Digital Stalking in Relationships

Report

What is stalkerware, and do people recognize it?

kaspersky BRING ON THE FUTURE

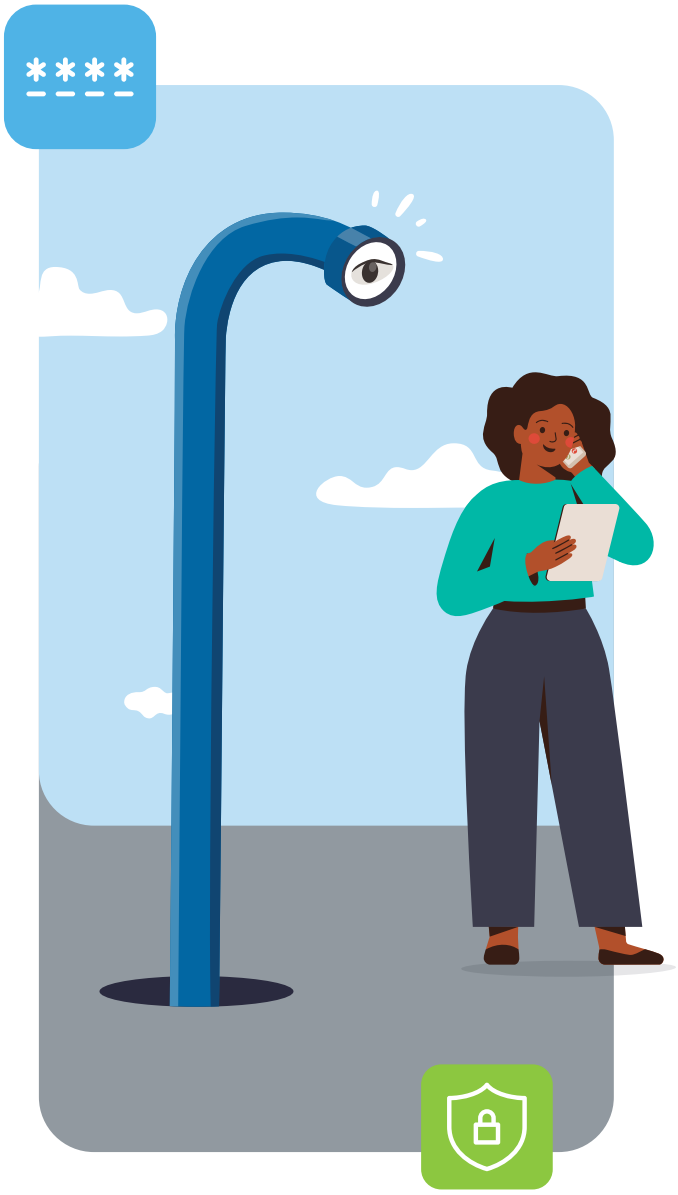
Index

Introduction

In 2021, people become more connected than ever – largely thanks to the prevalence of digital technology and the wide range of communications channels opened up by smart devices. Whilst there are very many positive uses for this technology: it brings us closer together, reduces the impact of geographical distance and facilitates new relationships to name a few, the ease of access to other people and their personal information also has the unfortunate potential to be misused.

In certain circumstances, digital technology can be used by immoral actors as part of a broader campaign of domestic abuse. This may take the form of one partner using monitoring applications known collectively as 'stalkerware' to keep track of their partner's whereabouts, interactions, and internet usage.

This report analyses research undertaken by SAPIO, on behalf of Kaspersky and several NGOs working in the area of domestic violence, to better understand the pervasiveness of stalkerware and how its toxic impact can be mitigated safely and effectively.



The research aimed to measure how widespread the use of stalkerware – or 'spouseware' as it is sometimes called – actually is, and to collect data to help domestic violence practitioners better understand the topic and enhance support for survivors.

Objectives included:

- Understanding how many people are aware of stalkerware and its capabilities
- Finding out the degree to which people are willing to monitor their partner
- Uncovering the types of data that people are happy to share and what they prefer to keep secret
- Understanding how many people have been victims of stalkerware
- Knowing which devices are commonly used by abusers to monitor victims

Our research found that the majority of people don't know what stalkerware is – 60% of respondents to our survey answered as such. However, that leaves a significant minority of people that do know what these tools are for.

What is stalkerware, and do people recognize it?

Stalkerware is monitoring software that people typically use to spy on their partner or significant other. It is commercially available and easy to install on someone else's smartphone. A perpetrator only needs physical access to their victim's phone once to activate stalkerware, and, as this report demonstrates, most people trust their intimate partner enough to give them this opportunity at some point.

Stalkerware falls into a legal grey area, despite clearly being unethical. Often stalkerware or spouseware apps operate under the guise of parental control apps or anti-theft solutions, which allow them to also remain accessible via app marketplaces such as Android Apps. But how aware are the general public that applications with this kind of functionality exist and are easily purchasable?

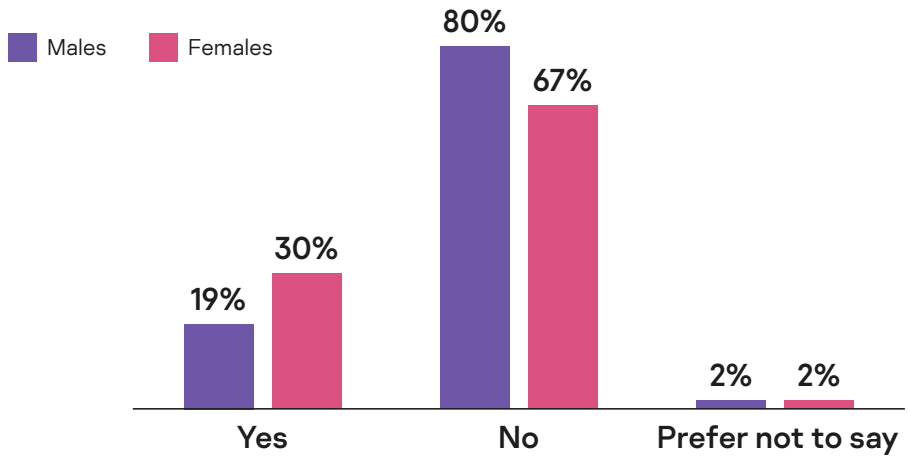
Our research found that the majority of people don't know what stalkerware is – 60% of respondents to our survey answered as such. However, that leaves a significant minority of people that do know what these tools are for. A particularly pessimistic interpretation could suggest that almost half of the surveyed population has personal experience of stalkerware, either as a victim or user.

However, it is not necessarily the case that someone needs to have direct experience of something to be familiar with it as a concept. It should also be taken into account that stalkerware has a fairly self-explanatory name, and people could draw on their familiarity with things like spyware to infer the function that stalkerware performs. That said, even a generous interpretation shows that stalkerware is clearly commonplace enough to be causing breaches of privacy to thousands of people and must be taken seriously and tackled accordingly.

Demographic divides and capability confusion

There are some important disparities to be aware of when it comes to awareness levels of stalkerware. Firstly, more men are aware of stalkerware's existence than women (44% vs 36% respectively). And secondly, younger people are more likely to be familiar with stalkerware than older respondents: 46% of 16-34 year-olds would recognize it compared to just 28% of people who are 55 and over.

Have you ever experienced violence or abuse by your partner?



Examining the data more closely, some potential reasons for this emerge. More males (10%) than females (8%) admitted to installing stalkerware on their partner's phone. And because stalkerware operates in a clandestine way, it makes sense that those who are more frequent users of it are more aware of its existence than those who are more likely to be victims. This is borne out further by the fact that women are significantly more likely than men to have been victims of domestic abuse at the hands of their partner (30% vs 19%).

In terms of the age disparity, younger respondents (45% of 16-34 year-olds) are more than twice as likely to worry about a partner violating their digital privacy than older respondents (20% of those aged 55 and over). This could be because younger respondents have grown up living in a digital-centric world for a greater proportion of their lives. Or it could be because they are more keenly aware of the possibility that their digital privacy could be compromised through the use of malicious stalkerware.

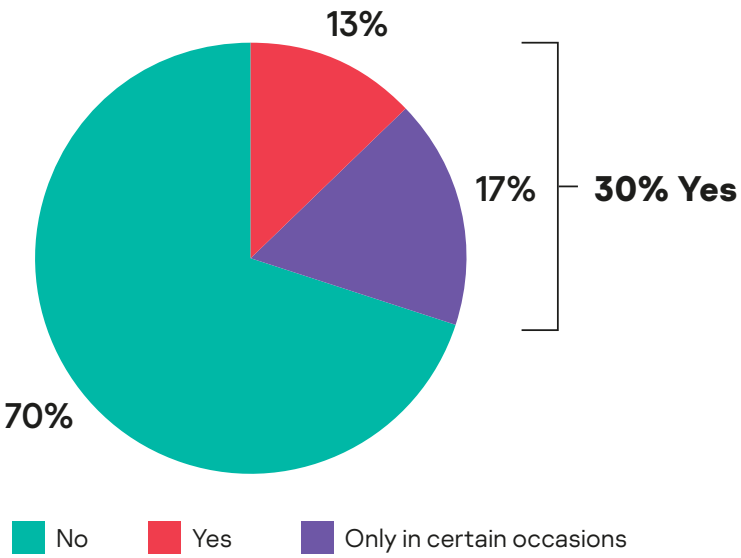
But even amongst those who are familiar with stalkerware, there are higher levels of awareness about certain functionalities than others. People do know that stalkerware performs functions like monitoring internet activity (72%), recording location (68%) and recording video and audio (60%). But they are less aware that it can inform the perpetrator when a victim tries to uninstall it (42%). So, there is still clearly work to be done in terms of educating the broader population about the existence of stalkerware, and the specifics of how it works by applying a victim-centered approach. This means that the wishes and needs of victims are the crux of the matter.

Erica Olsen, Safety Net Project Director, National Network to End Domestic Violence (NNEDV), offers a warning which should not be ignored: "An abusive person may increase or escalate their abusive behaviour if confronted or when stalkerware is removed. Survivors should do what they feel is safest for them in the moment and talk to a victim service provider for information on options."

Digital monitoring and consent

The conversation around stalkerware (and monitoring software more generally) hinges on the issue of consent. Thankfully, the vast majority of respondents to our survey (70%) do not believe it is acceptable to monitor their partner without consent. But this still leaves a concerningly significant minority (30%), who believe that it is ok (at least under some circumstances).

Is it ok to monitor your partner without their knowledge?



This figure is particularly alarming because it suggests that some of the 21% of respondents who suspect an intimate partner has spied on them using an app are likely to be correct. It is also higher than experts who work directly with the victims of abuse anticipated, especially amongst the 13% of people who believe it is acceptable to monitor their partner without introducing the caveat 'under certain circumstances'. Experts point out that perpetrators of abuse frequently use issues such as safety concerns as a false justification for their stalking.

The survey shows that almost two thirds of those who feel it is OK to monitor their partner would do so if they believed their partner was being unfaithful (64%), if it was related to their safety (63%), or if they believed them to be involved in criminal activity (50%). The mention of concerns around infidelity, in particular, exemplifies the abusive, coercive controlling nature of stalkerware app usage. As Berta Vall Castelló, Research and Development Manager, European Network for the Work with Perpetrators (WWP EN), highlights, such suspicion isn't a justifiable reason, despite a worrying number of people believing it to be.

"These findings emphasize an ideal of romantic love, which is particularly strong among teenagers, where partners are not permitted privacy, and sharing everything with your partner is a way of showing your love and trust," comments Berta Vall Castelló, Research and Development Manager from WWP EN.

There are also obvious flaws in the supposed justification around partner safety. If monitoring was genuinely due to safety concerns, the other party should be aware, consent to it, and be able to remove the application as they wish. As for suspicion of criminal activity, there are far more obvious and effective ways of tackling this than using monitoring software.

Non-consensual use of stalkerware is a much more widespread issue in some countries than others. India (45%), Malaysia (31%) and China (27%) ranked highest amongst our survey respondents for thinking it's ok to monitor intimate partners without their knowledge. Portugal/Colombia (7%), Spain/Czechia/Mexico/Peru (6%), and Argentina (5%) were least likely to agree with this. This could be partly due to cultural perceptions around a right to privacy – less than one in four respondents in India (24%) think everyone has a right to privacy, compared to 65% in Spain/Mexico.

When consent is introduced into the conversation, there is a corresponding increase in the number of people open to monitoring their partner. Almost half (48%) would theoretically monitor their partner consensually: 25% in the interests of 'full transparency' in a relationship, and a further 24% under certain circumstances (if it was about physical safety, or if the monitoring was mutual).

Digital abuse – how big is the issue?

In short, digital abuse is a massive, widespread problem. One in four people (25%) have experienced some form of abuse by their partner, although males are less likely to have suffered abuse (19%) than females (30%). In terms of the types of abuse perpetrated, psychological abuse is the most common form experienced by the sample at 72%, followed by physical abuse at 46% and economic abuse at 34%.

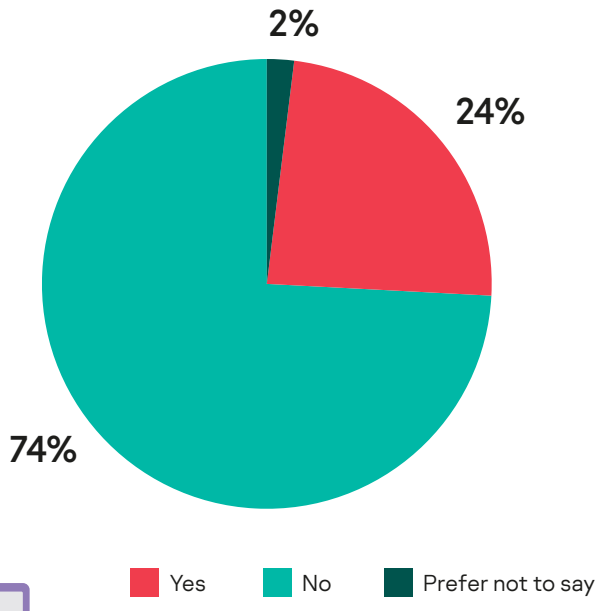
The evidence suggests that digital abuse through stalkerware apps could be a key enabler of psychological abuse. Almost a quarter of respondents (24%) have been stalked by means of technology, and 37% of people worry about their partner violating their digital privacy.

Many of the concerns about how such an invasion of privacy might manifest revolve around information accessible via a smartphone, and therefore at risk from stalkerware. The digital information that respondents were most worried about partners accessing includes social media (53%), text messages (51%) and emails (45%). This is particularly disconcerting given that half of those who have been stalked using technology were monitored through a phone app (50%).

Another nuance of privacy worries is that they are more of a concern in some localities than others. More than half of respondents from Peru and Colombia (56%) worry about their intimate partner violating their digital privacy, compared to just 20% in Germany/the Netherlands. There could be several reasons for this, including cultural attitudes to privacy or a variance in the amount of personal information that people choose to share and invest in digital devices across different locations.

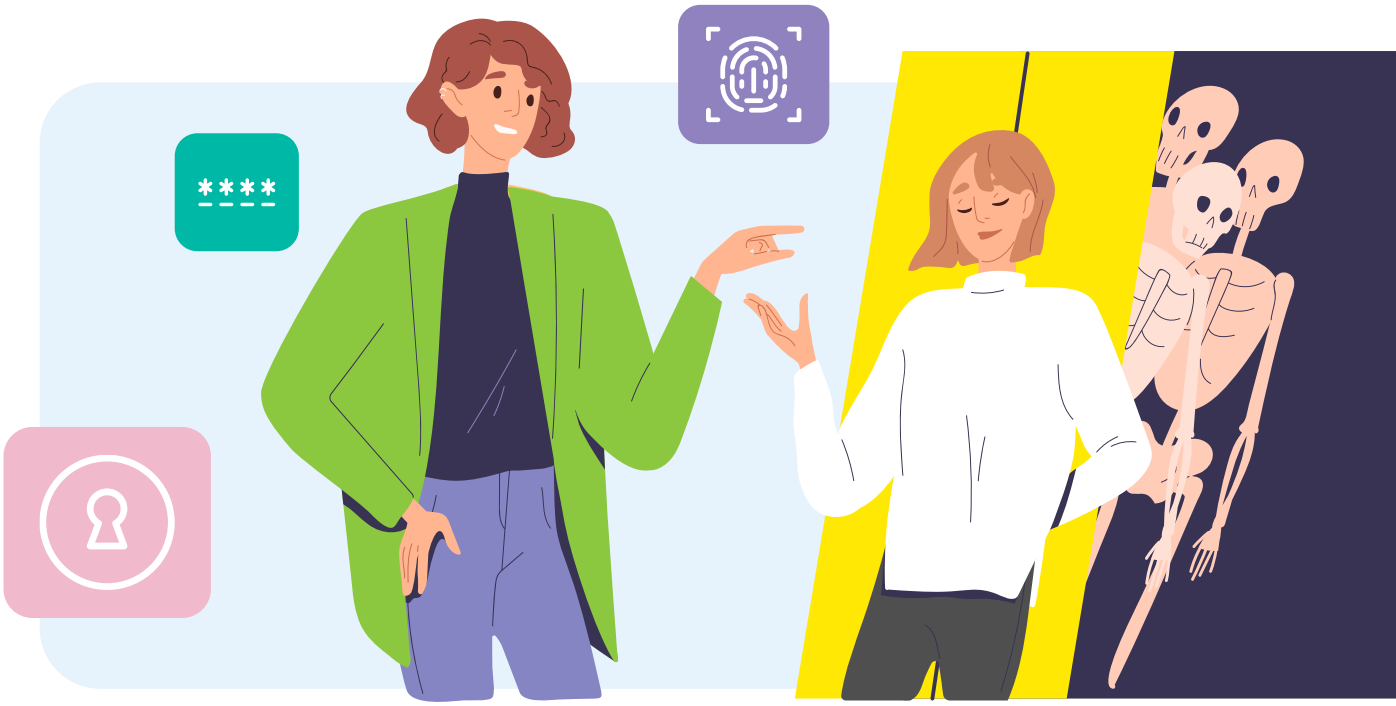
However, even in the lowest ranking countries, one in five people expressing privacy concerns is a considerable number that suggests issues exist which need to be addressed.

Have you ever been stalked by means of technology?



Personal vs private – what information will people willingly share with partners?

Privacy is a complex issue because people have unique boundaries regarding the information they are willing to disclose to their partner or allow them to have access to. For example, more than half of our survey respondents (57%) have shared their phone password with their partner, and a similar proportion (56%) know the password to their partner's phone. For more than two in five people (42%), it's also normal to share iCloud or Google log in details within their families. This suggests that many people are happy for their intimate partner and/or immediate family to have access to their digital lives.



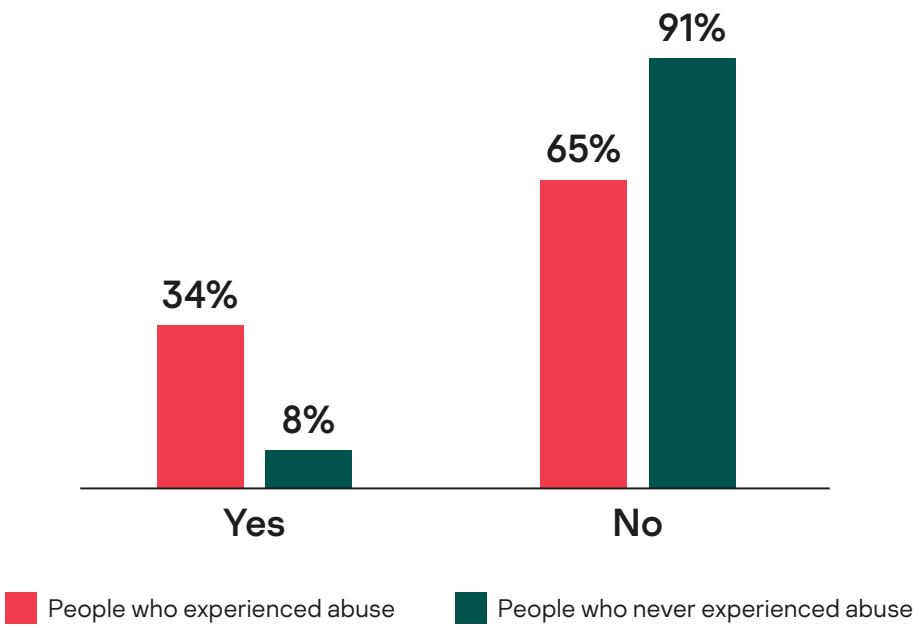
But again, this is under consensual circumstances where the situation is mutual rather than one-sided, and therefore indicative of a healthy relationship rather than an abusive one. Also, even with a password, a partner would need physical access to a device to view the information it holds. This access could be withheld or the password updated if the device owner changed their mind about it at any point in a healthy relationship.

Even in relationships where one or both partners are willing to share their digital information, certain data types are more freely given than others. Two in five respondents would never share passwords (38%), a quarter would never share phone call recordings (26%), and 25% would not share payment info with their intimate partner. By contrast, just 10% would be unwilling to share photos, and only 17% would be reluctant to disclose social media activity or camera access.

Quite disconcerting: one in 10 people (9%) admit installing monitoring apps on their partner's phone

Stalkerware thrives specifically under circumstances where there is a disparity between the level of access to information that one partner wants, and that the other wishes to disclose: 15% of people have been required by their partner to install a monitoring app, but this number is disproportionately higher in respondents who have experienced abuse (34%) compared to those who have not (8%). This is perhaps the clearest indication of the direct link between stalkerware and abuse that our research demonstrates.

Has an intimate partner ever required you to install a monitoring app?



Younger people (aged 18-34) are also much more likely (53%) than those who are aged 55 and over (8%) to have received such a demand from a partner. This is another key takeaway: stalkerware is linked to abuse, and younger people are vastly more vulnerable to its ill effects.

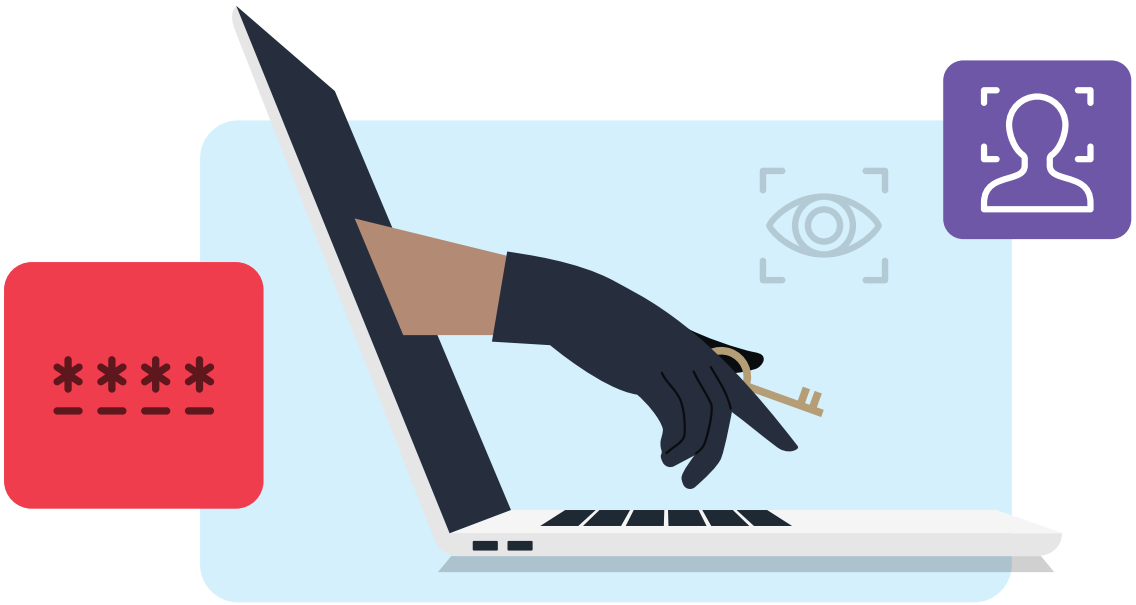
Most respondents to our survey (84%) do not willingly allow their partners to install or set parameters for their phone. But there are considerable geographical disparities in relation to this. For example, over a third of Indian respondents (38%) say their partner installs or sets parameters for their phone, whilst just 7% of Australian respondents would say the same.

The proportion of people who go on to break boundaries and attempt to access this information anyway (or do not ask in the first place) is quite disconcerting: one in 10 people (9%) admit installing monitoring apps on their partner's phone, and 9% have used smart home features to monitor their partner without their consent.

How do people react to stalkerware?

There is a clear divide in responses from people who are or suspect that they are under surveillance from stalkerware apps. This is unsurprising, as it reflects the huge variation in personal circumstances that people find themselves in when it comes to their level of stability and vulnerability, and the support networks they have available to them, alongside the broader context of cultural attitudes to abuse and behaviour within relationships.

Around half (50%) of people would investigate if they found a monitoring app on their device and confront the person who installed it. Most respondents to our survey (83%) would confront their partner if they found out a monitoring app was installed on their phone without their consent. However, standing up to a partner in this situation will only escalate the risk that a stalkerware victim faces, which is something experts from domestic abuse organizations strongly discourage. This highlights the work needed to train, educate, and support people around complex stalkerware concerns.



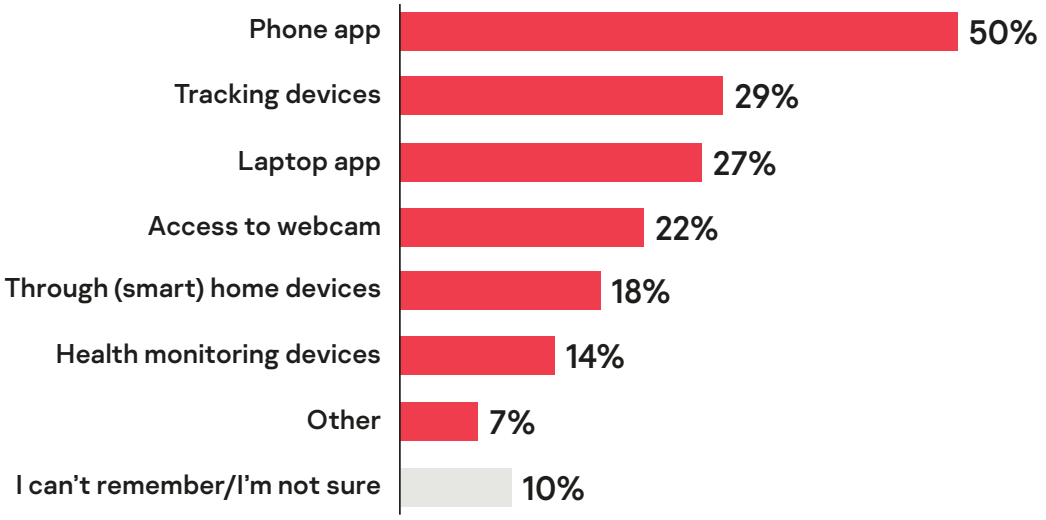
Only 17% of respondents would call a helpline or visit a support center in this situation. In Europe, the number is just 12%. This might be due to the low recognition of stalkerware as a real problem connected to intimate partner violence (IPV) or a lack of understanding about the kind of support these services can offer, among other possible reasons.

"Victims of domestic violence who confront their partner after finding stalkerware on their phone could escalate risk and leave themselves open to severe harm. The low number of respondents who would call a helpline or visit a support center is worrisome. In cases of coercive control by a partner, it is crucial to get support from victims' services, in order to proceed according to a safety plan developed with professionals," advises Berta Vall Castelló from WWP EN.

Of the respondents who wouldn't confront their partner if they found a monitoring app on their smartphone, a quarter say this is because they think that discussing the situation wouldn't help (26%), that they'd have no way to prove their partner was responsible (24%), or that they would prefer another exit strategy (24%). These reasons are concerning and indicative of an unhealthy relationship, with a strong possibility of broader abusive patterns.

If one partner feels unable to discuss something that crosses a personal boundary with their significant other, it is likely they are fearful of the consequences of doing so. Even if they feel discussing it would make no difference, their relationship is clearly not one where their autonomy and preferences are valued. Preferring a different exit strategy is a recommended reaction, and certainly, a very sensible one where someone fears for their safety. But how exactly can they go about this?

By means of what technologies were you stalked?



"When stalkerware is used as part of domestic abuse or intimate partner violence it can indicate that the abuser is very controlling and worryingly it could be a sign that violence may get worse. I really urge anyone who is experiencing stalking—either in real life or through stalkerware—and who feels it would be unsafe or dangerous to confront their abuser, to reach out to a domestic abuse organisation to get advice and support," says Karen Bentley, CEO of WESNET and a technology safety expert. "The Safety Net project led by NNEDV in the US and WESNET in Australia also have online safety and privacy toolkits that have advice for survivors about technology abuse as part of domestic violence," she adds.

Unfollowing stalkerware – how can people protect themselves from digital surveillance?

The research findings show beyond doubt that stalkerware is an unpleasant and pernicious issue. So, what are the key indicators that your device may be being monitored? Although spying apps try to conceal themselves, most reveal their presence in one way or another. Mobile data running out quicker than expected or the battery dying similarly fast are two red flags. If you notice either problem, be on your guard and check which apps are consuming your phone's resources.

Equally, look at which apps are accessing your location. If you don't find anything on your Android phone, but you still suspect someone may be spying on you, check which apps have access to Accessibility (Settings -> Accessibility).

Accessibility lets apps snoop on other programs, alter settings and do lots of other things acting as the user. That makes its permission very useful to stalkerware. Accessibility is one of the most potentially dangerous permissions in Android – we'd recommend that you only give that kind of access to your antivirus utility and nothing else.

Protect your phone with a strong password that you never share with your partner, friends, or colleagues

Other detection methods involve using a cybersecurity solution for your mobile devices, such as Kaspersky Internet Security for Android or TinyCheck (under a service organization's supervision), as outlined here. If one of the above methods detects spyware on your smartphone, think twice before deleting it. The person who installed it will notice, and that could make things worse. Uninstalling the program also could erase evidence that you might need later.

As with all facets of security, take protective measures first. For example, if you're being tracked by a potentially violent partner, before doing anything with the stalkerware app, contact a help center for victims of domestic abuse (see here for more information).

In some cases, it's easier to replace your smartphone altogether and then make sure that no one can install spying apps on the new device. To ensure you do not become a victim of stalkerware, Kaspersky recommends the following advice:

- Protect your phone with a strong password that you never share with your partner, friends, or colleagues
- Change passwords for all of your accounts, and don't share them with anyone either
- Download apps only from official sources such as Google Play or the App Store
- Install a reliable security solution immediately, and scan the device regularly. However, this should only be done after the potential risk to the victim has been assessed as the perpetrator may notice the use of a cybersecurity solution.
- Do not rush to remove stalkerware if found on the device as the abuser may notice. It is very important to consider that the abuser may be a potential safety risk. In some cases, the person may escalate their abusive behaviours in response.
- Contact local authorities and service organizations supporting victims of domestic violence – for assistance and safety planning. A list of relevant organizations in several countries can be found on www.stopstalkerware.org.

For more information about spyware and how to deal with it, visit the Coalition Against Stalkerware, which brings together domestic abuse organizations and the security community to tackle the threat.

About the research

The survey was conducted among 21,055 people from 21 countries who currently are in a relationship or have been in a relationship in the past.

At an overall level, results are accurate to ± 0.7% at 95% confidence limits, assuming a result of 50%.

The interviews were conducted online by Sapio Research in September 2021 using an email invitation and an online survey.

SAPIO RESEARCH

Audience | Brand | Content Research

Digital Stalking in Relationships

Report

kaspersky BRING ON THE FUTURE