Everyone’s afraid of the internet

(and no one’s sure what to do about it)

Malwarebytes™

Introduction

There's no denying it: while the digital world and its constant evolution have brought significant benefits, it has also introduced a never-ending bevy of threats related to online safety and security. As technology has advanced, so have people's fear and anxiety of what risks they may experience as a result of their digital footprint. With new apps and technologies always emerging, it can feel daunting to figure out how to stay safe online—or if doing so is even possible.

The reality is the more we engage online, the more vulnerable we are to the very cybersecurity threats that worry people the most: compromised data, breached financial accounts, identity theft, exposure of personal information, and so much more. While there's no turning back on our digital world, it is possible to better safeguard our data and protect ourselves from threats.

In order to better understand people's attitudes and behaviors toward online safety and security, Malwarebytes commissioned an independent research study among people ages 13-77 in North America. We surveyed 1,000 internet users to dig deep into what they worry about when it comes to online security, what activities they typically engage in, and what measures they take to stay safe online.

While "everyone's afraid of the internet" may seem like an exaggerated statement, the research validates this fear and shows that our online behaviors (or lack thereof) are often at odds with ensuring our safety. It's clear through the research that there is a critical need for education on how to protect ourselves in an ever-evolving online world.

The internet needs more helpers—people who will listen to others in need, answer simple tech questions without judgment, and build products for everyone, teaching every user along the way. Malwarebytes promises to put those people in charge of crafting a better, safer internet.

- Oren Arar, VP of Consumer Privacy, Malwarebytes

8 things to know

Online fear is high

Everyone worries about online security threats, and nearly 80% say they are "very" concerned about the risks of being online. Only half feel confident in their ability to keep themselves safe. Financial and data breaches are people's top concerns.

Risky behaviors

People readily give up a host of private info online by engaging in activities such as using the same password across accounts (65%), sharing their birthdate on social media (59%), interacting with strangers (54%) and taking quizzes that reveal personal info (45%).

Cognitive dissonance

Despite high anxiety and the fact that 70% have experienced cybersecurity threats before, only a handful use cybersecurity tools, with the most dominant being antivirus at only 35%. In general, there's a serious disconnect between people's fears, their online behaviors, and their general lack of cybersecurity protection.

New tech, new fears

Generative AI and TikTok users aren't sure they can trust these relatively new players just yet. 69% of generative AI users and 63% of TikTok users are concerned their data might be misused or stolen.

A new kind of security

Gen Z's top online fear is having private details of their lives exposed, such as sexual orientation and mental health struggles (81% are concerned vs. 72% of older generations)—1 in 3 worry this can lead to bullying or physical harm.

Identity theft anxiety

Identity theft ranks as people's third biggest concern when it comes to online security, just behind fear of financial accounts and personal data being breached (both of which play into identity theft as well). 64% agree identity theft protection is important, but only 13% have it.

Spying for safety?

71% of parents monitor their kids online in some way—either by reading their texts/emails/DMs, tracking their location, or checking out their search history. 62% of partners do the same. Most parents (69%) say monitoring helps them keep their children safe, indicating monitoring is an important safety mechanism for some.

Feeling resigned

One in four feel there's no point in using cybersecurity tools given the vast number of threats, and 41% are unsure how cybersecurity tools can help protect them, highlighting a critical need for education.

1.

Nearly everyone agrees: the internet comes with a host of serious threats

Almost everyone (97%) is worried about cybersecurity threats (79% are “very” concerned), including everything from hackers accessing accounts to advertisers capitalizing on tracked behaviors. Financial breaches, personally identifying information (PII) being revealed, and identity theft/fraud rank as the top three biggest fears.

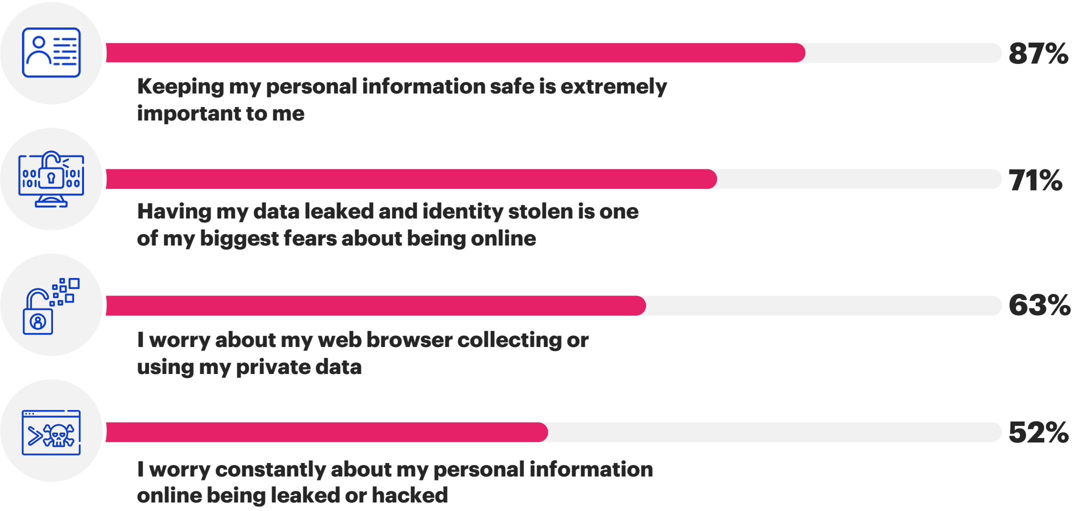
While there’s concern across the board about traditional cybersecurity threats, there’s an interesting privacy divide between Gen Z and older generations. Gen Z is unique in ranking their fear of private information being exposed (such as their mental health, sexual orientation, relationship issues) as their top online safety concern, highlighting a new way to think about online security. Gen Z worries that this information being revealed online could lead to real-world consequences, including the potential of physical harm, bullying, emotional damage, and ruined reputations.

Cybersecurity fears loom large for internet users

79% Say they are "very" concerned about online privacy and security risks, including everything from malware to embarrassing photos being leaked.

There is significant anxiety around private data being collected and breached

In a time where every aspect of our identity is increasingly shared online, safeguarding private data is top-of-mind for nearly everyone. The possibility of data leaks and identity theft are a major concern for most, and more than half find themselves worrying about it constantly.



87% Keeping my personal information safe is extremely important to me

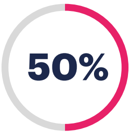
71% Having my data leaked and identity stolen is one of my biggest fears about being online

63% I worry about my web browser collecting or using my private data

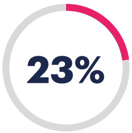
52% I worry constantly about my personal information online being leaked or hacked

Despite serious concerns, only half feel confident they know how to stay safe online

Few claim to be an expert when it comes to keeping themselves safe online, underscoring the need for better education.



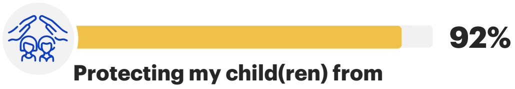
I have excellent online safety and privacy habits



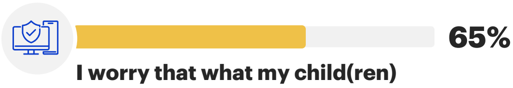
I would consider myself a cybersecurity pro

Parents of Gen Z are especially worried when it comes to their children's safety online

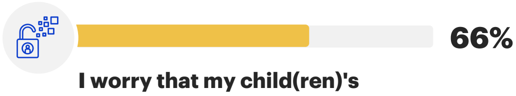
As parents of the first generation to grow up online, there's genuine concern that Gen Z's online activity could result in data breaches or identity theft. Parents agree: protecting their children's data is a top priority.



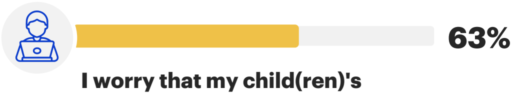
Protecting my child(ren) from having their personal information/data stolen is very important to me



I worry that what my child(ren) share online puts their safety at risk



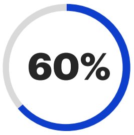
I worry that my child(ren)'s online behaviors may lead to identity theft someday



I worry that my child(ren)'s online behavior puts them at risk for getting their personal information stolen

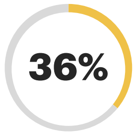
Most Gen Zers are confident they know best how to stay safe, though only 1 in 3 parents agree

Gen Z



I know more about online safety and security than my parents do

Parents of Gen Z



My child(ren) know more about online safety and security than I do

Three in four parents feel they need better tools and education to keep kids safe online

While more than half of parents of Gen Z feel they know how to keep their children safe online, their overwhelming desire for more education speaks to how serious online security threats have become.

55% I'm confident I know how to keep my child(ren) safe and secure online

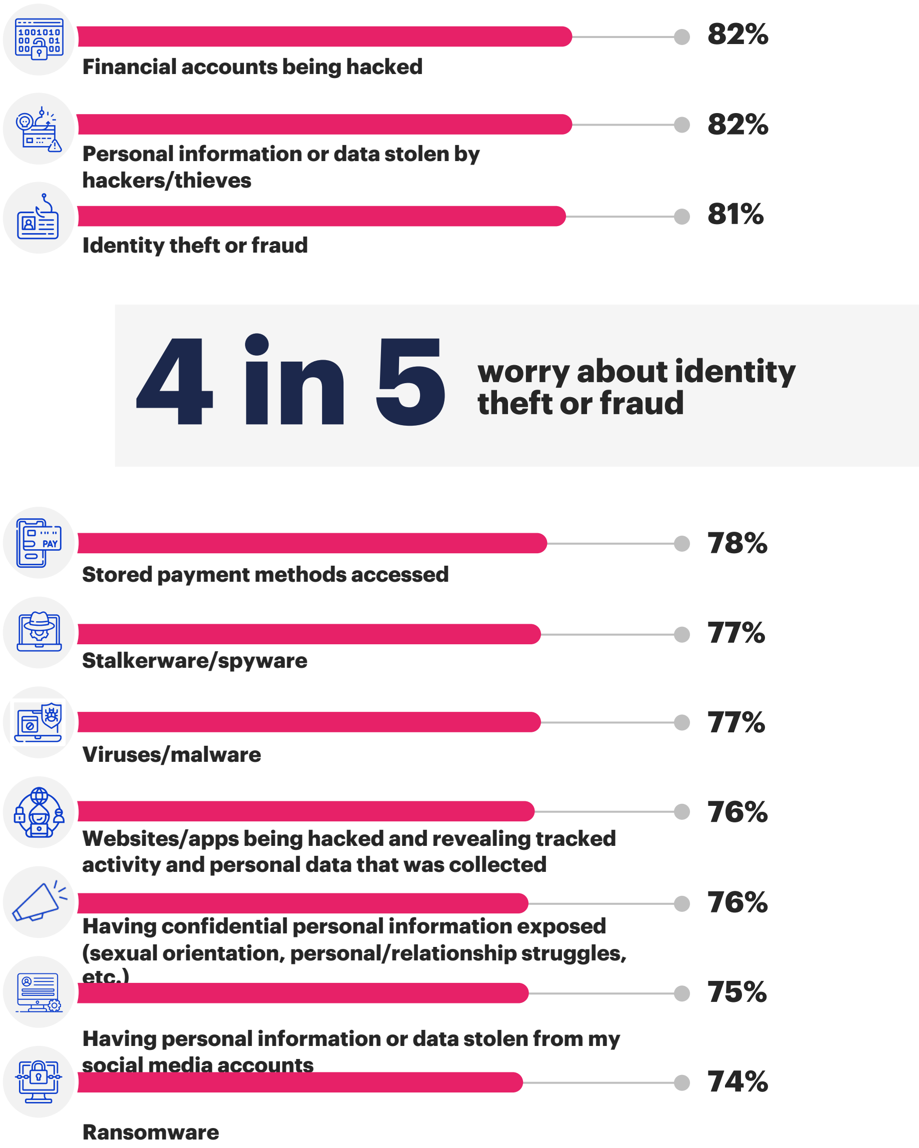
76% I wish there were more tools and education to help me keep my child(ren) safe online

Internet users strongly fear hackers and thieves will exploit their information

Almost everyone (80%+) worries about their financial and personal information and identity being compromised, but the full spectrum of cybersecurity threats evokes anxiety. Nearly as many worry about newer threats like behavioral tracking (76%) as they do about traditional threats like viruses and malware (77%).

Top 10 online safety concerns

> **“**
>
> **My biggest concern is that the activity in my phone or online will give someone the information they need to steal my identity.**
>
> **- Millennial survey respondent**

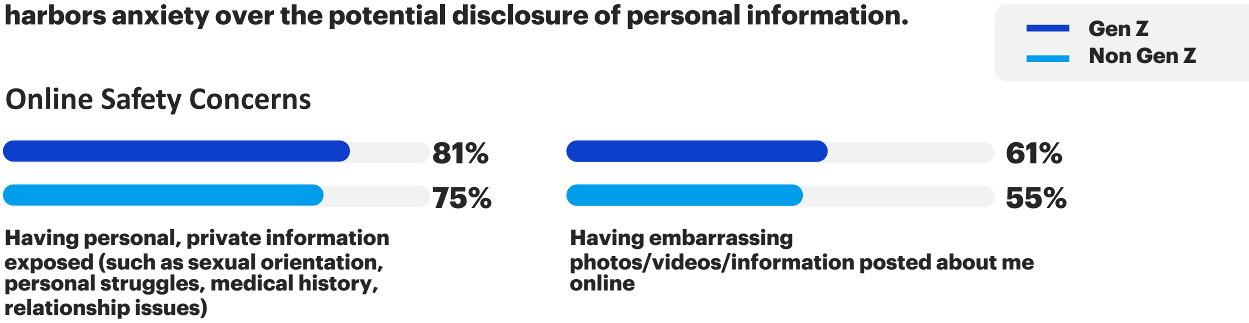


4 in 5 worry about identity theft or fraud

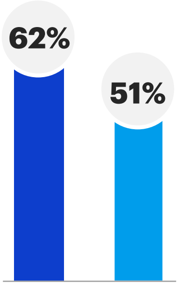
Gen Z worries most about personal, confidential info being exposed

For Gen Z, having confidential information about their lives revealed ranks as their top concern when it comes to online security. As the generation who has had the unique ability to share their lives online from a young age, it's no surprise Gen Z harbors anxiety over the potential disclosure of personal information.

Online Safety Concerns



Gen Z admits they're more anxious about private info being exposed than they are about traditional cybersecurity threats



Agree with the statement: I am more worried about my private information being exposed online (like embarrassing/compromising photos/videos, mental health, sexuality) than I am about typical cybersecurity threats (like viruses, malware)

Cybersecurity fears spur real world concerns for Gen Z

Gen Z is significantly more likely than older generations to worry that their private information being exposed online could lead to being bullied or physically harmed. Many Gen Zers (54%) also worry that breaches of confidential information could negatively impact their relationships with family and friends.

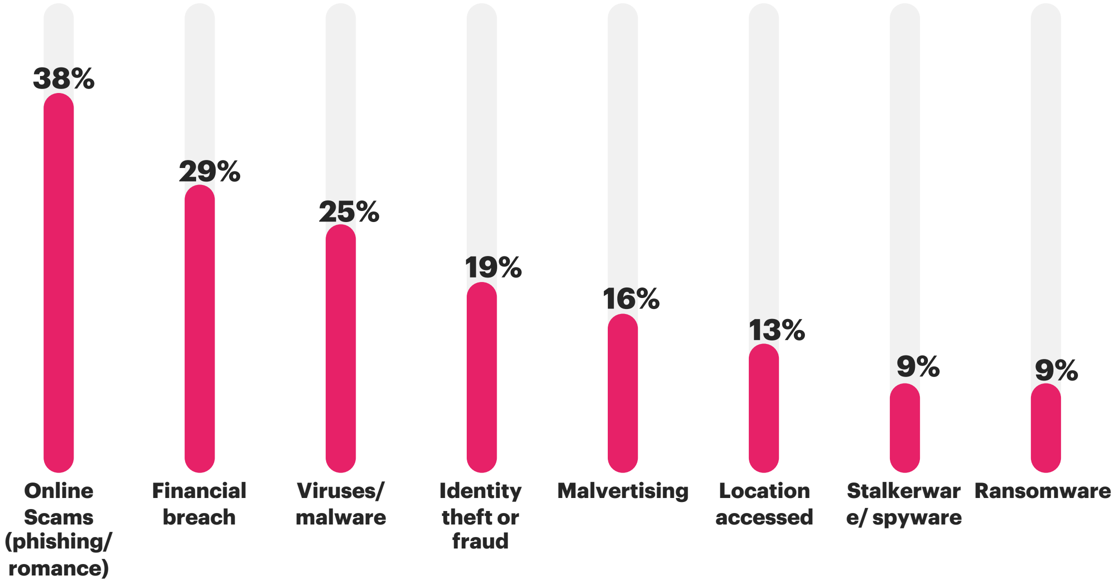
36% worry about being bullied (vs 22% non Gen Z)

34% worry about being physically harmed (vs 27% non Gen Z)

For many, cybersecurity concerns are grounded in actual experience

Nearly three in four people (70%) have experienced some kind of cybersecurity threat with the most dominant being online scams, financial breaches, and viruses/malware. Roughly one in ten have experienced serious, personal violations like their location being accessed, stalkerware/spyware, and ransomware.

Have experienced this...



Many—especially Gen Z—have also experienced emotional harm as a result of online behavior

More than one in three say they've been harmed emotionally as a result of something they or someone else did or posted online—for Gen Z, this number grows to 50%. This underscores the potential real-world consequences of people's confidential information being exposed and shows that Gen Z's fear of this happening is well-founded.

37%

Have experienced one or more of these:

- My confidence was hurt because of how I was portrayed
- People incorrectly assumed something about me
- I was stalked or bullied
- I lost a friend/someone important to me
- Worsening of mental health

2.

There's a disconnect between people's online fears and their behaviors

There's a high degree of cognitive dissonance when it comes to online safety and security. People worry significantly about privacy and security threats, but we all engage in online behaviors that could compromise our data and personal information. Gen Z is especially lax despite their very real concern that the details of their personal lives could one day be exposed online. Everyone frets about what could happen, but very few use cybersecurity tools that could help protect them from their biggest fears.

Nowhere is this more obvious than when talking about identity theft and fraud. While this is one of the biggest fears for many (81% worry about it happening to them), identity theft protection is among the least used cybersecurity tools, indicating a strong need for further education.

Most engage in online behavior that could unknowingly expose them to security risks

While online fears are high, the reality is that for many of us, our lives are inextricably linked to the digital world. However, even typical online behavior can leave people vulnerable to cybersecurity threats.

Many people inadvertently share critical information that dangerous actors could capitalize on, such as birthdates (59%), password hints (52% participate in online quizzes which can sometimes reveal password hints), email addresses (48% participate in online giveaways that require personal info like an email address), and clues about their home and personal lives (72% share photos/videos, 57% have personal information stored). While this behavior is simply part of normal digital life, it highlights how we leave an extensive trail of digital breadcrumbs that potential attackers could exploit. The need for online protection and cybersecurity education has never been greater.

Top 10 online behaviors that could pose a cybersecurity risk

72%
Share photos/videos on social media

65%
Use the same password or a few passwords across accounts

62%
Fill out applications online that require personal information

59%
Share my birthday online

57%
Have personal information stored on websites

54%
Have followers I don't know/message with people I don't know

52%
Participate in online quizzes (e.g., favorite animal/sports team/etc., which movie/show/book character am I?)

51%
Have my credit card(s) stored on websites for purchases

50%
Use public Wi-Fi networks without a VPN

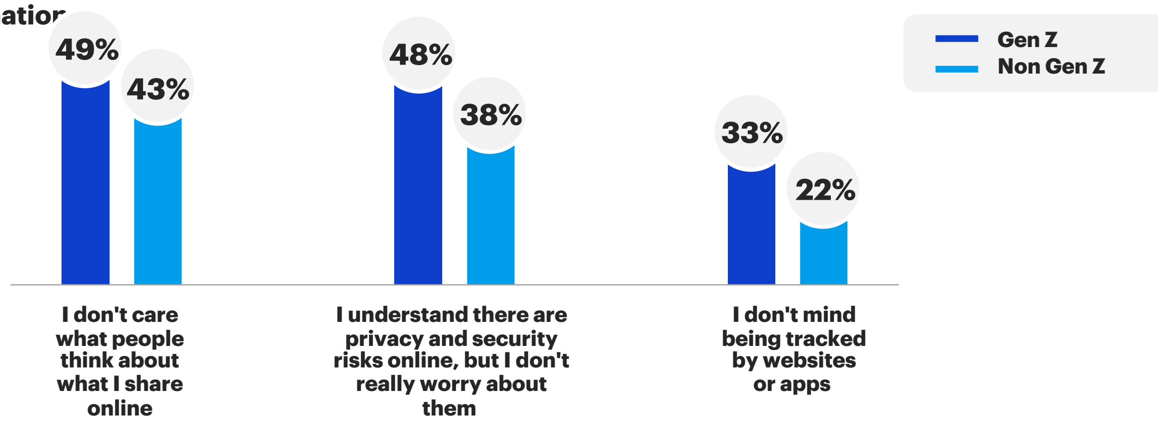
48%
Participate in online giveaways, freebies, etc. that require some sort of personal information like an email address

45%
Share personal information about my child(ren) on social media (e.g., graduation, dances, sports, etc.)

65% **Use the same or a few passwords across their online accounts, representing a major security threat**

Gen Z is especially carefree about how they engage online

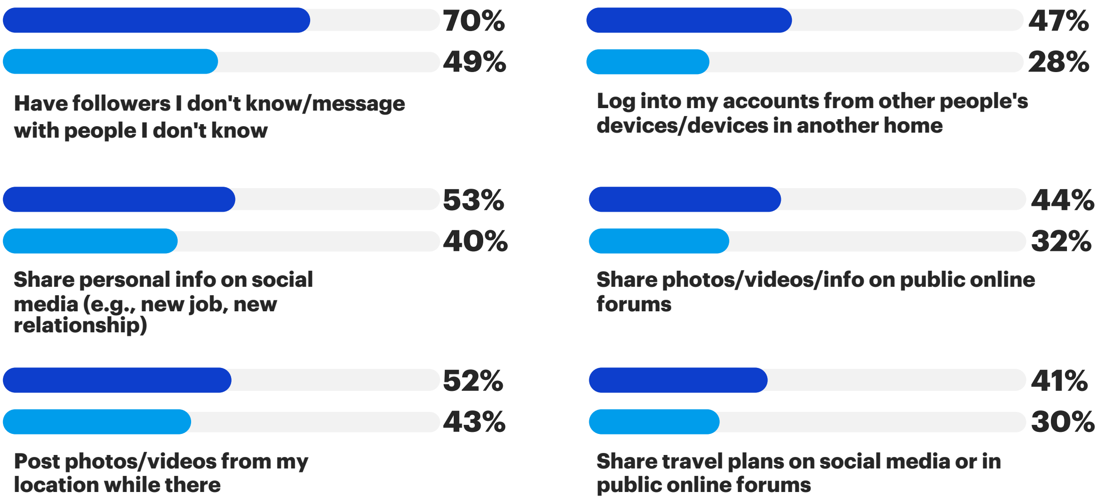
Counter to their concern that the details of their personal lives could be exposed online, almost half of Gen Zers claim they aren't overly worried about online privacy and security risks, highlighting a potential lack of understanding around how their online behavior may leave them susceptible to breaches of private information



Gen Z's relaxed attitudes are reflected in their willingness to be more open online

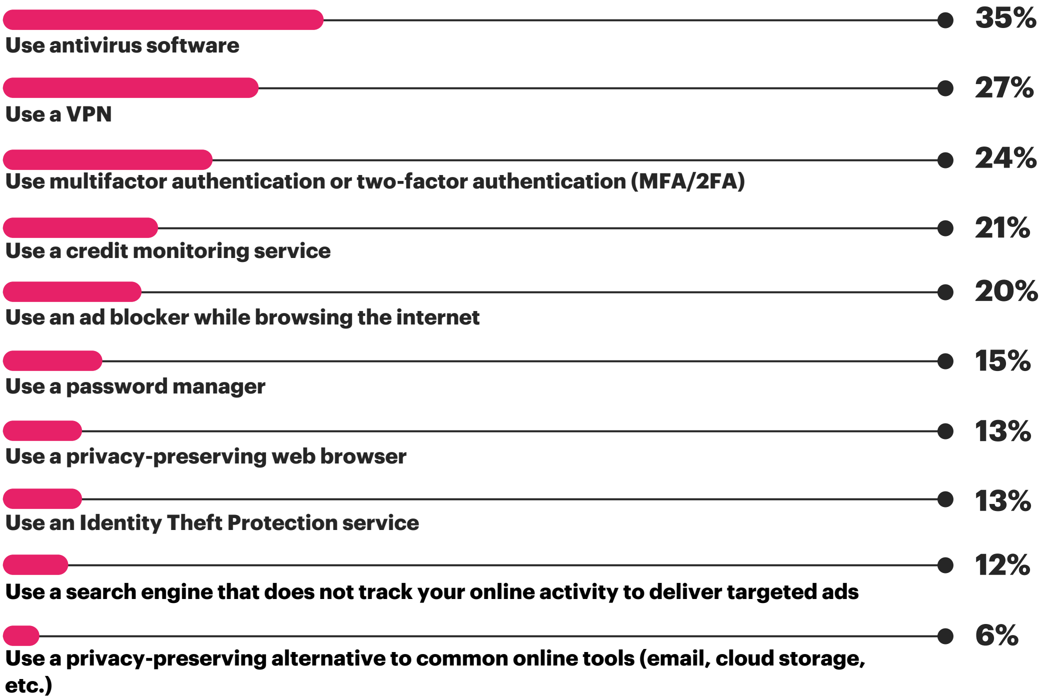
Gen Zers are even more open than older generations when it comes to what they do and share online. They are significantly more likely to interact with strangers and share details of their personal lives such as life updates, real time photos/videos of their whereabouts, and travel plans. Gen Z's large digital footprint, coupled with their laidback attitudes and behaviors, may make them more vulnerable to cybersecurity threats.

Online behaviors that could pose a cybersecurity risk



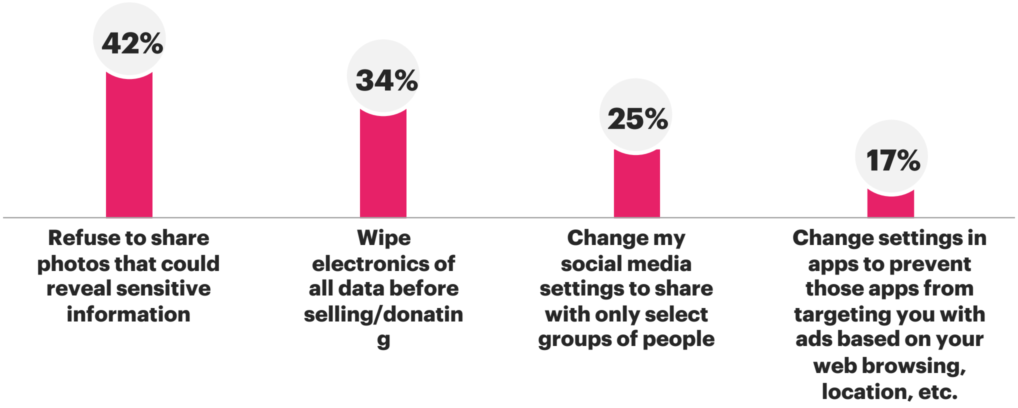
Very few are using cybersecurity tools and products that can help mitigate their fears

While people have serious cybersecurity concerns, very few actually use common cybersecurity tools, reflecting a disconnect between people’s fearful attitudes, relaxed online behaviors, and lack of cybersecurity protection.



Even basic self-directed steps are often ignored

Relatively few take important precautionary measures to safeguard their data. Less than half refuse to share photos that may contain sensitive information, and even fewer take precautions such as wiping electronics, adjusting social media settings, and saying no to app tracking.



The disparity in online attitudes and behavior is most evident when it comes to identity theft

Fear of identity theft is rampant—as are the online behaviors that can lead to it. Yet, despite people voicing their anxiety, very few opt for identity theft protection services. This highlights a major vulnerability in how people engage online.

81%

worry that identity theft or fraud could happen to them

71%

say having their data leaked and identity stolen is one of their biggest fears

64%

think identity theft protection is one of the most important cybersecurity tools available

only 13%

Use an identity theft protection service

People admit that while they're afraid of their identity being stolen, they aren't proactive in protecting themselves

> Identity theft is very scary and it's a real problem. It's possible to protect yourself from it but being actively online makes it more possible [to experience identity theft]. I don't actively protect myself which is also a part of my concern.
>
> - Gen Z Adult Survey Respondent

> I think it is possible to protect yourself against identity theft because with how far technology has come there are hundreds of different programs to help protect your identity. Currently, I am not really doing anything to protect myself.
>
> - Gen Z Adult Survey Respondent

> I am worried about identity theft period and I'm not sure how much you can protect yourself from it.
>
> - Gen X Survey Respondent

3.

Spying for safety?

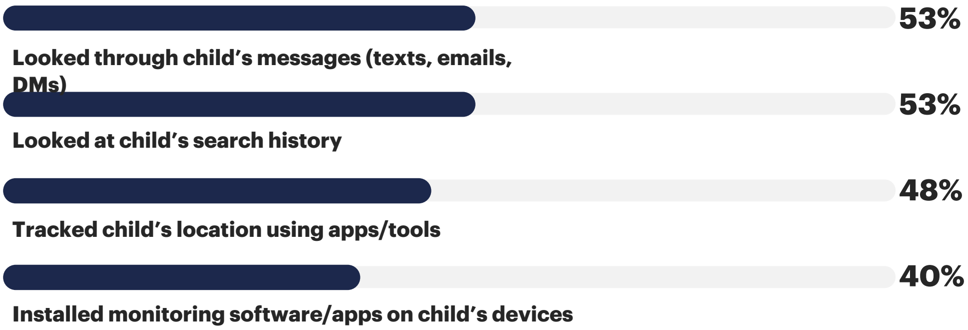
Online monitoring activities such as GPS tracking, reading texts, checking search histories, and using monitoring apps have become commonplace for many families. And it's not just parents monitoring their children—it's also spouses and partners monitoring one another. While many partners and parents do monitor offline as well, the numbers are lower at a statistically significant level, highlighting the fear that surrounds what people are up to online.

For parents, monitoring offers comfort that they're doing what they can to keep their children safe, and for many, doing so allows them to give their kids more independence. Even so, people are generally divided on whether monitoring is an invasion of privacy. Regardless, the subject of monitoring offers a unique take on the question of how to stay safe online.

Online monitoring is commonplace for many families

84% of parents agree it's their right to monitor their children's online activities. Parents who monitor say doing so makes them feel they're keeping their kids safe (69%) and for two in three, monitoring is a way of giving their children more freedom. That said, nearly half of parents (47%) agree monitoring tools/apps are an invasion of privacy.

71% of parents have monitored their kids online

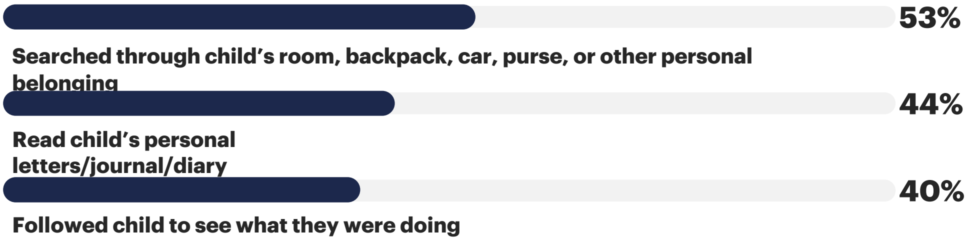


51% of parents monitor their kids online without their children's permission

Many parents also monitor their kids offline

While roughly two in three parents also monitor their children offline, significantly fewer do so compared to online monitoring. This discrepancy like reflects parental fear of the internet as well as the wealth of options available for easy online monitoring. Interestingly, there are conflicting standards around when it's okay to monitor. For example, significantly fewer parents read their children's personal letters/journal (44%) versus read their texts, emails, or DMs (53%).

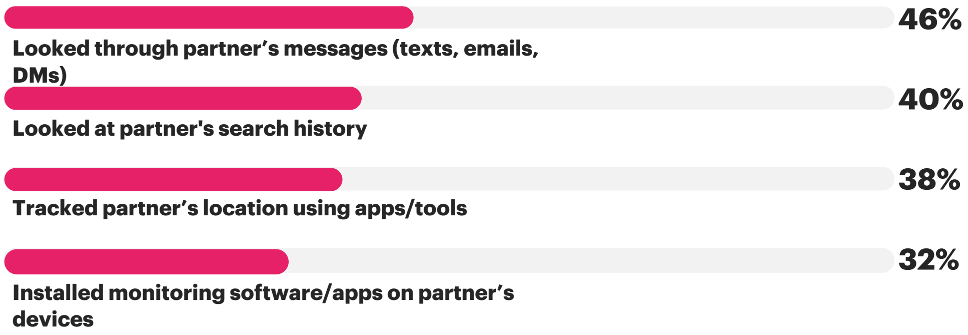
67% of parents monitor their children offline



Partners monitor as well, though their reasons appear less virtuous

Despite many people monitoring their partners, only 38% actually agree it's okay to do so. And unlike with parents, only about half of partners who monitor do so for safety reasons, indicating trust issues are likely a factor as well.

62% monitor their partners online

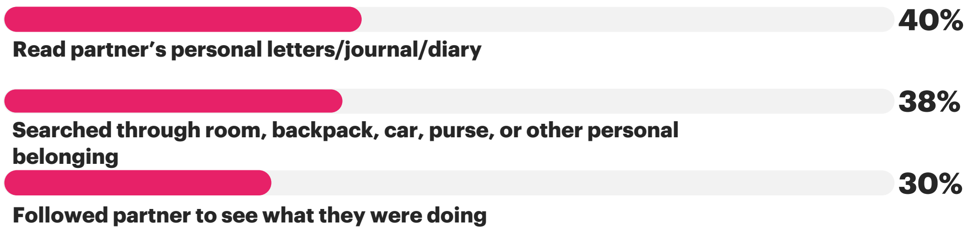


41% Monitor their partner **without permission**

Half also monitor their partners offline

Compared to monitoring online, significantly fewer are monitoring their partners in the real world.

50% monitor their partners offline



4.

Looking ahead: New tech brings new fears—and the need for education

Though usage of TikTok and generative AI continues to grow (especially among Gen Z), even users of these newer technologies feel somewhat wary of them when it comes to security concerns. There's some clear skepticism in how TikTok and generative AI handle personal data, and many feel they could be an easy gateway for thieves to steal data.

As new technologies emerge and evolve, new cybersecurity fears come to light, only further emphasizing the need for better education around online safety. This also reinforces the importance of adopting better cybersecurity practices as too many seem to be unaware of how cybersecurity tools can help keep them safe.

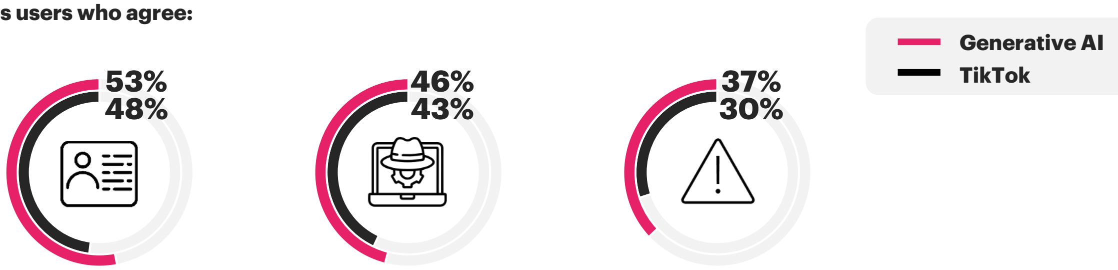
TikTok and generative AI bring heightened concerns around online security

A majority of TikTok and generative AI users worry that the app and technology could misuse their data or open them up to data theft. In terms of TikTok specifically, 47% use the app with a public account, which can leave users more vulnerable to having their personal information exposed or misused.

69% of generative AI users feel the technology poses some kind of security risk

63% of TikTok users feel the app poses some kind of security risk

This includes users who agree:



Worry about how much personal data this collects and how they might use it

Seems like an easy way for thieves to gain access to personal information/data

Is a personal security threat

Many generative AI users feed the technology critical personal information

Despite feeling somewhat wary of the technology, many provide generative AI with information like sensitive work info, personally identifying information, and personal plans. While popular generative AI platforms like ChatGPT promise to safeguard personal data, this speaks to people's willingness to part with personal or sensitive details.

50% Have used generative AI for work tasks or with sensitive work information

43% Have given generative AI personal data or used it for personal planning

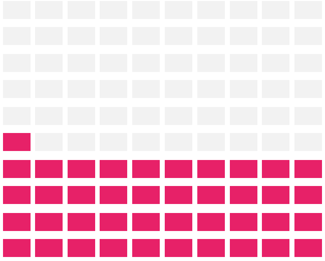
40% Have used generative AI for school to help with assignments or to complete an assignment

1 in 5

Gen Zers admit they've used generative AI to cheat on a school assignment

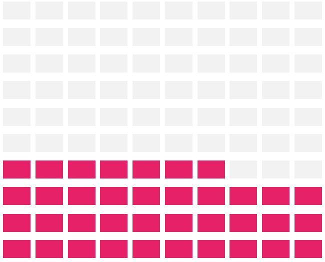
Many people need a better understanding of how to protect themselves online—and how cybersecurity tools can help

Nearly half admit they don’t fully understand how cybersecurity products can help keep them safe, while one in four see no point in using cybersecurity products given the sheer volume of existing threats. And, despite cybersecurity tools evolving alongside the internet, one in three still think cybersecurity products only address viruses and malware. Overall, there is a clear need for comprehensive education around online threats and how to counteract them, both in terms of adjusting online behaviors and in using proactive, protective cybersecurity tools.



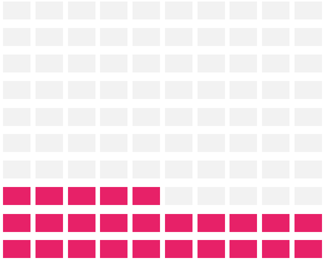
41%

I don't fully understand how different cybersecurity products can protect me



37%

Cybersecurity products only really help with things like viruses and malware



25%

There's no point in using cybersecurity products since there are too many online threats

Marcin Kleczynski
CEO, Malwarebytes

> **The lesson that most people have learned online is that the internet cannot be trusted, and, yes, the internet did give my family computer its first virus. But the internet also connected me with the very people who helped me fix it.**
>
> **This research should serve as a teaching moment. Too few people use antivirus, two-factor authentication, and password managers, but not because they don’t know the risks. It’s because they don’t know how to act against them. Malwarebytes is committed to empowering people to understand that just because the internet cannot be trusted, doesn’t mean we can give up.**

Methodology:

Malwarebytes conducted this research using an online survey prepared by an independent research contractor and distributed via Forsta among n=1,004 survey respondents ages 13-77 with n=759 from the United States and n=245 from Canada. The sample was equally split for gender with a spread of ages, geographical regions, and race groups. Data was collected from July 25 to August 3, 2023.

About Malwarebytes:

Malwarebytes believes that when people and organizations are free from threats, they are free to thrive. Founded in 2008, Malwarebytes CEO Marcin Kleczynski had one mission: to rid the world of malware. Today, Malwarebytes' award-winning endpoint protection, privacy and threat prevention solutions along with a world-class team of threat researchers protect millions of individuals and thousands of businesses across the globe daily. Malwarebytes solutions are consistently recognized by independent tests including MRG Effitas, AVLAB and AV-TEST. The company is headquartered in California with offices in Europe and Asia. For more information and career opportunities, visit https://www.malwarebytes.com.