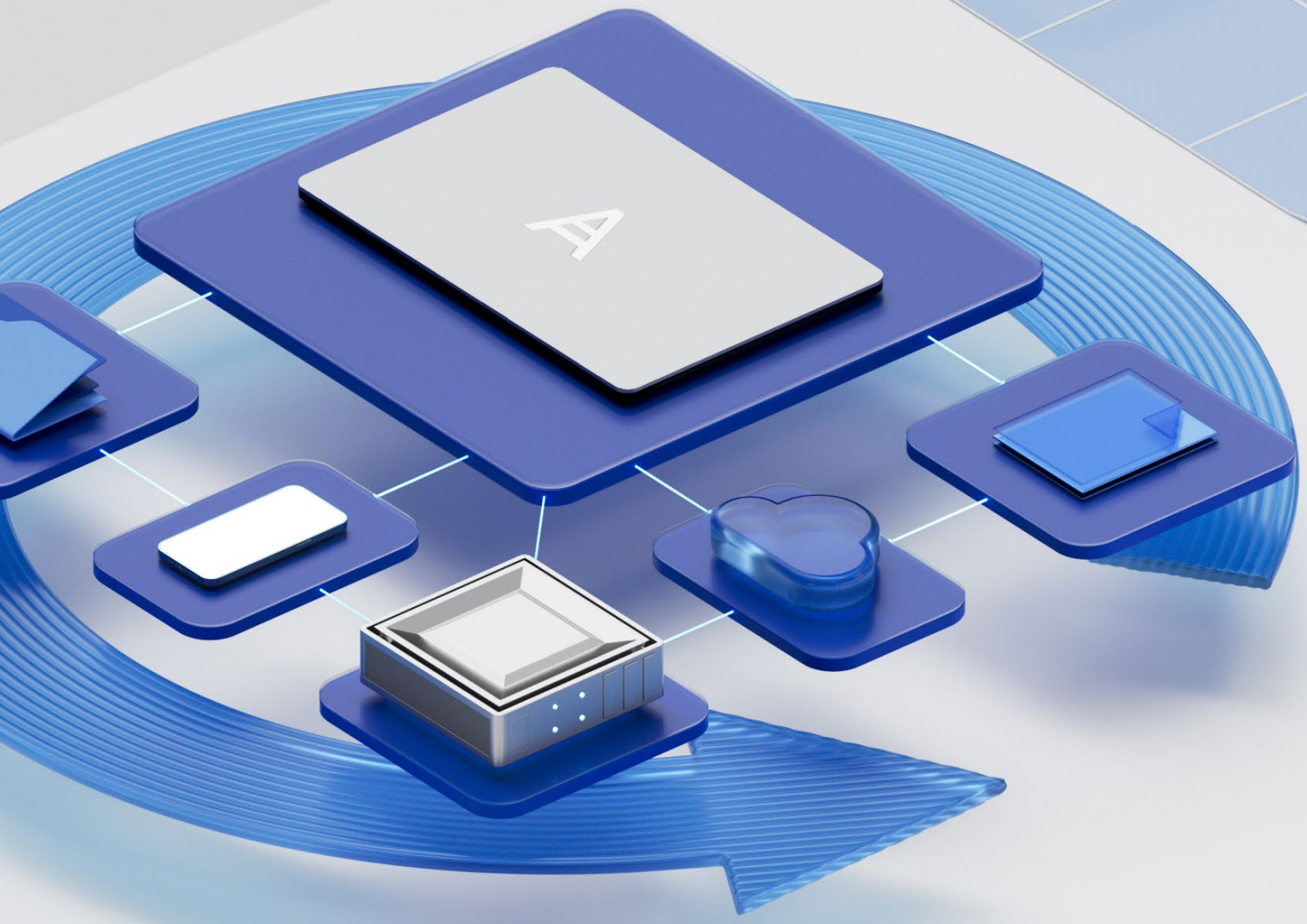
Acronis

Survey
2025



Data privacy in 2025:

A survey to explore consumer views on cyber protection

Table of contents

Introduction

Three decades or so into mainstream use of the internet, much has changed. Consumers have shifted from using a single desktop or laptop computer for surfing to using multiple devices to shop, bank, chat and share media of all kinds.

The expansion of digital footprints and data collection has also brought cyberthreats that menace consumers every time they go online. Data Privacy Day, observed on January 28, serves as an important reminder of the growing need for data protection. Failing to safeguard critical information can lead to severe financial and even personal consequences.

How do consumers feel about cyberthreats in this dangerous era? What do they know about data protection, and what are they doing to keep their information safe? Acronis posed questions to nearly 2,500 consumers across eight countries to understand public perceptions of data protection and the steps individuals are taking to safeguard their personal information through cybersecurity practices. The findings and trends are detailed in this report.

Consumer cybersecurity practices have come a long way, but still have far to go

The survey reveals that many consumers are becoming more sophisticated in their understanding of security threats, with 64% of global respondents putting data breaches at the top of a list of privacy concerns. And many are taking at least some proactive steps to protect their data.

However, notable gaps in how consumers approach data privacy are evident, with nearly 30% finding security tools too difficult to set up and manage, and almost half admitting they don't worry about data protection at all.

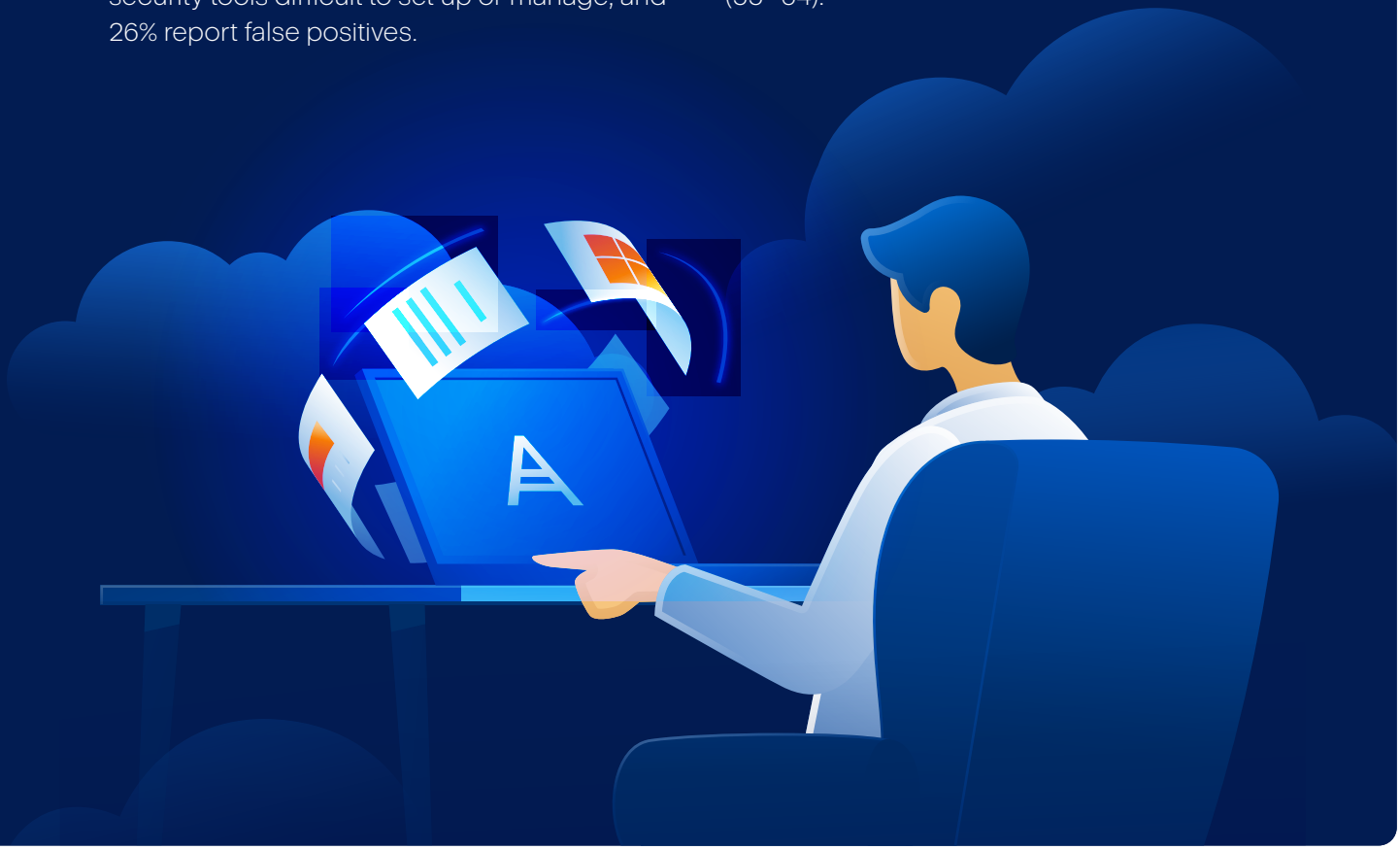
There are also gaping holes in consumers' cybersecurity practices: About 35% of respondents said they don't back up data regularly, and 4% don't even know what backup means.

Critical observations

The Acronis Data Privacy in 2025 Survey explores consumer attitudes toward cybersecurity and examines how everyday users protect themselves online. Some broad trends emerged, with a few revealing a paradox between thinking and behavior, and others indicating that consumers still aren't protecting themselves as completely as they should.

Key findings:

- **Solid adoption of backup practices:** Two thirds of respondents (66%) back up their data regularly, and 9% don't back up their data at all.
- **High engagement with privacy tools, lingering privacy worries:** Almost 60% of respondents use antivirus software, while 36% rely on firewalls and 24% use VPNs. Nevertheless, 64% of respondents cite data breaches as their top concern.
- **Awareness and adoption of basic cybersecurity practices:** More than two thirds (68%) of respondents use strong, unique passwords, but 21% of respondents only update passwords when prompted.
- **Challenges with cybersecurity software complexity:** Almost 30% of respondents find security tools difficult to set up or manage, and 26% report false positives.
- **Appreciation of cybersecurity features not backed by usage:** Real-time threat detection (43%) and malware protection (41%) are the most valued features. However, the number of respondents using those features is smaller.
- **Low awareness and adoption of mobile security:** Forty-three percent of users use a mobile security app, but 35% report they are unfamiliar with mobile security solutions.
- **Prevalence of cyber incidents:** A quarter of respondents have experienced data loss or theft, and nearly 24% have been victims of a data breach.
- **Behavioral differences among age groups:** Younger respondents (under 35) reported more breach incidents than older age groups (55–64).



Data privacy in 2025 survey: The data

Data Privacy Day provides an opportunity to gauge consumer sentiment toward a topic that's critically important, but sometimes misunderstood. Survey responses reveal concern among consumers about cybersecurity that they don't always necessarily back up with behavior. Awareness is stronger in some areas than in others; for instance, adoption of and attitudes toward mobile security lag despite the prevalence of smartphones.

Data privacy attitudes and behaviors

Many, but not all consumers are worried about data privacy

Most respondents understand the importance of protecting data, but a surprising number are blasé about it. When asked to measure the importance of data security on a scale of one to 10 — 10 being the most important — more than 60% of respondents identified themselves as believing security is very important, about a quarter said protecting data is only somewhat important and more than 10% said it wasn't important at all.

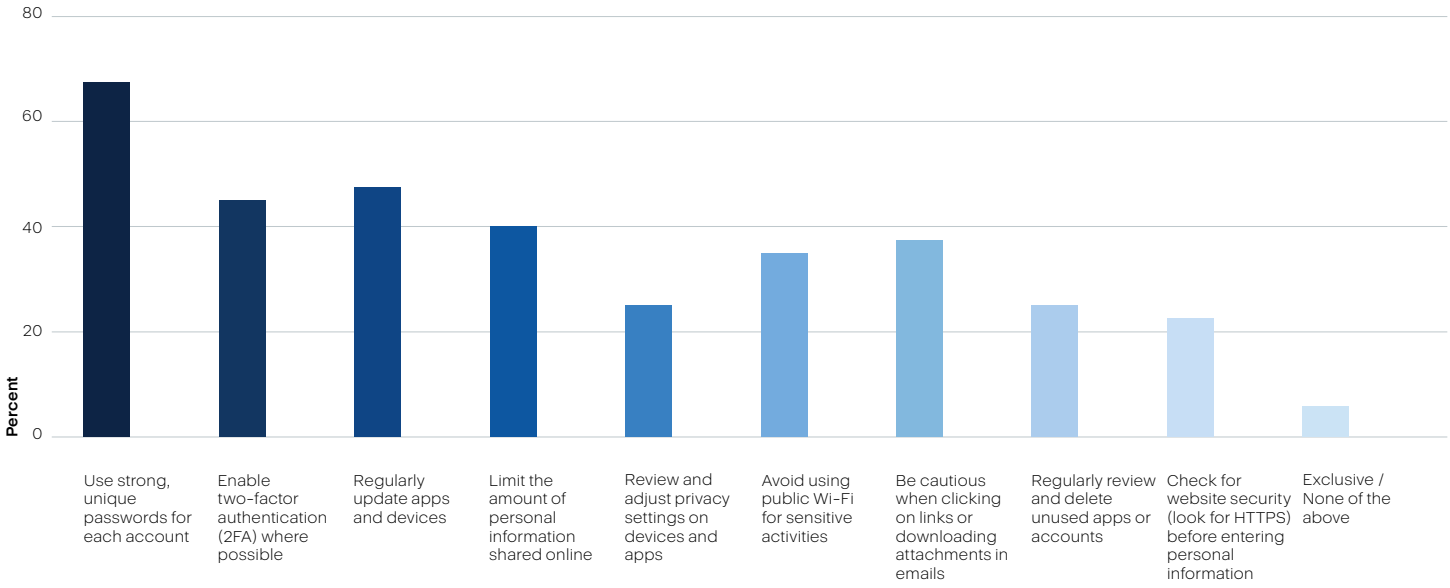
When asked how concerned they are about the security of their personal data, fewer than half of respondents showed strong concern for protecting their confidential information, while one in five reported not being very concerned at all. If more than half of consumers are only a little worried about data protection or not concerned at all, cyberattackers have a long list of potential victims.

Data privacy behavior shows deviation from best practices

Two thirds (68%) of consumers say they are using strong, unique passwords, but fewer than half of respondents (46%) reported using two-factor authentication (2FA), an essential tool for protecting passwords and online identity. Public Wi-Fi remains an issue, with almost 70% of respondents saying they don't avoid using. Four in 10 say they're cautious when clicking on links or downloading email attachments, which could represent growth in the level of phishing and malware awareness.

Updating and remembering a new password is an essential cybersecurity best practice that continues to elude consumers. About 40% of respondents update their passwords less frequently than once a year, and about 30% either wait until they're forced to, or don't update at all.

What data privacy best practices do you regularly follow? Select all that apply.



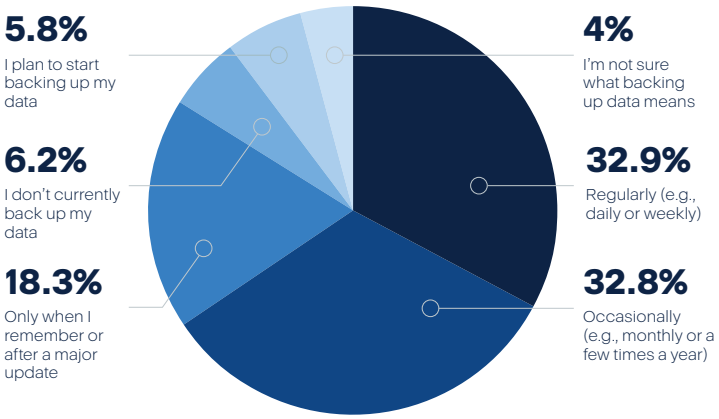
Backup practices

Consumers understand that data backup is important, but only one third perform backups regularly

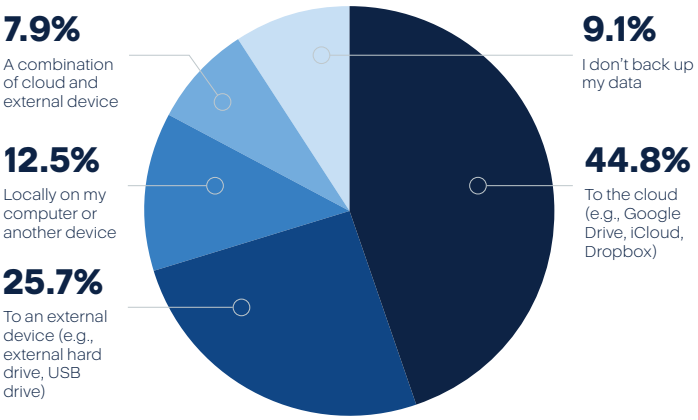
A strong majority of respondents reported backing up data at least somewhat regularly, with 33% backing up daily or weekly and 33% doing it monthly or a few times a year. However, 18% of respondents back up only when they remember or after a major update, and 4% don't know what backup means.

The excellent news is that roughly half of consumers understand that the cloud, which has geographically dispersed data centers managed by organizations, is a safer backup option than a physical device. External hard drives and other local devices are subject to physical disasters such as fires and hurricanes as well as to theft.

How often do you back up your important data?

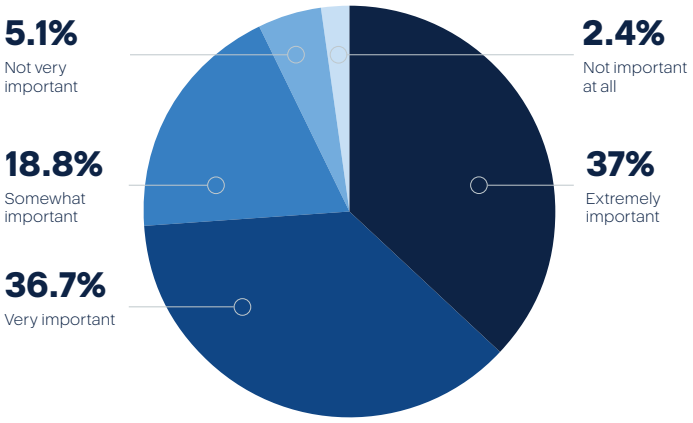


Where do you back up your data to?



Some of the data revealed in these responses is contradictory. Almost 10% of respondents said they don't back up their data at all, but only about 2% said data backup isn't important at all. Another 5% said data backup isn't very important, so there must be some respondents who find data backup important but still don't do it.

How important is it for you to have a backup of your personal data (from devices like smartphones, laptops, tablets, desktops, external hard drives, etc.)?

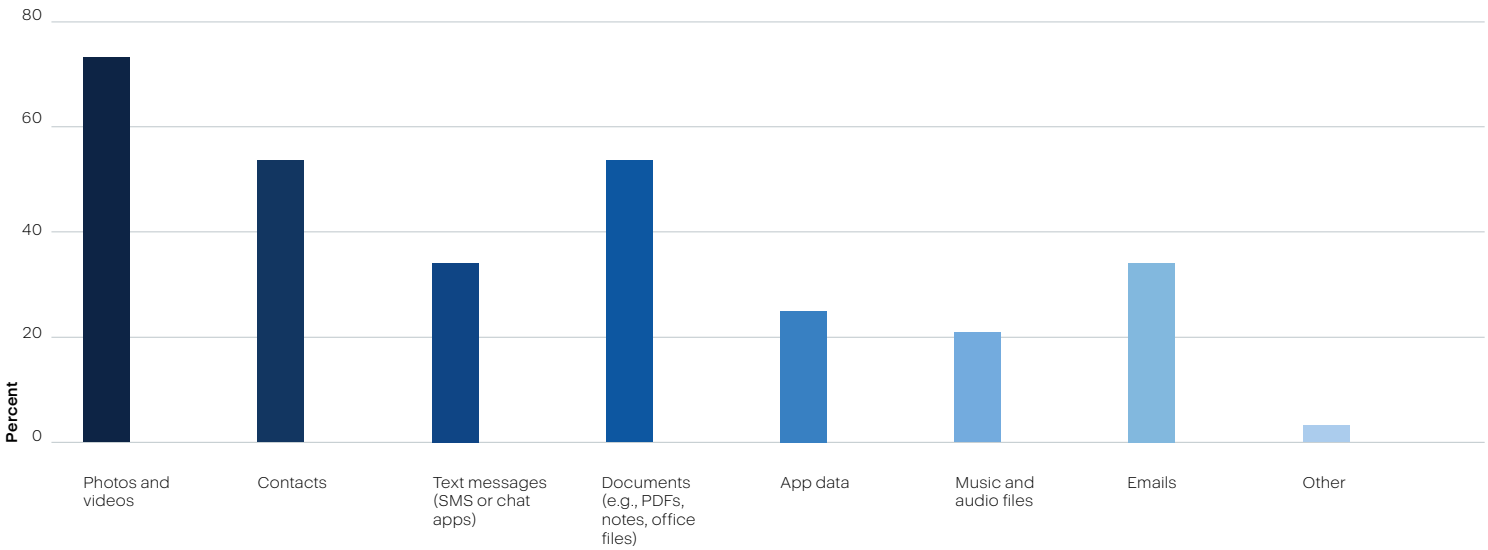


Everybody wants to preserve photos and videos, so the answers to a question about which files are the most important to back up don't come as a surprise. However, little more than half of users report backing up documents, which is surprising.

While emails and documents can include critical business and personal information — and be of greater monetary value — protecting personal photos is the chief priority for 73.8% of consumers. Fifty-four percent cite documents and contacts as their top priority, and 33.1% say protecting text messages is most important.

Only a third of respondents say email is the top priority, possibly because their emails rest on a provider's servers in the cloud and aren't obvious targets for backup. Nevertheless, email is a critically private channel that consumers should consider backing up elsewhere.

What types of files on your devices are most important for you to back up? Select all that apply.



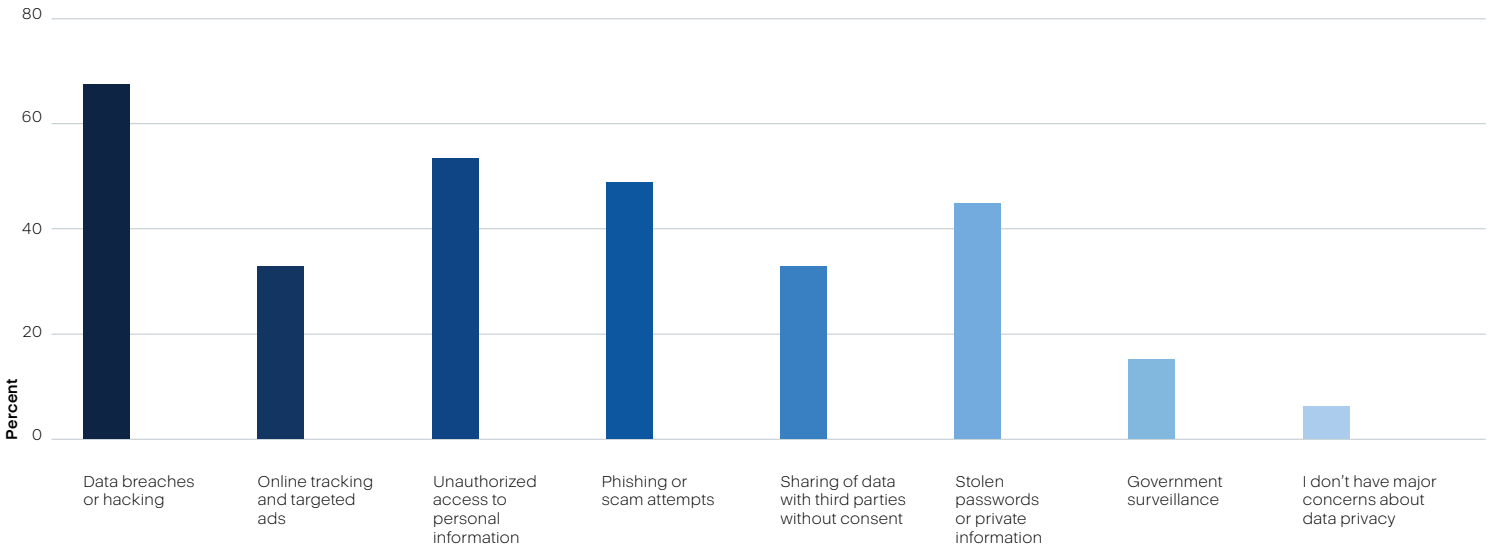
Data breaches

Consumers are most concerned about data breaches and unauthorized access, and many have already been victims

Responses to questions about data privacy concerns are among the headlines of the survey, with 64% of respondents citing data breaches as their top concern. Unauthorized access to personal information (53%) and phishing or scam attempts (49%) follow closely behind.

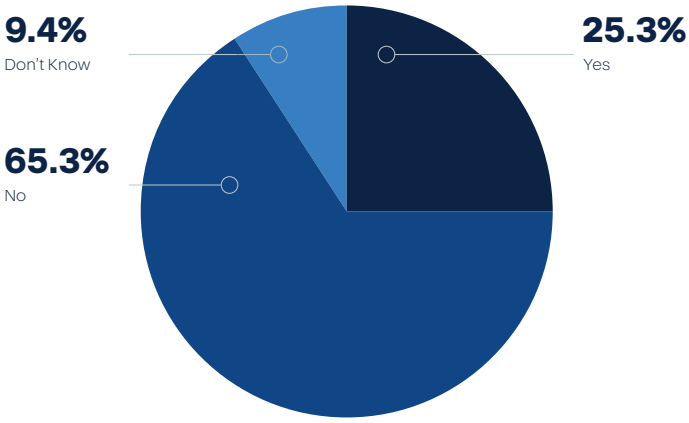
What these numbers reveal is that consumers have a more sophisticated understanding than they used to of the nature of online threats.

What are your biggest concerns regarding data privacy? Select all that apply.

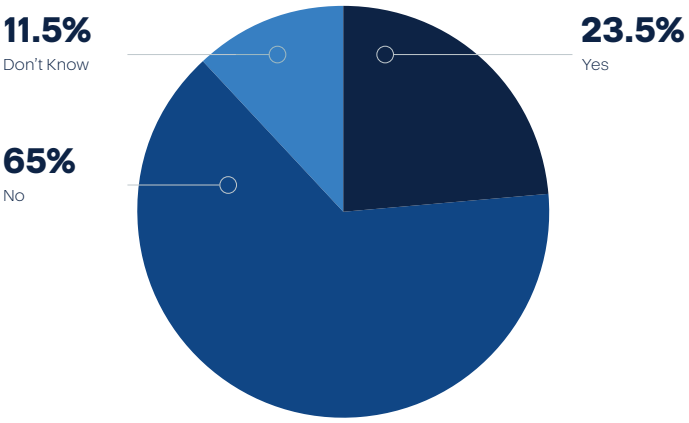


Perhaps the most surprising result is that a quarter of users report data theft or loss, and more than 9% don't know whether they've lost data or had it stolen. Data theft can go on for weeks or months before consumers know it's happening, so they could be unaware that they're in the grip of a cyberattack at any moment.

Have you ever had your personal data lost or stolen?



Have you ever been a victim of a data breach?



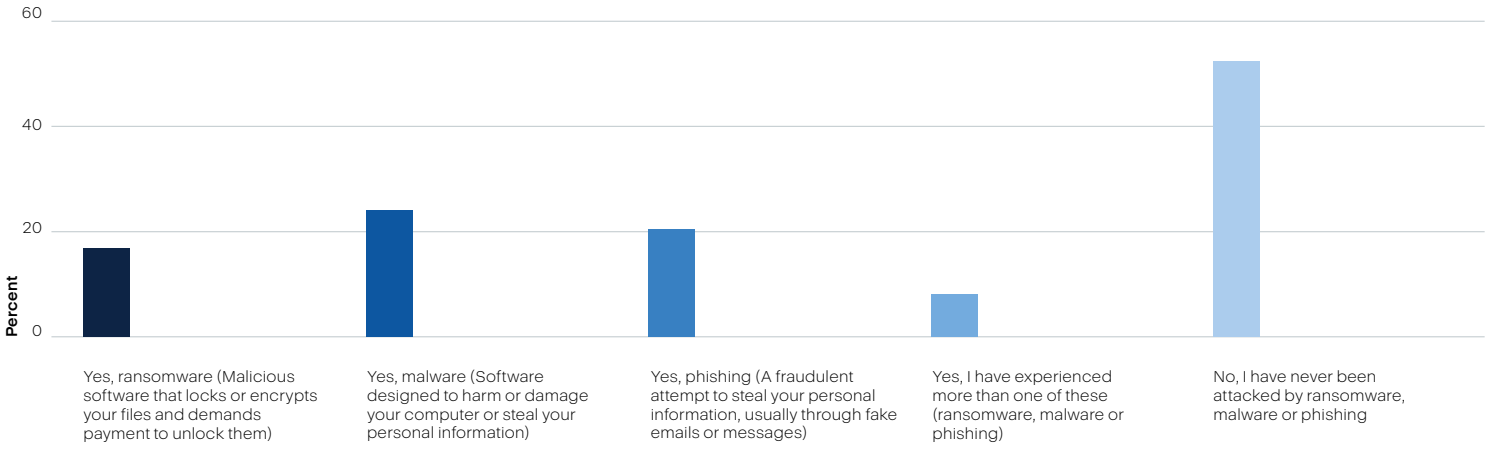
As for data breaches, 65% of consumers said they have not been a victim, and 12% of consumers said they don't know. It's possible that those who say they haven't been breached might have been without realizing it.

Phishing, malware and ransomware

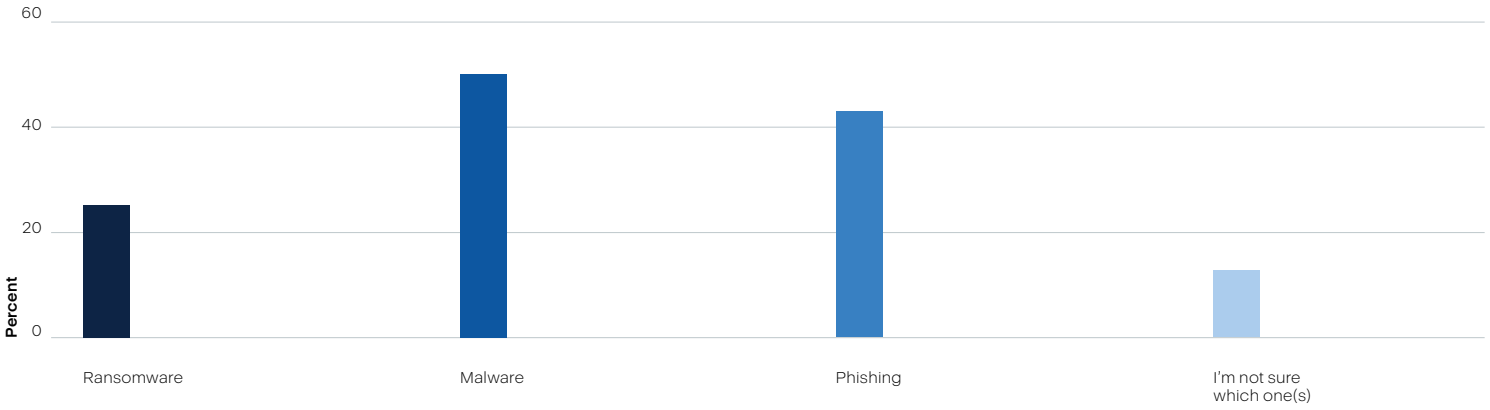
While most consumers say they've avoided data theft, others have fallen victim to email threats and malicious websites

Phishing, malware and ransomware are among the most widespread attack vectors, with each of those affecting roughly 20% of consumers. About 7% of respondents said they'd suffered more than one attack, with malware (49%) and phishing (42%) being the most common, and 50% of consumers said they've never experienced phishing, malware or ransomware. This high number could be a result of phishing and malware often going undetected by security software and unnoticed by consumers.

Have you ever been attacked by ransomware, malware or phishing? Select all that apply.

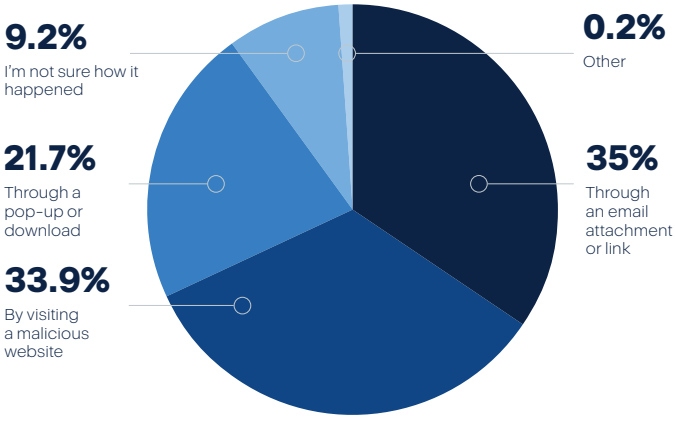


If more than one, which ones did you experience? Select all that apply.



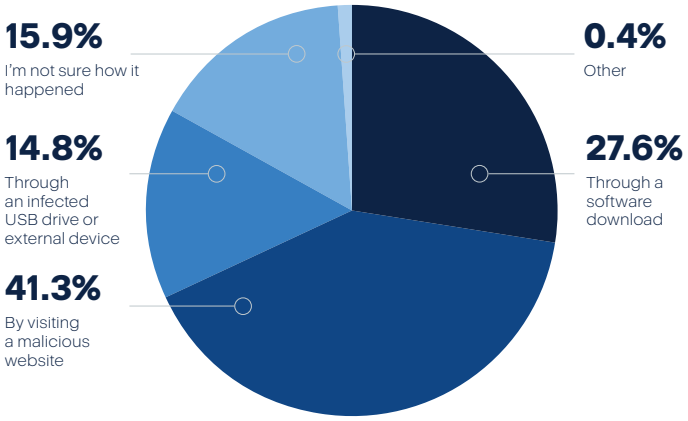
Email is still the preferred channel for ransomware attacks: 35% of consumers who fell victim to ransomware did so via email. But the percentage of respondents who experienced a ransomware attack from visiting a malicious website (34%) is equally high. It speaks, perhaps, to users not doing due diligence before visiting websites. Pop-ups and downloads were the third highest source (22%) of ransomware attacks, and 9% of consumers were not sure how they became victims.

If ransomware, how did it happen?



As for malware attacks, software downloads were the largest source of infection (28%), while USB drives or external devices were the source of 15%. Also of note is that 15% of respondents don't know how they encountered malware, which shows how subversive cyberattacks can be, and that basic defenses such as antivirus and anti-malware might not be enough to protect users. Defense in depth, with multiple methods of protection in use, is a better strategy.

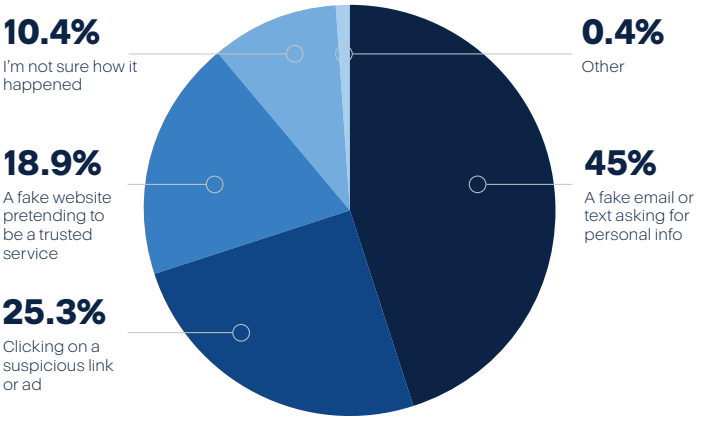
If malware, how did it happen?



Phishing emails were once relatively easy to spot, but they look deceptively credible now — free of grammar and spelling errors. That's true in part because AI is helping cyberattackers create increasingly convincing phishing emails and text messages. Phishing emails and text messages were the source of 45% of attacks, revealing the difficulty many consumers have in determining what is legitimate and what isn't. Links, too, are easier for attackers to mask, as 25% of respondents who clicked on a suspicious link probably now know.

While businesses make for more lucrative targets, attackers do target consumers. Nearly a quarter of respondents reported having fallen victim to attacks. Malware and phishing remain the biggest threats to consumers, though.

If phishing, how did it happen?



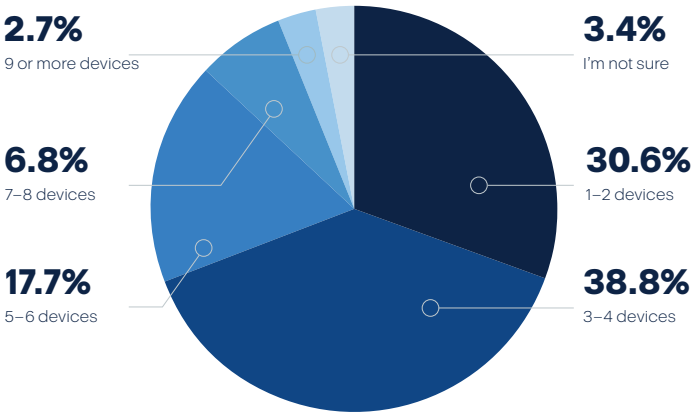
Because no security tool is foolproof, users need to be aware of the warning signs of phishing scams, including urgent language, unexpected links or unfamiliar senders. They should verify links by carefully hovering the cursor over them before clicking — or just not clicking at all — and be cautious about entering personal information online.

Mobile device security

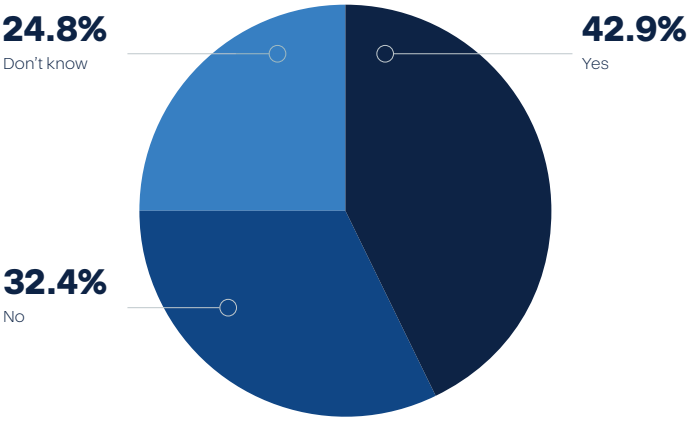
Many consumers are in the dark about mobile device security

Survey responses show that only about 30% report having more than four devices at home. Nevertheless, mobile devices are firmly entrenched as part of consumers' lives, with about 70% of respondents reporting having more than two devices. How well consumers are securing those devices is another question.

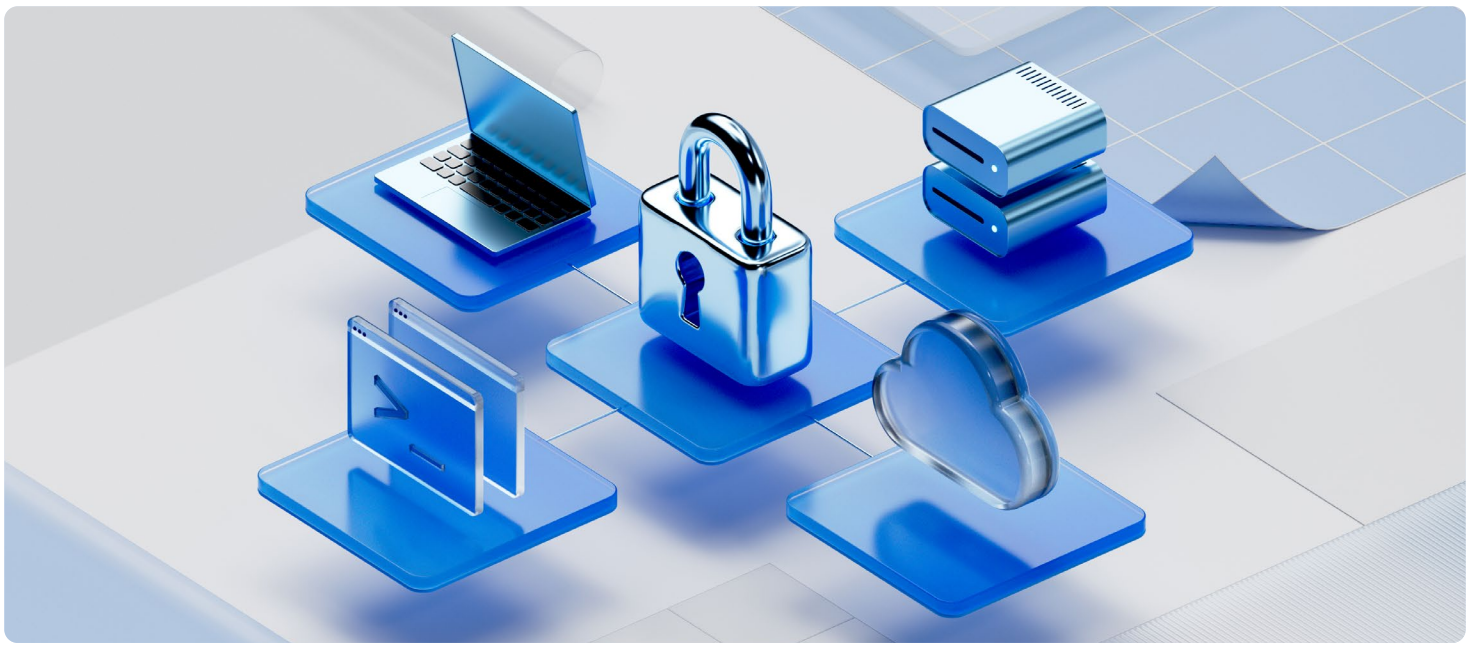
How many personal devices (such as smartphones, laptops, tablets or desktops) are in your household?



Do you currently use a mobile security application to protect your device?



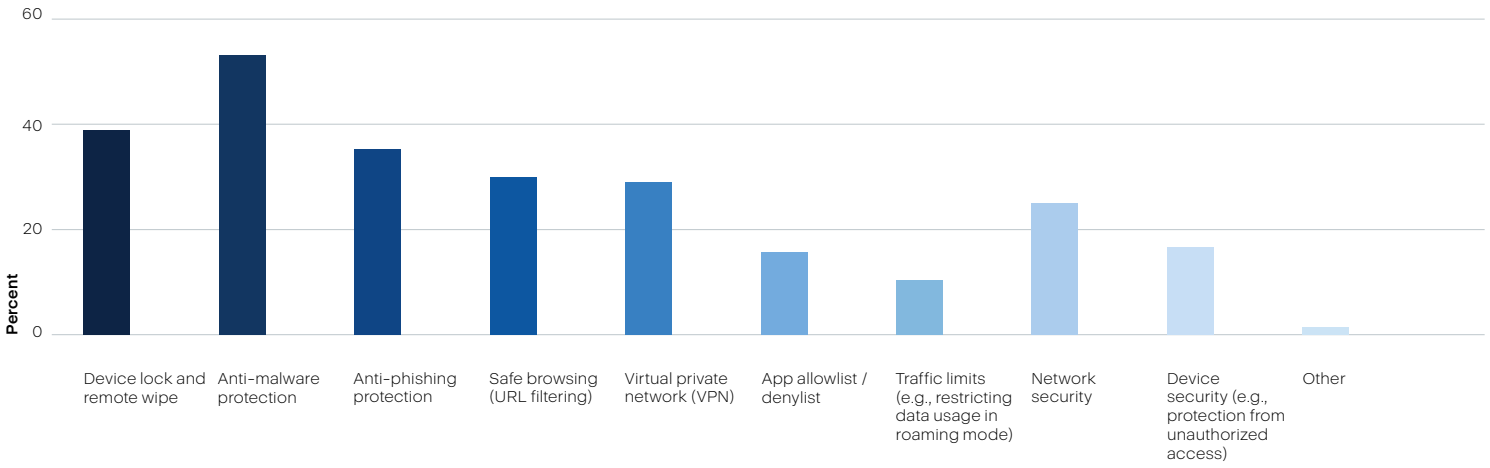
Mobile security is so critical in an era when phones have become extensions of many people's arms, but a significant number of respondents aren't protecting mobile devices at all. These consumers seem more aware of the threat of a cyberattack involving a laptop or computer, although smartphones are ubiquitous and in much wider use.



A quarter of respondents say they don't know whether or not they have mobile security. Fewer than half (43%) say they use security applications for mobile devices, and almost a third (32%) say they do not, meaning they're leaving mobile data wide open to theft.

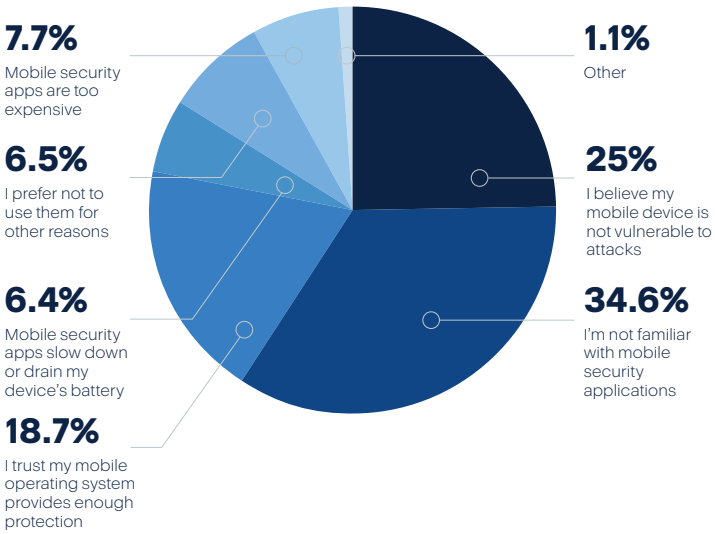
The good news is that some critical elements of mobile security have decent uptake among those who protect their devices. More than half of consumers have anti-malware protection for mobile; however, none of the other features comes close to reaching the 50% mark, so consumers have a way to go before they really lock down their devices.

If yes, which features do you currently use to protect your device? Select all that apply.



Almost one fifth (19%) of consumers rely on their mobile operating systems to protect their devices. Unfortunately, mobile operating system security on its own doesn't provide comprehensive protection. Furthermore, 35% of respondents don't know anything about mobile security applications, so some consumers are putting blind trust in mobile devices to protect their data.

If no, why are you not using a mobile security application on your mobile device? Select one.

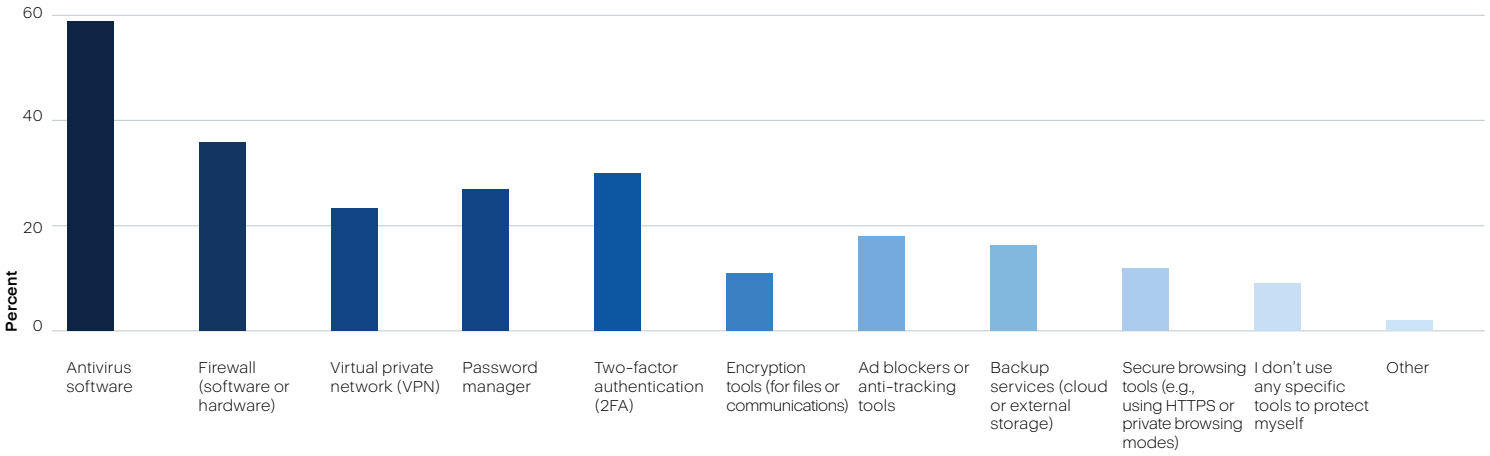


Cybersecurity software usage and challenges

Most consumers rely on antivirus and firewalls for protection, but cybersecurity tools present challenges

Almost 10% of respondents don't do anything to protect themselves online. Many users rely solely and heavily on antivirus applications. Other essential means of protection, including firewalls, password managers and 2FA, all fall well below a 50% usage number. Antivirus is just one element of cyber protection. Defense in depth is critical, and consumers should be using every tool on this list.

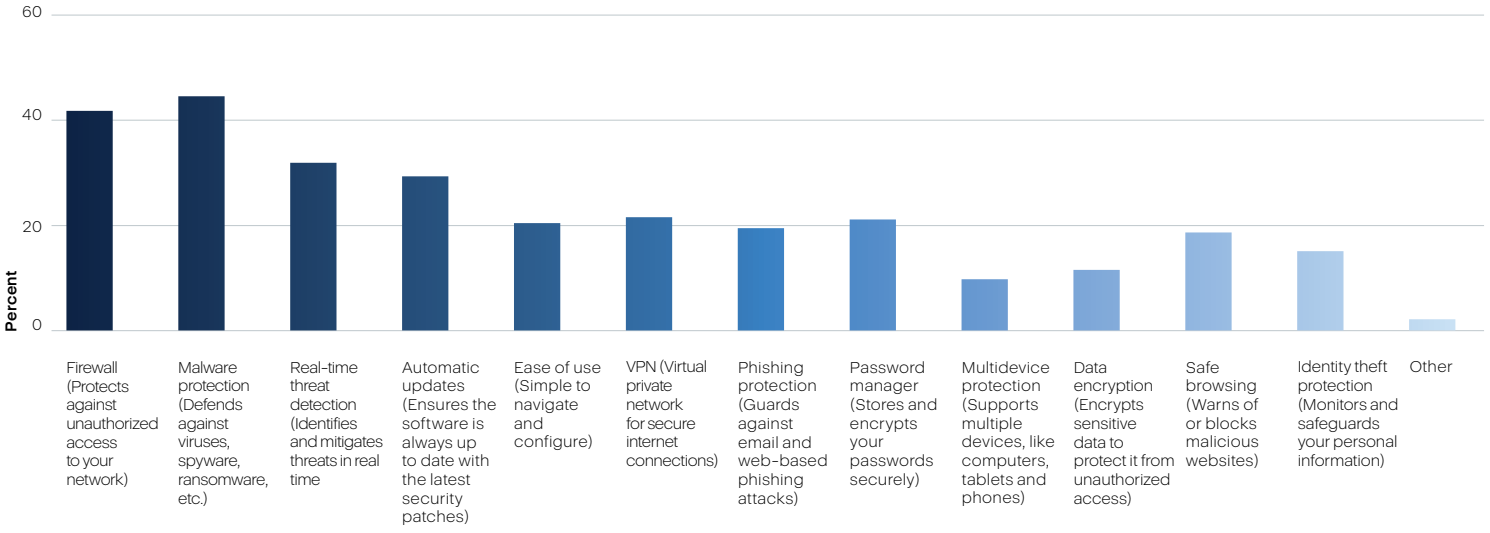
Which tools do you use to protect yourself against cyberthreats and to secure your data? Select all that apply.



A paradox appears in the answers to a question about security software usage. Firewalls top the list of most valuable methods of protection, and yet only about 36% of consumers use them. Users understand the value of many of the tools on this list, but might not know whether they use them or not. Given the prevalence of phishing attacks, it's surprising to see phishing protection so low on the list.

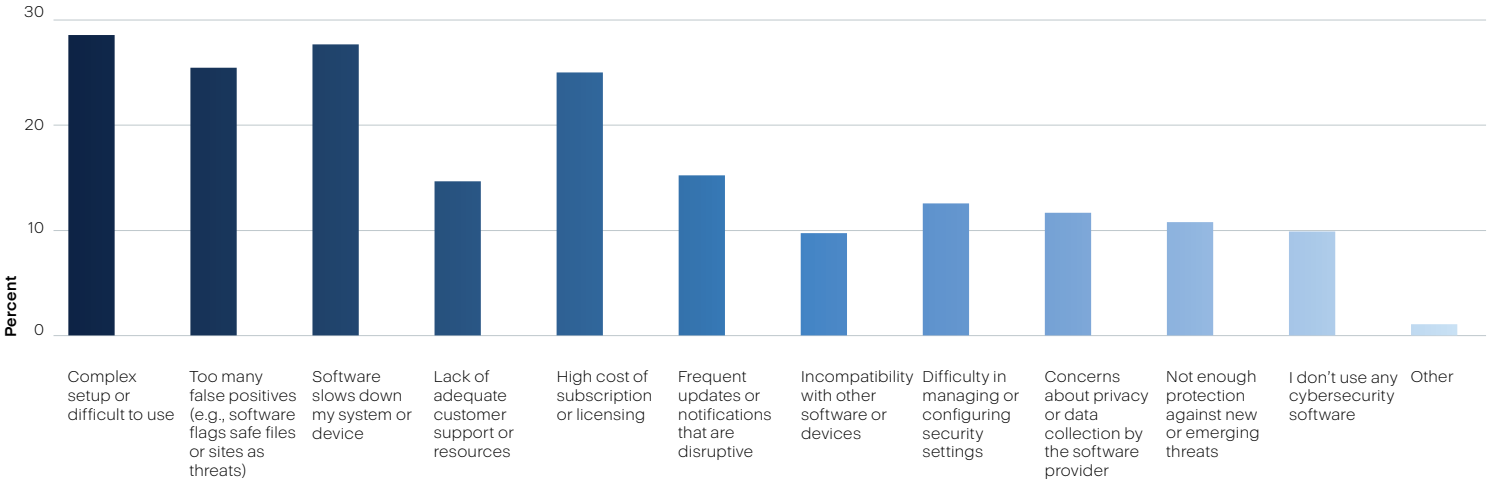
Tools such as VPNs and antivirus software can enhance privacy, but no single tool or capability provides a complete defense.

What features do you find most valuable in a cybersecurity tool? Select all that apply.



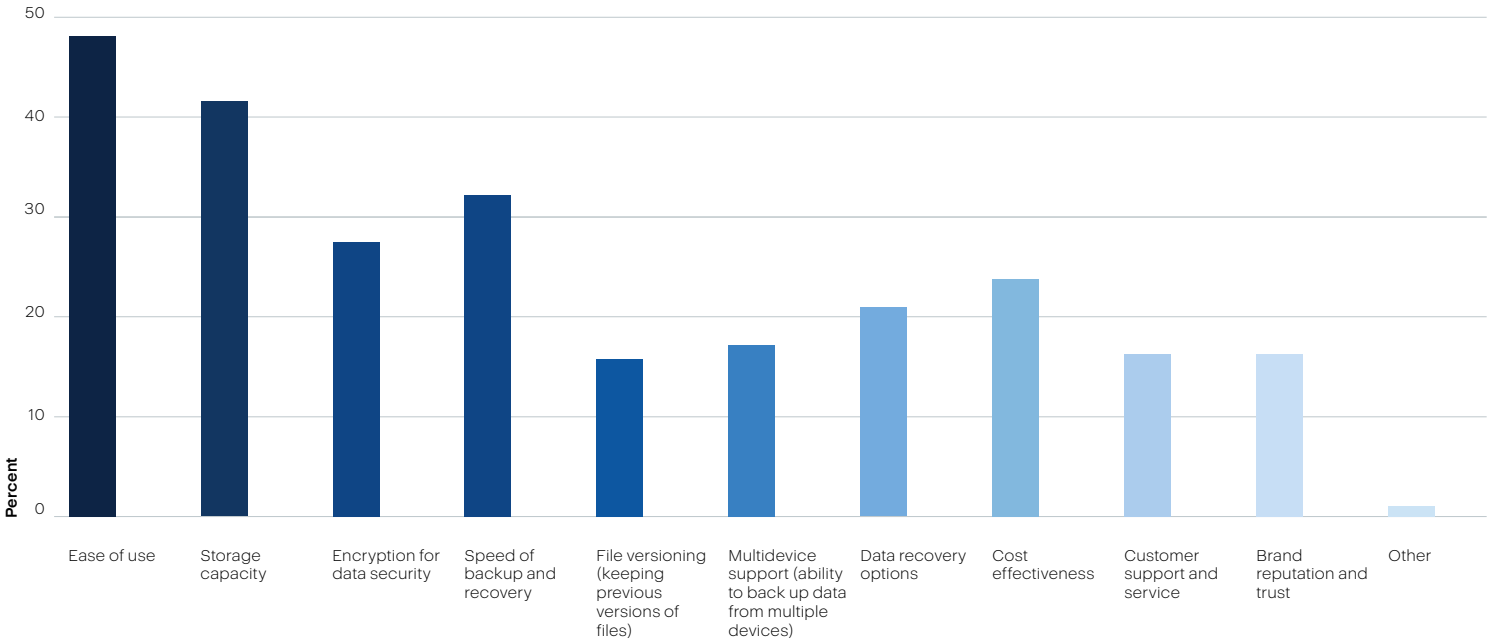
Almost 30% of respondents said security tools are complex or hard to use. Twenty-eight percent said security slowed their system or device, and a quarter of consumers said that security tools produced too many false positives. This indicates that many security tools might be both complex and too sensitive — or perhaps too hard for consumers to configure themselves. Additionally, 25% of respondents find security applications expensive.

What challenges do you face when using cybersecurity software? Select all that apply.



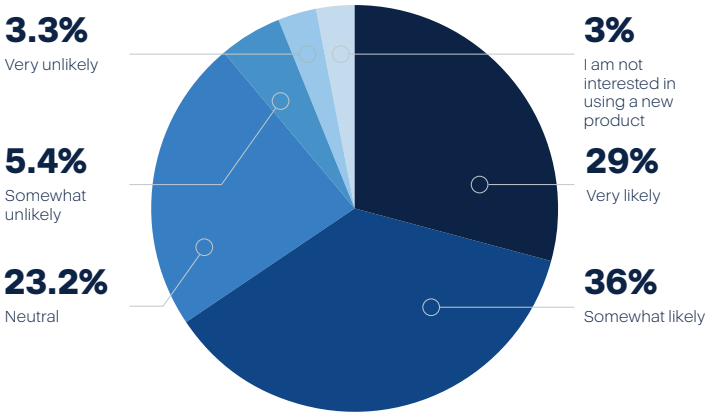
Ease of use and speed are huge factors for consumers, with storage space placing second in importance. Consumers are sending a clear message that they won't put up with slow computing and difficult interfaces. They would rather just not back up their data in many cases — a dangerous and unwise choice.

What features are most important to you when choosing a backup solution? Select all that apply.



Users don't want to spend a lot of time backing up data, and they don't want to find it difficult to do. Storage space, which some users might find too expensive, is the greatest obstacle to data backup. In fact, nearly 20% of consumers cited cost as a challenge to backing up data. But speed and ease of use are essential.

How likely are you to use a new cybersecurity and data protection product if it offers better protection at a lower cost?



Price is important, but it's not everything. About 35% of consumers indicated not being interested even in a cheaper solution for storing and protecting data. Still, the majority would like better protection for less money.

There is a clear $100 per-year ceiling for consumers with regard to spending on backup. Almost 17% don't have a budget and might not have backup tools at all. But $100 seems to be the tipping point at which consumers decide that data protection and backup are important enough to purchase.

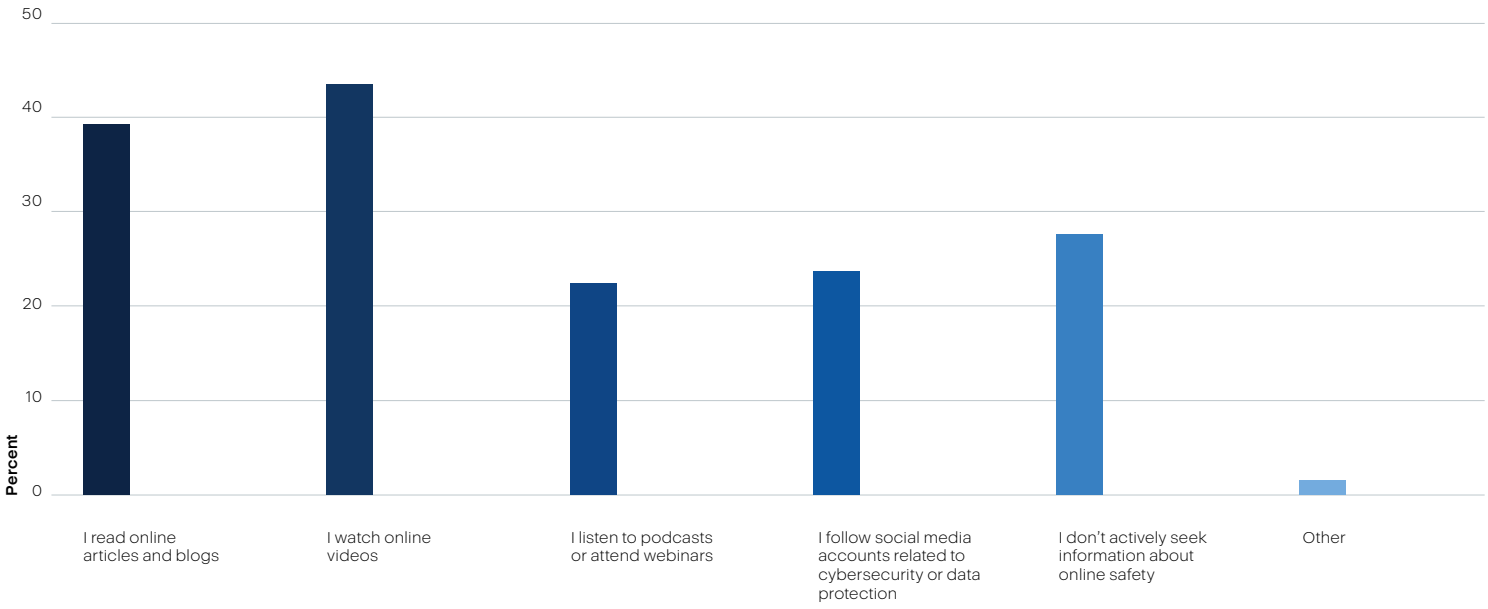
Cybersecurity awareness

Protecting data is a daily commitment

The Acronis Data Privacy in 2025 Survey shows that while many consumers are moving in the right direction, there are still areas where they could improve both attitudes and behaviors, while also continuing cybersecurity education.

The good news is that interest in cybersecurity education appears to be growing. Video has emerged as the preferred medium for learning about online safety, surpassing written materials, with 44% of respondents seeking information through online videos and 38% reading online articles and blogs. These numbers suggest that accessible, engaging resources could play a critical role in raising consumer awareness.

How do you stay informed about online safety and cybersecurity best practices? Select all that apply.



Conclusion

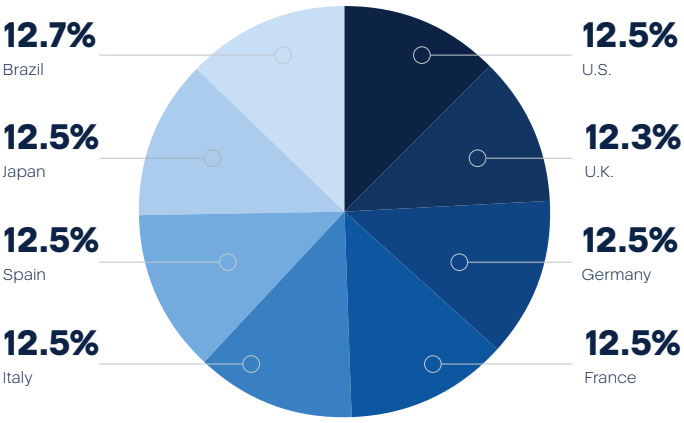
Data Privacy Day serves as an annual reminder of the critical importance of safeguarding personal information and maintaining strong data privacy. It's a wake-up call for consumers who may lack awareness of good cybersecurity habits or aren't consistently practicing the habits they know they should. However, protecting data and staying informed about data protection best practices shouldn't be a once-a-year effort — it requires continuous attention to understand and improve cybersecurity habits.

But there are still behavioral gaps that put consumers at risk. Consumers need to take control of their digital lives by engaging in positive cybersecurity behaviors, including using strong passwords, backing up data regularly, improving phishing awareness and practicing defense in depth.

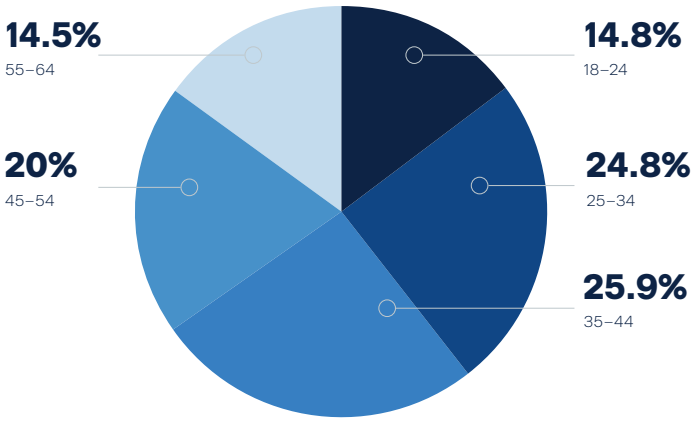
Methodology

Acronis surveyed 2,480 general-population consumers aged 18–64 in eight countries, including the U.S., the U.K., Germany, France, Italy, Spain, Japan and Brazil.

In which country do you currently reside?



What is your age range?



About Acronis

Acronis is a global cyber protection company that provides natively integrated cybersecurity, data protection, and endpoint management for managed service providers (MSPs), small and medium businesses (SMBs), and enterprise IT departments. Acronis solutions are highly efficient and designed to identify, prevent, detect, respond, remediate and recover from modern cyberthreats with minimal downtime, ensuring data integrity and business continuity. Acronis offers the most comprehensive security solution on the market for MSPs with its unique ability to meet the needs of diverse and distributed IT environments.

A Swiss company founded in Singapore in 2003, Acronis has 45 locations across the globe. Acronis Cyber Protect is available in 26 languages in 150 countries and is used by over 20,000 service providers to protect over 750,000 businesses. Learn more at www.acronis.com.

Acronis

Learn more at
acronis.com