

Independent Tests of Cybersecurity Solutions



IT Security Survey 2026

LAST REVISION: 9TH FEBRUARY 2026

WWW.AV-COMPARATIVES.ORG

Security Survey 2026

We are proud to present our annual Security Survey for 2026. This initiative is part of our ongoing commitment to optimising our service to the end-user community. We want to thank all the respondents who contributed their valuable time and energy to help improve various aspects of anti-virus software and its testing.

Key data

Survey Period: **20th November 2025 – 17th December 2025**

Valid responses of real users: **1,328**

The survey was carefully designed with control questions and checks to ensure the authenticity and validity of responses. The insights gained are invaluable to us and help to shape the future of cybersecurity services.

Overview

In today's digital landscape, where cyber threats loom large, understanding user behaviour, preferences, and concerns is essential for developing effective cybersecurity strategies. This comprehensive survey explores the experiences of users worldwide, offering valuable insights into their digital lives. It highlights the operating systems and applications they rely on, the security measures they adopt, and their concerns about IT security.

The report delves into the factors influencing choices of browsers, operating systems, and security solutions, while also addressing privacy concerns and the need for transparency and independence from organizations that protect our digital world.

Survey findings showcase the diverse ages, expertise levels, and regional backgrounds of participants, all of which shape user decisions and concerns. The data reflects loyalty to specific operating systems, growing preferences for particular browsers, and fears of cyber threats influenced by regional and technical factors.

This report offers a global perspective on current cybersecurity trends, serving as a foundation for further research. Beyond statistics, it aims to provide meaningful insights for users, providers, and testers in the cybersecurity field. We encourage you to reflect on these findings and consider their implications for your own cybersecurity strategies.

The survey, conducted by AV-Comparatives between November 20 and December 17, 2025, gathered responses from about 1,300 participants globally, focusing on IT security. We hope the insights presented here will guide you in strengthening your cybersecurity approach.

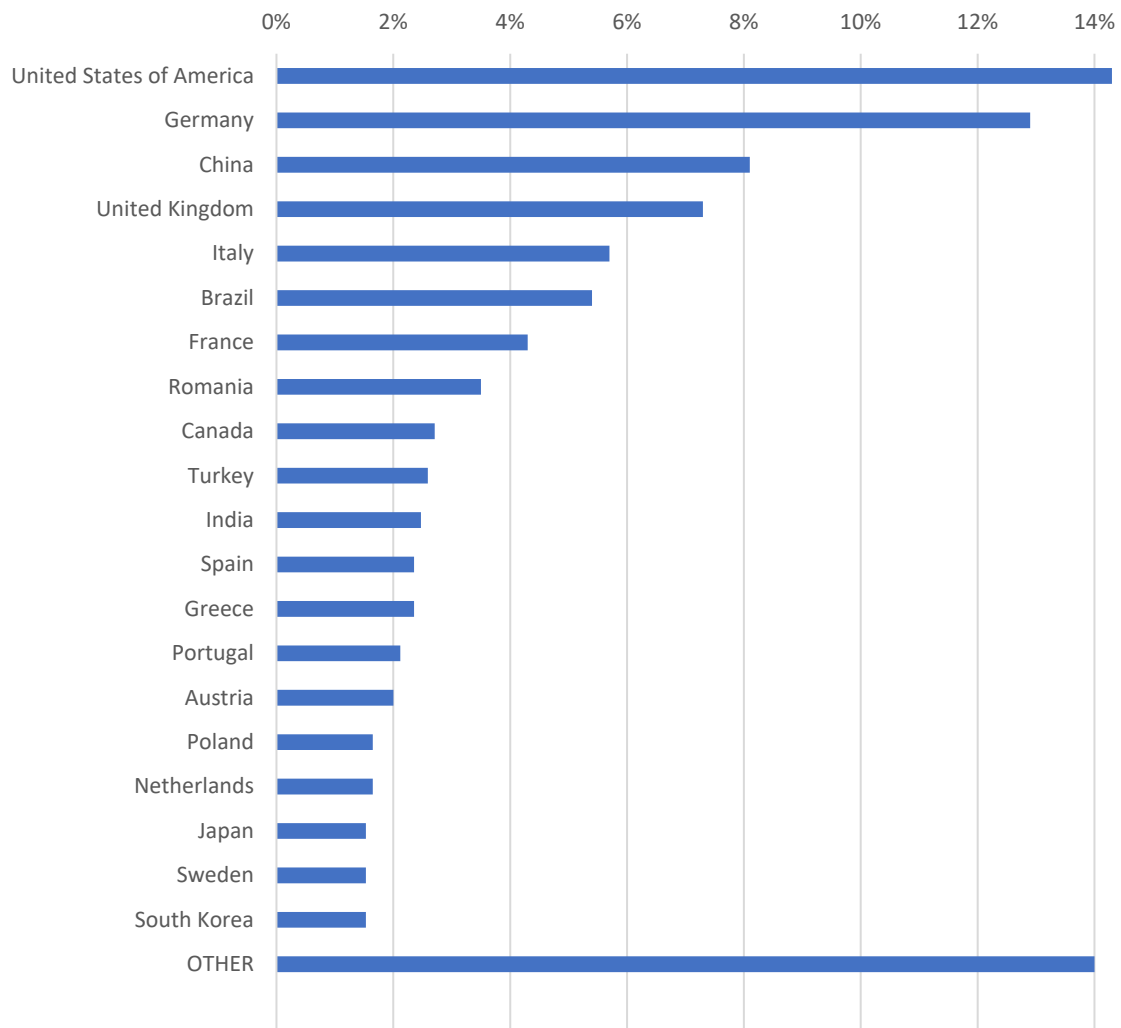
We extend our gratitude to all survey participants. Your input is invaluable in improving the relevance and impact of our tests, helping manufacturers refine their products and benefiting both the industry and its users. We are proud to see our test results frequently cited in security product reviews. For full transparency, all public test results from AV-Comparatives are freely available at www.av-comparatives.org

Key results

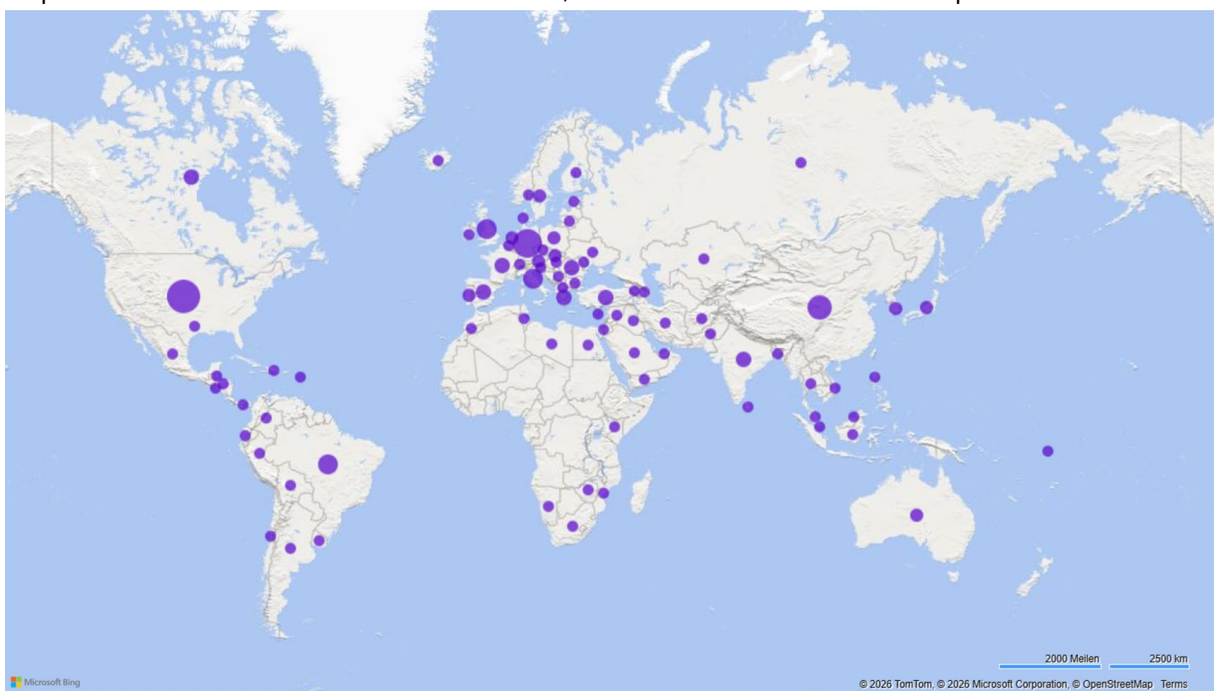
The Key findings of the survey are listed below, by question number. Please note that they all refer only to our survey participants, not the general public.

1. **Origin of Respondents:** Respondents hailed from 87 countries. The United States had the most respondents from a single country, followed by Germany and China.
2. **Age of Respondents:** The youngest and oldest age groups had the fewest respondents, with the remaining responses being split roughly equally between the other age groups.
3. **Level of expertise:** about 70% of participants identified as advanced or IT/expert users
4. **Free vs Paid Security Solutions:** 75% of survey participants paid for their chosen desktop security programs. Advanced users overwhelmingly prefer paid tools.
5. **Operating System Preferences:** A majority now seem to prefer Windows 11 over Windows 10, with older Windows versions being used by a shrinking number.
6. **Browser Preferences:** Mozilla Firefox and Google Chrome remain the most preferred browsers.
7. **Mobile OS Trends:** Android dominates (74%), but iOS is preferred by advanced users.
8. **Mobile Security:** 40.3% use no mobile anti-malware, including 43% of IT professionals. Top vendors vary regionally, with Bitdefender, Kaspersky, and ESET consistently prominent.
9. **Desktop Security:** Microsoft, Bitdefender, ESET, and Kaspersky dominate globally. ESET leads in North America and Europe; Kaspersky tops Asia, and South America.
10. **Trusted Test Sources:** AV-Comparatives and AV-Test are the most trusted.
11. **Requested Consumer Tests:** Bitdefender, ESET, Microsoft, and Kaspersky top the list for future evaluations.
12. **Enterprise Solutions Demand:** Avast, CrowdStrike, Sophos, and Trend Micro join the requested consumer leaders in business/enterprise requests.
13. **Windows 11 Adoption:** Over 76% had to purchase new hardware before switching to Windows 11.
14. **Top Fears:** Among survey respondents rated fears related to technology highest.
15. **Most-Feared Actors:** Russia (60%), China (57%), USA (41%), and North Korea (36%) are seen as the top cyber threats among the survey participants. 24% fear their own country (domestic surveillance).

1. Where are you from?

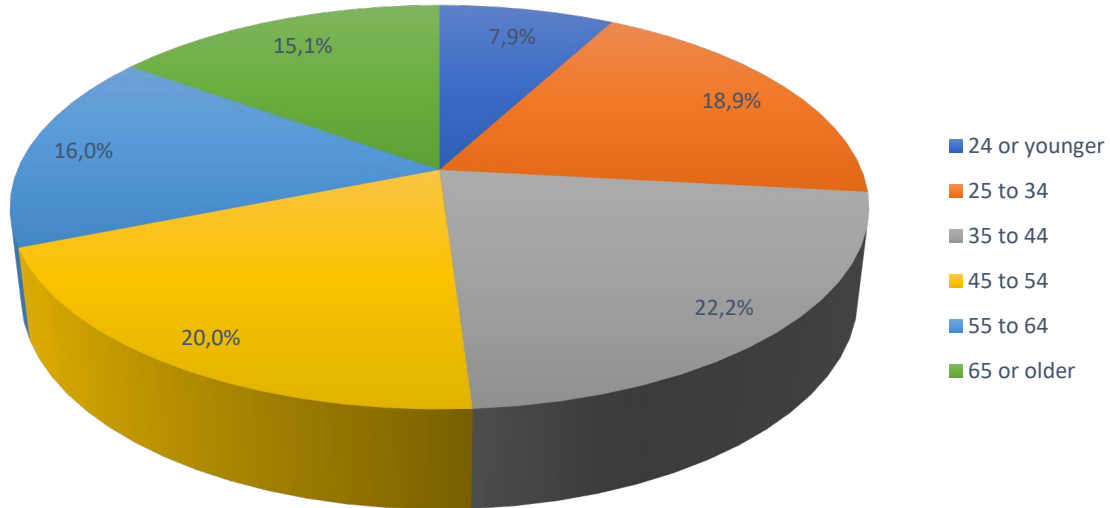


The graph above displays the top 20 countries from which our survey participants originate. In total, respondents hailed from 87 different countries, which are illustrated on the map below.

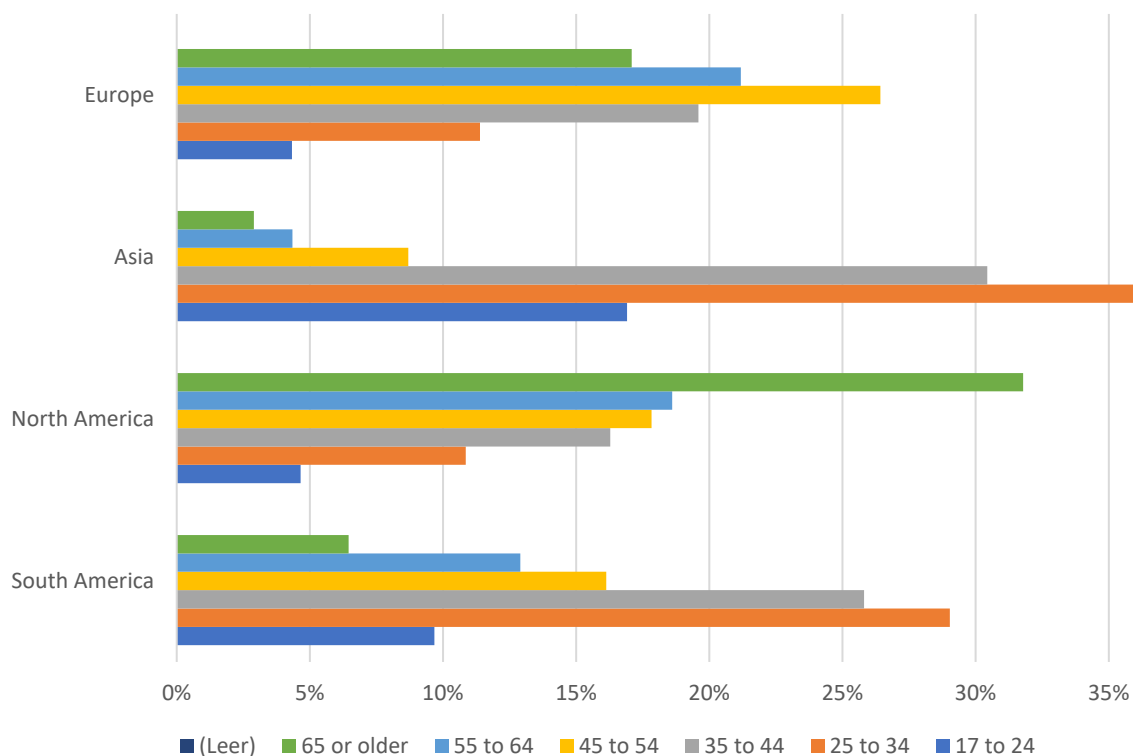


2. How old are you?

The survey results reveal a wide age range among participants from various continents. The youngest group, aged 24 or younger, makes up a modest 7.9% of the total. The two largest groups of respondents belong to the 35-44 and 45-54 age groups, representing 22.2% and 20% respectively. These are followed by the 25-34 age group, with 18.9%. This reflects a balanced distribution among middle-aged participants. Those aged 55-64 constitute 16%, while the oldest group, aged 65 or older, represents 15.1% of the total.

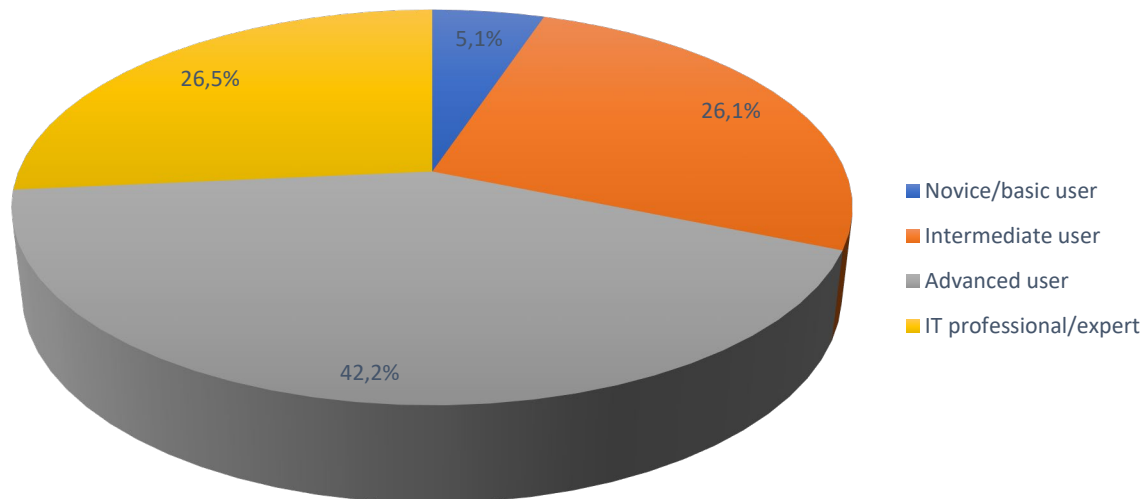


The overall age distribution is displayed above, with a breakdown by continent provided below. Geographically, North America has the oldest age profile, with over half of participants aged 55 or older. This contrasts sharply with Asia and South America, which both skew younger with over 80% and 60% of respondents being less than 44 years old. Europe participants largely belong to the middle-aged groups, with approximately 45% of participants aged between 35 and 54.



3. How would you rate your level of expertise in using computers?

The survey also explored the participants' self-assessed level of computer expertise, revealing insights into their technological proficiency. Overall technical expertise is shown in the chart below:

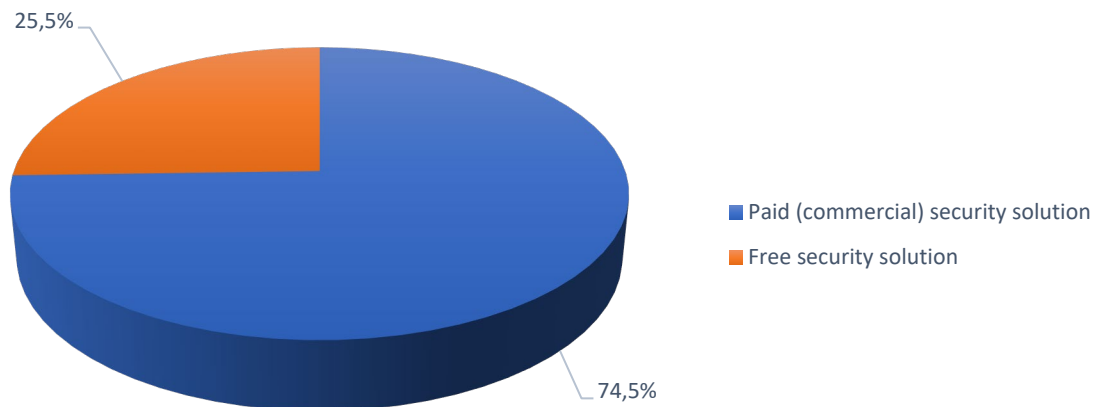


A small portion of participants, roughly 5%, identified themselves as novice or basic users, suggesting limited familiarity or comfort with computer technology. This is considerably outweighed by those who described themselves as intermediate users, accounting for 26.1% of respondents. These individuals likely have a solid grasp of standard computer functions and applications.

The largest group, making up 42%, classified themselves as advanced users. These participants are presumably skilled in a wide range of computer functionalities and may have specialized knowledge in software and/or hardware. Finally, 26.5% of respondents identified as IT professionals or experts, reflecting a high level of proficiency and likely a strong involvement in computing as a key part of their career or daily life.

This distribution underscores a strong presence of tech-savvy individuals within the participant pool, with a significant proportion possessing advanced skills or professional expertise. This may explain why survey respondents' preferences, such as their choice of operating system or browser, differ from those of the public.

4. Which type of desktop security solution do you primarily use?

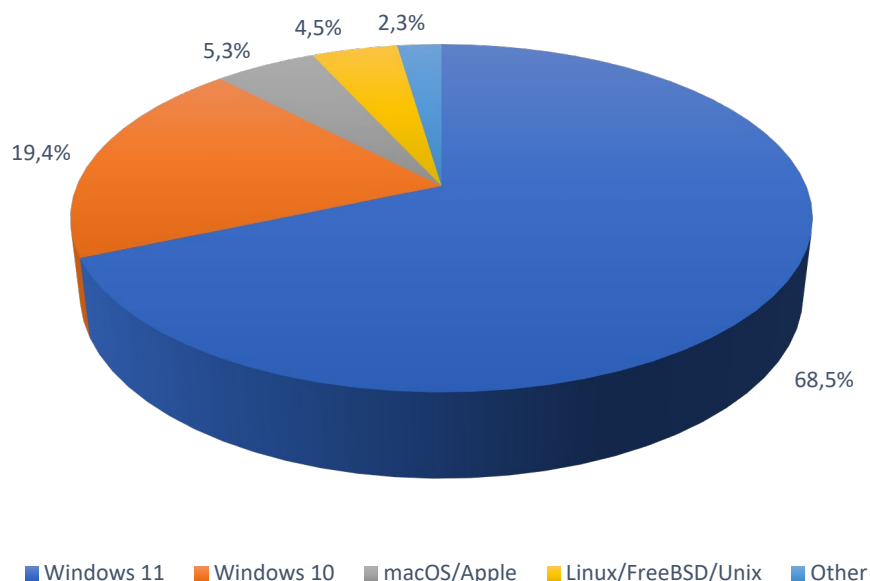


The survey's exploration of desktop security solutions used by participants highlights a clear preference for paid or commercial products over free alternatives, as illustrated in the chart above. Specifically, 74.5% of respondents reported using paid/commercial security solutions, while the remaining 25.5% opted for free versions.

An interesting age-related trend emerges in the choice of security solutions. Younger users, particularly those aged 34 or younger, show a greater inclination toward free security solutions, with approximately 30% using them. In contrast, only 20% of respondents over the age of 34 rely on free versions on average. This disparity may stem from factors such as financial priorities, differing perceptions of risk, or the extent of digital assets requiring protection.

Additionally, the survey reveals a correlation between users' self-assessed computer expertise and their choice of security solution. Among novice users and intermediate users, 32% use free solutions, while only 60% opt for commercial products. In contrast, advanced to expert users overwhelmingly prefer paid solutions, with 75% choosing commercial security options. This suggests that as users gain more knowledge and proficiency with computers, they may increasingly recognize the value and necessity of comprehensive, paid security solutions to safeguard against sophisticated threats.

5. Which desktop operating system do you primarily use?



The survey results for desktop operating system preferences among participants – depicted in the chart above – reveal a strong preference for Windows, with about 90% of respondents using it. Specifically, 68.5% are using Windows 11, while some – 19.4% – are still using Windows 10.

Only a small portion, 5.3%, use macOS, highlighting its niche presence within the participant pool. Our review and testing of Mac security products¹ can be found at <https://www.av-comparatives.org/consumer/testmethod/mac-security-reviews/>.

Linux, an open-source platform, is used by 4.5% of respondents. The user base for both macOS and Linux is gradually growing, possibly reflecting broader industry trends or evolving user preferences. Other operating systems, including older versions of Windows such as 7 and 8, make up just 2.3%.

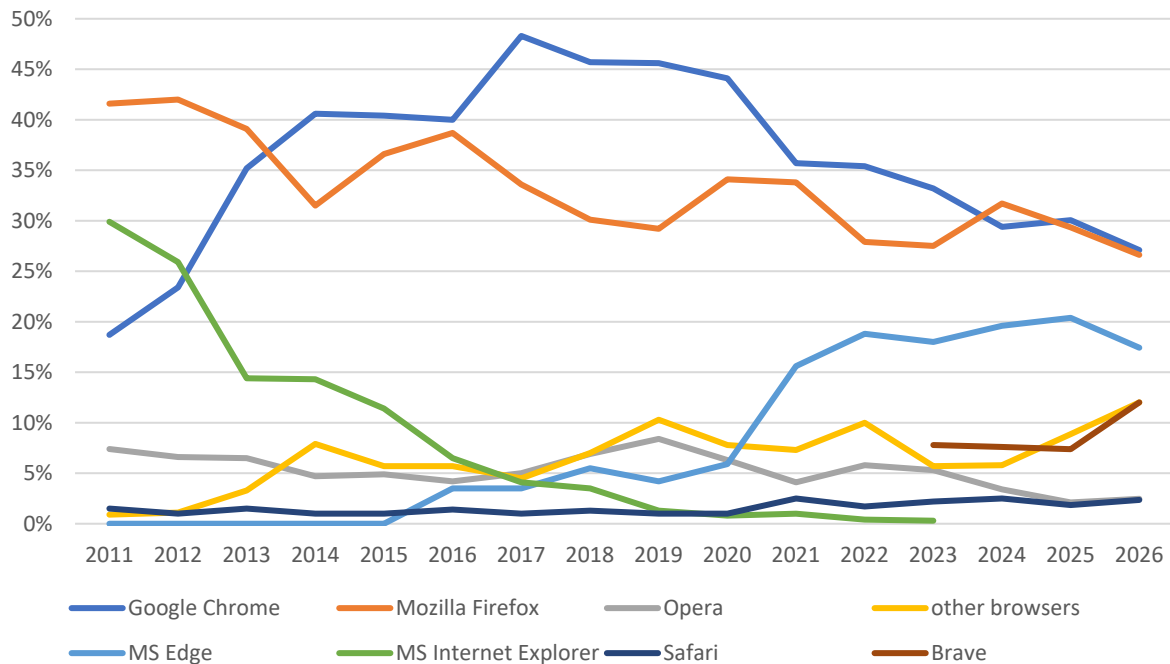
The survey also indicates that IT professionals are more likely to use Linux/FreeBSD/Unix, suggesting a preference for this system in certain professional environments.

At AV-Comparatives, we adopted Windows 11 as the primary operating system for our tests in 2025. Additionally, it's worth noting that Microsoft has stopped providing mainstream support for Windows 10 as of October 2025, though paid security updates will continue for an additional three years².

¹ A list of Mac security products can be found here: <https://www.av-comparatives.org/list-of-av-vendors-mac/>

² <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/plan-for-windows-10-eos-with-windows-11-windows-365-and-esu/ba-p/4000414>

6. Which browser do you primarily use?



As illustrated in the diagram above, Google Chrome is used by 27.1% of respondents, followed closely by Mozilla Firefox, with 26.6% of respondents using it as their primary browser. Microsoft Edge remains the third most popular option, with 17.4% of users adopting it.

This shifting browser landscape highlights a diversification of user preferences, likely influenced by factors such as performance, privacy concerns, or specific feature sets. The results also highlight the growing relevance of the Brave browser, which is used by 12% of respondents, surpassing other options like Opera, Safari, Vivaldi, Yandex, and DuckDuckGo. This indicates a rising interest in privacy-focused browsing solutions among a segment of users.

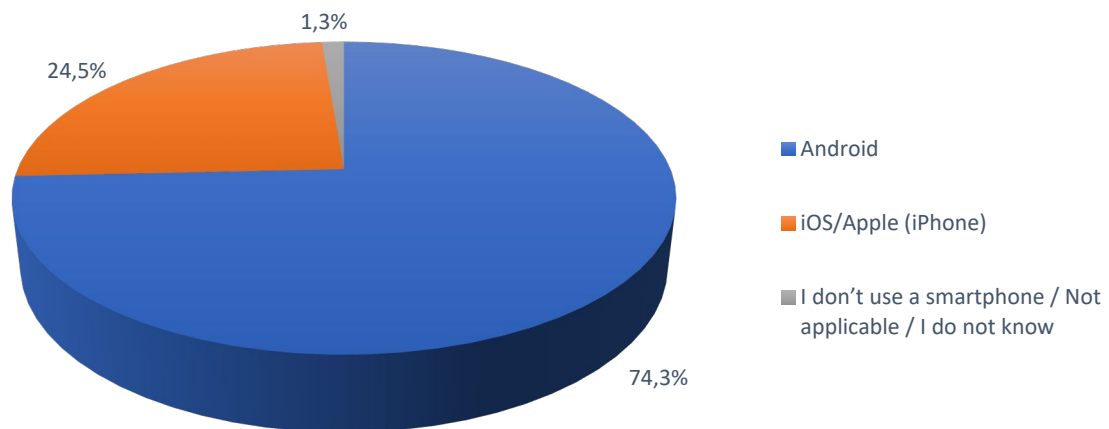
While statistics show that Google Chrome remains the most popular browser among the general public, accounting for nearly two-thirds of all users, we at AV-Comparatives continue to use Chrome in our tests due to its widespread adoption.

The data also reveals differences in browser preferences based on user expertise. Novice and basic users predominantly favour Microsoft Edge, with 15% of this group choosing it. In contrast, more advanced users tend to prefer Mozilla Firefox, aligning with its overall popularity in the survey. Advanced users also show a stronger inclination toward niche browsers like Brave, likely reflecting their preference for customization, privacy, or specialized functionalities.

Among macOS users, Safari usage has stabilized around 38%, similar to previous years result. Chrome and Firefox are now used by 14% and 11% of macOS users, respectively.

Given the increasing diversity in browser usage, we encourage AV vendors to ensure their browser plug-ins, particularly those for URL-blocking features, are compatible with a wide range of browsers, not just the most popular ones. This will help deliver comprehensive security solutions that cater to the varied preferences of users across different browsers and operating systems.

7. Which mobile operating system do you use?



The survey offers a detailed look at mobile operating system preferences among participants. As shown in the chart above, Android dominates globally, accounting for approximately 74% of users. This widespread adoption highlights Android's accessibility and its diverse ecosystem, which caters to a broad range of devices across various price points.

A notable correlation exists between users' technical expertise and their choice of mobile operating system. Advanced and professional users show a stronger preference for iPhones, with 28% using iOS, compared to just 13% among basic and novice users. This inclination may be driven by factors such as security features, build quality, or specific functionalities that appeal to more tech-savvy individuals.

Our Mobile (Android) security review and test report can be accessed at <https://www.av-comparatives.org/testmethod/mobile-security-reviews/>.

8. Which mobile anti-malware security solution do you primarily use on your smartphone?

The survey’s findings on the use of mobile anti-malware security solutions highlight a significant divide in cybersecurity practices across different user groups. Overall, 40.2% of respondents do not use any security solution on their mobile devices. This substantial percentage may reflect a combination of trust in built-in security features, limited awareness of mobile threats, or a perceived inconvenience of installing additional security software.

Interestingly, IT professionals are the most likely to forgo mobile security solutions, with 44% not using any. This could stem from their advanced expertise and confidence in managing mobile risks manually, or a preference for maintaining optimal device performance without additional software. In contrast, only about 39% of novice or basic users do not use any security solution, this gap has continuously narrowed compared to previous years’ surveys.

Globally, the ten most used mobile security manufacturers, in descending order, are: Bitdefender, ESET, Kaspersky, Avast, Norton, McAfee, Sophos, Malwarebytes, AVG, F-Secure.

The list below highlights the ten most popular mobile security manufacturers used by survey participants, broken down by continent. Due to insufficient responses from certain regions, Australia/Oceania and Africa are not included in the breakdown.

Europe	North America	Asia	South/Central America
1. Bitdefender	1. Bitdefender	1. Kaspersky	1. Bitdefender
2. ESET	2. ESET	2. Bitdefender	2. ESET
3. Kaspersky	3. Avast	3. Avast	3. Kaspersky
4. Avast	4. Malwarebytes	4. Norton	4. McAfee
5. Norton	5. F-Secure	5. ESET	5. AVG
6. Sophos	6. McAfee	6. McAfee	6. Norton
7. Trend Micro	7. AVG	7. AhnLab	7. Panda
8. McAfee	8. Sophos	8. Malwarebytes	8. Avast
9. AVG	9. Avira	9. F-Secure	9. Avira
10. Malwarebytes	10. Trend Micro	10. Dr.Web	10. Sophos

Bitdefender, ESET and Avast were among the most popular mobile security products in all four regions.

Major security products for mobiles were reviewed by AV-Comparatives in a report³ in 2025.

³ <https://www.av-comparatives.org/testmethod/mobile-security-reviews/>



9. Which desktop anti-malware security solution do you primarily use?

Globally, the twelve most commonly used manufacturers of anti-malware products for Windows platforms among survey participants are (in order): ESET, Bitdefender, Kaspersky, Microsoft Defender, Avast, Norton, McAfee, Malwarebytes, AVG, Avira, F-Secure, and G Data.

Across all four continents with significant results, the same four vendors consistently appear in the top five positions. These are (in alphabetical order): Bitdefender, ESET, and Microsoft.

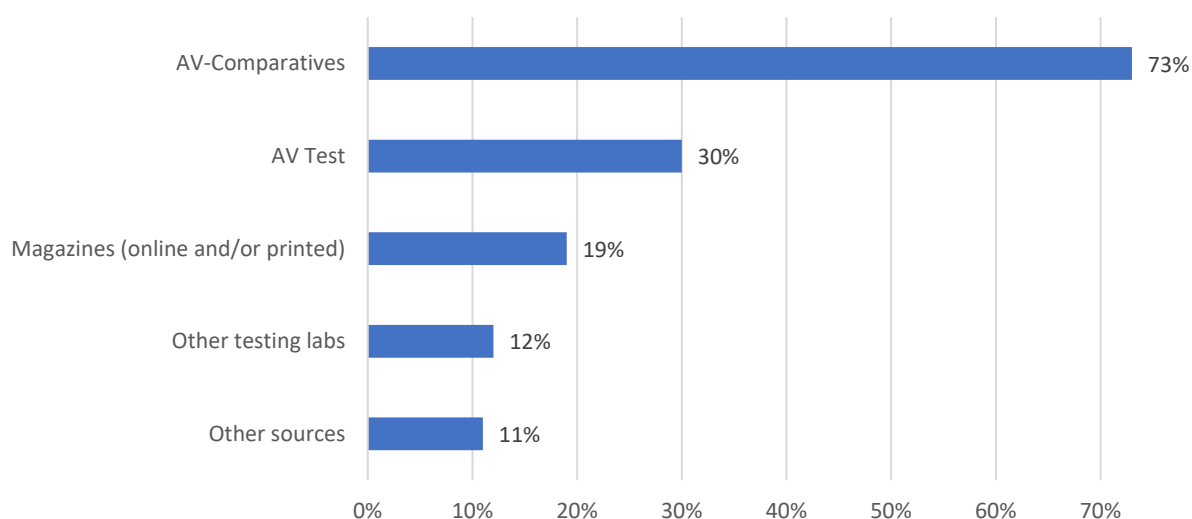
Meanwhile, Kaspersky has been overtaken by ESET, Bitdefender, and Microsoft. Kaspersky remains the most popular desktop security solution in Asia and South/Central America.

Differences between continents

The table below shows the twelve products most commonly used by survey participants, by continent:

Europe	North America	Asia	South/Central America
1. ESET	1. ESET	1. Kaspersky	1. Kaspersky
2. Bitdefender	2. Bitdefender	2. ESET	2. Microsoft
3. Microsoft	3. Microsoft	3. Bitdefender	3. ESET
4. Kaspersky	4. Malwarebytes	4. Avast	4. Bitdefender
5. McAfee	5. Norton	5. Microsoft	5. Avast
6. Avast	6. McAfee	6. Norton	6. Malwarebytes
7. Norton	7. F-Secure	7. AhnLab	7. AVG
8. AVG	8. Webroot	8. AVG	8. McAfee
9. F-Secure	9. AVG	9. Trend Micro	9. Avira
10. G Data	10. Sophos	10. Qihoo	10. G Data
11. Sophos	11. VIPRE	11. Tencent	11. Avira
12. Trend Micro	12. Panda	12. K7	12. Sophos

10. What are your main sources for anti-virus/security test results?



The most trusted sources for AV/security test results are listed above in order of preference. It's important to note that respondents were asked to provide their answers in an empty text box, ensuring that the responses reflect the sources they genuinely use rather than being influenced by pre-selected options.

The responses reveal a diverse landscape of preferences and trust, with certain key players standing out in the industry. AV-Comparatives is the most prominent, mentioned by 73% of respondents, indicating a high level of credibility and trustworthiness among users. We believe this reflects our commitment to independence from vendor influence, our comprehensive and meticulously designed testing methodologies, the significant number of samples we use, our transparency, and the detailed, freely available test reports we provide. Additionally, our policy of allowing other publications to cite our results (with proper attribution) further enhances our visibility and reach.

AV-Test ranks as the second most popular source, used by 30% of respondents. The fact that a majority of users rely on both AV-Comparatives and AV-Test highlights a preference for established testing labs with over two decades of experience in the field of AV testing. This underscores the importance of trust, reliability, and a proven track record in shaping user confidence in test results.⁴

Traditional magazines, both online and printed, such as PCmag, ComputerBILD, PC World, Heise c't, CHIP, Security.nl, TechRadar, and BleepingComputer among others, are also significant sources, mentioned by 19% of respondents.

Forums and Online Communities are mentioned by a number of respondents. These communities offer discussions and user feedback about antivirus solutions. Other testing labs like MITRE, Virus Bulletin, SE Labs, MRG-Effitas, AVLab, and as well as analyst-firms such as Gartner, Forrester, and Frost & Sullivan. Respondents frequently state that they cross check results across multiple testing labs. Especially more experienced users are more likely to compare results between multiple labs. This group also consistently rank testing labs like AV-Comparatives and AV-Test among their top sources for credible information. We view this as a strong endorsement of professional, independent testing agencies by those with technical expertise.

⁴ <https://www.av-comparatives.org/spotlight-on-security-why-independent-testing-of-anti-virus-software-is-important/>

11. Which CONSUMER/HOME-USER desktop security solutions would you like to see in our yearly public consumer main-test series?

Below are the 15 most-requested consumer/home-user products:

1. Bitdefender
2. ESET
3. Microsoft
4. Kaspersky
5. Avast
6. Norton
7. McAfee
8. Avira
9. Malwarebytes
10. F-Secure
11. AVG
12. Trend Micro
13. G Data
14. Sophos
15. Panda

12. Which BUSINESS/ENTERPRISE desktop security solutions would you like to see in our yearly public enterprise main-test series?

Below are the 20 most-requested business/enterprise products:

- | | |
|----------------|------------------------|
| 1. ESET | 11. ThreatDown |
| 2. Bitdefender | 12. Fortinet |
| 3. Microsoft | 13. Check Point |
| 4. Kaspersky | 14. Broadcom |
| 5. Avast | 15. Trellix |
| 6. CrowdStrike | 16. WithSecure |
| 7. Sophos | 17. Palo Alto Networks |
| 8. Trend Micro | 18. SentinelOne |
| 9. Cisco | 19. WatchGuard |
| 10. G Data | 20. VIPRE |

Most of the popular vendors are usually included in at least some of our public tests and reviews of consumer and business software⁵, while most of the other vendors commission separate tests and/or participate privately in certain tests.

⁵ Consumer: <https://www.av-comparatives.org/consumer/>
Enterprise: <https://www.av-comparatives.org/enterprise/>

13. Adoption of Windows 11

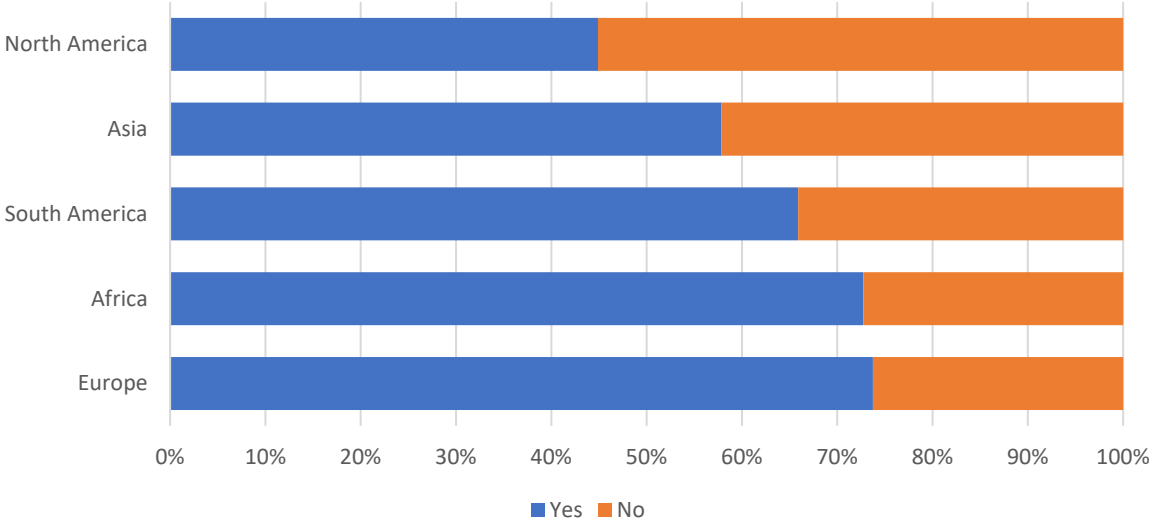
We adopted Windows 11 as the standard operating system for our tests in 2025. We asked survey participants about the switch to the newest version of the Microsoft Windows operating system. Almost half of the survey participants told us, that they made the switch to Windows 11 before the end-of-life (EOL) of Windows 10 in October 2025. A small portion of respondents made the switch to a different operating system, with 2.6% switching to macOS and 4.1% to Linux. Advanced and expert users were much more likely to make the switch to Linux, this is likely because Linux is considered to have a steeper learning curve compared to Windows and being more popular amongst IT experts. Novice users were the group least likely to have switched before the EOL of Windows 11.

Over half of the novice users reported having to purchase new hardware to upgrade to Windows 11. This proportion is significantly lower for more experienced users. A likely explanation for this is that novice users upgrade their hardware less frequently and therefore are often still using older hardware. This is further corroborated by the fact that less experienced users often waited until the EOL of Windows 11. Less than half of these respondents made the switch before Windows 11's EOL.

It is also of note that younger users were somewhat more likely to have already started using Windows 11, whereas older users are more likely to continue using Windows 10.

15. Companies located in the US

We also asked survey participants, if they are concerned that many of the companies providing digital services (cloud storage, OS manufacturers, AI companies, social media platforms, messengers, etc.) are based in the USA.



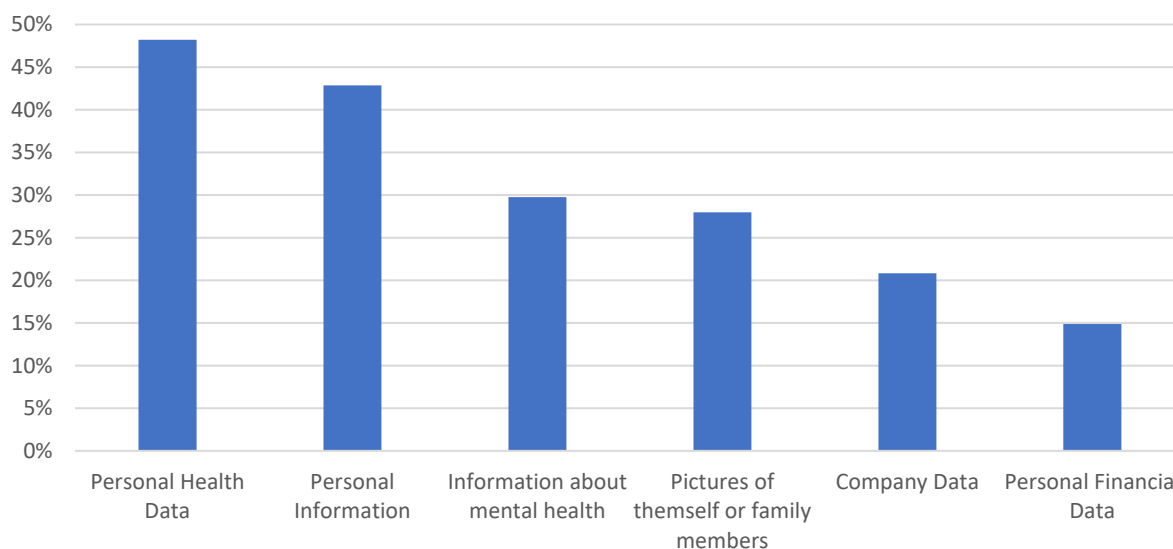
Two in three survey respondents are worried by this fact, providing a variety of reasons for being concerned. The most common sentiments, present among those concerned by the prevalence of US-based services, are a high value assigned to privacy and data protection (16%), concerns about political instability and a lack of trust in leadership, and worries about government surveillance when data is stored in their jurisdiction. 10% of the concerned respondents also highlighted the importance of digital services based in the EU or otherwise outside of the US' jurisdiction. Several European countries (Denmark, Austria, Netherlands, Germany, and Sweden) have an even higher level of distrust, with over 80% of respondents being concerned about US based companies.

Of the respondents not concerned by the prevalence of US-based services (34.8%) common reasoning for this was having nothing to hide and trusting in laws providing privacy to users. However, there is also a small portion of respondents (3.7%) state a kind of resignation to the inevitability of their data not being private as well as stating that other countries are no better in regard to data protection.

Unsurprisingly, European survey participants are most concerned about digital services located in the US, with 74% stating that this worries them. Accordingly, North American respondents are those least likely to report concerns about this. Less than half of North American survey participants are concerned by this fact.

16. AI Chatbots

One of the new questions for this year is asking whether participants, if they use ChatGPT or similar AI chatbots and if they have ever shared sensitive or personal information with these chat bots. The bar chart below shows how many users shared different kinds of information with AI chat bots.



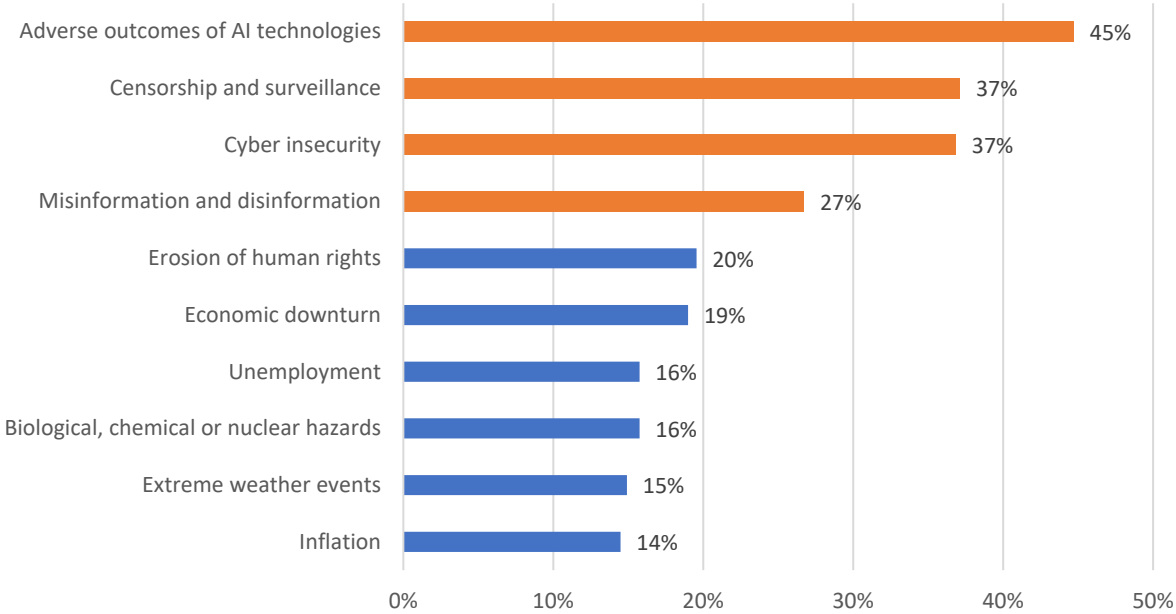
The two most common kinds of information shared are personal health information and personal information, such as Name, date of birth, or address. This is a concern observation as there have been cases of AI chat bot data leaks in the past⁶. These leaks have included user information and prompts. We strongly advise that chat bot users are cautious about sharing personal information with chat bots.

Looking at chat bot usage and age reveals a clear trend of younger users using chat bots more frequently. Over 90% of respondents under 25 uses chat bots, this number declines with age. Of respondents 65 and older, only 40% use AI chat bots. There is a similar trend with users, which have shared personal information, where the younger age groups are more likely to share personal information compared to older generations.

Another observation made, was that more technically skilled users are more likely to use chat bots and at the same time less likely to share personal information. This suggests that these users see both the potentials and the risks in these technologies.

⁶ <https://cybernews.com/security/ai-chatbots-vyro-data-leak/>

17. What are your five greatest concerns for the next two years?



This year we again asked survey participants about their fears for the future. The options given are like those given in the WEF’s Global Risk Survey of 2025⁷. Four of the top ten threats are identical between the respondents of both surveys: Cyber insecurity, Misinformation and disinformation, Erosion of human rights, Economic downturn, Biological, chemical or nuclear hazards, Unemployment, and Extreme weather events. A key difference being that respondents to our survey rank Cyber Insecurity higher. This is likely because our readers are more informed of the continuously developing threat landscape. In general, our readers seem to be more concerned about issues related to technology (we have highlighted these in orange). Worries about adverse outcomes of AI technologies is one of the highest concerns amongst our respondents but 31st among respondents of the WEF survey. This also applies to censorship and surveillance, like last year ranked 2nd amongst our respondents and only 16th among WEF respondents. Since over 70% of survey participants rank themselves as advanced or expert users it seems reasonable to assume that those with more contact with technology are more likely to also see the threats that come with them.

Comparing the responses for different age groups reveals certain concerns being more prevalent among younger respondents. For example, those under the age of 25 are more concerned about Censorship & surveillance and Cyber insecurity. Similarly, the younger generations are more concerned about economic threats such as inflation, debt, unemployment and lack of economic opportunity. The older generations are significantly less concerned about these issues. Younger generations are also more concerned about societal polarization compared to older generations. The most likely reason for this is that older generations are likely to already be in retirement and therefore less concerned about employment and other more long-term issues as they will not be as affected by these.

Concerns, which are more common among the older generations are worries about Chronic health conditions and involuntary migration. Similarly, less than 25% of respondents under the age of 55 are concerned about misinformation and disinformation whereas over 30% of those 55 and older are concerned about this.

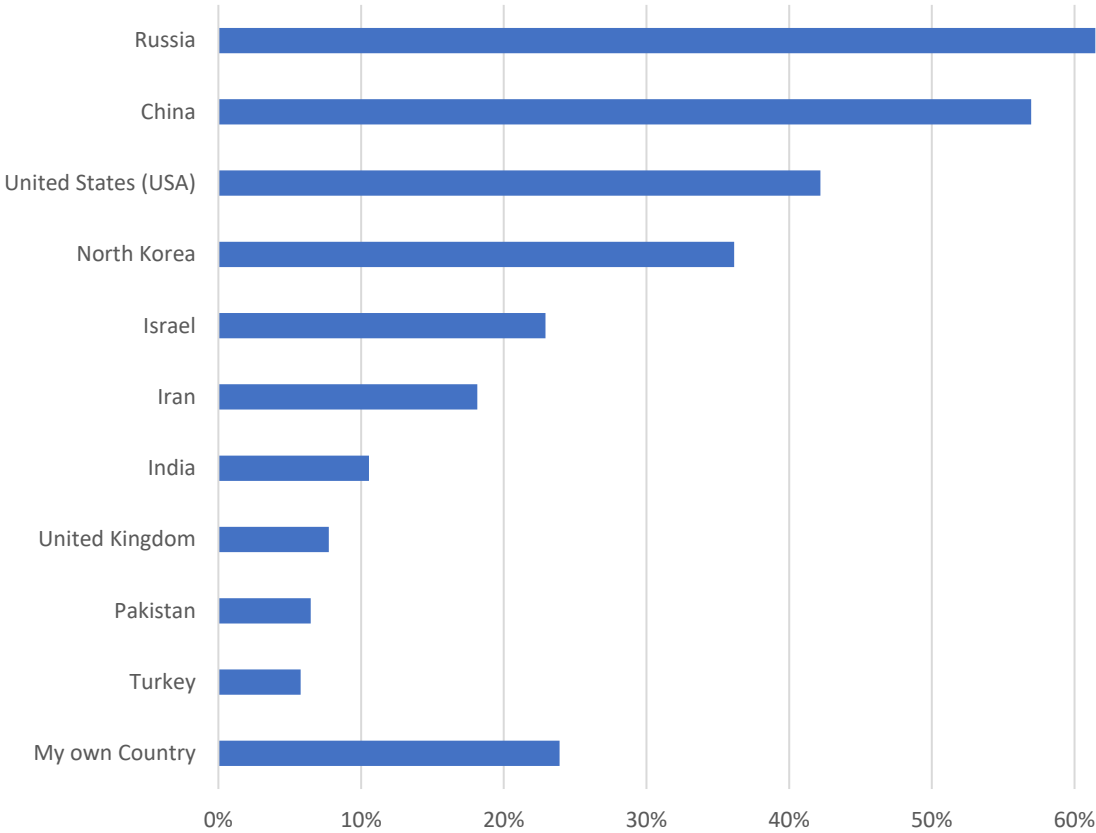
⁷ [https://reports.weforum.org/docs/WEF Global Risks Report 2025.pdf](https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf)



Our survey also revealed that respondents with a higher degree of technical proficiency are more concerned about technological threats. For example, 15% of respondents are describing themselves as novice or basic users are concerned about censorship and surveillance. This number rises the more experienced users are, reaching 37% amongst expert users. Similarly, 7% of novice users are concerned about misinformation and disinformation, this number rises to over 30% among the most experienced user group. IT professionals and expert users are also more than twice as concerned with technological power concentration.

There are also some key differences regarding concerns, based on the continent of the respondent. Amongst respondents from Africa and South/Central America concerns about biodiversity loss are much more common compared to other continents. One likely explanation for this is that the global south is already more affected by climate change and will likely more affected in the future as well. Lastly, respondents from Europe, Asia, and South America are more concerned about the potential of a third world war compared to those from other countries. With the ongoing conflicts between Russia and Ukraine, surrounding Israel and in Venezuela nearby it is of no surprise that these concerns are more present here.

18. Which country or entity, including both governments and individuals within that country, do you fear the most in terms of the potential for a cyberattack on your personal or organisational data?

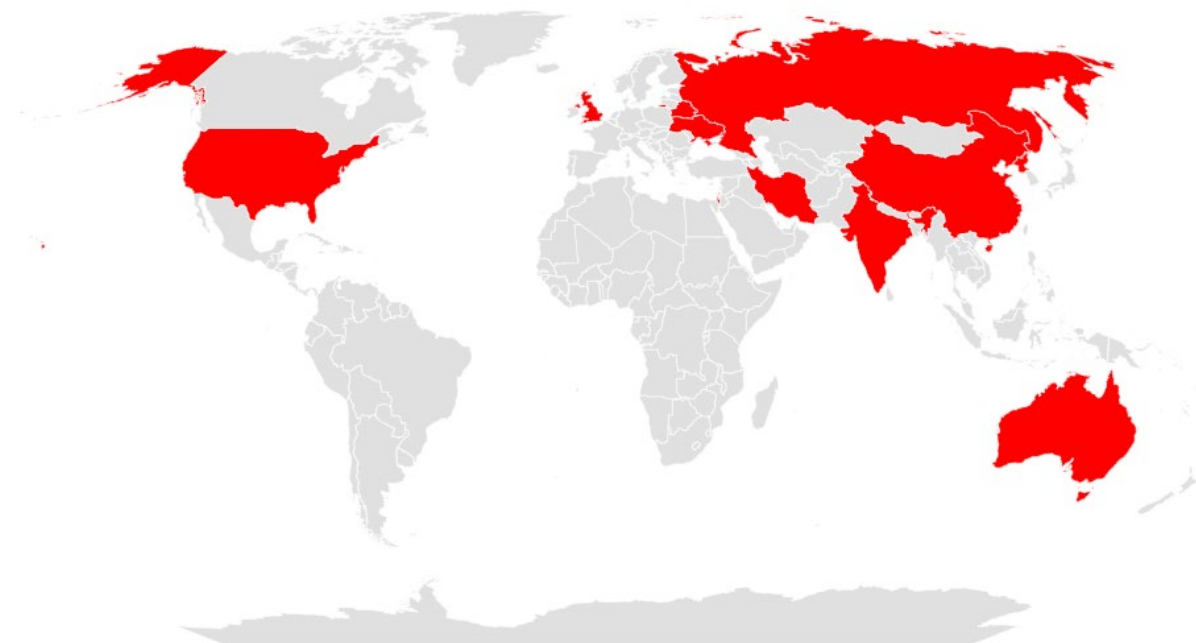


The survey reveals a geopolitical landscape⁸ of perceived cyber threats, as shown in the graph above. Russia tops the list, with 61% of participants identifying it as the primary source of concern for cyberattacks. China follows at 57%, while the USA is cited by 42% of respondents, respectively. These results reflect widespread concerns about the cyber capabilities of these nations⁹.

Interestingly, 24% of respondents cited their own country, reflecting concerns about domestic surveillance, data privacy laws, or mistrust in local governments and corporations¹⁰. This highlights awareness of internal threats and the impact of national policies on privacy and security. The list also includes North Korea, Israel, Iran, India, United Kingdom, Pakistan, and Turkey, representing diverse geopolitical powers and regions, each seen as contributing to global cyber tensions and uncertainties.

⁸ <https://www.av-comparatives.org/spotlight-on-security-politics-and-cyber-security-a-troubled-relationship/>
⁹ <https://www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/>
¹⁰ <https://www.av-comparatives.org/av-comparatives-explains-the-implications-of-takeovers-in-the-it-security-industry/>

Map of the top 10 most feared countries



Most feared countries by continent of respondent

Asia		Europe		North America		South America	
	China		Russia		Russia		China
	Russia		China		China		Russia
	USA		USA		North Korea		North Korea
	My own Country		North Korea		USA		USA
	North Korea		Israel		Israel		My own Country
	Australia		My own Country		My own country		Iran
	Israel		Iran		Iran		Israel
	India		Belarus		UK		India
	Iran		India		Ukraine		UK

Breaking down fears by continent, the survey reveals regional differences in threat perceptions. China is most feared in Asia and South America, while Russia tops the list in Europe and North America. Respondents rank their own countries between fourth and sixth. The four most feared countries - China, North Korea, Russia, and the USA - remain consistent across all regions. Factors like political relations, media coverage, historical cyber incidents, or geographic proximity likely shape these perceptions. For instance, North Americans fear China, while Asians fear their own countries, highlighting the complex and varied nature of cyber-threat perceptions globally.

Most feared countries by country of respondent

Brazil			China			France ¹¹			Germany		
	China	↑		China	≡		China	-		Russia	≡
	Russia	↓		USA	≡		Russia	-		China	≡
	USA	≡		Russia	≡		France	-		Germany	↑
	Brazil	≡		Australia	↑		USA	-		USA	≡
	North Korea	≡		Israel	≡		Iran	-		Iran	≡

India			Italy			UK			USA		
	China	≡		Russia	≡		Russia	≡		China	↑
	North Korea	↑		China	≡		China	≡		Russia	↓
	Pakistan	≡		USA	≡		USA	↑		USA	≡
	USA	↓		Italy	↑		UK	↑		Iran	↑
	Russia	≡		Israel	≡		Israel	↑		Israel	↑

The symbols behind each country's name indicates its position compared to last year. Among the eight countries with the most respondents, the top five most-feared countries consistently included China, Russia, and the USA. Except for India respondents also cited their own country as a source of concern. Significant changes Israel entering the top five most feared countries in the UK and USA, North Korea is no longer in the top five for Germany, Italy, UK, and USA. Australia also is now on the list of feared countries in China.

The survey underscores a global sense of vulnerability and concern over cyberattacks from various actors, reflecting awareness of the capabilities and historical actions of specific nations in the cyber domain. For governments, organizations, and individuals, understanding these perceptions is vital for shaping cybersecurity strategies, international policies, and cooperative efforts to mitigate threats and reassure the public. It also highlights the need for robust, transparent, and trust-building measures within countries to address domestic concerns about privacy¹² and cyber security.

¹¹ France was not included last year, therefore the annual comparison is not available

¹² <https://www.av-comparatives.org/data-transmission-in-consumer-security-products/>



Copyright and Disclaimer

This publication is Copyright © 2026 by AV-Comparatives®. Any use of the results, etc. in whole or in part, is ONLY permitted after the explicit written agreement of the management board of AV-Comparatives prior to any publication. AV-Comparatives and its testers cannot be held liable for any damage or loss, which might occur as result of, or in connection with, the use of the information provided in this paper. We take every possible care to ensure the correctness of the basic data, but a liability for the correctness of the test results cannot be taken by any representative of AV-Comparatives. We do not give any guarantee of the correctness, completeness, or suitability for a specific purpose of any of the information/content provided at any given time. No one else involved in creating, producing or delivering test results shall be liable for any indirect, special or consequential damage, or loss of profits, arising out of, or related to, the use or inability to use, the services provided by the website, test documents or any related data.

For more information about AV-Comparatives and the testing methodologies, please visit our website.

All emojis designed by [OpenMoji](#) – the open-source emoji and icon project. License: [CC BY-SA 4.0](#)

AV-Comparatives
(February 2026)