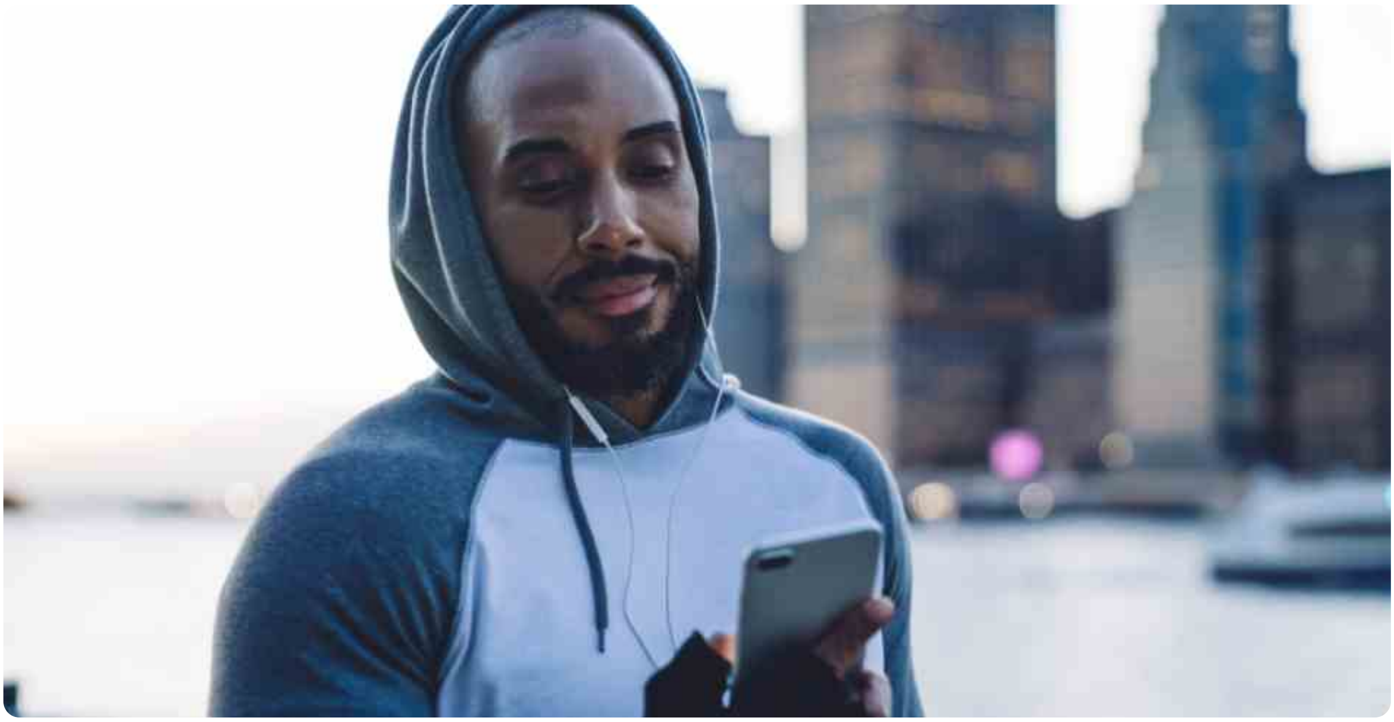


Demographics of Cybercrime Report

This is a story of inequality online. It is a story of women feeling dramatically less safe and less private on the Internet than men. It is a story of how Black people, Indigenous populations, and all people of color see some of the barriers they already face in the physical world transposed into cyberspace. It is a story of how money (or its absence) changes our sense of safety, and how education can prepare some for a safer, more private experience online.

> “This is the story of how cybercrime hurts some groups more than others, and how, while making the Internet essential for all, we only made it safe for some.“

Overall, 50 percent of people say they do not feel private online, and 31 percent do not feel safe online. Using the Internet has become less and less optional for everyday living and more and more a requirement. If these types of sentiments on safety and privacy applied to, say, walking on the sidewalk or driving to work, they would rightfully cause a collective moment of reflection: How can we accept this level of uncertainty? Why do we continue to make people do things they are clearly uncomfortable doing?

Think about it. Applying for a job, filing taxes, purchasing groceries, scheduling a doctor's appointment, checking bank accounts, even voicing concerns to government representatives—all of it, today, can and does happen online. And all of it, today, often requires the transfer of sensitive information like names, addresses, and credit card numbers.

People everywhere, no matter their gender, race, income level, education, or age, deserve to feel safe and private online.

Why then, do they not?

The answers are complex and overlapping, as revealed in this report, "The Demographics of Cybercrime," presented by Malwarebytes in partnership with Digitunity, a nationally recognized non-profit dedicated to eliminating the technology gap, and Cybercrime Support Network, whose non-profit mission is to serve individuals and small businesses impacted by cybercrime throughout the country.

By polling 5,000 people across the United States, the United Kingdom, and Germany, our report shows that not only do some populations face more types of cybercrime than others, and more frequently, but that some populations feel more emotionally burdened and are more likely to financially suffer. When coupled with the fact that some populations face targeted cybercrime events in ways that other populations do not, the trend becomes clear:

Not everyone's online experience is the same, and therefore, not everyone's feelings about the Internet are the same.

For example, women whose social media accounts get hacked are more likely than men to have that hack result in someone sending suspicious messages to friends and family (48 percent compared to 43 percent). Black people, Indigenous people, and People of Color (BIPOC) are more likely to have their identities stolen than White people (21 percent compared to 15 percent), and BIPOC people are the least likely to avoid any financial impact due to cybercrime (47 percent compared to 59 percent of all respondents). And for high-income earners, it isn't necessarily that the Internet is a safer place, it is merely that the Internet's threats have less impact. Despite high-income respondents actually losing more money in cyberattacks, they were less likely to experience a "substantial increase" in stress as a result (13 percent of high-income respondents compared to 18 percent of low-income respondents).

Lastly, it is impossible to ignore people's familiarity and use of cybersecurity tools like antivirus products, VPNs, and password managers. While those who use such products did show greater trust in their safety and privacy online, there were still a shocking number of people who did not know enough about these products. In fact, 21 percent of all respondents were neither "familiar" or "very familiar" with antivirus tools.

The fact that more than one fifth of the population lacks a strong or comfortable familiarity with the tool most likely to help combat the broadest range of cyberthreats is unacceptable, and it's on the cybersecurity community to fix it.

Key takeaways from the report:

- ✓ Not a single person in our survey avoided any suspicious online activity, no matter their gender, race, age, income, or education level
- ✓ 50 percent of people do not feel private online
- ✓ Globally, women feel the least private online (53 percent compared to 47 percent of men)
- ✓ 31 percent of people do not feel safe online
- ✓ Globally, women also feel the least safe online (35 percent compared to 27 percent of men)
- ✓ 21 percent of all respondents were neither “familiar” or “very familiar” with antivirus products
- ✓ 10 percent of those who use antivirus do not know what it protects them from
- ✓ 46 percent of women said they had their social media accounts hacked, compared to 37 percent of men
- ✓ 16 percent of women who had their identities stolen said the likely cause was an earlier theft of their purse or wallet—twice the rate of men.
- ✓ BIPOC people had the lowest rate of successfully avoiding any financial impact due to cybercrime. Only 47 percent of BIPOC respondents avoided any financial impact compared to 59 percent of all respondents.
- ✓ 21 percent of women and 23 percent of BIPOC respondents said they experienced “substantial” stress in dealing with online suspicious activity, compared to 17 percent of all respondents

Safety and privacy

Though not enough people, overall, believe that the Internet is either a safe or private place to spend their time, women, BIPOC, and younger generations showed even lower rates of feeling safe or private online.

Perhaps unsurprisingly, women feel dramatically less secure than men, with only 37 percent of women saying they feel "somewhat" safe and "very" safe online as opposed to men (49 percent). Similarly, only 26 percent of women feel like their information is private online, a large drop from men, of whom 32 percent feel the same way.

37%

of women feel safe

49%

of men feel safe

26%

of women feel their information is private

32%

of men feel their information is private

The reasons for this could be many, but when looking strictly at the data, more women suffered from some types of suspicious online activity than men. Not only that, the impacts of these suspicious online activities were also different based on gender.

When we asked individuals what kind of suspicious activity they have experienced in the past, most said they received text messages from unknown numbers instructing them to click on links (76 percent). People also said they clicked on phishing scams (43 percent), had social media accounts hacked (42 percent), had their credit card information stolen (29 percent), had their identity stolen (17 percent), and were attacked by ransomware (16 percent).

76%

Of all respondents received text messages from unknown numbers instructing them to click on links

43%

Clicked on phishing scams

42%

Had their social media accounts hacked

29%

Had their credit card information stolen

16%

Were attacked by ransomware

Women, it turns out, did experience several of these threats at significantly higher rates than men, as 79 percent of women said they received text messages from unknown numbers trying to get them to click on links, as opposed to 73 percent of men. Further, 46 percent of women reported having social media accounts hacked in comparison to only 37 percent of men.

Interestingly, not every single suspicious online activity that we asked about affected more women than men. Women were slightly more likely to experience online suspicious activity in the past three months than men (33 percent compared to 30 percent), women were more likely to receive multiple suspicious text messages than men (84 percent compared to 81 percent), and though both women and men had their identities and credit card information stolen at similar rates, women were twice as likely to say they had their identity stolen through a real-life attack: Having their purse or wallet stolen first.

Again, we see the blurring between a person’s real-life lived experiences and their experiences online. The two worlds are no longer separate, and what happens in one area directly affects the other. And what happens online for women can be frightening.

Women are more frequently the victims of nonconsensual pornography (sometimes called "revenge porn"), according to the Cyber Civil Rights Initiative. Women are more likely to be the targets of "deepfake" nonconsensual pornography, too, according to data released in 2019. And women are also more likely to be victimized by stalking behavior, according to the US Department of Justice, which found during a 12-month study released in 2009 that 20 out of every 1,000 women aged 18 and up were victimized by stalking compared to 7 out of every 1,000 men. Further, 26 percent of those who said they were stalked also said that at least one form of cyberstalking was used. In 2016, the Department of Justice found that more people reported experiencing "stalking with technology only" than those who reported experiencing "traditional stalking only."

"Again, we see a blurring between a person's real-life lived experiences and their experiences online. The two worlds are no longer separate."

All of these problems share an overlap between both privacy and safety, showing that, for some cybercrimes, an invasion of privacy is also an invasion into a sense of security. But these problems also show that, for women in particular, online threats can overlap into other parts of their lives too—they can come from real life experiences and carry over into real life experiences after the fact. Nonconsensual pornography, for example, can threaten relationships, harm career chances, and, if posted with a real name and corresponding contact information—as is sometimes the case, according to a 2014 report by Danielle Keats Citron and Mary Anne Franks—even lead to physical confrontations from strangers.

Though women showed the most dramatic differences in feeling safe and private online compared to men, BIPOC respondents also showed a lower feeling of safety than White respondents.

Broadly, BIPOC respondents feel less secure than White individuals, with 38 percent of BIPOC users stating they feel "very safe online" and "somewhat safe online," as opposed to 44 percent of White users. (Interestingly, White and BIPOC consumers feel similar about their own privacy, with 29 percent of White consumers and 28 percent of BIPOC consumers believing their information is private online.)

To understand these feelings, we again looked at our data and found, once again, that some —but not all—types of online suspicious activity affected BIPOC respondents more. For instance, 45 percent of BIPOC consumers had their social media accounts hacked, as opposed to 40 percent of White consumers, and more BIPOC consumers said they had their identities stolen (21 percent) than White consumers (15 percent). The impacts of these attacks for BIPOC respondents, and possibly what caused them, also diverge from the answers of White respondents.

For example, though BIPOC respondents were less likely to have their credit card information stolen than White respondents (29 percent compared to 33 percent), BIPOC respondents were far more likely to say that their credit card information was likely stolen because of a physical attack, just like women; 14 percent said their credit card information was likely stolen because their wallet or purse was stolen beforehand, compared to 8 percent of White respondents who said the same.

> **“BIPOC respondents showed a lower feeling of safety than White respondents.”**

BIPOC respondents also said they were more likely to encounter a link sent through a text message that asked for financial information or compensation (17 percent compared to 12 percent for White respondents). This is no surprise. In fact, online scams have long taken advantage of breaking news events as a way to trick individuals into donating money to a cause that might personally affect them. Shortly after the World Health Organization declared a pandemic due to Covid-19, countless phishing emails asked for donations to bogus charities and hospitals. Likewise, after the murder of George Floyd by police in the United States, multiple scam websites asked for donations to fraudulent nonprofits, claiming alignment with the Black Lives Matter movement.

Separately, according to a survey performed by the Pew Research Center in 2017, 1 in 4 Black Americans faced online harassment due to their race or ethnicity, and notably, the survey found that “nearly six-in-ten [Black] internet users (59 percent) say they have experienced any form of online harassment compared with 41 percent of [White Internet users] and 48 percent of Hispanics.”

Though our survey did not specifically address online harassment, the external data cannot be ignored—minority communities are suffering different experiences online, and this is likely influencing their feelings of safety and privacy when using the Internet.

Interestingly, such influences were already measured by the Pew Research Center. According to its survey, “after witnessing online harassment… 43 percent of [Black] Internet users and 44 percent of Hispanics have felt anxious that something similar might happen to them, compared with 33 percent of [White] Internet users."

A separate survey on online harassment released this year by the Anti-Defamation League also showed a large spike in reported online harassment against Asian-Americans. According to the survey, "in a year of coronavirus-related bigotry and surging physical attacks, the biggest jump in severe harassment was reported by Asian-Americans, at 17 percent, compared to 11 percent reported a year ago."

Finally, younger generations feel less private than older generations with only 26 percent of 18 – 34-year-olds believing their information is confidential online, as opposed to the older generations (35 – 65+ years of age). But no matter how old they are, most people still feel cautious and unsafe when online, with younger ages (18 – 34-year-olds) feeling less safe than older generations (35 – 65+ years old).

Already, it's easy to see why these trends in age groups might emerge. Younger generations have vastly different experiences online than older generations. Today's teenagers are the first generation to be fully raised with an advanced, consumer-ready Internet experience. They use multiple social media platforms. Their high school and college experiences follow them from the classroom to the smartphone, documented on video, shared on TikTok, commented on at all hours.

Younger generations are also the first generation to, at their age, learn about the privacy failures of the very same social media platforms that surround them. There was no time in most teenagers' lives when Facebook was private. There was no time, likewise, when the Internet was not the number one source of swiped identities and stolen credit card numbers.

Younger generations, like women and BIPOC, face different rates for different online suspicious activity. For starters, individuals who are 18 – 34 years of age were most likely to suffer any social media hack and ransomware as opposed to older generations (35 – 65+ years of age).

Younger generations were also the most likely to solve their Internet problems without any outside help. For all respondents who said they suffered a hack of their "email or other accounts (Netflix, Bank login, etc.)," younger generations contacted customer support the least (16 percent for those aged 18 – 24, compared to 38 percent for those aged 65+), and they deleted their account profiles the most, either to create a new profile to continue using the service (16 percent for those aged 18 – 24, compared to 7 percent for those aged 65+), or to simply stop using the service altogether (12 percent for those aged 18 – 24, compared to 5 percent for those aged 65+).

16%

Younger generations (aged 18 – 24) contacted customer support the least

38%

Compared to those aged 65+

This independence could be a function of their age. Raised with the Internet, perhaps younger generations better understand how to fix many problems of the Internet.

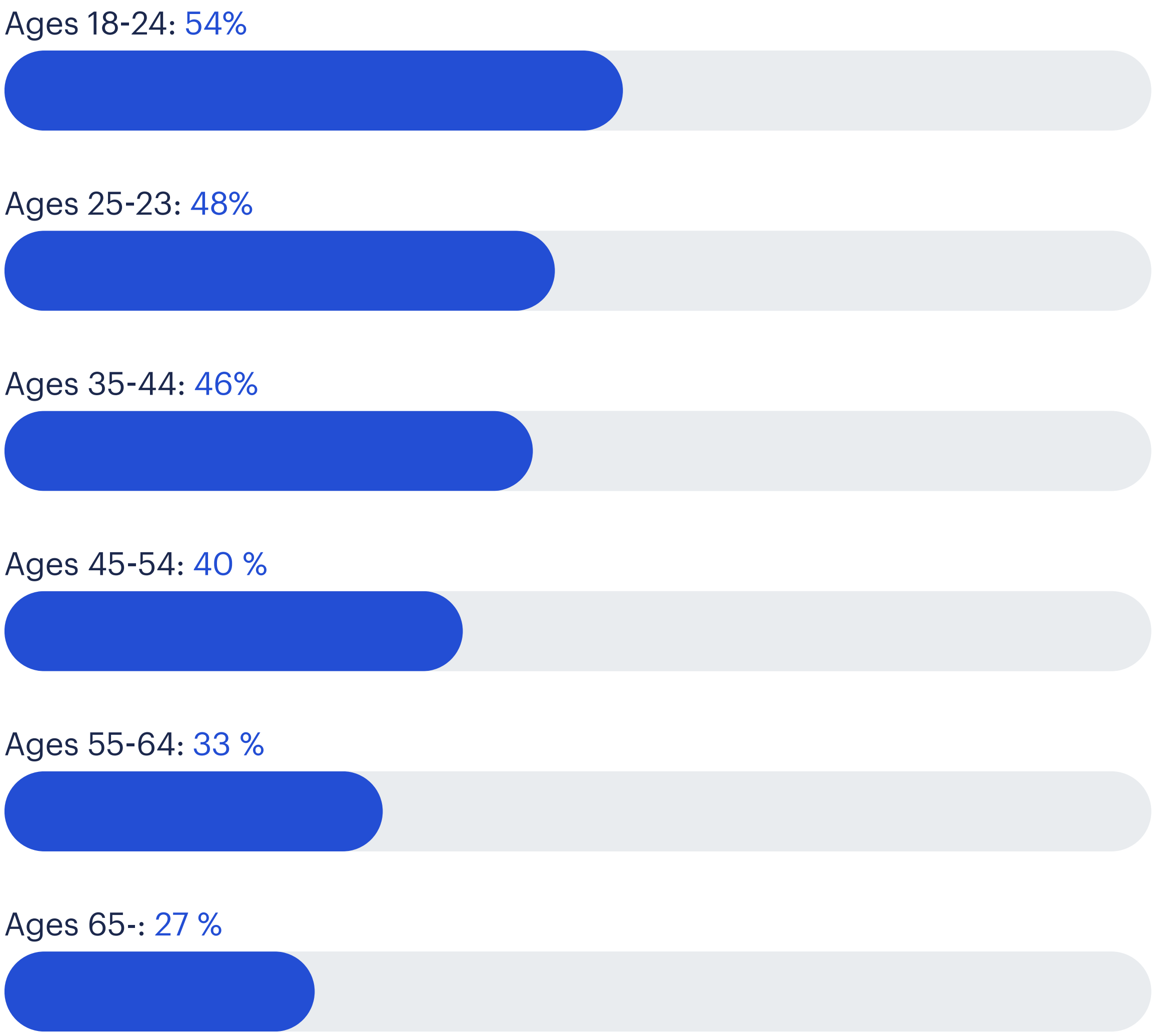
But, again, external data supports this finding. The National Cybersecurity Alliance's 2017 survey on parent and teen online safety showed that "in general, teens feel as though it is mostly their responsibility to keep themselves safe online. Among online teens, 62 percent say it is 'mostly my responsibility,' compared with 10 percent who feel it is mostly their parents' job to keep them safe."

That survey also found, like ours, that teens were quite concerned about online privacy. Teenagers said they were "very concerned" that "someone will access their accounts without their permission (41 percent), that someone will share personal information about them online that they prefer to keep private (39 percent), or that someone will post a private photo or video of them online (36 percent)."

So, if women do not feel safe or private online, and BIPOC respondents do not feel safe online, and teenagers do not feel particularly private, either, who, if anyone, is feeling as though they have at least a somewhat safe, private experience when using the Internet?

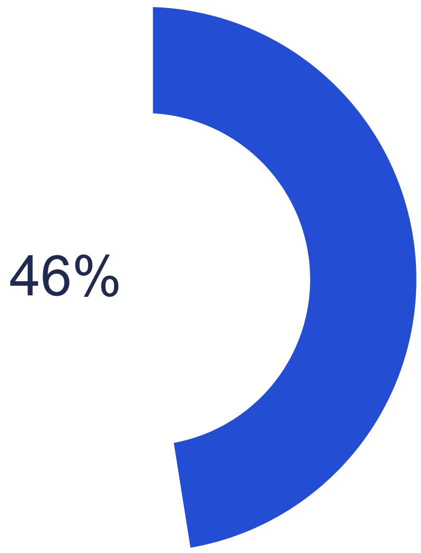
It turns out, people with more money and more education.

Age demographic: Hacked social media accounts

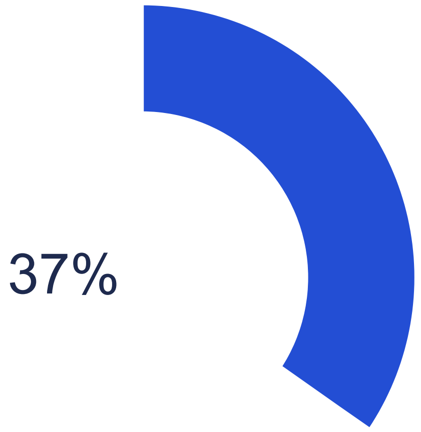


Gender demographic: Hacked social media accounts

Female



Male



Income, education, and defenses to stress

In the above section, we noted that women, BIPOC respondents, and respondents from younger generations all felt disparate impacts from the suspicious online activity they encountered. The end result was different, the cause was different, even the surrounding circumstances differed.

But one statistic distressed us the most: When answering whether or not they suffered any financial impact from an encounter with suspicious online activity, BIPOC respondents were the least likely, by far, to avoid a hit to their finances.

A staggeringly low 47 percent of BIPOC consumers said there was “no financial impact” from the suspicious online activity they encountered. This rate was lower than White respondents (59 percent), all men (60 percent), all women (56 percent), all age groups, and every broad income and education level.

This massive discrepancy also highlights another layer to the data, which is that, when it comes to feeling safe and private online, income and education matter deeply. Almost unique to every demographic analyzed, income levels tracked more closely to feelings of safety and privacy than any other variable.

Individuals with a higher income (51 percent) feel safer online than individuals with a lower income (40 percent), and the data shows a stairstep pattern between increased income and increased feelings of safety. The same pattern is true for education level and feelings of safety. Users who have the highest level of education feel more secure (48 percent) than those who completed only university or college (44 percent) or online high school or secondary school (40 percent).

As for privacy, similar, if weaker, trends emerged.

No longer present is the clear, linear path between income and safety. Instead, individuals only at the highest income level feel more private online, with 36 percent of high-income consumers considering their data is secure, compared to 29 percent of lower to middle-income consumers.

The same pattern happens with education levels; individuals with the highest-level education are the ones that feel most private online with their data (35 percent), as opposed to individuals with a college/university degree (28 percent) or only a high school or secondary school diploma (29 percent).

What is most interesting about this relationship, though, is that as income increased, so too did the likelihood of experiencing stolen credit card information (Lower income 26 percent; Medium income 30 percent; Higher income 36 percent). That's not all. As income increased, the likelihood of avoiding any financial impact caused by suspicious online activity instead decreased, meaning that, the more money an individual made, the more likely they would lose any amount of that money in a potential cyberattack.

The same trend is true for education. Though individuals who attained higher levels of education were more likely to say they felt safe online, they were also more likely to experience stolen credit card information (Diploma/High School/Secondary school 27 percent; College/University 28 percent; Higher education 36 percent).

17%

Of all respondents experienced a substantial increase in stress levels

When asked about stress level changes based on their experience with suspicious online activity, 17 percent of respondents stated that they experienced a substantial increase in stress levels.

Of the 17 percent who reported a substantial increase in stress levels, 21 percent of women felt substantially more stressed than men (13 percent), and 21 percent of BIPOC consumers felt substantially more stressed than White consumers (17 percent).

These numbers must be presented in the context of the relationship between income and education level and feelings of safety and privacy. Remember that as income and education increased, so too, did the likelihood that a respondent would face a financial impact. And remember that such an impact could actually mean more dollars lost—higher-income respondents said they lost a median of about $2,108, compared to lower-income respondents who lost about $1,311.

Understandably, though, people with a low-level income were significantly more stressed (18 percent) than those in high-level income circumstances (13 percent), even though they lost less money.

The unfortunate finding from this data points to one possible answer: The more money you make, the more comfortable you are online, even if you lose more of that money to an attack.

Money, it appears, plays an enormous role in feeling safe and private online.

But so does cybersecurity.

If you answered Yes to having a financial impact, “Approximately, how much money did you lose because of this experience?”

Total respondents, for reference:

$1,494

BIPOC:

$1,709

Women:

$1,338

(lower than men, $1,684.8)

Ages 18 – 24:
$879

Ages 25 – 34:
$1,648

Ages 35 – 44:
$2,096

Ages 45 – 54:
$1,739

Ages 55 – 64:
$1,309

Ages 65+:
$1,152

Income: Higher income, higher lost dollars

Lower income:
$1,311

Medium income:
$1,516

Higher income:

$2,109

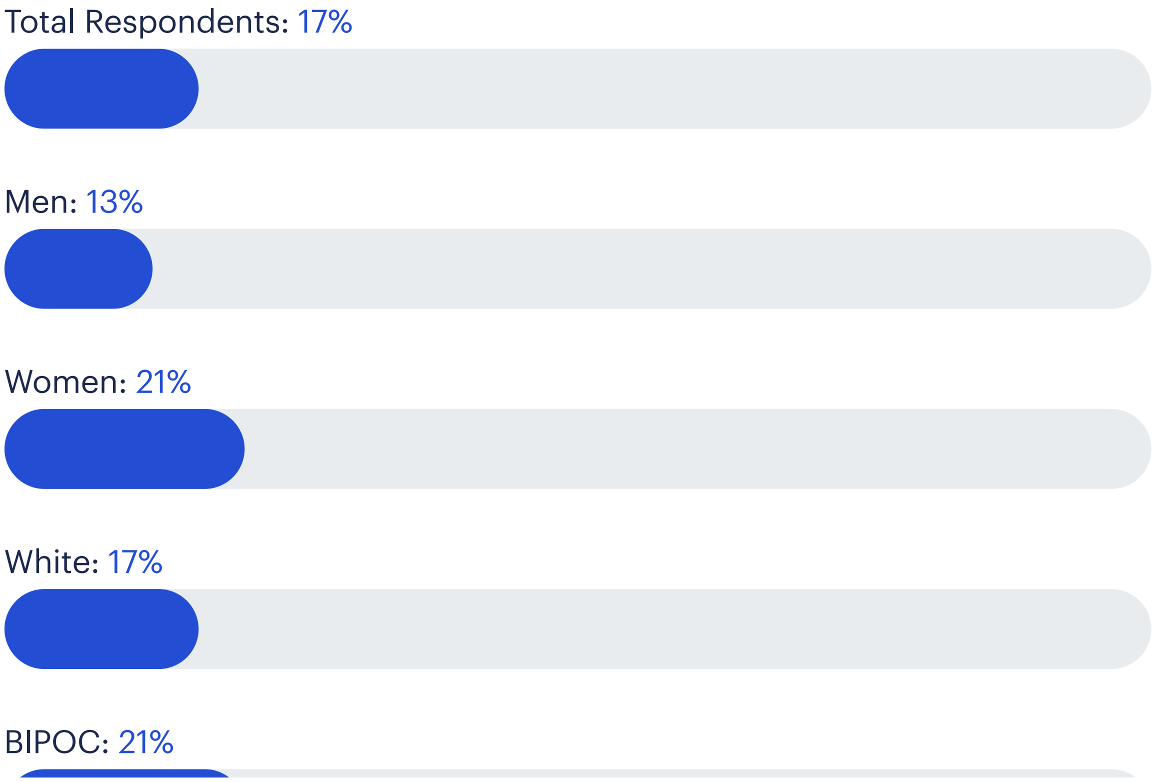
Education: Higher education, higher lost dollars

Diploma/high school/Secondary school:
$1,311

College/University:
$1,432

Higher education:
$2,157

And how has your stress level changed because of the suspicious online activity you experienced? Answer: I experienced a substantial increase in stress levels



Total Respondents: 17%

Men: 13%

Women: 21%

White: 17%

BIPOC: 21%

Cybersecurity familiarity and use

Unsurprisingly, the most well-known security tool amongst our respondents was antivirus. However, despite widespread use and availability—and billions of dollars of promotion—stretching back more than 30 years, 21 percent of our respondents did not feel “familiar” or “very familiar” with this cornerstone cybersecurity technology. And this lack of comfort with antivirus is likely reflected in the actual adoption of it—just 67 percent of all respondents said they used antivirus protection.

The cyberthreats faced by smartphone users are no less real than those encountered on home computers, but they are different. Which may explain why those aged 18 – 24 are more likely to use a VPN than any other age group, with 44 percent of respondents in that cohort adopting the heavily-marketed privacy tech.

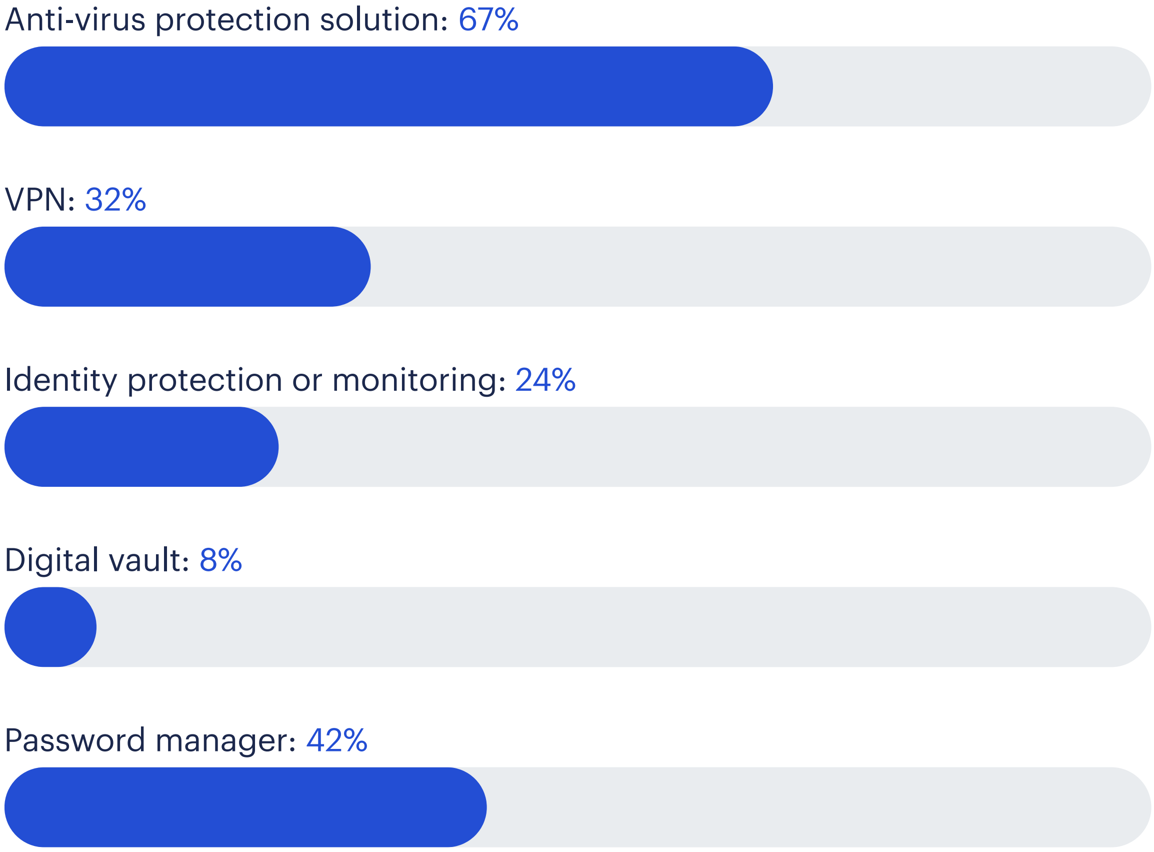
But while the types of tools people use vary by age, familiarity with all tools increased with income and education level. People with higher incomes and higher levels of education were more likely to use antivirus (75 percent), more likely to use identity protection (37 percent and 32 percent), and more likely to use digital vaults (14 percent and 12 percent) than other groups. This trend across income also partly tracked across age groups. Individuals aged 25 – 44 years old with higher incomes said they had higher familiarity with cybersecurity tools than their lower income counterparts of the same age. (Oddly, the impact of income appeared to dissipate for the youngest respondents, with no significant difference between cybersecurity familiarity no matter the income level for those aged 18 – 24.)

The reasons for all of this are not clear: It could be that these groups have more awareness of the threats they face, feel they have more to lose, have more resources to devote to the problem, or some other reason entirely. Whatever the cause, it seems that the wealthy and educated are better protected online. If the Internet were optional, perhaps that wouldn’t matter, but it is not.

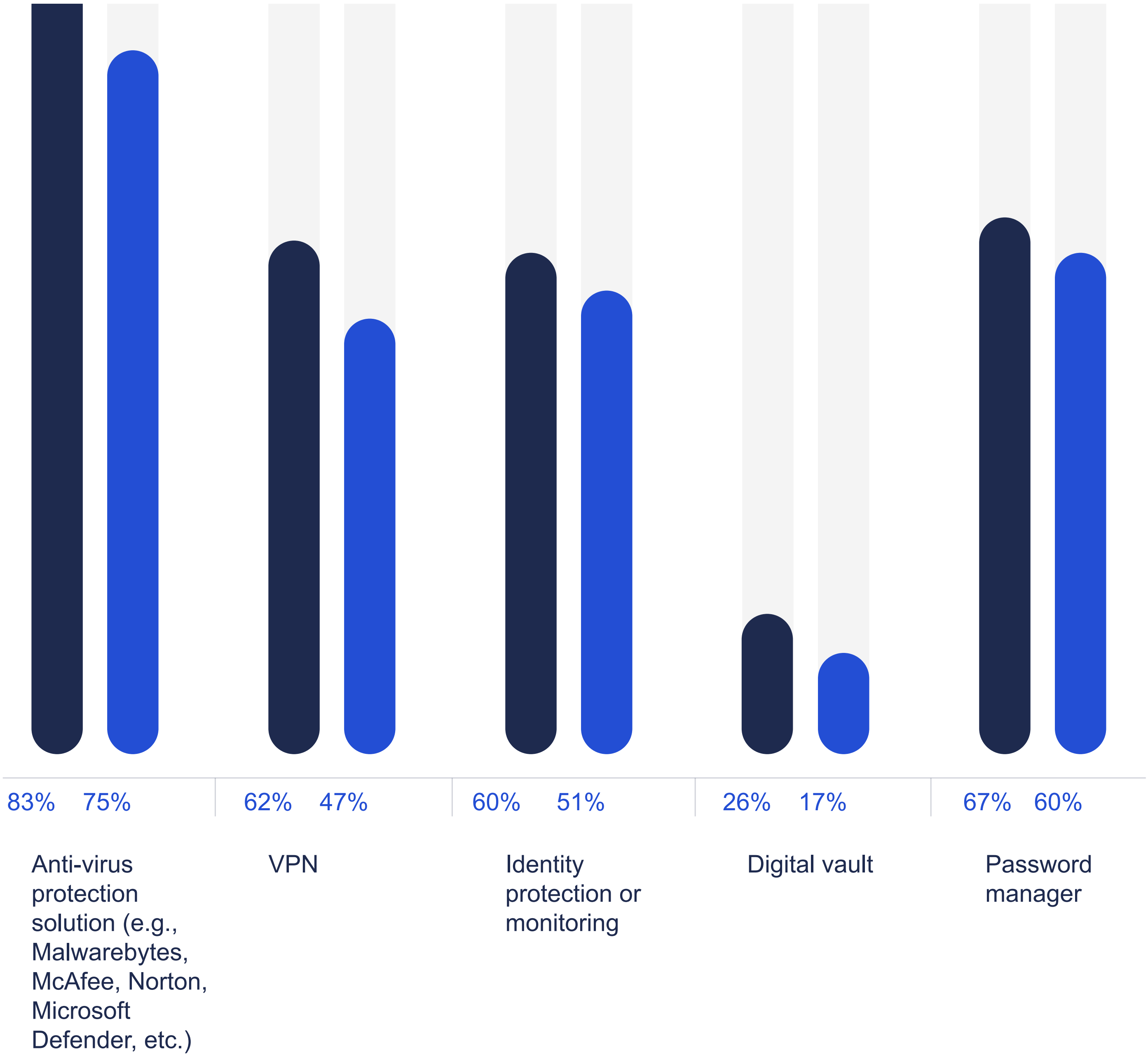
And finally, for every tool in our question, our female respondents declared themselves less familiar. Of course, it is possible that they are as familiar as men and simply set a higher bar for declaring themselves familiar, but the disparity between the sexes is also reflected in their use of cybersecurity tools. For every tool in our question, our female respondents also said they used cybersecurity tools less frequently than men.

“For every tool in our question, our female respondents declared themselves less familiar”

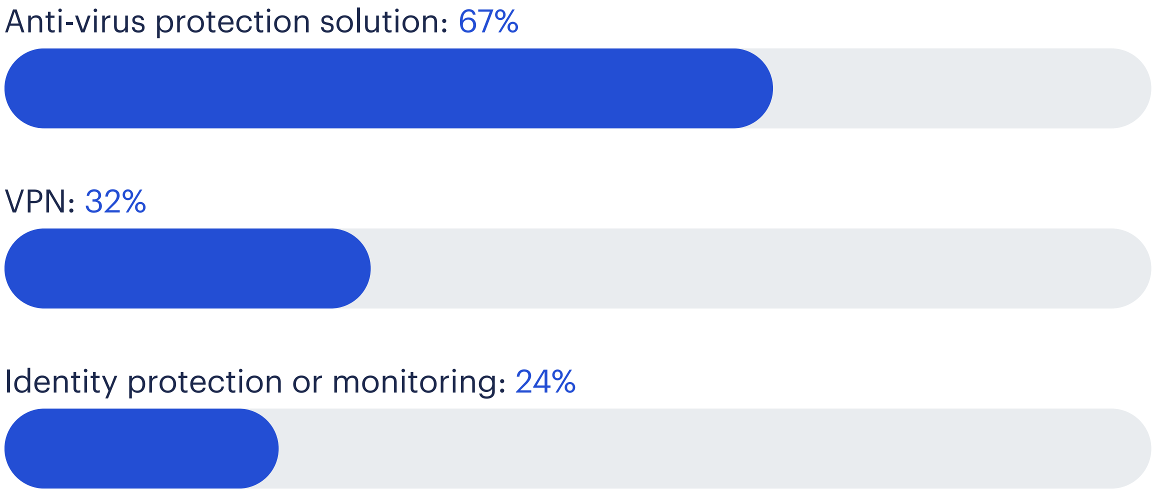
“To what extent are you familiar with each of the following when it comes to protecting yourself online?” (Results including “familiar” and “very familiar,” combined)

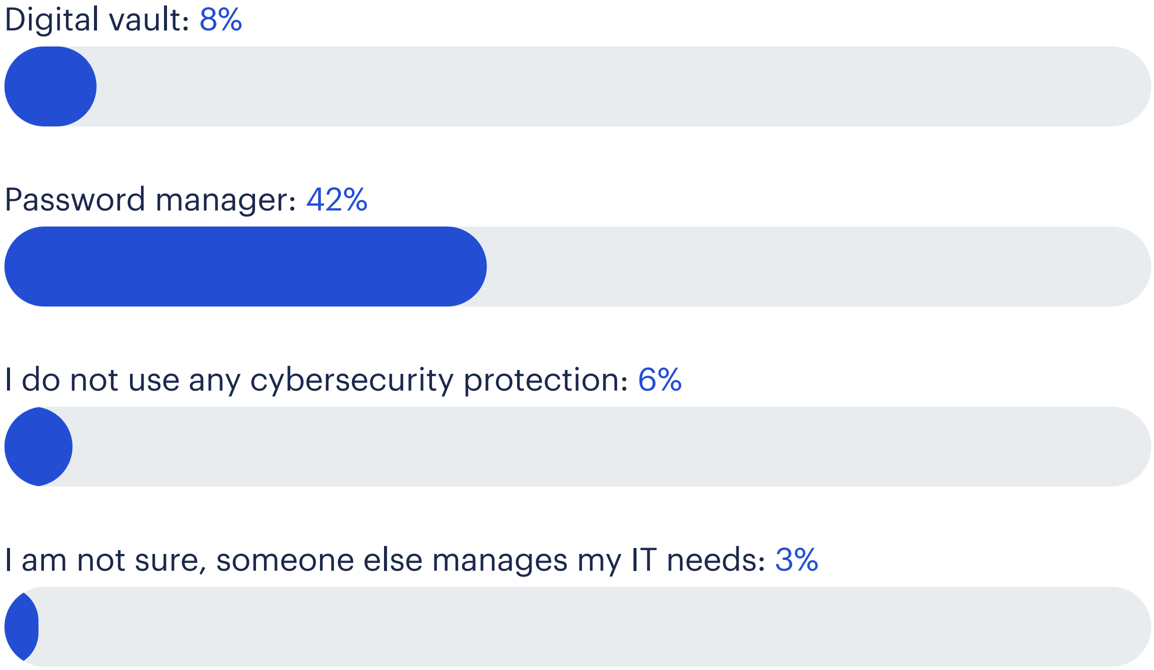


“To what extent are you familiar with each of the following when it comes to protecting yourself online?”



Which of the following forms of cybersecurity protection methods do you use?





Conclusion: A better Internet

The results from our report are clear. People do not feel safe or private online at nearly the levels they deserve, and for some populations, those feelings deepen, sometimes reflected by real-life experiences that happen away from a computer screen or a mobile phone.

Reflexively, the cybersecurity community might assume it already has the solution to these problems: Use the products it develops, particularly antivirus tools. Such tools can protect against malicious downloads that are delivered through deceptive emails, prevent ransomware from locking up a person's computer, and, with modern add-ons, even warn people about dangerous websites that have been identified in connection with online scams.

There's an attractive convenience to those ideas. In the US, UK, and Germany, for groups that had high usage of cybersecurity, without income taken into account, those same groups reported feeling safer online.

But 21 percent of respondents—a little more than one in five—did not have strong or baseline familiarity with antivirus protection, and within those respondents, we found a correlation between their antivirus familiarity and their feelings of safety online.

As a community, cybersecurity vendors have to listen to what people are saying. Nearly a third do not feel safe, and half do not feel private. Women feel least private and safe of all. It is not enough to develop these products and assume that everyone can access them and use them to the same degree.

Instead, the cybersecurity community should consider why its products are not reaching so many vulnerable populations. Companies must commit to better outreach and product design, creating education and tools that no longer assume equal familiarity for whole segments of the global population, and ensuring better awareness and access for all.

The Internet can be a better place. It's up to us to help make that happen.

Methodology

Research findings are based on a survey conducted by Savanta Inc. across the US, UK, and Germany between July 27th and August 9th, 2021. For this study, 5,000 respondents were asked general questions around suspicious online activities. Respondents are recruited through a number of different mechanisms, via different sources to join the panels and participate in market research surveys. They are invited to take part via email and are provided with a small monetary incentive for doing so.

Results of any sample are subject to sampling variation. The magnitude of the variation is measurable and is affected by the number of interviews and the level of the percentages expressing the results. In this particular study, the chances are 95 in 100 that a survey result does not vary, plus or minus, by more than 1.4 percentage points from the result that would be obtained if interviews had been conducted with all persons in the universe represented by the sample.

Malwarebytes

Cyberprotection for every one.