity for abusive partners who constantly perceive a threat of cheating in their relationships. This also speaks towards a sense of ownership and a lack of healthy communication which are central concerns in abusive relationships.

We believe that beyond the obvious need for legal regulation, capacity-building and general awareness raising on the issue of digital violence, it is of the utmost importance that abuse-supportive attitudes regarding tech-facilitated abuse are addressed in a widespread manner and from an early age. Studies such as the State of Stalkerware report are an important check on the status quo, but we must do more to change it. With the #NoExcuse4Abuse, developed and implemented in cooperation with Kaspersky, we took a first step towards addressing harmful social attitudes towards technology-facilitated abuse and stalkerware.

WWP EN is a European network with 69 members from 34 countries. We believe that without an approach for targeting perpetrators of domestic violence and holding them accountable, any strategy to stop intimate partner violence is incomplete. Our work focuses on stopping men's violence, holding them accountable, and promoting the Istanbul Convention. Find out more:

https://www.work-with-perpetrators.eu

Together keeping up the fight against stalkerware

Stalkerware is foremost not a technical problem, but an expression of a problem within society which therefore requires action from all areas 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 notification 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 not only informs the user about the presence of stalkerware on the device, but also warns the user that if stalkerware is removed the person who installed the app will be alerted. This may lead to an escalation of the situation.

Coalition Against 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 7 different languages, provides victims with help and guidance in case they may suspect stalkerware is present on their devices.

DeStalk
detect and stop stalkerware and cyberviolence against women

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 130 professionals have completed the e-learning course with a further 80 currently participating. Although the DeStalk project has ended, the e-learning course is still available on the DeStalk project website https://www.work-with-perpetrators.eu/destalk.

TinyCheck®

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 or not you are a victim of stalkerware, here are a few tips 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 the case of potentially already installed stalkerware, this should only be done after the risk to the victim has been assessed, as the abuser may notice the use of a cybersecurity solution.

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.

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

The Coalition Against Stalkerware was founded in November 2019 in response to the growing threat of stalkerware. The Coalition seeks to combine its partners' expertise in domestic violence survivor support and perpetrator work, digital rights advocacy, and cybersecurity to address the criminal behavior perpetrated by stalkerware. All members commit to fighting domestic violence, stalking, and harassment by addressing the use of stalkerware and raising public awareness about this issue.

The Coalition Against Stalkerware:
https://stopstalkerware.org

TinyCheck:
https://tiny-check.com

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com