Independent Tests of
Anti-Virus Software

**AV**
comparatives

# IT Security Survey 2024

LAST REVISION: 1ST FEBRUARY 2024

WWW.AV-COMPARATIVES.ORG

# Security Survey 2024

We are proud to present our annual Security Survey for 2024. 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: **11th December 2023 – 31st December 2023**
Valid responses of real users: **1,350**

The survey, conducted over approximately two weeks, 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 a digital world constantly under the shadow of cyber threats, understanding user behaviour, preferences, and concerns is crucial to creating effective cybersecurity strategies. Our comprehensive survey taps into the experiences of global users, revealing insights into their digital lives. It indicates the operating systems and applications they use, the security measures they adopt, and the worries they may have about IT security.

We dive into a myriad of preferences influencing choices of browsers, operating systems, and security solutions. We also look at concerns regarding user privacy and the need for transparency and independence from all the entities that safeguard our digital domain.

The survey reveals a wide range of ages, expertise, and regional influences among participants, all of which influence user choices and concerns. Our enquiry indicates loyalty to certain operating systems, a rising preference for specific browsers, and various fears of cyberthreats influenced by regional and expertise factors.

This report acts as a means of understanding current cybersecurity perspectives from users worldwide. It lays the groundwork for further research. Our objective is to deliver more than statistics; we aim to provide insights and implications crucial for users, providers, and testers within the cybersecurity realm. We invite you to reflect on how these insights might impact your own cybersecurity strategies or practices.

The findings are derived from an Internet-based survey conducted by AV-Comparatives between 11th December 2023 and 31st December 2023, with the participation of 1,350 users across the globe, focusing on IT security. We hope the insights shared will help and guide you in your cybersecurity journey.
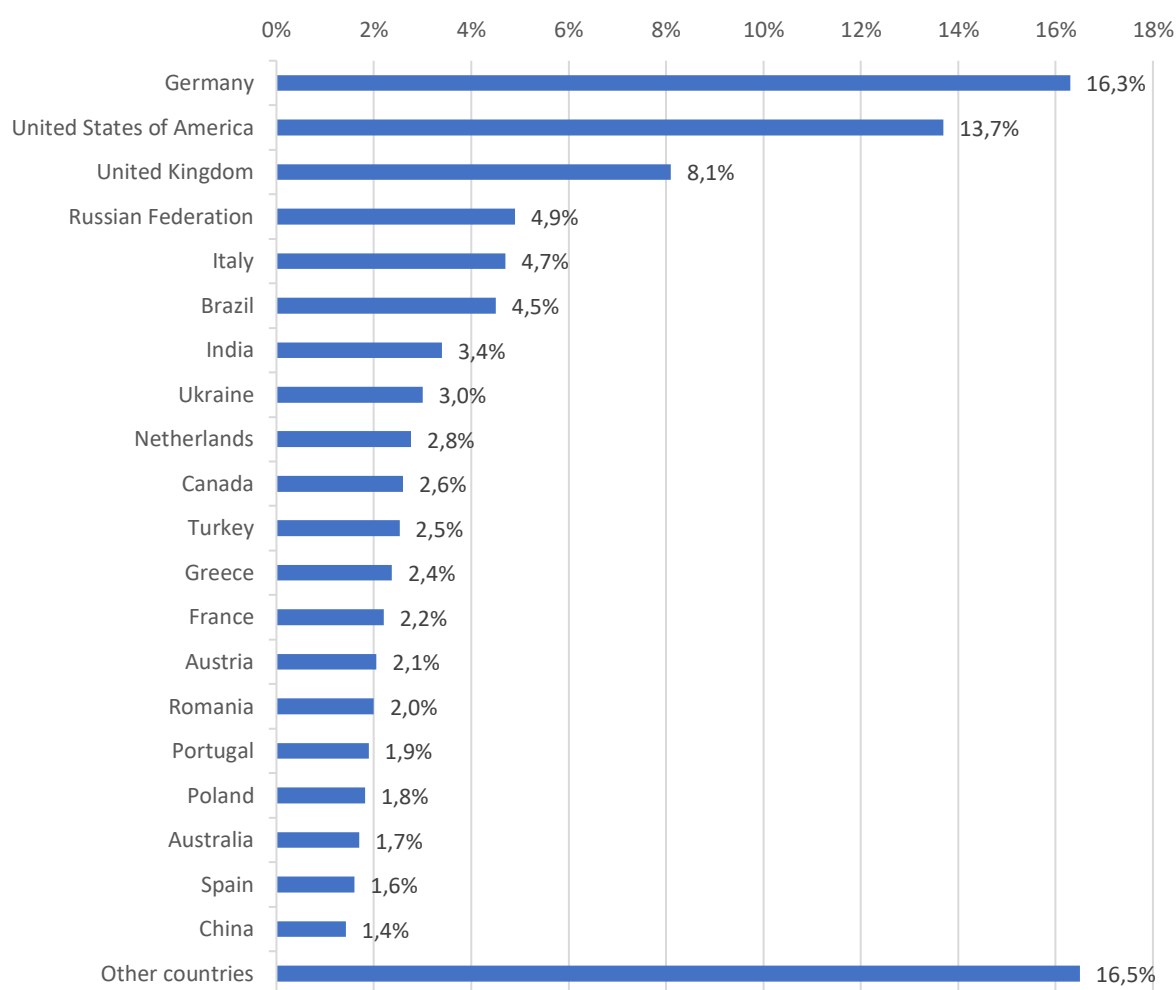
We extend our thanks to all who participated in the survey. Your feedback is invaluable and will be used to enhance the effectiveness and relevance of our tests. This, in turn, empowers manufacturers to refine their products, benefiting both the industry and users. We are also delighted to note that our test results are frequently cited by other publications in their security product reviews. Please note that all of AV-Comparatives' public test results are freely accessible at www.av-comparatives.org, ensuring transparency and widespread availability.
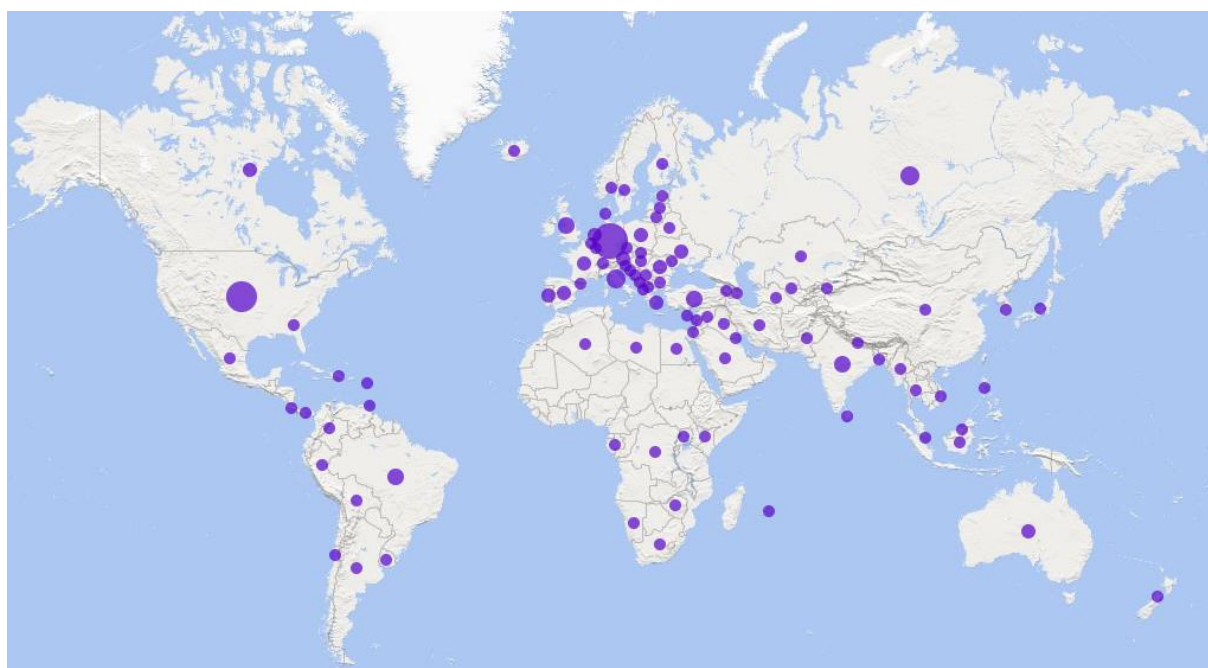
**Key results**

The Key findings or 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***: Survey participants came from all over the globe. Germany had the most respondents from a single country, followed by the United States and the United Kingdom.
2. ***Age of Respondents***: The youngest and oldest age groups had the fewest respondents, with the 25-34 category providing the most.
3. ***Level of expertise***: Getting on for half of the participants described themselves as Advanced Users, with Intermediate Users and Professionals/Experts each accounting for about a quarter.
4. ***Free vs Paid Security Solutions***: over two-thirds of survey participants paid for their chosen desktop security programs.
5. ***Operating System Preferences***: A majority now seem to prefer Windows 11 over Windows 10, with older Windows versions generally used more by non-expert users.
6. ***Browser Preferences***: Mozilla Firefox has overtaken Google Chrome as the most preferred browser, perhaps due to additional features and security aspects.
7. ***Mobile OS Trends***: Android dominates globally, except in North America, where iOS holds an almost equal market share. Younger generations show a higher preference for iOS.
8. ***Change of Mobile OS***: Most respondents said they were staying with their current mobile OS, with only a few switching from Android to iOS or vice versa (about 6% in each case).
9. ***VPN solutions***: Over a third of participants did not use a VPN, while those that do had a wide range of preferred products.
10. ***Password Managers***: Password-management products were used by about 6 out of 10 respondents, whereby advanced users were more likely to employ them.
11. ***Parental Control Software***: This is something of a niche market, with only about 1 in 10 participants making use of it. The Android-integrated Google Family Link was the most popular product amongst those that do so.
12. ***Mobile Anti-Malware Products***: Bitdefender, ESET and Kaspersky were the most popular mobile AV solutions worldwide. Over half of respondents use a mobile security program.
13. ***Desktop Security***: Users primarily rely on a select few reputable manufacturers for anti-malware products, with Bitdefender, Kaspersky, Microsoft, and ESET being the most favoured worldwide.
14. ***AV Trial versions***: almost two thirds of survey respondents used a free trial before purchasing an anti-virus product, with younger users being significantly more likely to do so than older ones.
15. ***Most-Requested Consumer Desktop AV Products for Testing***: Unsurprisingly, there was a very strong correspondence between the most commonly used desktop security solutions, and those which respondents wanted to see tested; the top 9 products in each case were identical.
16. ***Most-Requested Business Desktop AV Products for Testing***: the top 5 most-requested products here were from vendors that are popular in the consumer market too.
17. ***Concerns Over Cyber Threats***: Ransomware, malware, data breaches, and password compromises are top concerns, with notable fears about tracking and big tech corporations.
18. ***Perception of Cyber Threat Actors***: China, Russia and the USA are perceived as the top three potential sources of cyberattacks (by either governments or individuals), reflecting geopolitical concerns.
19. ***Testing Lab Credibility***: Independence, transparency, and free access to comprehensive test reports are critical for users in deeming a testing lab credible.
20. ***Information Sources for Test Results***: The most trusted sources are established testing labs with over 20 years of experience in the field of AV testing, with preferences varying by age and technical proficiency.

## 1. Where are you from?

| Country | Percentage |
|---------|-----------|
| Germany | 16,3% |
| United States of America | 13,7% |
| United Kingdom | 8,1% |
| Russian Federation | 4,9% |
| Italy | 4,7% |
| Brazil | 4,5% |
| India | 3,4% |
| Ukraine | 3,0% |
| Netherlands | 2,8% |
| Canada | 2,6% |
| Turkey | 2,5% |
| Greece | 2,4% |
| France | 2,2% |
| Austria | 2,1% |
| Romania | 2,0% |
| Portugal | 1,9% |
| Poland | 1,8% |
| Australia | 1,7% |
| Spain | 1,6% |
| China | 1,4% |
| Other countries | 16,5% |

The graph above shows the top 20 countries of origin of our survey participants. Altogether, respondents came from 97 different countries. Respondent countries are shown on the map below:

## 2. How old are you?

The survey results show a diverse age range of participants from across the continents. The youngest group, those aged 24 years or younger, comprises a minor 6.4% of the total. The most significant proportion of respondents falls within the 25-34 age bracket, representing 23.1%. The following age groups, 35-44 and 45-54, account for similar percentages of 19.8% and 20.5%, respectively, indicating a consistent distribution across middle-aged participants. Those aged 55-64 make up 18.3% of the total, while the oldest group, 65 years or older, accounts for 11.9%.
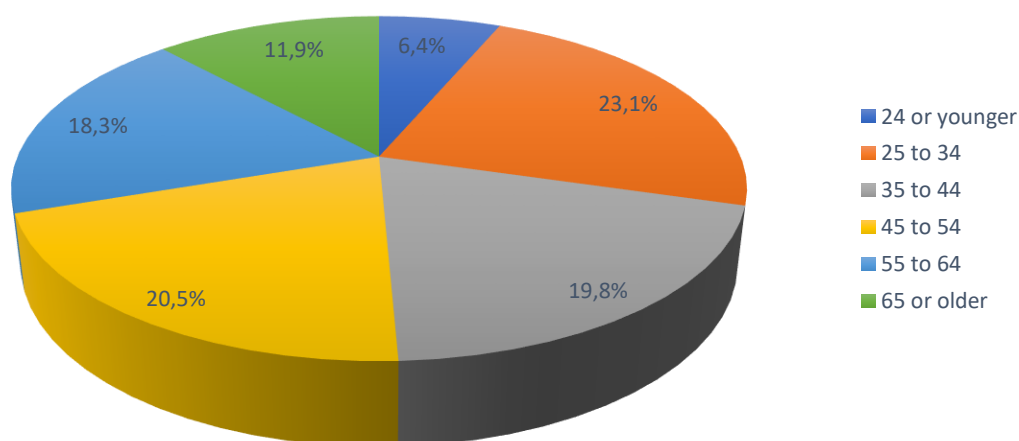


Age distribution overall is shown above and by continent below. Geographically, North America stands out with the oldest age profile, where 52% of participants are older than 55 years. This contrasts with Asia and South America, where the majority of respondents fall into the younger 25-34 age bracket, each with approximately 41%. Europe displays a dominance of the middle-age groups, with about 49% of participants aged between 35 and 54.
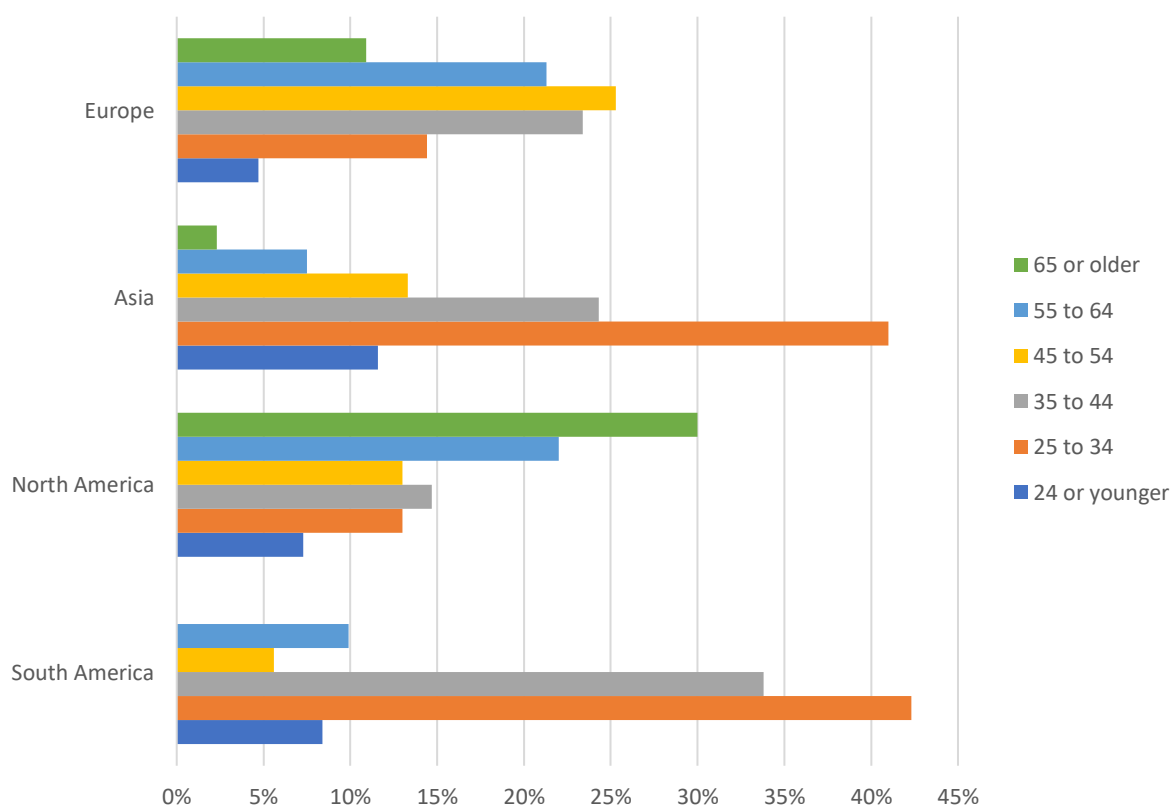
### 3. How would you rate your level of expertise in using computers?

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:
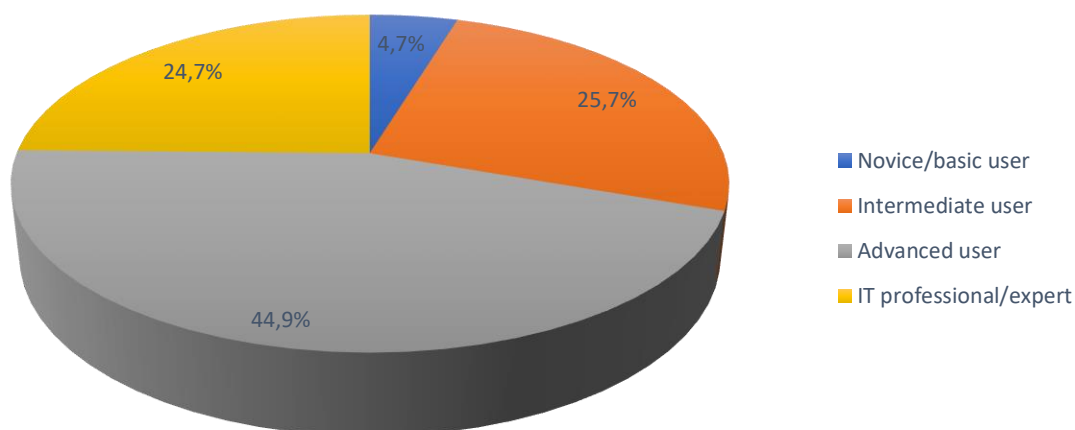


A small segment of the participants, 4.7%, considered themselves to be novice/basic users, indicating minimal familiarity or comfort with computer technology. This is significantly exceeded by those identifying as intermediate users, who made up 25.7% of the respondents. These individuals likely possess a solid understanding and capability in utilising standard computer functions and applications.

The largest group, comprising 44.9%, classified themselves as advanced users. These participants are presumably adept with a broad range of computer functionalities and may possess specialised skills in various aspects of software and/or hardware. Lastly, 24.7% of the respondents consider themselves IT professionals or experts, indicating a high degree of proficiency and likely involvement in computing as a significant aspect of their career or daily life.

The distribution highlights a predominance of computer-savvy individuals within the participant pool, with a substantial portion possessing advanced skills or professional expertise. This may account for survey respondents' preferences differing from the general public's when it comes to, e.g. choice of operating system or browser.

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



31,1%

68,9%

- Paid (commercial) security solution
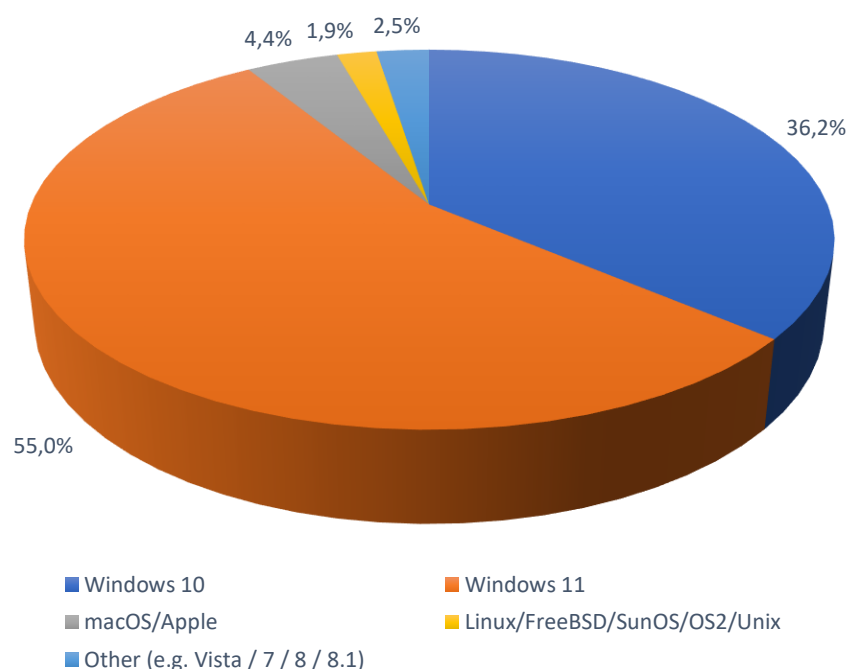- Free security solution
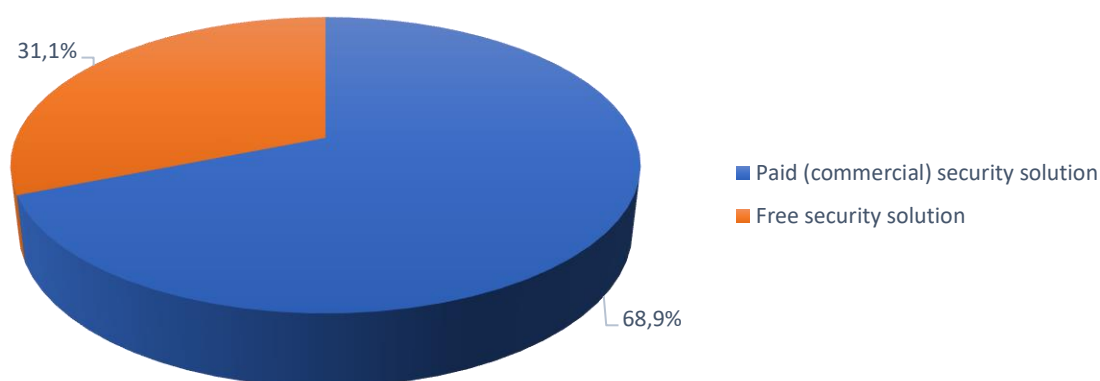
The survey's inquiry into the types of desktop security solutions used by participants reveals a clear preference for paid/commercial products over free security solutions, as shown in the chart above. Specifically, 68.9% of respondents utilise paid/commercial security solutions, while the remaining 31.1% opt for free versions.

Interestingly, there is a noticeable age-related trend in the preference for security solutions. Younger users, particularly those 24 years or under, are more inclined towards free security solutions, with about 39% utilising them. On the other hand, only 22% of the older generation, those above 55, opt for free versions. This could be attributed to various factors, including financial priorities, risk perception, or the level of digital assets requiring protection.

Moreover, the survey indicates a correlation between the users' self-assessed computer expertise and their choice of security solution. Novice to intermediate users are almost evenly split, with 45% using free solutions and 55% opting for commercial products. In contrast, advanced to expert users predominantly prefer commercial solutions, with 74% utilising paid security options. This might suggest that as users become more knowledgeable and proficient with computers, they may recognise the value and necessity of more comprehensive, paid security solutions to protect against sophisticated threats.

## 5. Which desktop operating system do you primarily use?



- ■ Windows 10
- ■ Windows 11
- ■ macOS/Apple
- ■ Linux/FreeBSD/SunOS/OS2/Unix
- ■ Other (e.g. Vista / 7 / 8 / 8.1)

The survey's results for desktop operating system preferences among participants – illustrated in the chart above – show a strong inclination towards Windows (93.7%). Specifically, 36.2% of respondents are using Windows 10, while a majority – 55% – have adopted Windows 11, marking it as the most widely used operating system version. This is particularly notable as it significantly exceeds the general[1] public's adoption rate of Windows 11, which stands at about 27%, suggesting that the survey's audience is more tech-oriented and quicker to embrace newer technologies.

Only a small fraction, 4.4%, use macOS, indicating a niche presence within the participant pool. This user base is slowly expanding, perhaps reflecting broader industry trends or a shift in user preferences. Linux, an open-source platform predominantly favoured by tech enthusiasts, is used by 1.9% of respondents, while other operating systems, including older versions of Windows like 7 and 8, account for 2.5%. Notably, all Windows versions before Windows 10 have reached the end of support[2]. Yet, they still persist among not quite 3% of users, primarily among novice/basic users who may not understand the security implications of using outdated systems.

The survey also reveals that IT professionals are more likely to use macOS, suggesting a preference for this system in certain professional circles. Our review/test of Mac security products[3] is available at https://www.av-comparatives.org/consumer/testmethod/mac-security-reviews/

At AV-Comparatives, we plan to use Windows 11 as the primary operating system for our 2025 tests, if the global market share statistics suggest that it is the most widely used Windows version by then. Additionally, Microsoft is only providing mainstream support for Windows 10 until October of 2025 (although it will provide paid-for security updates for a further three years[4]).
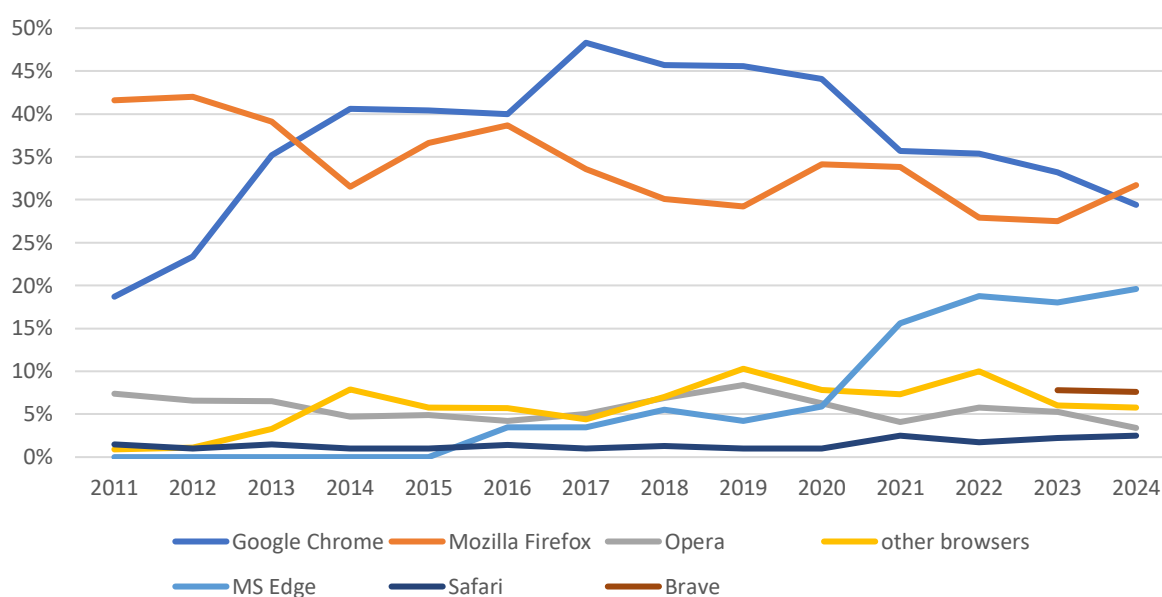
---

[1] https://gs.statcounter.com/os-version-market-share/windows/desktop/worldwide
[2] https://www.microsoft.com/en-us/windows/end-of-support
[3] A list of Mac security products can be found here: https://www.av-comparatives.org/list-of-av-vendors-mac/
[4] 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 shown in the diagram above, Google Chrome is used by 29.4% of respondents. It had long been the most popular browser in our survey but has now narrowly been surpassed by Mozilla Firefox, which 31.7% of the survey participants prefer, marking a shift towards this browser. Microsoft Edge has secured a solid position as well, with 19.6% of users employing it.

This evolving browser landscape suggests a diversification of preferences among users, possibly driven by different factors such as performance, privacy concerns, or specific feature sets. The results also show the increasing relevance of the Brave browser, which 7.6% of respondents use, outpacing other options like Opera, Safari, Vivaldi, Yandex, and DuckDuckGo. This underscores a rising interest in privacy-focused browsing options among a segment of the audience.

As statistics suggest that Google Chrome is still by far the most popular browser among the general public, accounting for nearly two-thirds of all users, we at AV-Comparatives continue to use this browser in our tests.

The data reveals a distinction in browser preferences based on user expertise. Novice and basic users predominantly stick with Google Chrome, representing 51% of this demographic's choice. In contrast, more advanced users lean towards Mozilla Firefox, aligning with the overall trend of Firefox's popularity in the survey. This might reflect the advanced users' preference for customisation, privacy, or specific functionalities that Firefox offers.

In the context of macOS users, Safari stands out as the overwhelming choice for 59% of the respondents, followed by Chrome at 23% and Firefox at 12%. This preference for Safari among Mac users is likely due to its seamless integration with the Apple ecosystem, performance optimisations, and consistent user experience across Apple devices.

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

## 7. Which mobile operating system do you use?
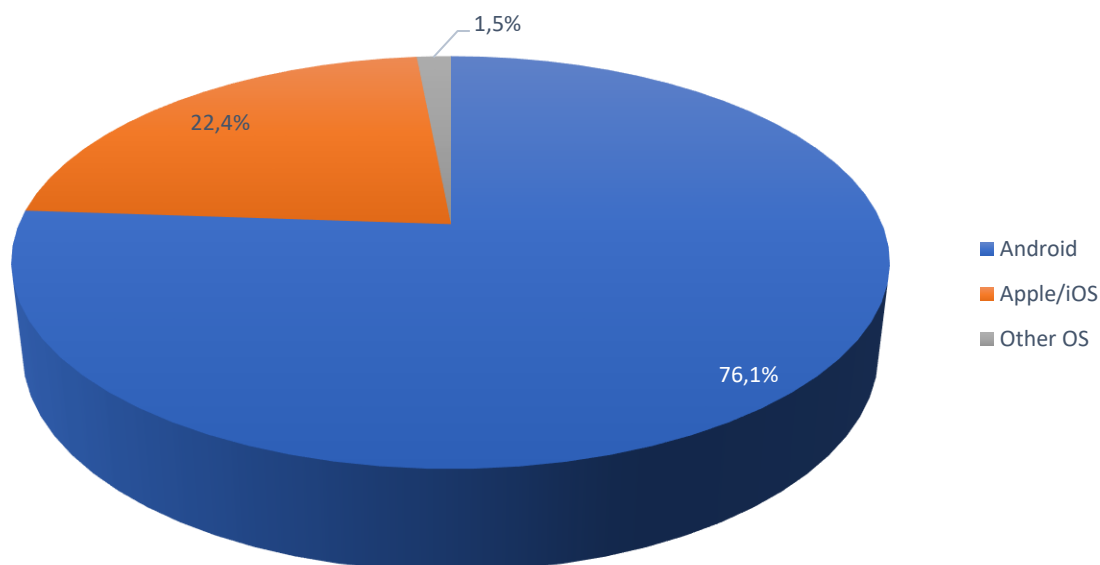


The survey provides an insightful overview of the mobile operating system preferences among participants. As illustrated in the above chart, it reveals a predominant worldwide preference for Android, which accounts for approximately 76% of users. This widespread adoption underscores Android's accessibility and diverse ecosystem, offering a wide range of devices across various price points.

Regionally, preferences diverge notably. In North America, iOS gains a stronger foothold, accounting for about 47% of users, suggesting a competitive balance between Android and iOS in this market. This is contrasted sharply with Asia and South America, where Android dominates with about 81% usage among participants. Such regional disparities might reflect economic factors, brand preferences, political issues, or varying levels of market penetration by the respective operating system providers. The survey also indicates a generational divide in mobile OS preferences. Younger generations show a higher inclination towards iPhones, with 33% using iOS compared to 22% among older generations. This could be attributed to various factors, including brand perception, user interface preferences, or the appeal of Apple's ecosystem among younger users.

Furthermore, a correlation is observed between the level of technical expertise of users and their choice of mobile operating system. Advanced and professional users tend to prefer iPhones more, with 31% using iOS, compared to only 10% among basic and novice users. This preference could stem from considerations of security features[5], build quality, or specific functionalities that appeal to more tech-savvy individuals.

Our Mobile (Android)[6] security review/test report is available at https://www.av-comparatives.org/consumer/testmethod/mobile-security-reviews/

---

[5] https://www.av-comparatives.org/mac-vs-windows-is-apple-really-more-secure/
[6] An overview of security products for Android can be found here: https://www.av-comparatives.org/list-of-mobile-security-vendors-android/

8. **Have you switched from an Apple iOS-based mobile device to an Android-based device, or vice versa, within the past 12 months, or do you plan to make such a switch in the next six months?**
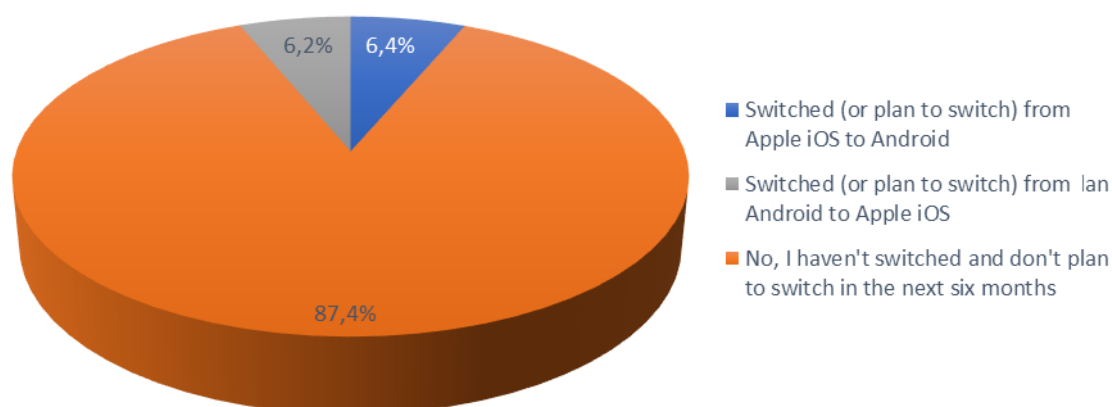


The survey sought to understand the fluidity or loyalty among users towards their mobile operating systems by inquiring about recent or upcoming switches between Apple iOS and Android-based devices. The findings, shown in the chart above, reveal a significant tendency towards consistency and loyalty among users, with 87.4% stating that they haven't switched and don't plan to switch in the next six months. This high percentage indicates a strong sense of satisfaction or comfort with their current choice, possibly due to familiarity, investment in the ecosystem, or the perceived hassle of switching.

Among those considering a change, 6.4% of respondents have switched or plan to switch from Apple iOS to Android. Conversely, a nearly equivalent proportion, 6.2%, report moving or intending to move from Android to Apple iOS. These similar percentages suggest a relatively balanced flow between the two ecosystems, with personal preferences, changing needs, or evolving device offerings likely influencing users' decisions to switch.

The relatively low percentage of users switching indicates that most individuals are content with their current mobile operating systems and the ecosystems they have invested in. Factors such as app availability, user interface, device compatibility, and brand loyalty may all contribute to this high rate of allegiance.

Understanding the stability in users' choice of operating systems can be crucial for developers, marketers, and manufacturers, as it highlights the importance of user retention strategies and the potential challenges of persuading users to switch. The data reflects the competitive nature of the mobile market, and the need for continuous innovation and customer satisfaction to maintain or grow market share. It also suggests that while users may be open to switching for compelling reasons, there is a significant inherent inertia to overcome due to the established loyalty towards their current operating system.

## 9. Which VPN solution do you primarily use?

The most popular VPN programs are listed below in order of preference:

1. Proton VPN
2. NordVPN
3. Kaspersky VPN
4. Windscribe
5. Bitdefender VPN
6. VPN of my employer/company OR self-hosted VPN
7. F-Secure Freedome
8. Avast SecureLine
9. Mullvad
10. SurfShark
11. ExpressVPN
12. CyberGhost
13. Avira Phantom VPN
14. Private Internet Access
15. Cisco AnyConnect

The survey delved into the usage of Virtual Private Networks (VPNs) among participants to understand the preferences for these online privacy and security solutions. It is notable that 36% of respondents do not use any VPN, possibly due to lack of perceived need, trust in their existing network security, or unfamiliarity with the technology.

For those who do use VPNs, the preferences vary, with Proton VPN leading as the most popular choice, possibly as it has a free version. Following closely are NordVPN and Kaspersky VPN, which both have large networks of servers, while Windscribe and Bitdefender VPN also make the list.

An interesting insight is the usage of employer/company-provided VPNs or self-hosted solutions, reflecting the needs of remote workers or those who prefer a more personalised or controlled security approach. This category ranks 6th, indicating a significant number of users rely on VPNs for professional or customised use. It should be noted that employer/company-provided VPNs have the principal function of allowing remote users to access their organisation's local network resources as if they were sitting at a computer in the office. This is in contrast to the other functions of VPNs – ensuring data privacy and overcoming geolocation restrictions – that appeal to the average private user.

The list continues with other reputable VPN services like F-Secure Freedome, Avast SecureLine, Mullvad, SurfShark, ExpressVPN, CyberGhost, Avira Phantom VPN, Private Internet Access, and Cisco AnyConnect. This diverse range shows that users have distinct preferences, possibly influenced by specific features, pricing, or recommendations. Additionally, some of the vendors produce security suites with anti-virus and other security functions. Users of these suites may well be inclined to use a VPN solution from the same vendor.

These findings underline the varied landscape of VPN usage and preferences among tech-savvy individuals. It also highlights the importance of privacy and security in the digital space, with users seeking different solutions that fit their specific needs, be it for personal security, bypassing geo-restrictions, or ensuring safe and private work connections.

At AV-Comparatives, we have conducted tests of a wide range of VPN products, the reports of which are available here:
https://www.av-comparatives.org/wp-content/uploads/2020/05/avc_vpn_2020.pdf
https://www.av-comparatives.org/wp-content/uploads/2021/06/avc_vpn_android_test_2021.pdf

## 10.    Which password manager solution do you primarily use?
The most popular password managers are listed below in order of preference:

1. Bitwarden
2. KeePass
3. 1Password
4. LastPass
5. Kaspersky Password Manager
6. Bitdefender Password Manager
7. Sticky Password Manager
8. Norton Password Manager
9. ESET Password Manager
10. RoboForm Everywhere
11. ProtonPass
12. Dashlane
13. NordPass
14. McAfee True Key
15. Keeper

Password manager apps enable the use of multiple complex passwords without the user having to remember them all while providing extra security features at the same time.

The survey reveals a notable dichotomy in cybersecurity habits among participants. While 38% do not use any password manager, indicating a potential gap in personal cybersecurity practices, the remaining majority utilise a variety of password management solutions, reflecting an awareness of the importance of securing personal credentials.

There is a clear trend correlating users' technical proficiency with the likelihood of using a password manager. Among basic to intermediate users, just over half (52%) utilise a password manager. Among advanced to professional users, a significant 76% employ a password manager, suggesting that as users become more aware of cybersecurity risks and complexities, they tend to adopt tools to manage them.

Bitwarden leads as the most preferred password manager, followed by KeePass. Both of these are open-source solutions, suggesting trust in the open-development process. Commercial options like 1Password and LastPass are also popular.

Other noted password managers include Kaspersky Password Manager, Bitdefender Password Manager, Sticky Password Manager, Norton Password Manager, ESET Password Manager, and RoboForm Everywhere, each with its unique features and user base. Some users opt for solutions like ProtonPass, Dashlane, NordPass, McAfee True Key, and Keeper, reflecting the diverse needs and preferences when it comes to managing digital credentials.

Some of the vendors in the list produce complete security suites with anti-virus and other security functions. Users of such suites may decide to stay with the same vendor for password management.

These findings highlight the role of password managers in contemporary digital security practices. They also point to the need for continued education and awareness efforts to bridge the gap among those who do not use these tools, particularly given the increasing complexity and number of online accounts individuals manage today.

## 11.    Which parental control solution do you primarily use?

The most popular parental control apps are listed below in order of preference:

1. Google Family Link
2. Kaspersky SafeKids
3. ESET Parental Control
4. Norton Family
5. Apple ScreenTime
6. McAfee Safe Family
7. SafeDNS
8. FamilyTime
9. Qustodio
10. Circle Home Plus

Parental control software is obviously a special case among the software solutions asked about in the survey, in that is not concerned with computer security or data privacy as such. It is obviously only applicable to the parents/guardians of children in certain age groups, who have differing opinions as to whether they should block their children's Internet access to any adult topics or electronically control their device usage time. Hence it is perhaps not surprising that the great majority of survey participants, 89%, do not use any form of parental control software. However, among those who do use parental control programs, novice and basic users are the primary adopters, with 39% of them utilising these tools.

Google Family Link leads the list of preferred parental control applications, likely due to its direct integration with Android devices and its no-cost entry point. Kaspersky SafeKids, ESET Parental Control and Norton Family are also popular, suggesting trust in established cybersecurity brands for managing family safety. Apple ScreenTime is notable as well, being integral to the iOS ecosystem, highlighting the role of operating system-based solutions in parental controls.

McAfee Safe Family, SafeDNS, FamilyTime, Qustodio, and Circle Home Plus round out the list. This variety indicates diverse needs and preferences among users when it comes to protecting and managing their family's digital experience.

AV-Comparatives conducts Parental Control Tests, the reports of which are available here:
https://www.av-comparatives.org/testmethod/parental-control-reviews/

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

The survey's insights into the use of mobile anti-malware security solutions reveal a notable split in cybersecurity habits across different user demographics. Overall, 43.5% of respondents do not use any security solution on their mobile phones. This sizable portion might reflect a combination of trust in built-in security features, a lack of awareness of mobile threats, or perhaps a perceived inconvenience of additional security software.

Interestingly, the propensity to forgo mobile security solutions is highest among IT professionals, with 49% not using any. This could be due to their higher level of expertise and confidence in managing mobile risks manually, or a preference for minimalistic, unobstructed device performance. Conversely, only about 19% of novice/basic users do not use any security solution, indicating a reliance on additional protective measures perhaps due to lower confidence or understanding of built-in security features.

Worldwide, the ten most commonly used manufacturers of mobile security products are, in decreasing order: Bitdefender, Kaspersky, ESET, Avast, Norton, McAfee, F-Secure, AVG, Sophos and Trend Micro.

The list below shows the 10 most popular mobile security manufacturers used by survey participants, according to continent. There were not enough responses from some regions to produce significant results. Therefore, Australia/Oceania and Africa are not shown.

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

Bitdefender, ESET and Kaspersky were among the most popular mobile security products in all 4 regions.

Major security products for mobiles were reviewed by AV-Comparatives in a report[7] in 2023.

---

[7] https://www.av-comparatives.org/testmethod/mobile-security-reviews/

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

Worldwide, the twelve manufacturers of anti-malware products for Windows platforms most commonly used by survey participants are (in this order): Bitdefender, Kaspersky, Microsoft, ESET, Avast, Norton, F-Secure, McAfee, Avira, Panda, Trend Micro and G Data.

On all 4 continents with significant results, the same 4 vendors can be found in the top 4 places. These are (alphabetically): Bitdefender, ESET, Kaspersky and Microsoft. Bitdefender now takes first place in Europe, as well as in North America. Kaspersky has dropped to second place in Europe, after taking the number one place there for many years. However, it 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.  Bitdefender | 1.  Bitdefender | 1.  Kaspersky | 1.  Kaspersky |
| 2.  Kaspersky | 2.  ESET | 2.  ESET | 2.  Microsoft |
| 3.  Microsoft | 3.  Microsoft | 3.  Bitdefender | 3.  Bitdefender |
| 4.  ESET | 4.  Kaspersky | 4.  Microsoft | 4.  ESET |
| 5.  Avast | 5.  Avast | 5.  Avast | 5.  Avast |
| 6.  Norton | 6.  Malwarebytes | 6.  McAfee | 6.  Norton |
| 7.  F-Secure | 7.  Norton | 7.  Norton | 7.  Malwarebytes |
| 8.  Avira | 8.  McAfee | 8.  F-Secure | 8.  McAfee |
| 9.  AVG | 9.  F-Secure | 9.  AhnLab | 9.  Panda |
| 10. G Data | 10. AVG | 10. K7 | 10. Avira |
| 11. McAfee | 11. Panda | 11. Dr.Web | 11. AVG |
| 12. Panda | 12. Avira | 12. Huorong | 12. Comodo |

### 14.    Do you typically use a trial version before purchasing an anti-virus product?
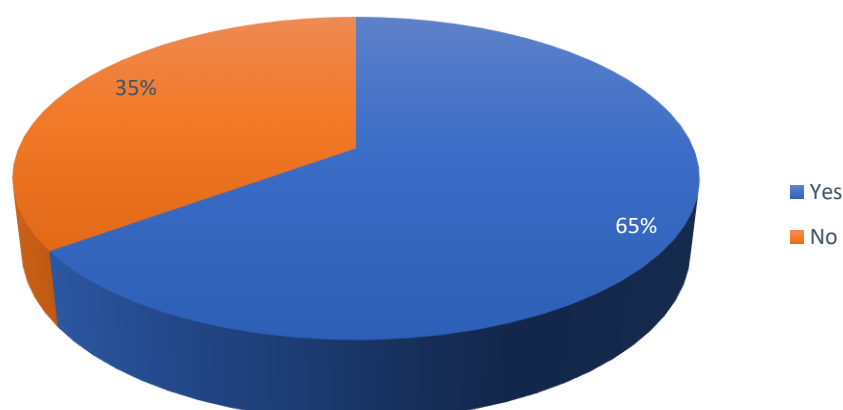


As shown in the chart above, the survey's exploration into the buying behaviours related to anti-virus products reveals a strong preference for 'try before you buy' among participants. A significant majority, 65% report typically using a trial version before committing to a purchase. This cautious approach indicates users' desire to personally test and evaluate an anti-virus product's effectiveness, user experience, and compatibility with their specific needs and systems before making a financial commitment.

Notably, the inclination to use trial versions varies with age. Younger individuals are more likely to engage with trial versions, with about 77% of this demographic sampling products before purchase. This trend might be attributed to several factors, including younger users' familiarity with technology options, their comfort in installing and uninstalling digital products, or possibly tighter budget constraints.

Conversely, only about 46% of older users (65+) opt for trial versions before purchasing, suggesting a more decisive or traditional approach to buying, possibly influenced by brand loyalty, a desire for simplicity, or a less experimental attitude towards technology.

These findings underscore the importance of offering trial versions in the anti-virus product market, as they appear to be a critical factor in the purchasing decision for a majority of users, particularly among the younger generation. For antivirus vendors, providing easily accessible, user-friendly, and fully-featured trials can be an effective way to demonstrate value and build trust with potential customers.

Understanding this situation can positively guide marketing strategies and product development, ensuring that offerings align with the varying preferences and behaviours of users. This approach can help in converting trial users into long-term customers, fostering loyalty and satisfaction through first-hand positive experiences with the product. Unfortunately, more and more AV vendors have started making trial versions less accessible by requesting payment or other information[8]. We regard this as a backwards step.

---

[8] https://www.av-comparatives.org/tests/summary-report-2023/

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

## 16.    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.  Bitdefender
2.  Kaspersky
3.  ESET
4.  Microsoft
5.  Avast
6.  Sophos
7.  Trend Micro
8.  Malwarebytes
9.  CISCO
10. CrowdStrike
11. G Data
12. Broadcom (Symantec)
13. Check Point
14. Fortinet
15. Trellix
16. WithSecure
17. SentinelOne
18. Palo Alto Networks
19. VMware Carbon Black
20. WatchGuard

Most of the popular vendors are usually included in at least some of our public tests and reviews of consumer and business software[9], while most of the other vendors commission separate tests and/or participate privately in certain tests.

---

[9] Consumer: https://www.av-comparatives.org/consumer/
   Enterprise: https://www.av-comparatives.org/enterprise/

## 17.　What are your 5 greatest concerns regarding online security and privacy? Please select up to 5 options that most align with your fears:

| Concern | Percentage |
|---|---|
| Ransomware attacks | 67,2% |
| Malware and viruses | 65,0% |
| Password leaks and compromise | 63,7% |
| Data leaks and breaches | 62,0% |
| Tracking, targeted ads, and spying by big tech corporations | 37,4% |
| Social engineering attacks (phishing, scams) | 34,7% |
| Lack of online anonymity | 26,6% |
| Impersonation by AI or deepfake technology | 25,6% |
| Digital money theft (e.g., cryptocurrency wallets) | 19,0% |
| Cyber extortion | 18,8% |
| Cyberwarfare and state-sponsored attacks | 17,3% |
| Internet of Things (IoT) vulnerabilities | 16,3% |

The survey's exploration of the greatest concerns regarding online security and privacy (overall results shown above) reveals a wide array of fears, with some issues standing out significantly among participants. The top concern is ransomware attacks, with 67.2% of respondents identifying it as a major fear. This is closely followed by worries about malware and viruses (65.0%) and password leaks and compromise (63.7%). Data leaks and breaches also feature prominently in user concerns, with 62.0% of respondents highlighting them. These top concerns reflect a general apprehension about the immediate, disruptive impacts of cyber threats on personal data and device integrity.

Tracking, targeted ads, and spying by big tech corporations concern 37.4% of participants, indicating a growing awareness and unease about personal privacy and data use in the digital age. Social engineering attacks, such as phishing and scams, are also a significant worry for 34.7% of users, showcasing the recognition of more sophisticated, human-targeted cyber threats.

Less prevalent but still notable concerns include lack of online anonymity, impersonation by AI or deepfake technology, digital money theft (including cryptocurrency wallets), cyber extortion, cyberwarfare and state-sponsored attacks, and Internet of Things (IoT) vulnerabilities. Each of these reflects specific anxieties about the evolving landscape of digital threats and the increasing sophistication and reach of potential attackers.

The survey also reveals differences in concern based on user expertise and geographic location. Professionals and experts are more worried about data leaks and breaches as well as password leaks and compromise, very possibly because they have little control over these things. Novice and intermediate users express higher concern for more direct threats like ransomware and malware/viruses, perhaps because they recognise their own lack of expertise when it comes to defending against such threats.

Geographically, Asia shows heightened concern for data leaks, whereas Europe and South America are particularly worried about ransomware. North America stands out for its concern over data leaks and a relatively higher worry about cyberwarfare compared to other continents, possibly reflecting the geopolitical situation or exposure to media reporting on state-sponsored activities.

Despite the variance in specific fears, no significant differences among age groups are noted, suggesting a universal understanding and concern for online security and privacy threats across this demographic.

Users' concerns about the many types of cyber-threat deserve to be taken seriously, and have implications not only for the individuals themselves, but for security vendors and organisations, as well as governments and other authorities. We suggest that a better public understanding of such threats can only help, by ensuring that everyone takes whatever steps they can to minimise security risks, and promoting the best use of public and private resources to take effective action against the greatest dangers.

**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?**

| Country | Percentage |
|---------|-----------|
| Russia | 35,0% |
| China | 25,4% |
| USA | 16,5% |
| My own country | 7,5% |
| North Korea | 2,8% |
| Ukraine | 2,5% |
| Israel | 1,7% |
| Iran | 1,6% |
| India | 1,2% |
| Brazil | 1,1% |
| Other | 4,7% |
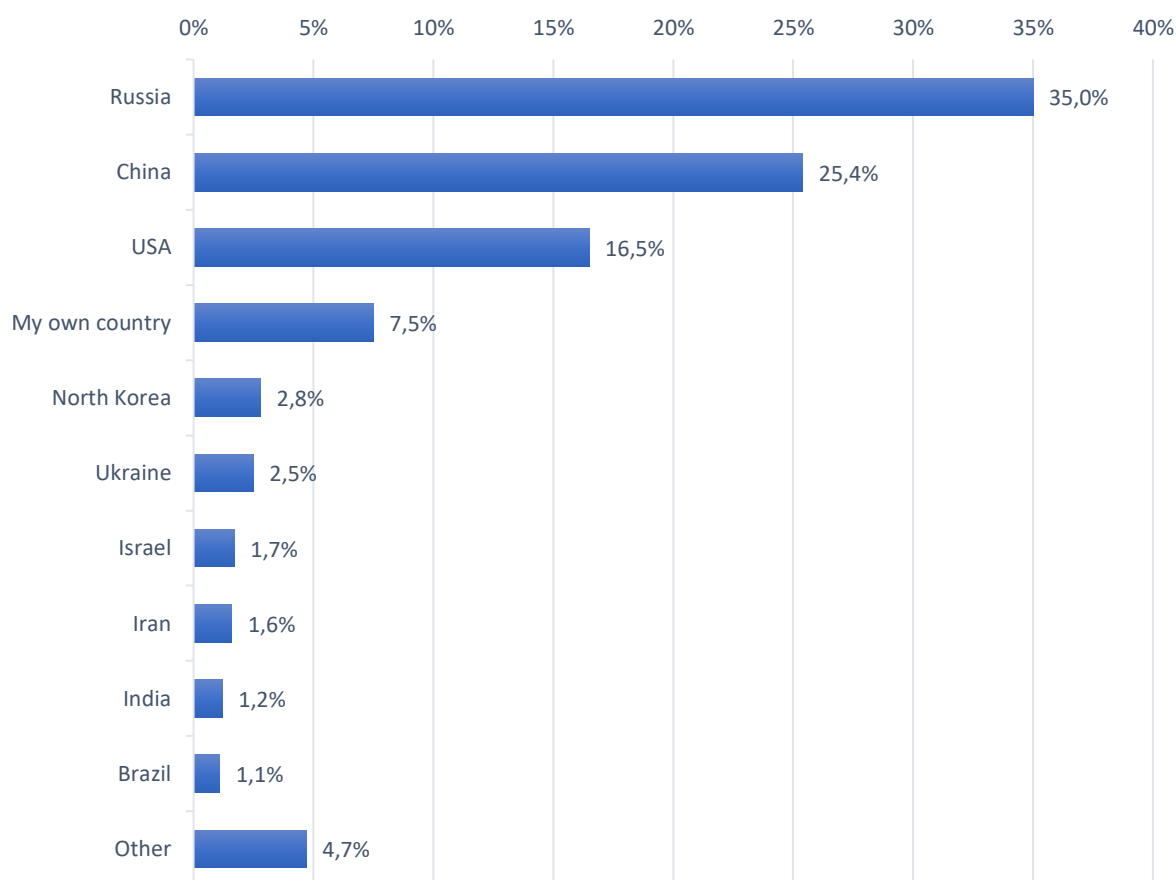
The survey's question about which country or entity respondents fear most in terms of potential cyberattacks on their personal or organisational data reveals a geopolitical[10] landscape of perceived cyber threats, illustrated in the graph above. Topping the list is Russia, with 35% of participants identifying it as the primary source of concern for cyberattacks. This is followed by China with 25.4% and the USA with 16.5%, reflecting widespread apprehensions about the cyber-attack capabilities coming from these nations[11].

Interestingly, 7.5% of respondents fear their own country the most, underlining concerns about domestic surveillance, data privacy laws, or mistrust in local government and corporate entities[12]. This self-referential fear is particularly poignant and indicates an awareness of the potential for internal threats and the impact of national policies on individual privacy and security.

The list continues with North Korea, Ukraine, Israel, Iran, India, and Brazil, each associated with various levels of cyber capability and international reputation in digital espionage, cyber-warfare, or cybercrime. These countries represent a broad spectrum of geopolitical powers and regions, each believed to be contributing to global tension and uncertainty in the cyber domain.

---

[10] https://www.av-comparatives.org/spotlight-on-security-politics-and-cyber-security-a-troubled-relationsh

[11] https://www.av-comparatives.org/origin-evolution-an-in-depth-exploration-of-advanced-persistent-threat-apt-groups/

[12] https://www.av-comparatives.org/av-comparatives-explains-the-implications-of-takeovers-in-the-it-security-industry/

## *Map of the topmost feared countries*



## *Most feared countries by continent of respondent*

| Asia | | Europe | | North America | | South America | |
|---|---|---|---|---|---|---|---|
| | China | | Russia | | China | | USA |
| | Own country | | China | | Russia | | China |
| | USA | | USA | | USA | | Russia |
| | Russia | | Own country | | Own country | | Brazil |
| | North Korea | | Ukraine | | North Korea | | Israel |
| | Iran | | Germany | | India | | Own country |
| | India | | North Korea | | Israel | | North Korea |
| | Pakistan | | Turkey | | Ukraine | | Canada |
| | Israel | | Israel | | Canada | | UK |

Breaking down the fears by continent, the survey provides a nuanced view of regional perceptions. China is most feared in Asia, while Russia takes this role in Europe. There is a notable concern about domestic threats in North America and South America, with the USA and Brazil being mentioned, respectively along with external entities. Political relations, media coverage, historical cyber-incidents, or proximity to the perceived threatening nations may influence this regional variation. The specificity of fears, such as North Americans fearing China, and Russians or Asians fearing their own countries, underscores the complex, multifaceted nature of cyber-threat perception.

## *Most feared countries by country of respondent*

| Brazil | Germany | India | Italy | Russia | Ukraine | UK | USA |
|---|---|---|---|---|---|---|---|
| 🇧🇷 Brazil | 🇷🇺 Russia | 🇨🇳 China | 🇷🇺 Russia | 🇷🇺 Russia | 🇷🇺 Russia | 🇷🇺 Russia | 🇨🇳 China |
| 🇨🇳 China | 🇨🇳 China | 🇮🇳 India | 🇨🇳 China | 🇺🇸 USA | 🇺🇦 Ukraine | 🇨🇳 China | 🇷🇺 Russia |
| 🇺🇸 USA | 🇩🇪 Germany | 🇵🇰 Pakistan | 🇺🇸 USA | 🇺🇦 Ukraine | 🇺🇸 USA | 🇺🇸 USA | 🇺🇸 USA |
| 🇷🇺 Russia | 🇺🇸 USA | 🇺🇸 USA | 🇮🇹 Italy | 🇨🇳 China | 🇨🇳 China | 🇬🇧 UK | 🇮🇳 India |

Amongst the eight countries with most respondents, the top four most-feared countries all included the respective own country, as well as China and the USA. With the exception of India, Russia is also among the top four most feared countries by these eight countries.

The survey's findings highlight a global sense of vulnerability and concern over the potential for cyberattacks from various actors. It reflects a general awareness of the capabilities and historical actions of specific countries in the cyber domain. For governments, organisations, and individuals, understanding these perceptions is crucial in shaping cybersecurity strategies, international policies, and cooperative efforts to mitigate threats and reassure the public. It also points to the need for robust, transparent, and trust-building measures within countries to address domestic concerns about privacy[13] and cyber surveillance.

---

[13] https://www.av-comparatives.org/data-transmission-in-consumer-security-products/

## 19.    When considering the credibility of a testing lab, which factors do you regard as the most crucial when making decisions? (multiple answers possible)

1.  Independence from direct affiliations with anti-virus industry memberships or lobbying groups to ensure impartiality and neutrality
2.  Transparent disclosure of testing methodologies within each report
3.  Test reports and evaluations are available free of charge on the website for all readers without a paywall
4.  Track record and reputation in the field (testing experience)
5.  Lack of involvement in selling or promoting anti-virus/security software
6.  Diverse and comprehensive range of testing methodologies covering various product aspects
7.  Industry-recognised certifications
8.  ISO certification

The survey's question about the crucial factors for determining the credibility of a testing lab reveals a strong consensus among participants on the importance of independence, transparency, and accessibility, as shown in the ordered list above. Over 60% of respondents highlight the significance of a testing lab's independence from direct affiliations with anti-virus industry memberships or lobbying groups, ensuring impartiality and neutrality in evaluations. This concern underscores a widespread demand for unbiased and fair assessments, free from any potential conflicts of interest that might skew results.

Similarly, over 60% of users value transparent disclosure of testing methodologies within each report. This transparency allows users to understand how tests are conducted, the criteria used, and the basis for the lab's conclusions, fostering trust and confidence in the results. Another equally important factor for over 60% of respondents is the availability of test reports and evaluations free of charge on the website, ensuring that crucial security information is accessible to all users without financial barriers.

Other significant considerations include the lab's track record and reputation in the field, cited by over 50% of participants. This reflects a reliance on historical performance and credibility as indicators of quality and reliability.

Over 50% of respondents also consider the lack of involvement in selling or promoting antivirus/security software as vital, as it further ensures the objectivity and impartiality of the lab's evaluations.

A diverse and comprehensive range of testing methodologies covering various product aspects is also crucial for over 50% of users. This diversity ensures a holistic and robust assessment of products, reflecting real-world performance and security efficacy.
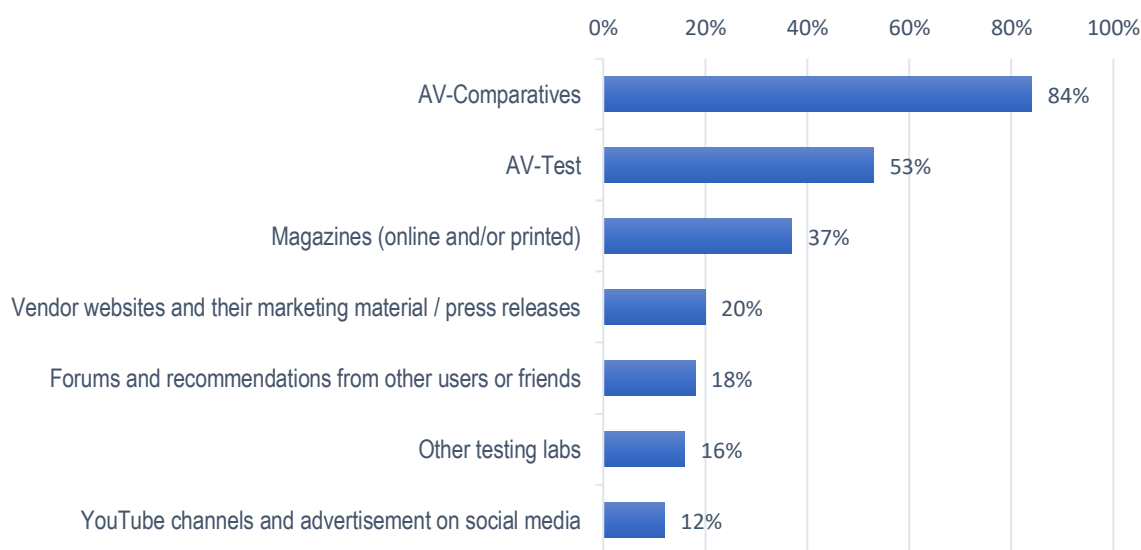
While industry-recognised certifications and ISO certifications[14] are deemed important by 35% of respondents, these factors are slightly less prioritised compared to the other criteria. However, they still contribute to the overall perception of credibility and professionalism.

---

[14] https://www.av-comparatives.org/about-us/certifications/

The survey also reveals a strong sentiment among over 90% of users regarding the need to reduce the influence of external factors like affiliate marketing and lobbying on testing companies. For these reasons, many respondents voiced concerns about AV vendors and testing labs being members in the same industry groups. There is a prevalent belief that these practices significantly impact the objectivity of some testing labs.

These findings highlight the paramount importance of integrity, transparency, and user-oriented practices in the perception of a testing lab's credibility. For testing organisations, adhering to these principles is essential in building and maintaining trust with the user community, ensuring that their evaluations are respected and valued as reliable sources of information in decision-making processes related to cybersecurity products and practices.

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

| Source | Percentage |
|--------|-----------|
| AV-Comparatives | 84% |
| AV-Test | 53% |
| Magazines (online and/or printed) | 37% |
| Vendor websites and their marketing material / press releases | 20% |
| Forums and recommendations from other users or friends | 18% |
| Other testing labs | 16% |
| YouTube channels and advertisement on social media | 12% |

The most trusted sources of AV/security test results are shown in order above. Please note that with this question, respondents were presented with an empty text box in which to write their answers. This aimed to elicit the sources that participants actually mainly use, rather than suggesting ones that they might use.

Responses as to the main sources for anti-virus and security test results reveals a varied landscape of preferences and trust, with a notable emphasis on certain key players in the industry. AV-Comparatives stands out prominently, being mentioned in 84% of the cases, suggesting a high level of credibility and trustworthiness as seen by users. We hope that our high rating recognises our independence from vendor influence, the comprehensive and carefully prepared methodology of our tests, the meaningful number of samples, transparency, and freely available test reports, which describe the tests in detail. Our willingness to allow other publications to cite our results (subject to proper attribution) also increases our visibility.

AV-Test is the second most popular source, used by 53% of respondents. The fact that a majority uses both AV-Comparatives and AV-Test indicates a user preference for established testing labs with over 20 years of experience in the field of AV testing.[15]

International magazines, both online and printed, such as PCmag, PC World, Heise c't, CHIP, ComputerBILD, Security.nl, TechRadar, Comss.ru, CNET, BleepingComputer, 3Dnews and Consumentenbond among others, are also significant sources, mentioned by 37% of respondents. These publications are valued for their accessible reviews and coverage of various products, suggesting a significant influence on user decisions by these media.

Other notable sources include vendor websites[16] and marketing materials, forums (such as Wilders Security, MalwareTips, Rokop Security, etc.), recommendations from peers, YouTube channels[17], social media advertisements, other testing labs like SE Labs, MRG-Effitas, AVLab, Virus Bulletin, and MITRE-Engenuity, as well as analyst-firms like Gartner, Forrester and others.

---

[15]    https://www.av-comparatives.org/spotlight-on-security-why-independent-testing-of-anti-virus-software-important/
[16] https://www.av-comparatives.org/blogs-of-security-vendors-news-sites/
[17] https://www.av-comparatives.org/youtube-security-channels/

With regard to demographics, IT professionals, experts, and more advanced users typically include testing labs like AV-Comparatives and AV-Test among their go-to sources for credible information. We regard this as an expert endorsement of professional, independent testing agencies.

Conversely, vendor sites are more popular among novice/basic users, who might be more trusting of their marketing claims. Forums and peer recommendations tend to be favoured by younger respondents.

Users under the age of 25 predominantly turn to YouTube channels and social media advertisements for anti-virus/security products, indicating the growing impact of such popular online media on younger audiences' decision-making. Meanwhile, those aged 25-34 are more inclined to rely on forums and recommendations from friends or other users.

As part of the survey, we asked participants for their feedback on AV information sources. Users appreciate AV-Comparatives' reports for their clarity, the detailed explanation of methodologies, and the comprehensive and varied testing of multiple product aspects. The availability of these reports free of charge, including PDF versions, is particularly valued. They commend AV-Comparatives for its inclusion of, and balanced approach to false positives[18], and for not universally awarding all tested products with top or excellence rankings (unlike some other labs in recent years), thus aiding meaningful differentiation among products.

However, users express concern over the potential bias in some testing labs due to the closeness to some AV-industry groups/memberships they are part of or the prevalence of affiliate links in some online magazines/websites showcasing anti-virus rankings. As a well-established source of information AV-Comparatives, noted for its independence, stands apart from these practices.

We have noted suggestions for overall improvement and have an ongoing commitment to presenting users with the most essential data in an easily accessible form, thus helping them better understand how tests are performed and the relevance of the results. We hope readers will appreciate that for reasons of confidentiality and resources, there are limits to the details we can supply to the general public regarding individual tests. Nevertheless, we will do our best to make our testing procedures as comprehensible as possible.

---

[18] https://www.av-comparatives.org/the-difference-between-av-comparatives-epr-test-and-mitre-attck-engenuity/

## Prize Raffle

This year, we ran again a prize raffle open to all our survey participants, to show our appreciation for their help. Over 90% of the respondents who participated in the raffle won various software licences, kindly provided by the respective vendors: **Avast, AVG, Avira, Bitdefender, ESET, Kaspersky** and **McAfee**.

Congratulations to the winners, and a big thank-you to everyone who took the time to complete the survey!

# Copyright and Disclaimer