moonlock by MacPaw

REPORT

Mac Security Survey 2025

From AI fears to password habits: a closer look at how Mac users perceive cybersecurity

About Mac Security Survey 2025

In 2023, Moonlock carried out the first Mac Security Survey to better understand the state of cybersecurity on Mac. Nearly 2,000 macOS users shared their worries, concerns, habits, and beliefs, unearthing a common theme: many believed that macOS was inherently immune to malware.

Since then, we've seen a **notable rise in malicious activity targeting macOS**, with significant growth in both variety and availability on the dark web. Meanwhile, the danger lies not only in how quickly malware is evolving, but also in the fact that threat actors are well aware of how carefree many Mac users feel.

At Moonlock, we wanted to see whether Mac users had begun to notice this shift in the landscape, and compare their perception of security with the results of the previous survey.

In June 2025, Moonlock conducted a new survey of **1,000 macOS users to capture their views on security.** This report presents the findings and compares them with previous results, supported by analysis from Moonlock's security researchers. It also provides references to additional resources for readers who want to explore the topic further.

Methodology

To understand the views of the American public, Moonlock surveyed **1,000 U.S. adults in June 2025.** Everyone who took part in this survey is **aged 18 and older**, a group of people recruited via Cint research platform. Interviews were conducted online with an average length of 10 minutes.

The margin of error is **±3 percentage** points at a **95% confidence level.** The survey was conducted using a non-probability online panel, so this figure should be interpreted as an approximate reference rather than a precise statistical bound.

Table of contents

Key findings

1 The myth of an untouchable Mac user is fading.

Only **15%** of Mac users think that malware does not exist on macOS. In 2023, the share was nearly **twice as high (28%).**

46% reported they need additional security software on Mac, because macOS is not secure enough on its own.

The share of respondents who believe their data is of no interest to cybercriminals has dropped from **32% to 25%.**

2 AI sparks serious concerns.

72% of Mac users fear that artificial intelligence (AI) accelerates the rise of advanced cyber threats. Only **34%** believe that AI-powered tools can make them feel more protected.

Over half of respondents feel they lack control over the data they share with AI.

3 Perceived dangers overshadow important threats.

72% of Mac users are concerned about identity theft, despite only **16%** experiencing it personally. Meanwhile, **64%** are concerned about malware, while **31%** have been affected.

Overall, **66%** of Mac users have faced at least one cyber threat within the past year.

4 Software beats safe habits as the key to safety.

64% of respondents believe that proper software alone can fully protect them from cyber threats.
At the same time, **48%** reuse passwords on multiple accounts and **59%** save them in web browsers.
25% of Mac users still often skip software updates.

5 Apple's built-in security tools are popular, but not XProtect.

Mac users actively rely on iCloud Keychain, FileVault, and Time Machine in their respective security software categories, but when it comes to malware protection, only **4%** name XProtect as their antivirus.

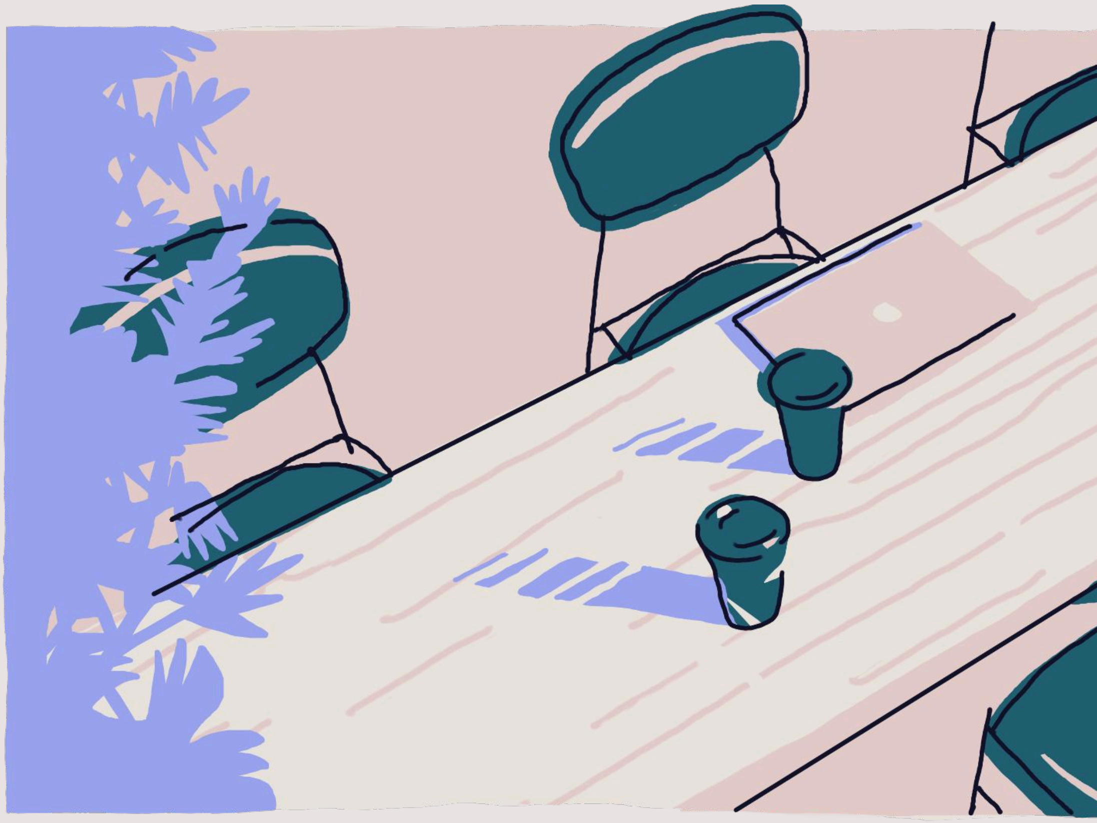
Antivirus is the tool most often purchased separately, **62%** of people who use it pay for third-party protection. For password managers, that number drops to just **30%.**

6 Mac users still need guidance and support.

Half of respondents actively seek information to stay informed about cybersecurity threats.

68% would like to talk to someone qualified about online safety. The share was **52%** in 2023.

Every third turns to AI-generated advice — the same share as those who seek help on forums, in articles, videos, or turn to their friends.

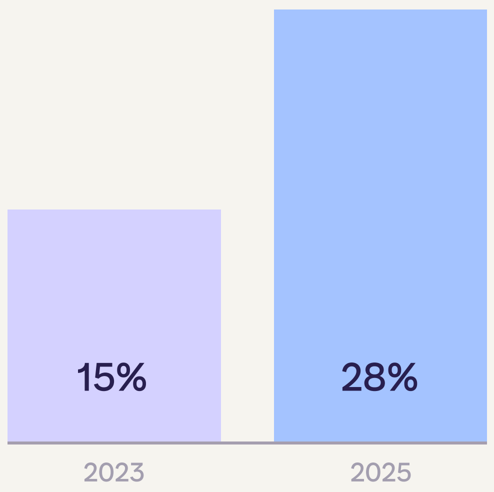


Perception of security and behavior

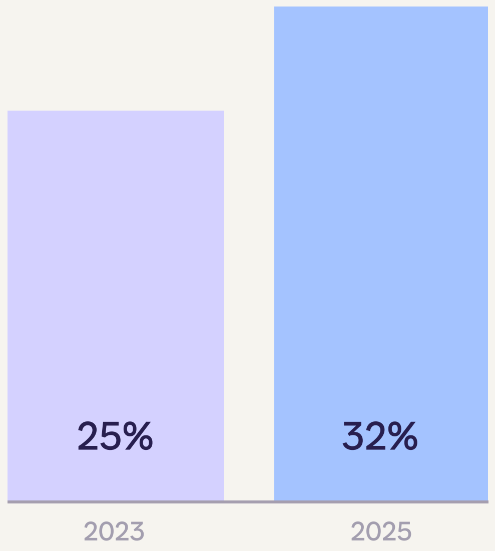
The myth of malware-free macOS is crumbling, yet too much faith is placed in security software over healthy safety habits.

Mac users rethink their immunity to cyber threats

Since 2023, the share of Mac users who think that malware does not exist on macOS has dropped **(15% vs. 28%)**



Respondents are less confident that cybercriminals are not interested in their data **(25% vs. 32%).**



In addition, the long-standing belief that macOS is inherently secure is fading. **Only 28% agree they don't need additional security tools on their Macs.** Respondents actively use iCloud Keychain & Passwords, Safari, and other security features from Apple.

Take a look at how Mac users view security software on their computers ↗

As concerns are rising, Mac users are turning to security software for protection. **64% of respondents believe that proper software alone can fully protect them from cyberthreats.** People expect software to provide the ultimate protection, forgetting that no tech can help if they neglect safety rules online.

"What can be behind the growing awareness among Mac users? MacPaw's in-house research team, Moonlock Lab, has a few hypotheses.

In 2024, **malware detections on Macs protected by Moonlock Engine rose by 20%** compared to 2023. As more people experienced malware firsthand, their perception of Mac security may have soured.

Security teams — including Moonlock Lab — work continuously to raise awareness about well-known and emerging threats, collaborating and sharing findings within the cybersecurity community. We hope that our public announcements circulating online help Mac users become more aware and less naive about their security.

Interestingly, detections declined again in 2025, nearing previous levels. But what might look like good news actually hides a dangerous trend.

macOS malware has become more serious and industrialized, and news about it leaves stronger impressions on Mac users. We're seeing hackers move on to more targeted, sophisticated malware, leaving adware and PUAs as petty tools. They create new macOS stealers and backdoors instead, draining victims of all passwords and credentials, leaving them with hacked accounts and empty digital wallets.

Mykhailo Pazyniuk

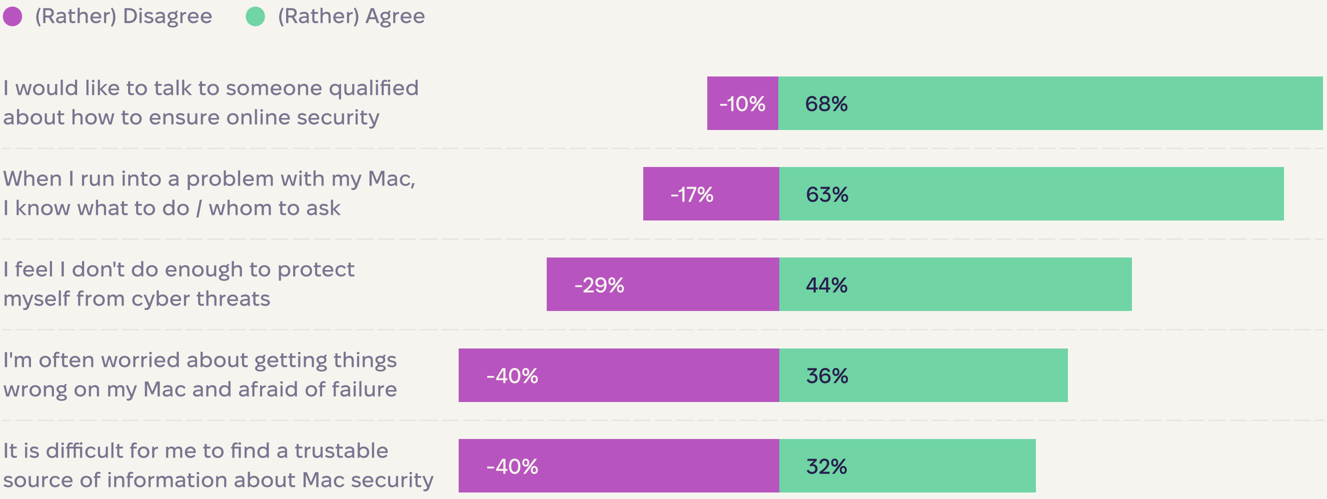
Malware Research Engineer
at MacPaw's Moonlock Lab

In the face of rising threats, Mac users still need support and guidance

As before, respondents feel they don't do enough to protect themselves from cyber threats **(44% vs. 45%).**

They are looking for information, and **32% say it's difficult to find a reliable source of information about Mac security.**

The share of Mac users who want to talk to someone qualified about online safety **has risen significantly (68% vs. 52%).**



Sample: Mac Users aged 18+, USA, N=1000. Respondents rated their agreement with each statement using a 5-point scale:
1 - Totally disagree, 2 - Rather disagree, 3 - Neither agree nor disagree, 4 - Rather agree, 5 - Totally agree.

The final chapter of this report goes into more detail on sources of information and cybersecurity guidance for Mac users.

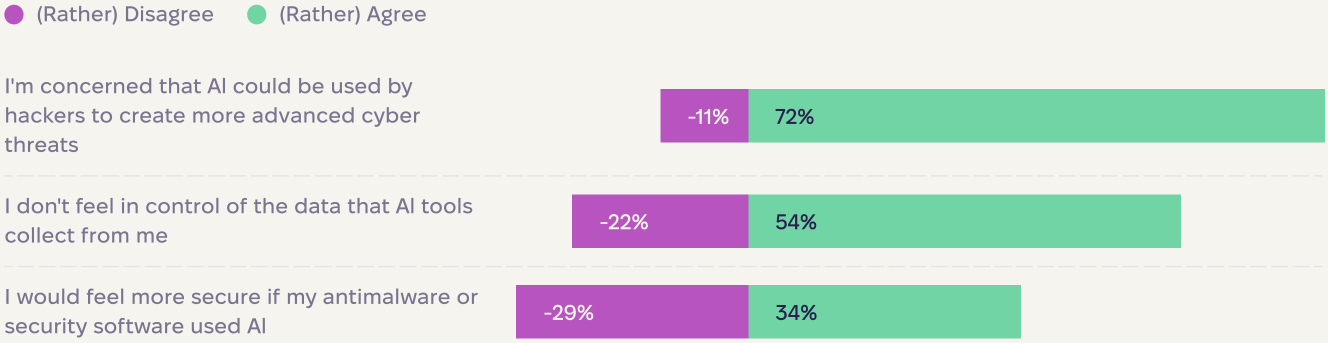
Jump there to find out more:

Guidance and support ↗

AI is only stirring the pot

72% are concerned that hackers could use AI to create more advanced cyberthreats, while only **34%** say they would feel more protected if their security software used AI.

More than half of Mac users feel they are not in control of the data they share with AI tools.



Sample: Mac Users aged 18+, USA, N=1000. Respondents rated their agreement with each statement using a 5-point scale: 1 - Totally disagree, 2 - Rather disagree, 3 - Neither agree nor disagree, 4 - Rather agree, 5 - Totally agree.

" A wild card in the fight between defenders and attackers

AI accelerates the cat-and-mouse game we're in. Malicious actors use it to boost performance of their social engineering attacks and scale them more quickly. On the other hand, security teams are getting faster in detection, analysis, and blocking threats with the help of AI too. Where will the scales tip? It seems it may never settle.

Recent findings from Moonlock Lab highlight how attackers are already using AI:

- A sample of macOS malware that hinted at the use of the OpenAI API to generate "highly personalized phishing content."
- A botnet that uses AI for social engineering and phishing through libraries like Selenium — suggesting that malware can control a web browser automatically.
- Moonlock reports on a Russian-speaking attacker, barboris, using ChatGPT to create a macOS stealer packaged with PyInstaller, despite having no coding experience. This malware extracted data from iCloud Keychain and targeted crypto wallets.

Read the full report here: Moonlock's 2024 macOS Threat Report

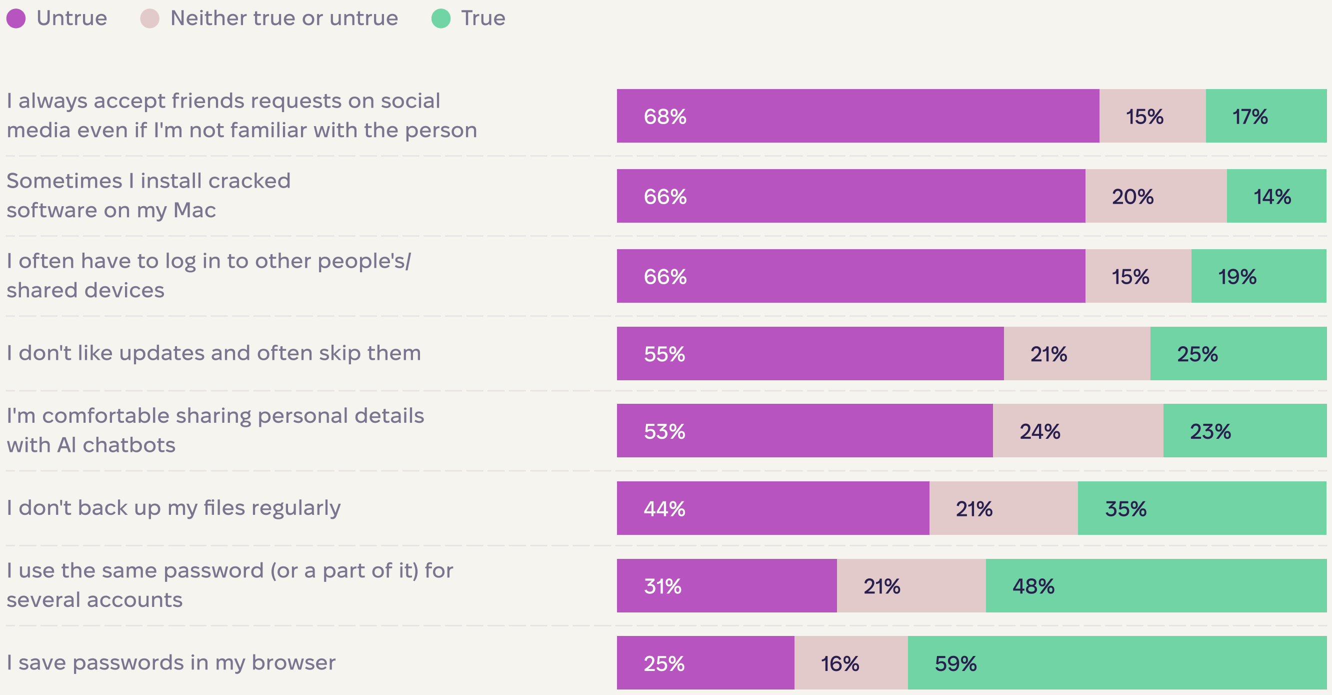
Kseniia Yamburh

Malware Research Engineer
at MacPaw's Moonlock Lab

Passwords are a critical weak point in Mac security

Since 2023, fewer Mac users report engaging in certain risky behaviors, such as installing cracked software, skipping app updates, or accepting friend requests from strangers. This shows a cautious shift toward safer digital habits.

The biggest risk still comes down to passwords. Nearly **half of respondents admit reusing passwords (or parts of them) and saving them in browsers.** Convenience keeps winning over secure habits, leaving passwords a major vulnerability.



” If we’re not careful with passwords, infostealer malware will come after them

Infostealers are growing on Macs, and how people handle their passwords can determine whether the damage stays minor or ends in a total account takeover.

Stealers evolve fast, easily breaking through browser safeguards to access stored passwords. One successful breach — and bad actors have access to your emails, accounts, and crypto wallets. The situation gets even worse when attackers also get access to corporate SSOs or Google Workspace. Then there is lateral movement, and complete control over the victim's personal and work life follows.

Storing passwords securely shrinks the attack surface and limits the damage if theft occurs. With a password manager, a breach of one service won’t put your entire digital life at risk.

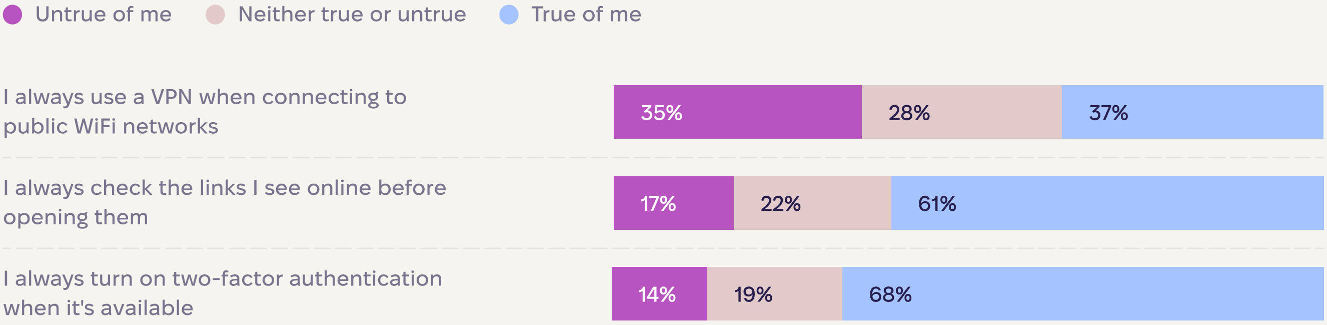
Kseniia Yamburh

Malware Research Engineer
at MacPaw’s Moonlock Lab

VPN adoption still has a long way

Most Mac users are already in the habit of avoiding suspicious links and enabling two-factor authentication. However, **only 37% of respondents said they consistently use a VPN when connecting to public networks.**

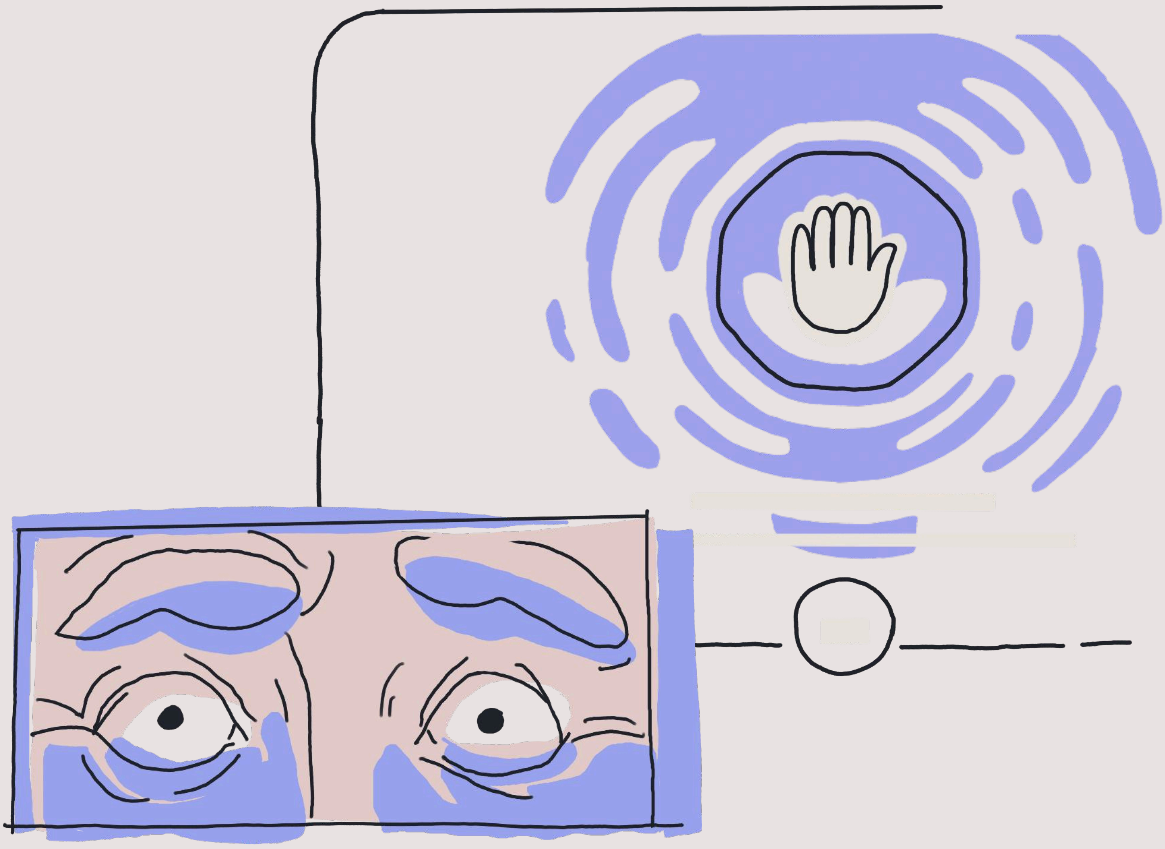
% of Mac users who say the following about these statements



In mid-2024, Australian Federal Police charged Michael Clapsis, 42, for setting up malicious twin Wi-Fi networks in domestic airports of Perth, Melbourne, and Adelaide, as well as on board flights. These networks harvested passengers' email and social media credentials.

This attack didn't target macOS vulnerabilities directly, but it exploited users' trust toward networks. A Mac can join a known SSID automatically without notifying the user, and once connected to an evil twin network, even Safari, Mail, and other apps could have their traffic intercepted.

A VPN provides a secure, encrypted tunnel for all internet traffic, even if a user connects to a malicious Wi-Fi access point. Since a properly configured VPN encrypts all traffic by default, attackers can't read or tamper with the data — even on an evil twin network.



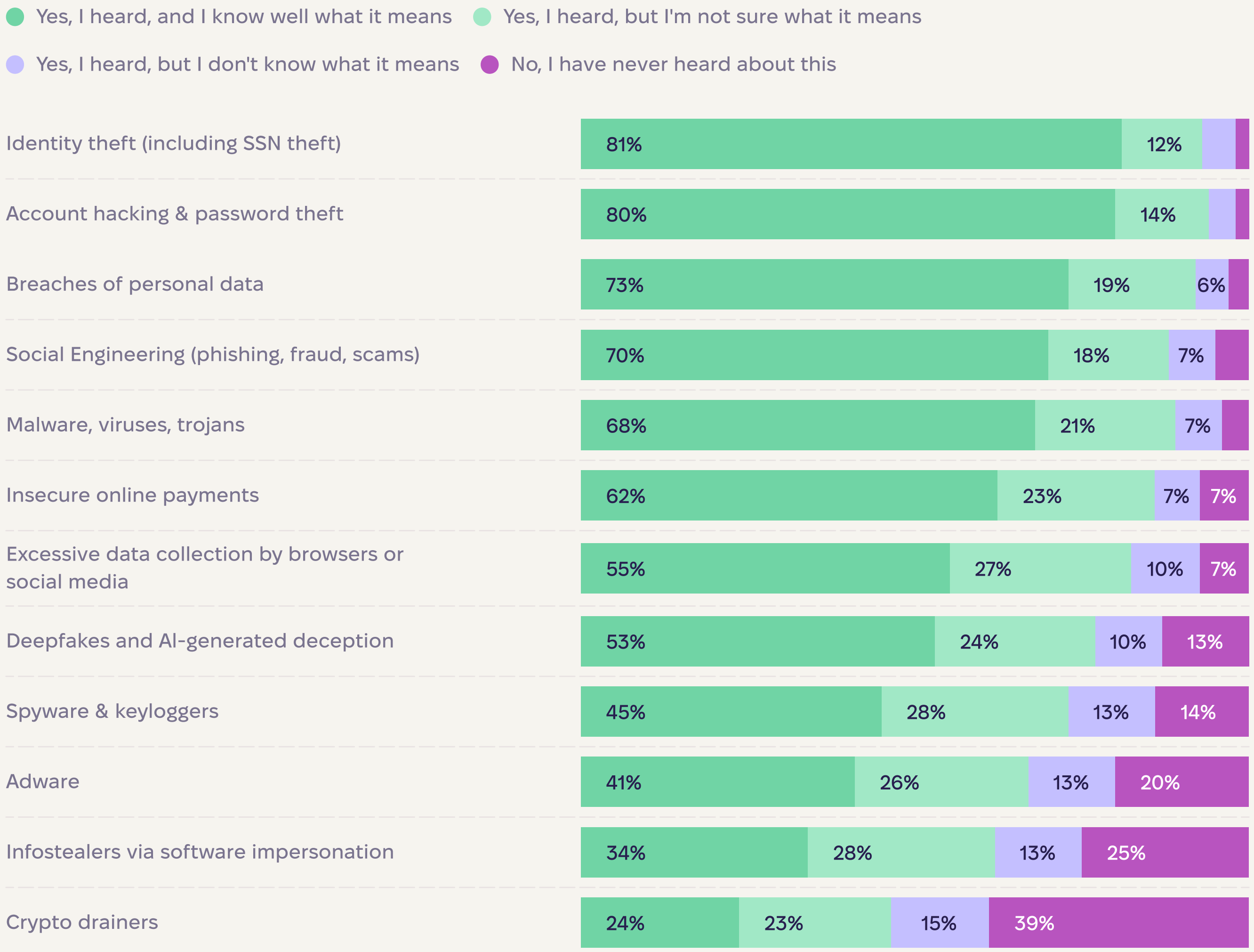
Awareness and experiences

Mac users recognize many cyber risks, yet they tend to overlook the rising threat of advanced malware.

55% of Mac users are well aware of cyber threats

That’s the share of respondents who heard and are familiar with 7 or more cyber threats out of 12 listed below.

Respondents were asked to agree or disagree with the following statements



Only 10% of Mac users are well-informed about all listed threats.

The share of respondents familiar with personal data breaches, identity theft, account hacking, and insecure online payments **has increased by 5 to 8 percentage points since 2023.**

In contrast, awareness is the lowest when it comes to adware, infostealers, and crypto drainers.

A dangerous gap in awareness and the reality of the Mac security landscape

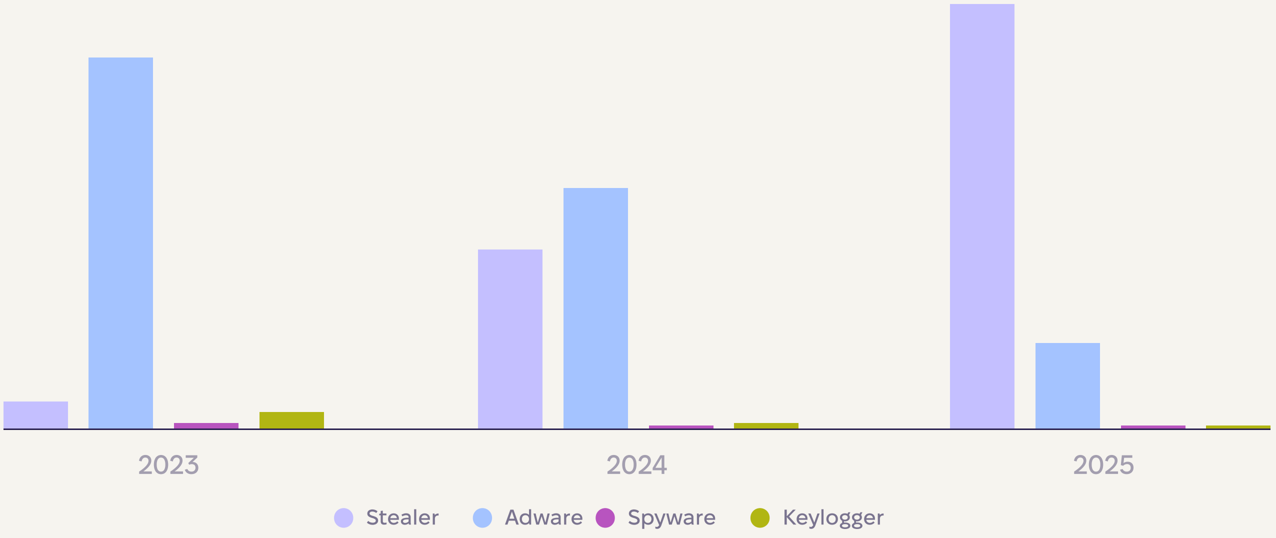
In 2025, we observe a growing number of macOS infostealers, which often double as crypto drainers, detected on Macs protected by Moonlock Engine. While this category of malware is peaking, others appear to be declining.

The decrease in other malware categories on Mac can also be explained by the fact that infostealers have started to include resident modules such as **backdoors, keyloggers,** and others as additional functionality. With this in mind, we can highlight how once-major malware types are fusing into a broader — and more dangerous — category of stealers.

Look at how these malware types spread on Macs:

- In 2023 there was **1 stealer infection for every 2,000 adware infections.**
- By 2025, that ratio shifted to **1 stealer case for every 135 adware cases.**

So even though adware still exists and is more likely to infect an unsuspecting Mac user, data stealers have increased their presence relative to adware by nearly 15 times since 2023.



Mykhailo Pazyniuk

Malware Research Engineer
at MacPaw's Moonlock Lab

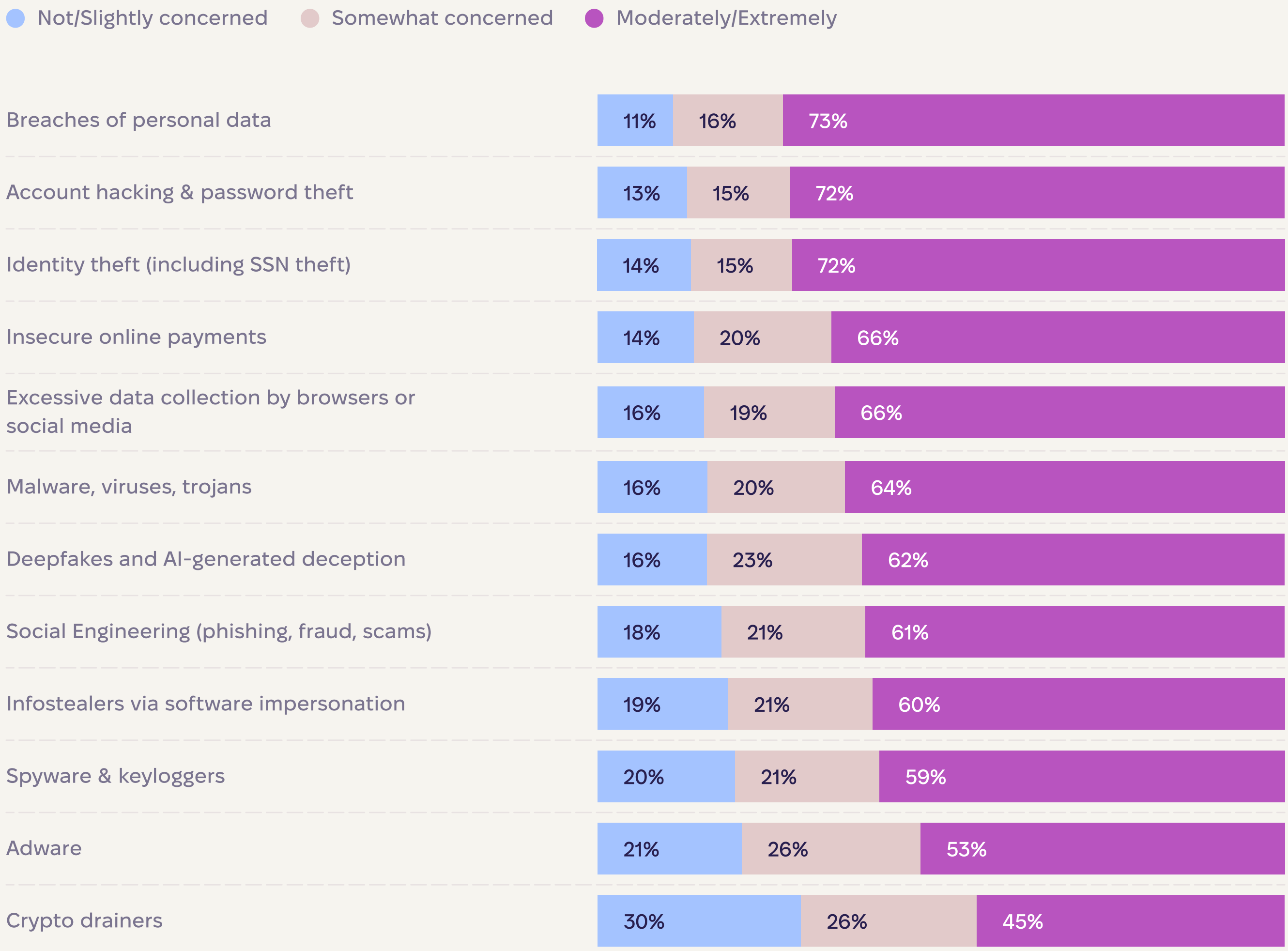
The more aware Mac users are of a threat, the greater their concern

Commonly known threats like identity theft, account hacking, and data breaches cause the most concern among Mac users. Some have grown significantly since 2023:

- **account hacking (+6 percentage points),**
- **excessive data collection (+6 percentage points),**
- **personal data breaches (+9 percentage points).**

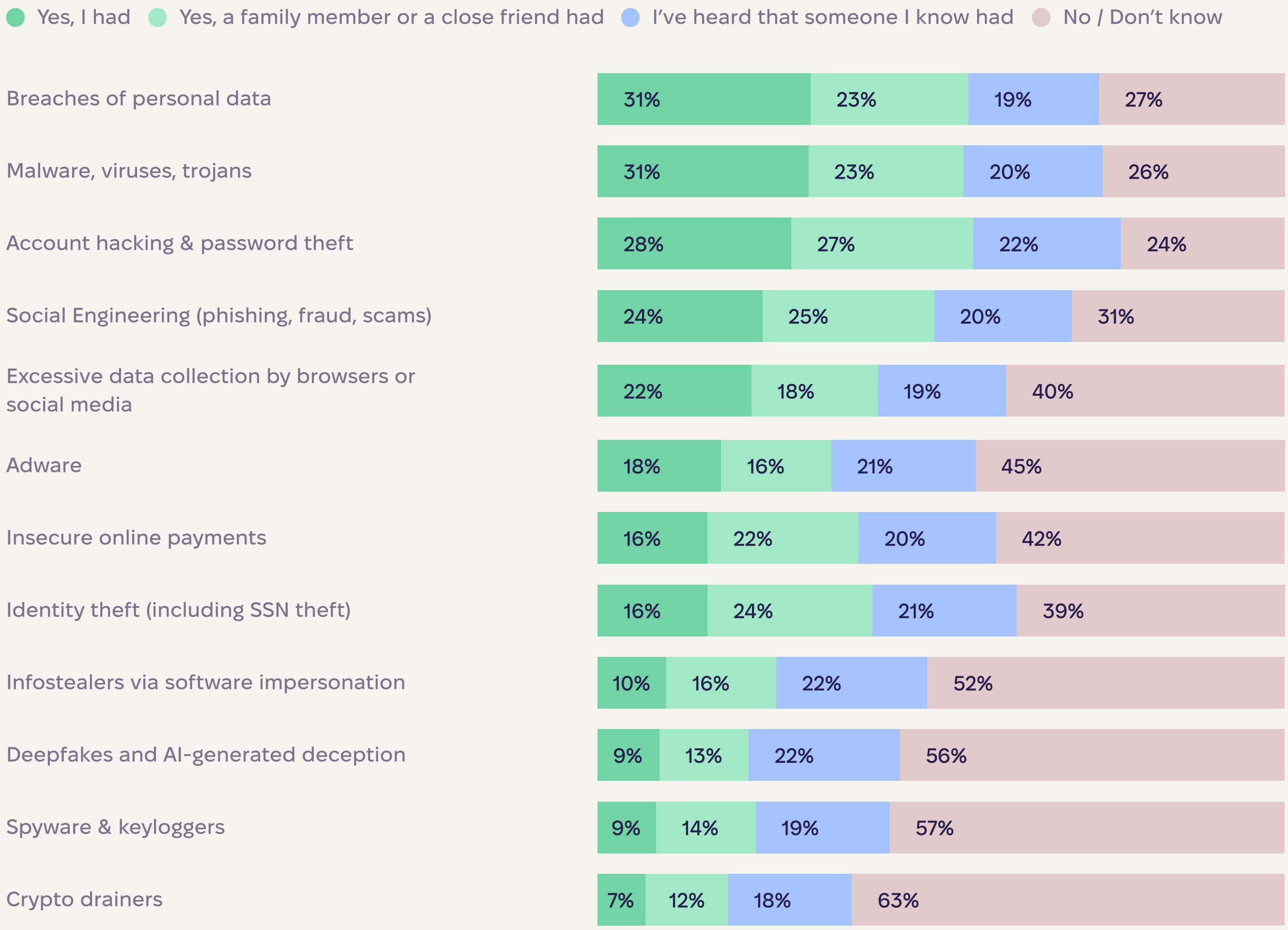
Meanwhile, lesser-known threats — adware, infostealers, and crypto drainers — sit at the bottom of the list.

How concerned do you feel about the following threats?



66% of Mac users have faced at least one of these threats within the past year

Have you, your friends, or your family experienced the following in the past 12 months?



When comparing concerns with experiences, it's clear that Mac users don't need to experience a threat personally to be worried about it.

Identity theft ranks as the second-biggest concern, yet few have actually experienced it.

Malware, on the other hand, has hit nearly one in three Mac users, but doesn't even make the top five concerns.

This contrast highlights a disconnect between perceived and actual risk, suggesting that user awareness is shaped more by perceived severity than by lived experience. It also shows that Mac users underestimate the damage malware can cause — and that security teams must work even harder to draw attention to its real impact.

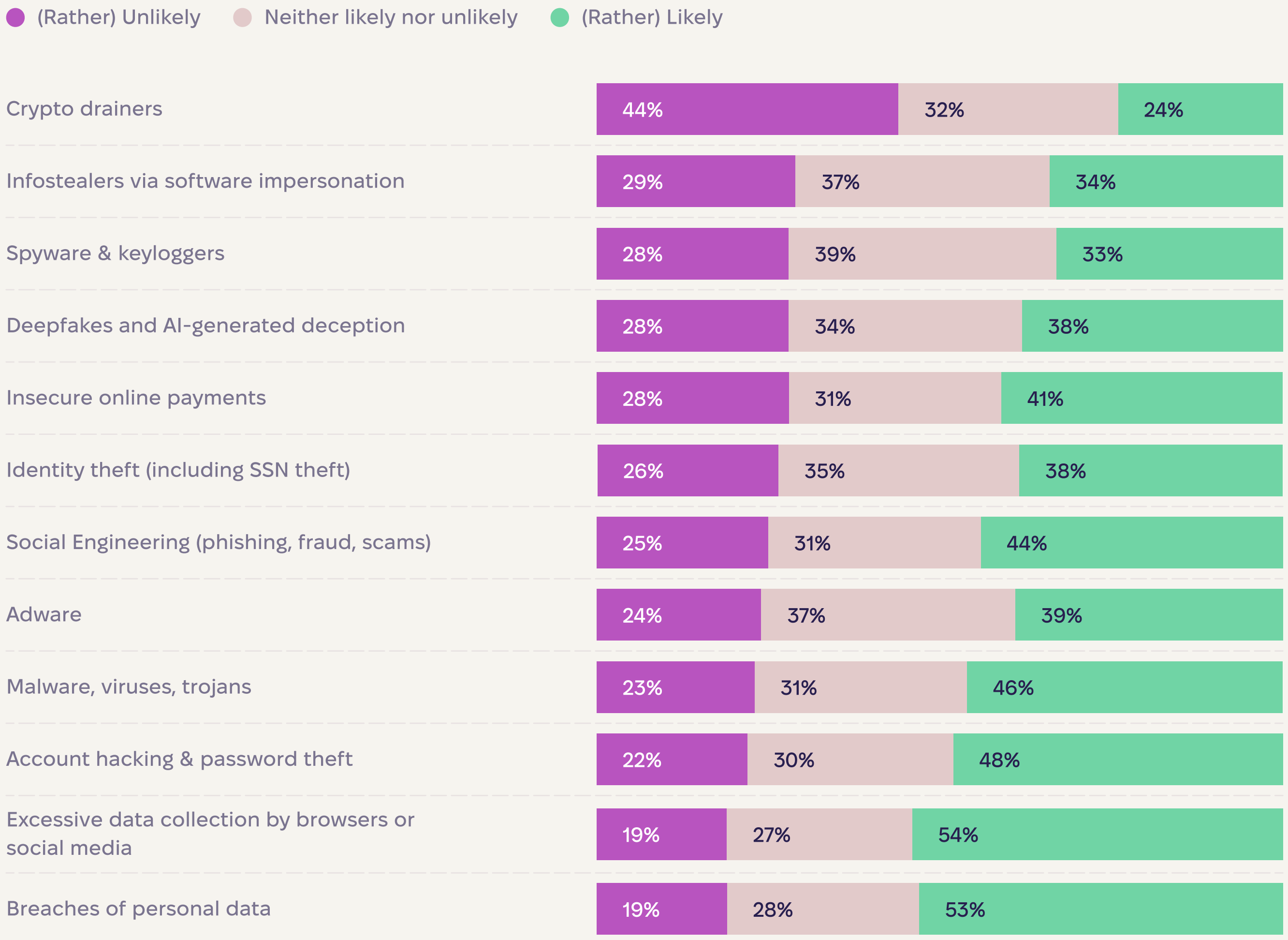
About half of Mac users highly estimate the likelihood of becoming a victim of a particular cyber crime

Account hacking, excessive data collection, and personal data breaches are seen as likely by approximately half of respondents.

The highest estimated likelihood is for **collection of personal data from browsers and social networks (54%),** although fewer respondents report to have actually experienced it compared to more common issues like malware.

Crypto drainers are seen as the least likely threat, likely due to the limited use of cryptocurrency in Mac users' daily lives.

To your mind, how likely are you to experience the following?

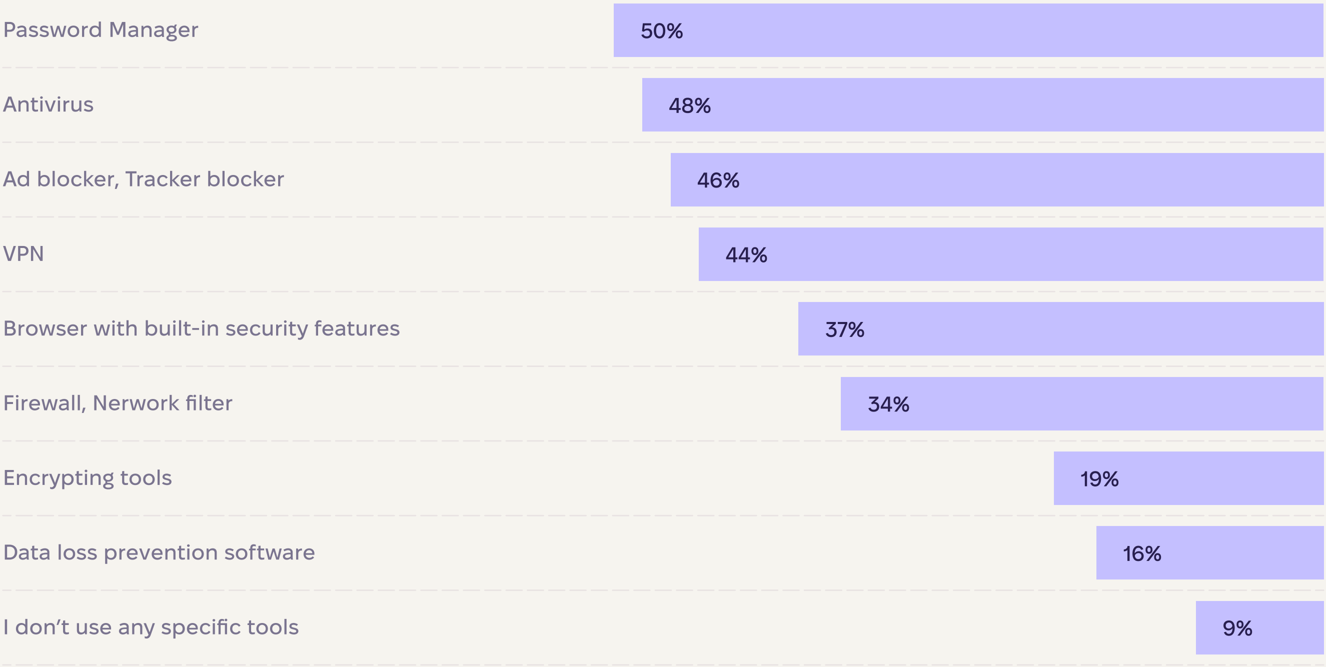


Security software usage

Mac users rely heavily on Apple's built-in security tools. Apple's default software covers a significant share of needs for security products.

Password managers are the leaders in the security software category among Mac users...

Only 9% of respondents reported not to use any specialized security tool whatsoever.



... but there’s a catch:

Password managers (50% => 42%)

8% of those using a password manager store their passwords exclusively in web browsers. If those are excluded, the share of password manager users decreases to 42%.

Secure browser (37% => 20%)

37% of respondents named Safari and Google Chrome as secure. If those answers are excluded, the share of users of browsers with built-in security features decreases to 20%. On top of that, 57% of those who say they use a secure browser are referring only to Safari or Google Chrome.

Mac users rely heavily on macOS built-in security tools

17%

of VPN users rely on the default macOS VPN

56%

of encryption tool users rely on FileVault

57%

of firewall and network filter users rely on the built-in macOS firewall

62%

of data loss prevention users rely on Time Machine

72%

of password manager users rely on iCloud Keychain

Respondents first answered whether they use any cybersecurity software and only then specified which tools they rely on. Those who mentioned macOS built-in tools did so consciously as active users, not because these tools are enabled by default.

This shows a strong level of trust in Apple's native security ecosystem, but also indicates that many users may not be exploring or adopting additional layers of protection beyond the defaults.

72% of password manager users rely on iCloud Keychain. Why might this be alarming?

Using a third-party password manager with a master key that is not tied to Mac login credentials or TouchID can help minimize these risks.

Cloud Keychain & Passwords is a key to everything: online accounts, mail, Wi-Fi keys, tokens — even codes for two-factor authentication. That makes it a prime target for attackers, who build advanced stealer malware designed to take everything in one sweep.

To do that, attackers have become masters of social engineering and deception. They often use fake macOS system alerts to trick users into entering a password that unlocks their Mac, system settings, and Passwords as well.

Kseniia Yamburh

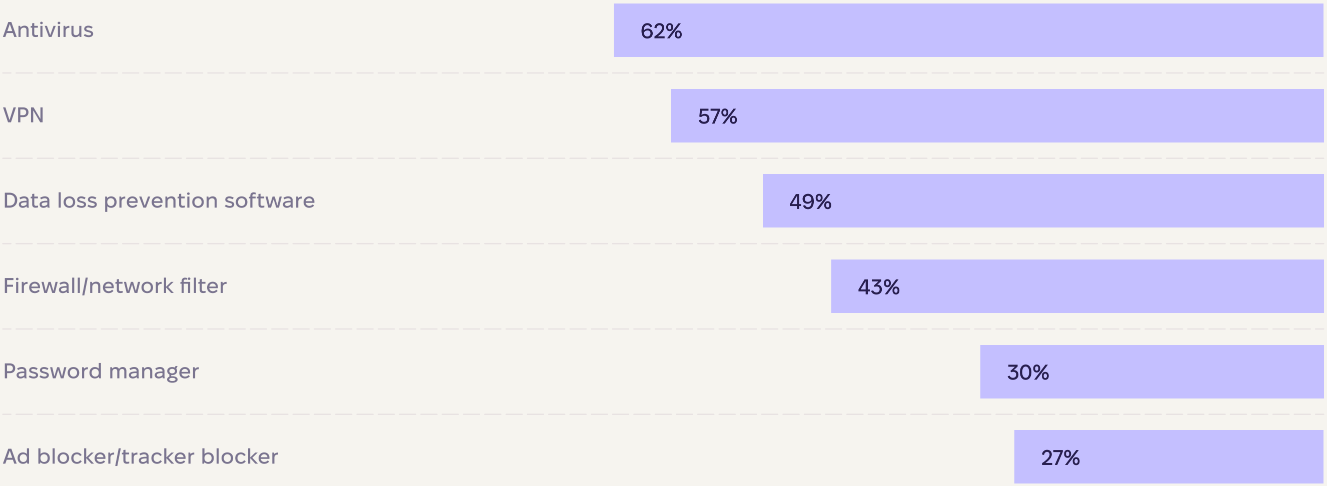
Malware Research Engineer
at MacPaw's Moonlock Lab

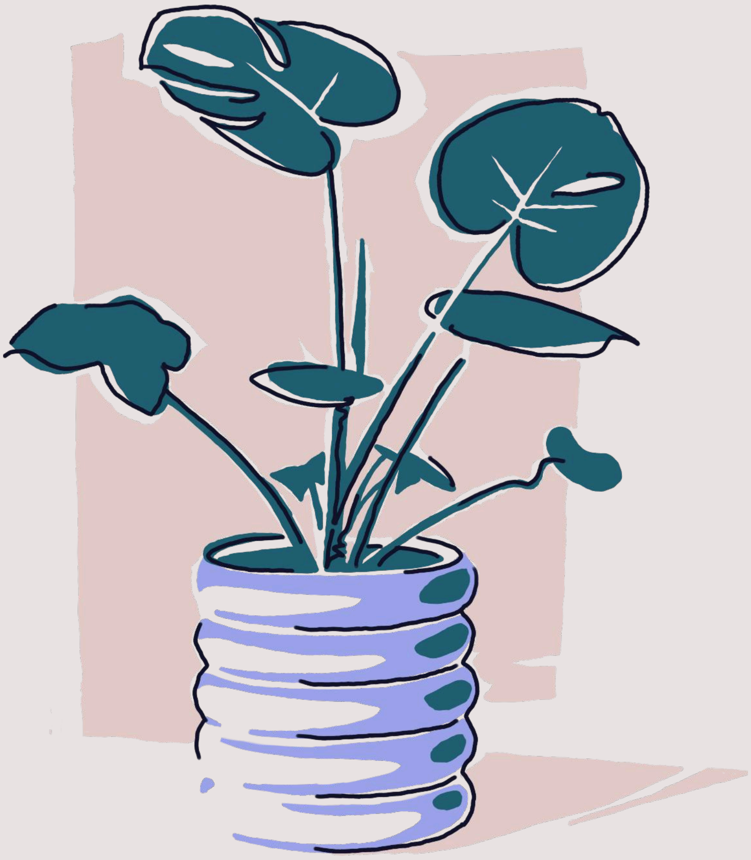
When it comes to malware protection, Mac users are more likely to seek help from third-party apps

Only 4% of those who reported to use antivirus on their Mac rely on Apple's XProtect.

62% of antivirus users are willing to pay for the tool. It's a clear leader among paid security software on Macs.

Share of paid users across different categories of security software on macOS





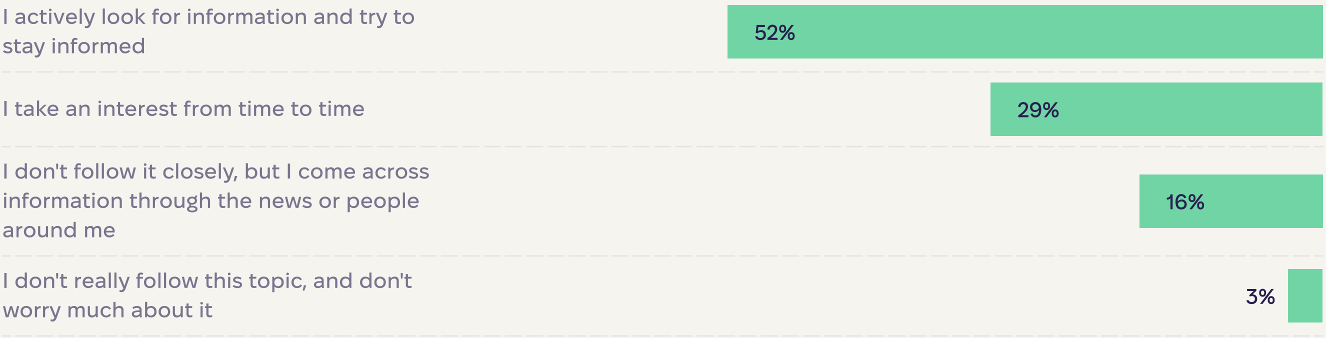
Guidance and support

Mac users learn about cybersecurity the same way they learn about most things: through social media, the news, and people they know.

Mac users are actively trying to stay informed about cyber threats

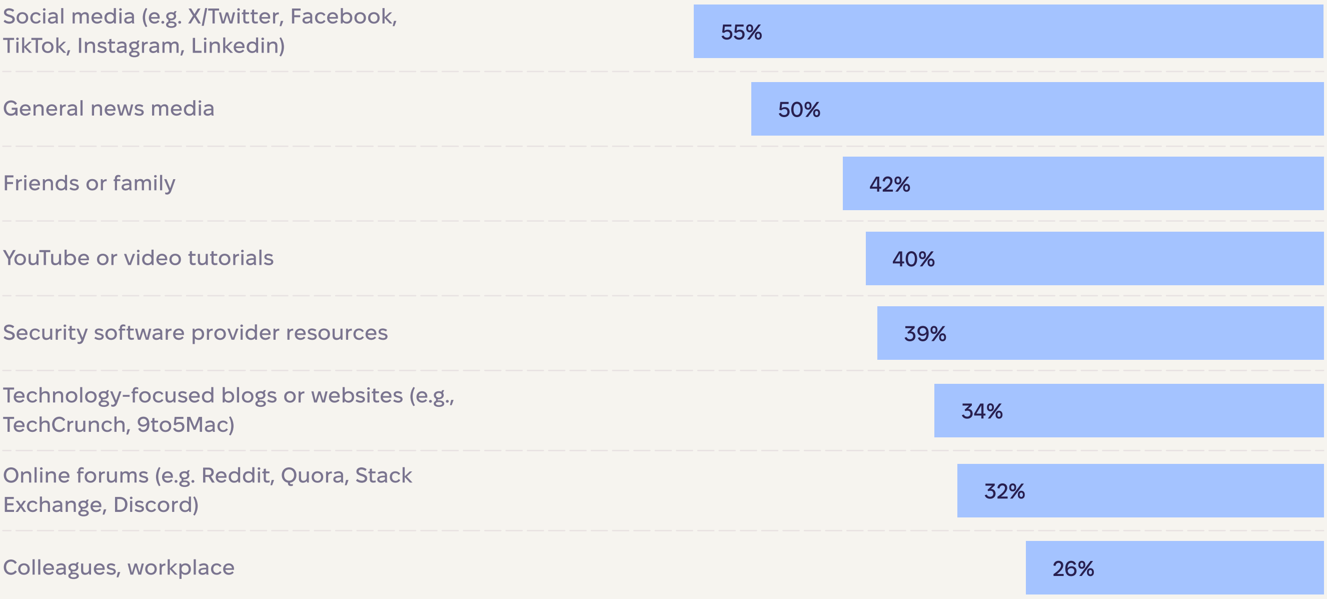
Half of respondents actively seek information to stay informed about cybersecurity threats, while another **45% show only occasional or passive interest.**

How closely do you follow news and updates about cybersecurity threats?



Social media and general news outlets are the primary sources of cybersecurity information for Mac users. About one in three respondents turn to tech sites and forums. Friends and family come up more often than the workplace as go-to sources of information.

Where do you usually get information about online security or digital safety?

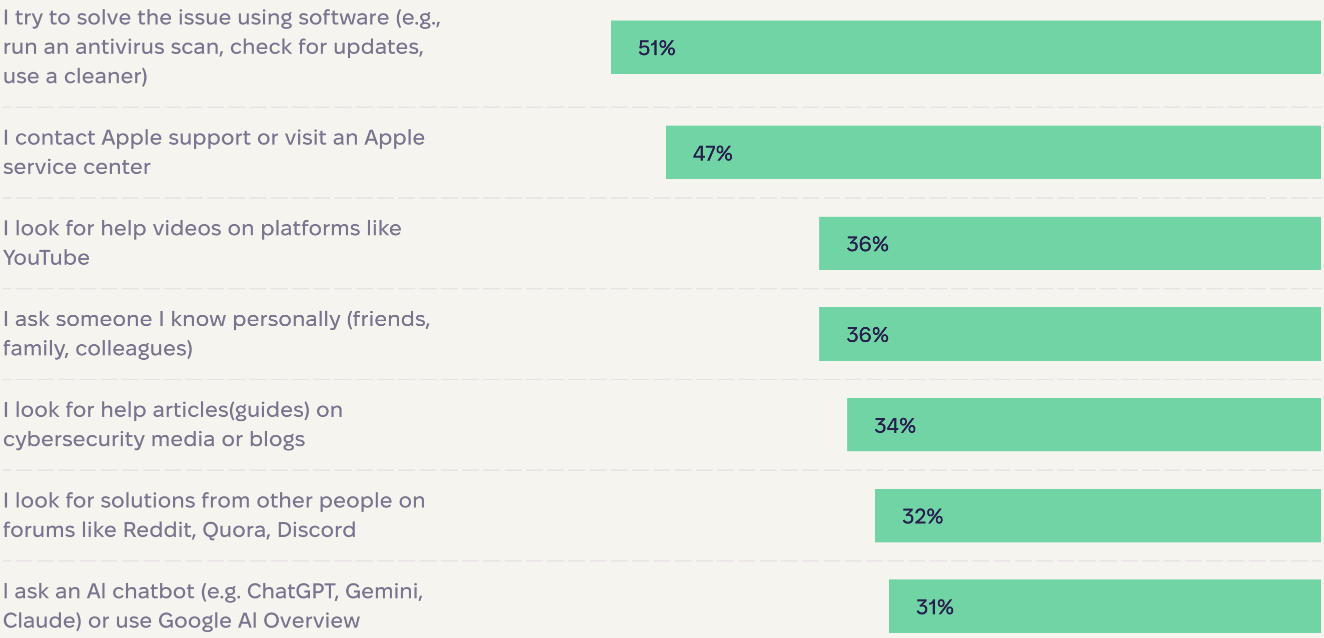


At signs of trouble, Mac users rely on software solutions to uncover the problem

When Mac users suspect a cybersecurity issue, their top actions are to run security software or contact Apple Support.

About one-third also turn to AI-generated advice — the same share as those who seek help in forums, articles, videos, or from friends.

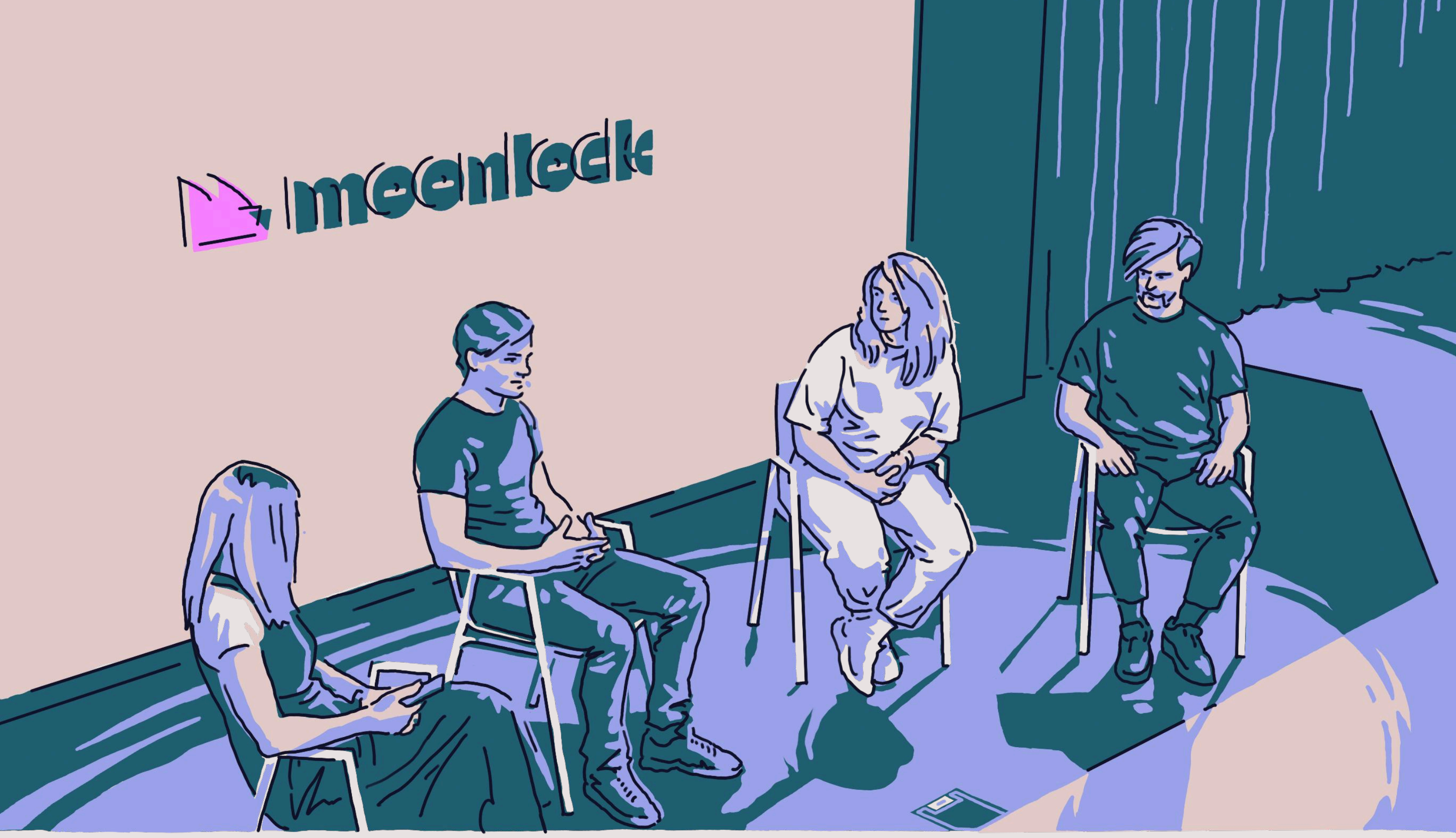
When you encounter a cybersecurity issue or something suspicious on your Mac, what do you usually do?



About Moonlock by Macpaw

MacPaw is a global software development company building a digital ecosystem designed to supercharge productivity for Mac users. Its cybersecurity division, Moonlock, focuses exclusively on the cybersecurity needs of Mac users.

Moonlock uncovers and studies cyber threats daily. The team has discovered new Atomic macOS Stealer variants, tracked down Poseidon developers, and exposed sophisticated malvertising campaigns targeting macOS. With original threat research at the core, MacPaw has built a proprietary anti-malware tech — Moonlock Engine — and has been actively protecting Mac computers all over the world.



Thank you!

Follow Moonlock for in-depth malware research, recent news and stories about Mac security, and new protective tech that guards Apple fans from cyber threats.

MOONLOCK.COM →