

Consumer Cyber Readiness Report

2026



Cyber Civil
Defense Initiative

CR Consumer
Reports

AD ASPEN
DIGITAL
an aspen institute

 GLOBAL
CYBER
ALLIANCE

Introduction

THE LOW COST OF reaching people using digital technology, poorly regulated payment platforms, a lack of rapid response or reporting mechanisms, and the abundance of personal data leaked on the dark web has led to billions lost in scams. For the last five years, Consumer Reports, Aspen Digital, and the Global Cyber Alliance have reviewed findings from nationally representative surveys fielded by Consumer Reports to examine how American consumers view and manage their digital security and privacy. In 2026, Consumer Reports continued to explore Americans' cybersecurity and privacy practices, but has taken a deeper look into frauds and scams. We wanted to understand their prevalence, who is more or less vulnerable, and what tips people off to scam attempts.

The bulk of this report deals with a single recent survey that asked

respondents about scams and scam avoidance. Through this survey, we learned that about nine in 10 Americans have encountered at least one type of cyberattack or digital scam attempt, and 17 percent have fallen victim to one. We define getting scammed or falling victim to a scam as losing money even if the victim's choice of payment method meant that they got their money back. Clearly, the stakes are high. Consumers are encountering scams on social media, text platforms, phone calls, and while shopping online.

In this year's report, we share who is most likely to lose money from a scam, who is likely to realize they are being scammed and walk away, and the precautions consumers are trying to take. Read on for a deeper understanding of how consumers are experiencing the scam economy in 2026.

9
in
10
Americans
have
encountered
at least
one type of
cyberattack
or digital
scam

Source: Consumer Reports
nationally representative
Cyber Readiness Survey
of 4,682 US adults



CRAIG NEWMARK
Founder of craigslist, craig newmark
philanthropies, and Take9



Scams are felt by everyone and rapidly evolving thanks to AI. We need to give consumers straightforward tools to keep them safe online, like with the [Take9](#) campaign, while continuing to push for better policies and industry support. The report shares a lot of good data on where we need to focus our efforts and who we need to support.

About the surveys

In Spring 2026, Consumer Reports conducted a custom-designed, nationally representative multimode [Cyber Readiness Survey](#). NORC at the University of Chicago administered the survey from March 13–April 10, 2026, through its AmeriSpeak® Panel. In total, NORC collected 4,682 interviews. The margin of error for the sample of 4,682 is +/- 1.91 at the 95 percent confidence level.

We conducted an additional nationally representative multimode [American Experiences Survey](#) administered by NORC at the University of Chicago from May 7–18, 2026, through its AmeriSpeak® Panel to a nationally representative sample of 2,082 adult U.S. residents.

Both of these surveys included trending questions repeated from previous iterations of these surveys. This includes nationally representative American Experiences Surveys from [June 2022](#) (administered to 2,103 U.S. adults from June 10–21, 2022), [May 2023](#) (administered to 2,000 U.S. adults from May 5–16, 2023), [April 2024](#) (administered to 2,042 U.S. adults from April 5–15, 2024), [May 2024](#) (administered to 2,022 U.S. adults from May 9–20, 2024), [April 2025](#) (administered to 2,158 U.S. adults from April 10–21, 2025), and [May 2025](#) (administered to 2,333 U.S. adults from May 8–19, 2025).

All differences and changes over time mentioned in this report were found to be statistically significant controlling for gender, age, household income, educational attainment, region, race/ethnicity, urbanicity, and political leaning.



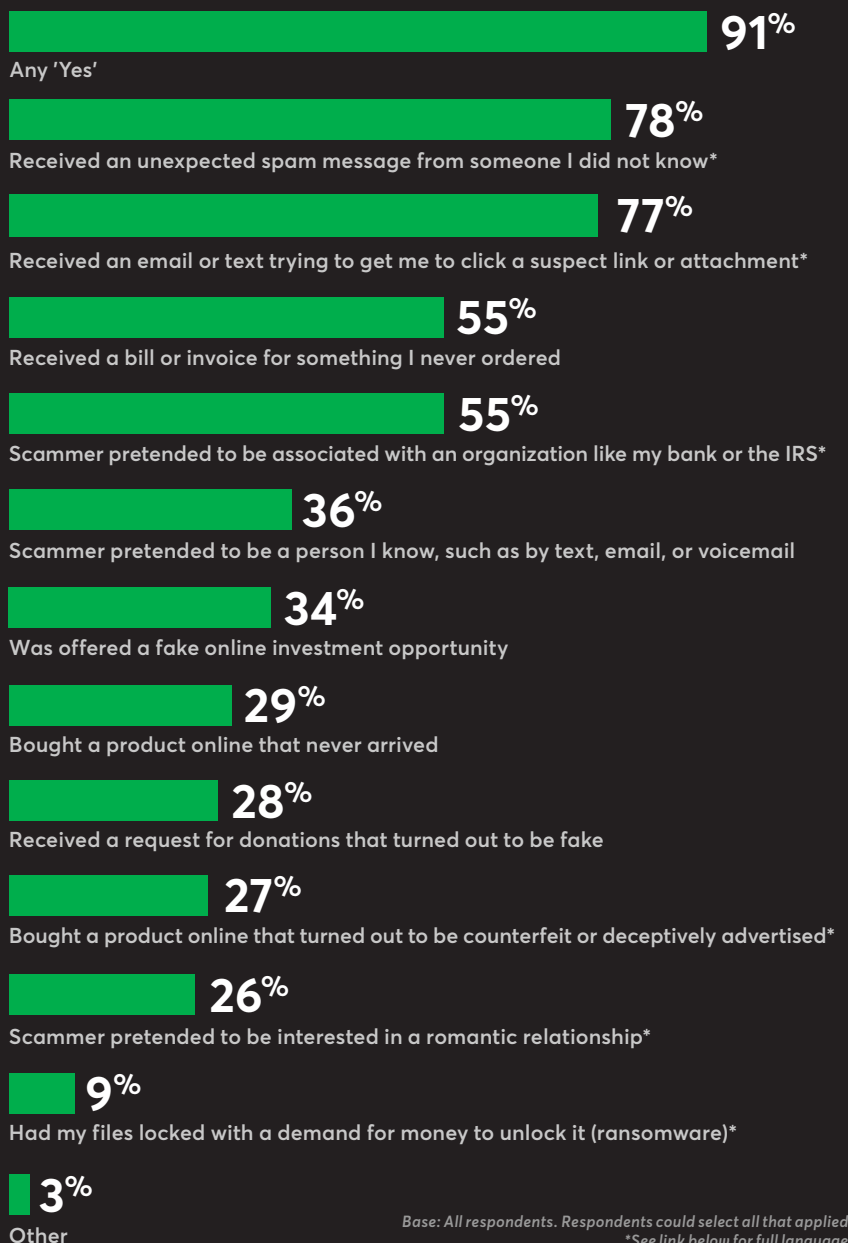
Digital scams are everywhere

SCAM ATTEMPTS

Digital scam attempts are incredibly common, with 91 percent of Americans reporting that they have encountered at least one type of cyberattack or digital scam attempt that we asked about. The most common attempts involve spam messages from people the recipient doesn't know (78 percent) and emails or text messages trying to get the recipient to click on a suspect link or attachment (77 percent).

But more than half of Americans also encountered fake invoices and scammers impersonating legitimate organizations, and about a third said a scammer pretended to be someone they know.

Which, if any, of the following types of cyberattack or digital scam attempts have you ever personally encountered?



Base: All respondents. Respondents could select all that applied.

*See link below for full language.

Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.

WHERE DID THE SCAMS START?

We asked Americans who had experienced an attack or scam attempt on what type of platform the most recent one began. Email was the most common platform, at 29 percent, followed by text messages or messaging platforms, at 18 percent. About one in 10 said it started with a phone call (11 percent) or on social media (10 percent). One in five (21 percent) were unsure where it started.

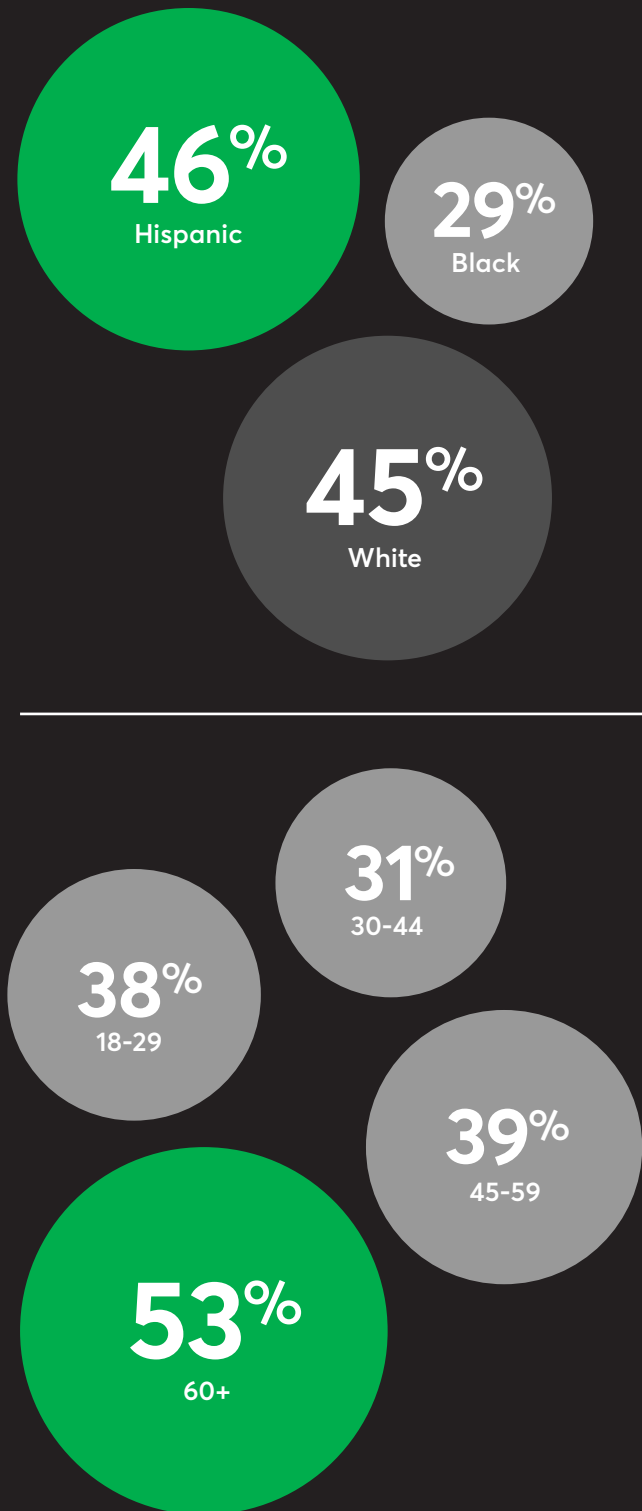
Given the prevalence of these scam attempts, losses are comparatively rare. Seventeen percent of Americans have fallen victim to a cyberattack or digital scam—that is, lost money, either permanently (10 percent) or temporarily (7 percent) said their payment method, like a credit card, allowed them to recover it).

For those who fell victim to a scam, their median loss (or what they would have lost if they were in the 7 percent who successfully recovered their money) was \$235.

WHO RECOVERED THEIR MONEY?

The oldest Americans (aged 60 and up) were also more likely to recover their money (53 percent vs. 39 percent or lower in younger groups). We also saw that Hispanic Americans were more likely to reclaim their money than Black Americans (46 percent for Hispanic Americans vs. 29 percent for Black Americans). While it looks like white Americans are also more likely to recover their money when compared with Black Americans in the circle chart to the right, the difference between Black and white Americans isn't statistically significant after controlling for other variables.

Percentage of Americans who were scammed who recovered money afterward (by demographics)

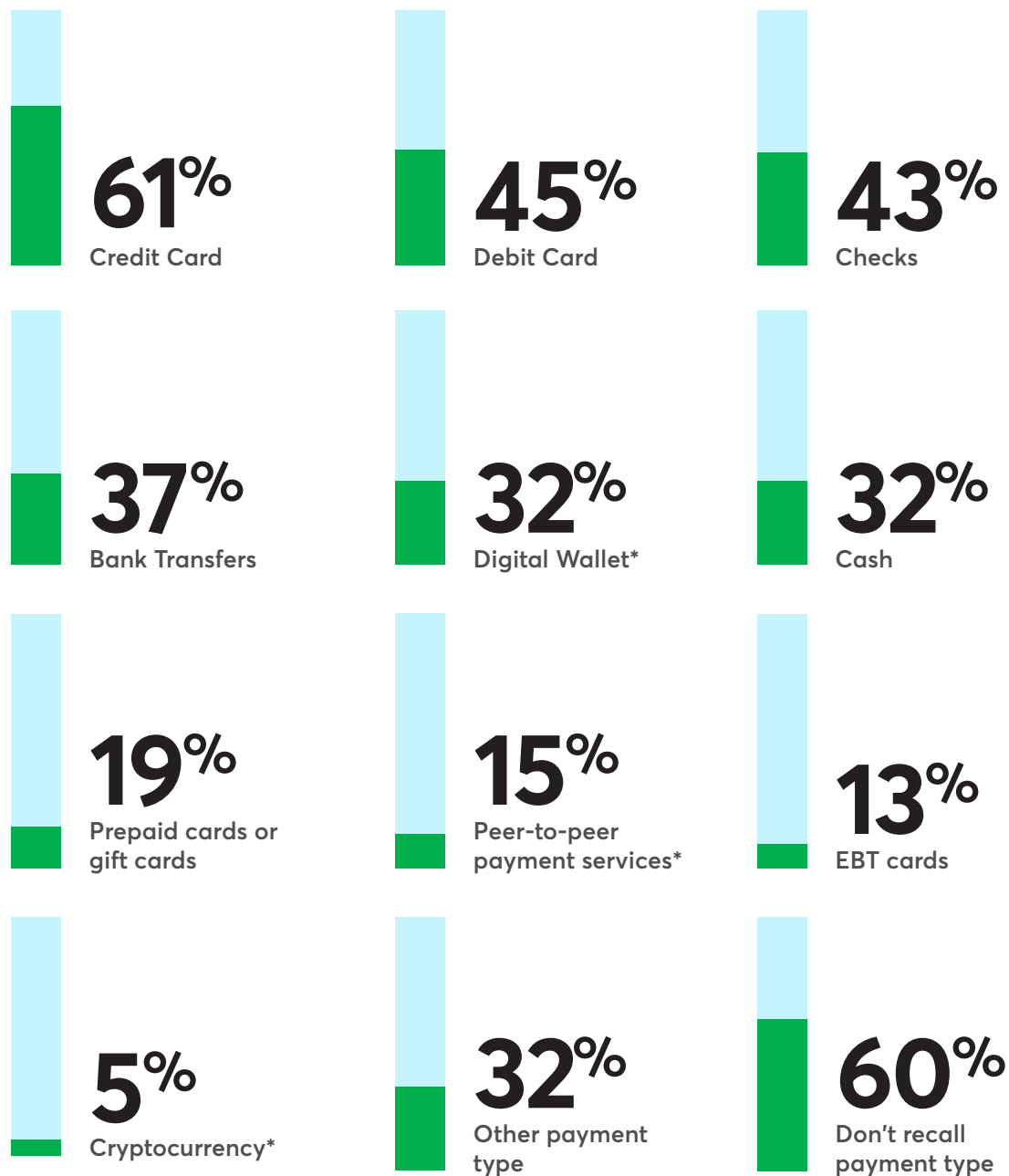


Base: Respondents who lost or would have lost money to a digital scam or cyberattack.
Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.

The ability to recover a payment made to a scammer was highly dependent on the payment method used, with credit cards being the safest—a majority of those who paid with credit cards recovered their money

(61 percent). This was higher than it was for those who paid with most other forms of payment, including debit cards and bank transfers. We will cover payment options again later, in the section on other risk factors.

Percentage of Americans recovering money after most recent scam (by payment method)



Base: Respondents who lost or would have lost money to a digital scam or cyberattack. *See link below for full language.
Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.

Account takeovers

IN ADDITION TO cyberattacks and digital scams, we also asked consumers about their experience with account takeovers, because these are often a precursor to a scam or used to scam others. For example, a scammer might take over an individual's Facebook account and then use the account to impersonate the original account owner to scam others.

We found that about three in 10 Americans have had at least one online account taken over. Such account takeovers could include those where a scammer impersonated the user, such as social media, email, or video game profiles, as well as

takeovers where the scammer simply used the account, such as streaming services, peer-to-peer payment services, or bank accounts.

Fourteen percent of Americans said they had a social media account taken over and used by a scammer, the most common of the impersonation-type takeovers we asked about. We believe the prevalence of such takeovers and their use as a potential vector for new scams indicates that social media platforms could do more to help users who experience an account takeover. For accounts that were taken over and then used by the scammer, the most common were bank accounts.



BRIAN CUTE
President and CEO
Global Cyber Alliance



The prevalence of account takeovers reminds us that basic cyber hygiene is still the single most important thing you can do. Strong, unique passwords for every account, multifactor authentication whenever it's available, and devices and apps updated with the latest security patches. These steps won't make you unhackable, but they can make you a much harder target.

Have you ever had an online account taken over this way?

Hackers or scammers take over people's online accounts and use them to post or send messages while pretending to be the account owner.



Yes, a social media account



Yes, an email account



Yes, an Amazon or other shopping account



Yes, a video game account (e.g., Steam)*



Yes, another type of account, please specify



No, none of my accounts have ever been taken over, as far as I know

31%

of Americans have had at least one account taken over in either type of way

Hackers or scammers take over people's accounts that do not have posting or messaging. The scammer does not pretend to be the account owner, but simply uses the account.



Yes, a bank account



Yes, a streaming service*



Yes, a peer-to-peer payment account*



Yes, a store or travel rewards account*



Yes, a food delivery account*



Yes, an investment or retirement account



Yes, another type of account, please specify



No, none of my accounts have ever been taken over in this way, as far as I know

Base: All respondents. Respondents could select all that applied. *See link below for full language.
Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.

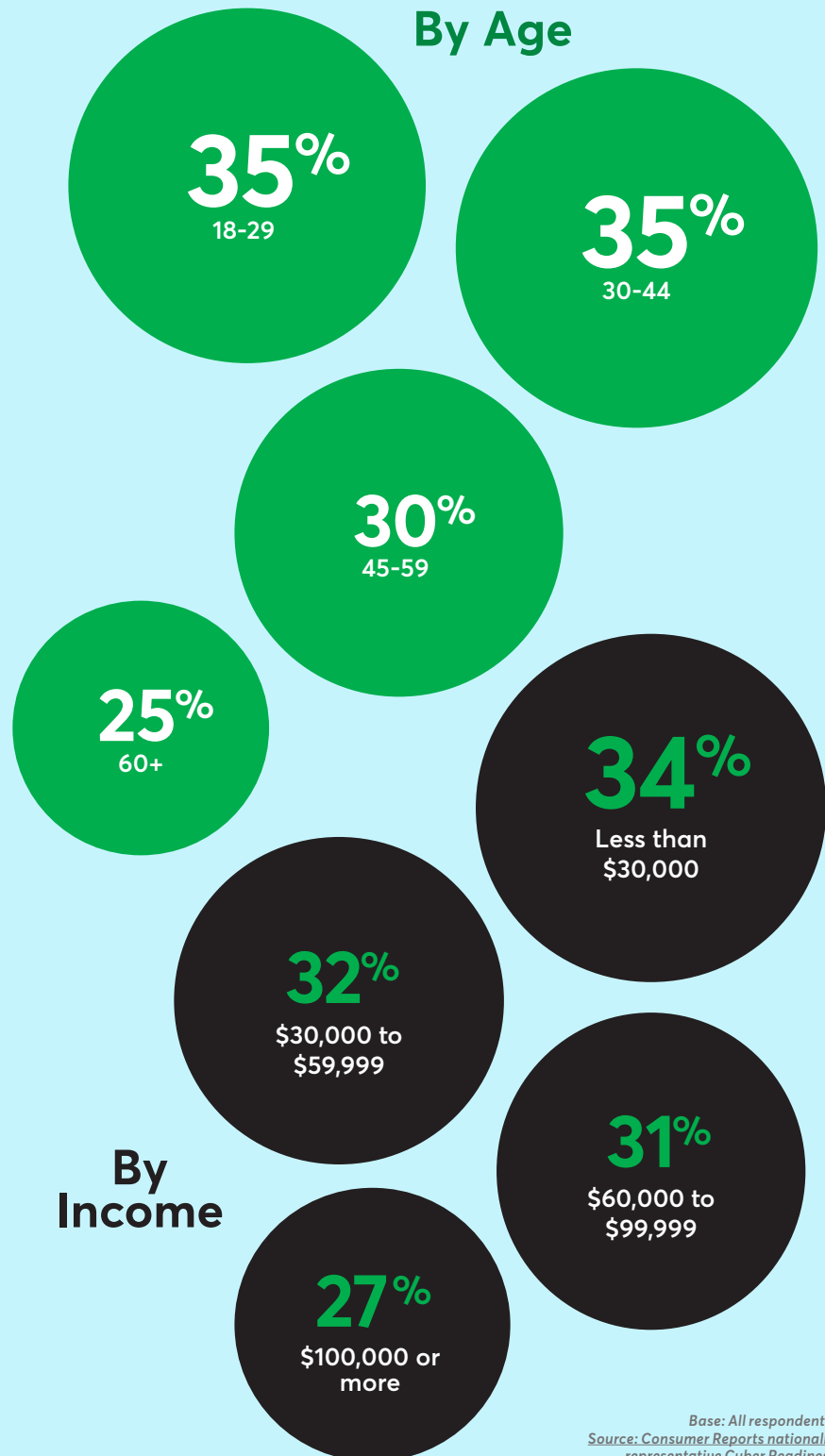
Percentage of Americans who have had at least one account taken over

HOW DO ACCOUNTS GET TAKEN OVER?

While about half of consumers who experienced an account takeover couldn't remember how scammers got access (48 percent), a third (34 percent) believe they were hacked at least once—that is, they had not shared any information. Thirteen percent said they were tricked into giving up their login information, such as a password or username, for at least one takeover.

Younger and lower-income Americans are more likely to have accounts taken over. About a third of Americans under 45 experienced takeovers (35 percent of both 18- to 29-year-olds and 30- to 44-year-olds) compared to just a quarter of those aged 60 and up. Similarly, the percentage of Americans who have had any account taken over drops from 34 percent of those with an annual household income of less than \$30,000 to just 27 percent among those with \$100,000 or more.

By Age



Base: All respondents.
Source: Consumer Reports nationally
representative Cyber Readiness
Survey of 4,682 US adults.

KEY FINDINGS



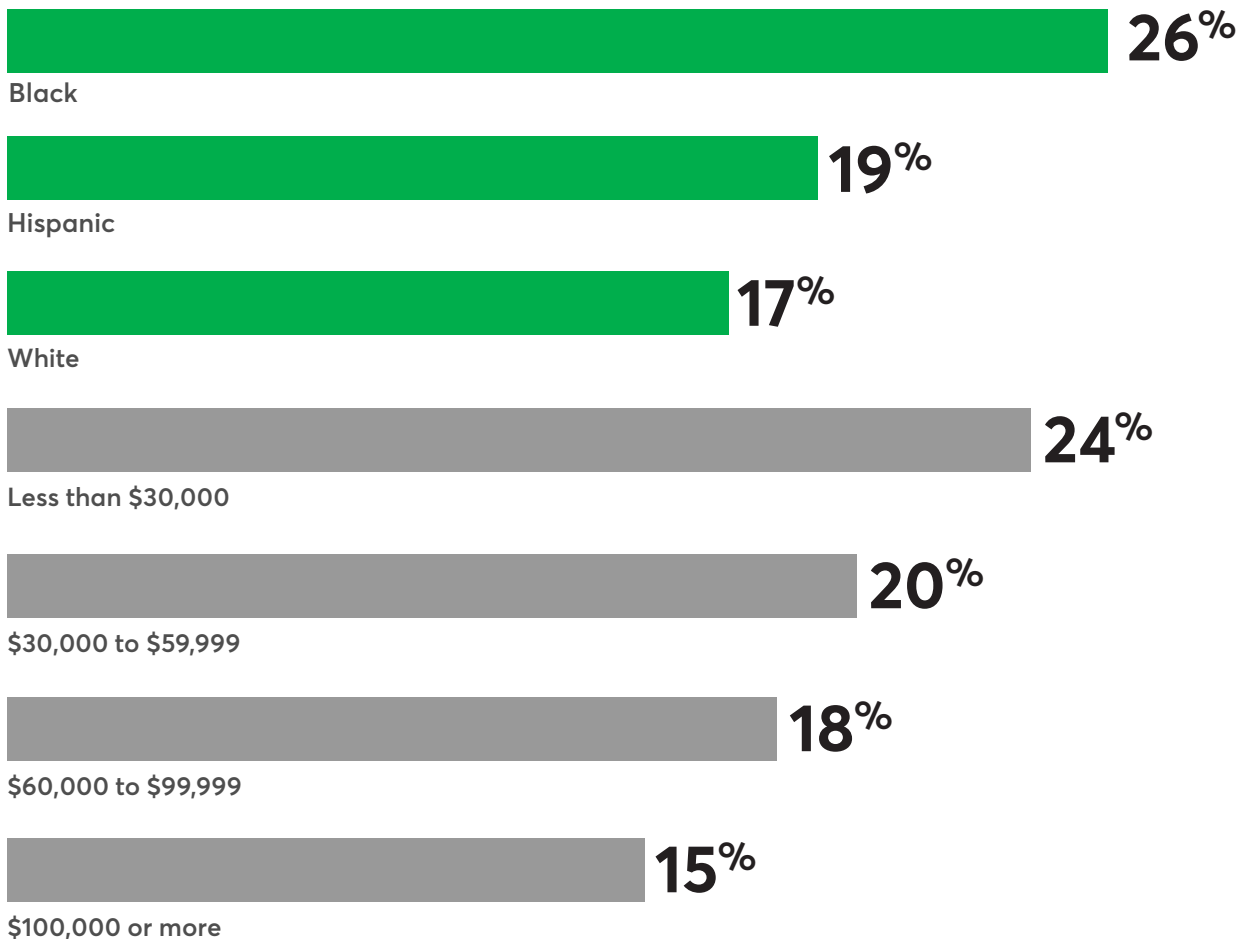
Who is getting scammed?

Building on the findings of previous Consumer Reports surveys, we explored whether certain kinds of people were more likely to be scammed. Of particular interest in this survey, we found that race/ethnicity and income level affected how likely someone was to be scammed. Being scammed or falling prey to a scam in the context of this report means having lost money whether or not the victim ultimately got it back. Black Americans who encountered any scam attempt

or cyberattack (26 percent) were more likely to be scammed than Hispanic (19 percent) or white (17 percent) Americans.

And the likelihood of being scammed went down as annual household income went up, from 24 percent among those who made less than \$30,000 annually to 15 percent among those who made \$100,000 or more.

Percentage of Americans who fell victim to a digital scam (by demographics)

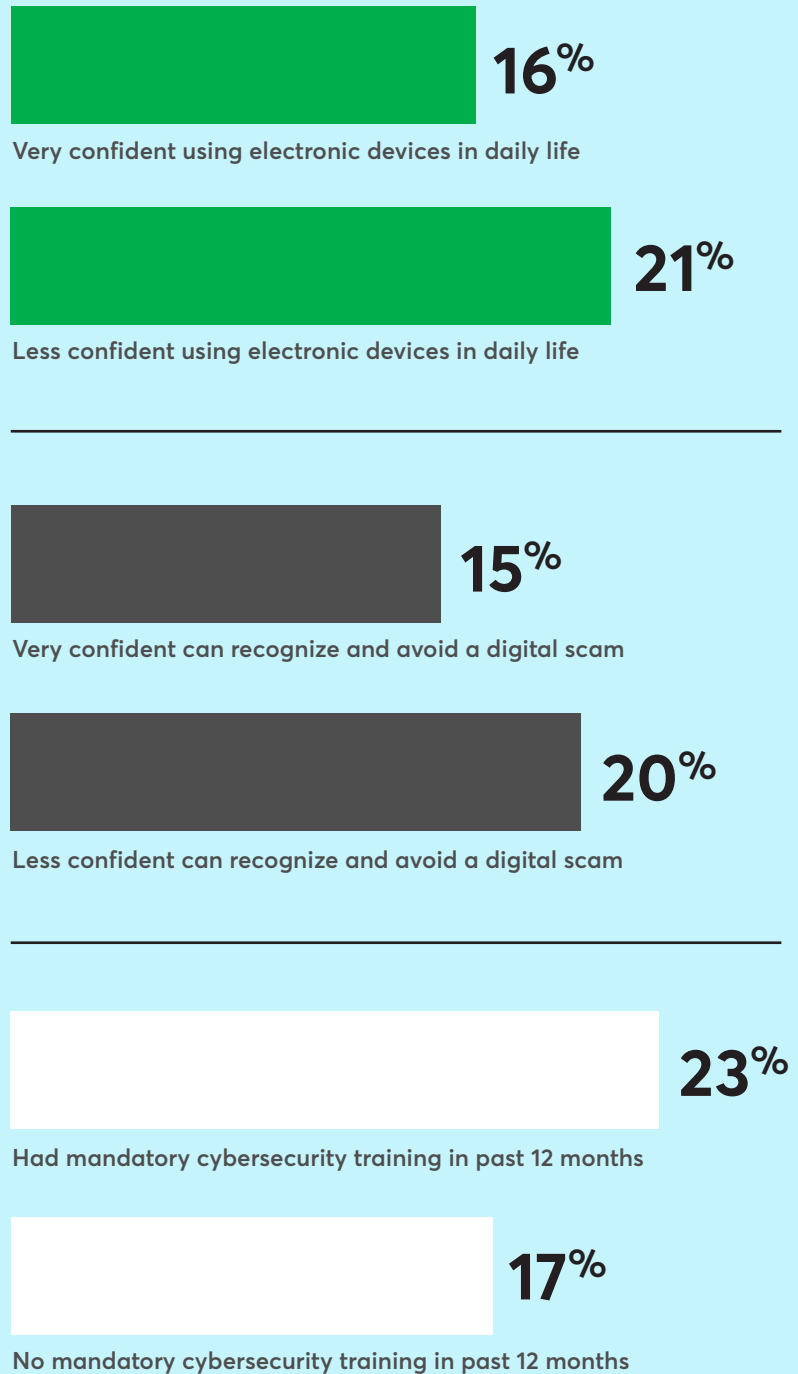


Base: Respondents who experienced any attack attempt or had an account taken over because someone tricked them into revealing login information. Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults

Percentage of Americans who fell victim to a digital scam (by attitude and behaviors)

IN ADDITION TO demographics, we looked to see if certain attitudes or behaviors affected the likelihood of being scammed. Many scammers intentionally prey on those who are less technologically savvy. Accordingly, we found that people who rated themselves “very confident” using computers, smartphones, and other electronic devices in daily life were less likely to get scammed than those who were less comfortable (16 percent vs. 21 percent). Similarly, those who said they were “very confident” they could detect and avoid digital scams were indeed less likely to be scammed than those who were less confident (15 percent vs. 20 percent).

On the other hand, Americans who said they did mandatory cybersecurity training for work or school in the past 12 months were actually more likely to report falling victim to a scam (23 percent, compared to 17 percent of those who did not). It’s unclear why this is the case. Perhaps people who are required to take cybersecurity training are exposed to more scams. However, given that one common suggestion for reducing scams overall is better education on cybersecurity, this is a question worth considering in more depth.



Base: Respondents who experienced any attack attempt or had an account taken over because someone tricked them into revealing login information.
Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.

KEY FINDINGS



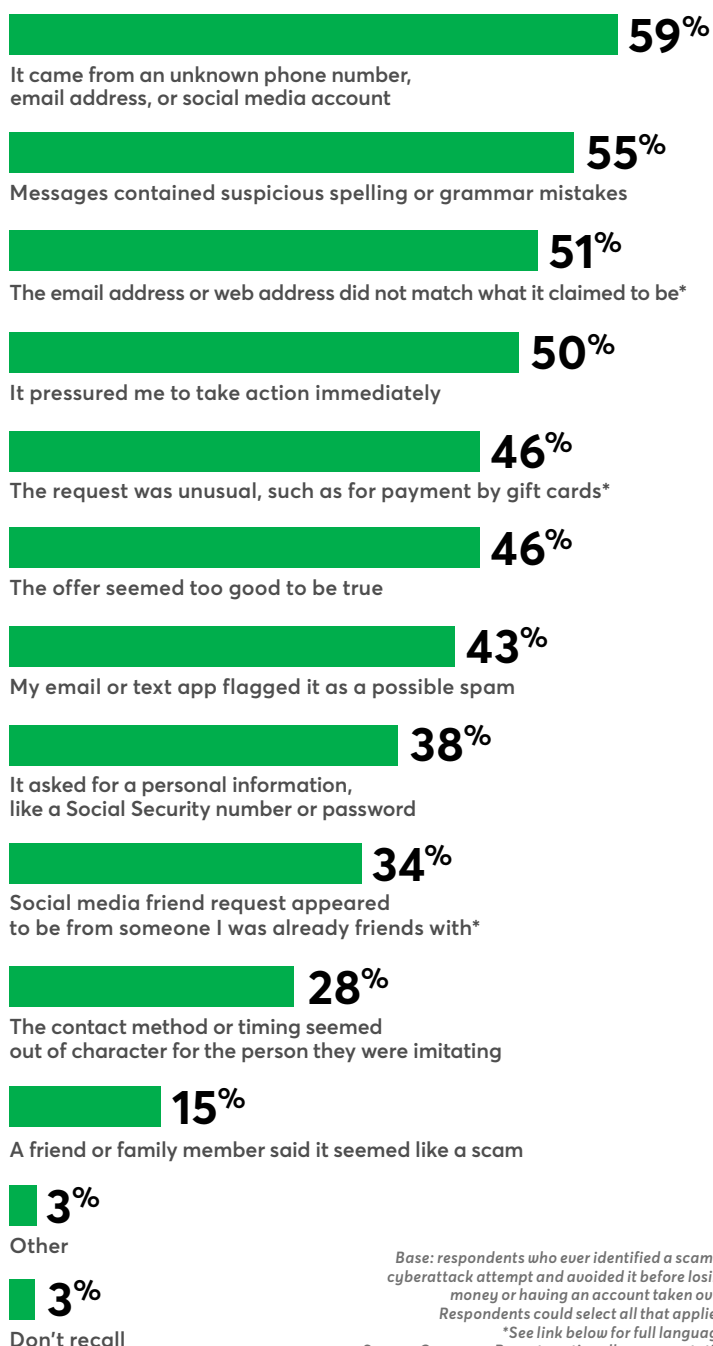
What stops people from falling prey to scams

ATTEMPTS TO SCAM Americans are common, as evidenced by the 91 percent of respondents who said they have encountered a scam attempt. But we also wanted to know what made certain consumers more resistant to falling for a scam or losing money from a scam. In this section, we discuss the risk factors associated with falling prey to a digital scam or cyberattack.

But first, it's worth looking at what makes people avoid falling for scams. We asked Americans who had encountered various situations we considered scam attempts if they had ever identified what *they* considered to be a scam or cyberattack attempt and avoided it before suffering any negative consequences. Forty-three percent had recognized an attempt immediately at least once. One in five (19 percent) said they had encountered at least one scam that they did *not* recognize as such immediately, but caught it before they lost money or control of an online account. These two categories were not mutually exclusive. Based on how we asked the question, someone might have caught one attempt immediately and been sucked in for the beginning of another. Our survey indicates that this happened to about four percent of Americans who have encountered a scam attempt or cyberattack. Forty-two percent said that, to their knowledge, they had not recognized a scam or cyberattack attempt and stopped it before it could go further. Interestingly, given that all of these people had encountered at least one situation we considered an attempted scam, but not all of them also reported falling victim to one, some people are probably evading scams without realizing it, such as by ignoring spam messages.

We also looked at what, specifically, made these people suspicious during a scam attempt and led them to disengage. It appears that taking time to closely look at an email or text message led people to discover flaws that were likely to prompt them to disengage from the scam.

Thinking about any scams or cyberattacks you avoided, which of the following made you suspicious?



Base: respondents who ever identified a scam or cyberattack attempt and avoided it before losing money or having an account taken over. Respondents could select all that applied.

*See link below for full language.

Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.



Risk factors

PERSONALIZATION

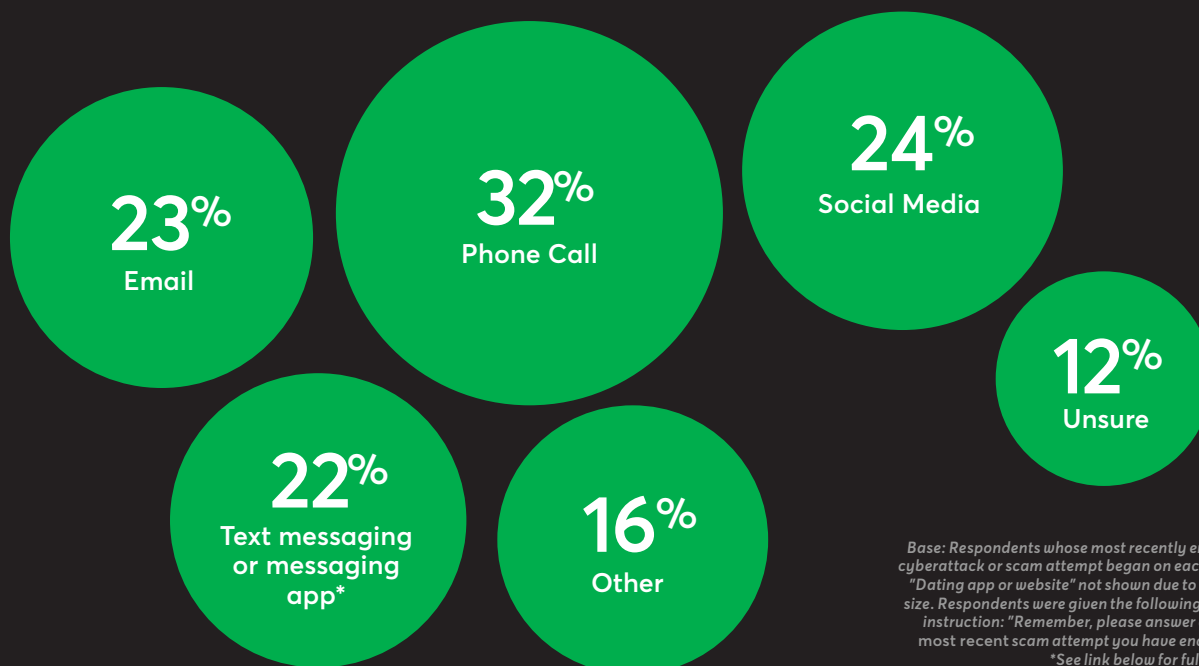
Many respondents who had encountered a scam reported that the scam attempt used some form of personalization. The information used to personalize a scam could come from poorly locked-down Facebook or Venmo privacy settings, for example; it could also come from actual data breaches.

Three in five consumers (61 percent) have experienced some type of data breach or compromise at some point, according to [2024 survey data from U.S. News and World Report](#). And the rise of relatively cheap access to large language models means it takes less work to use that personal data in customized scams. Overall, one in five people in CR's Cyber Readiness Survey said the most

recent scam or cyberattack attempt they encountered was customized using their personal details. Also relevant for anyone following the Federal Communication Commission's efforts to reduce the number of total scam calls by adding new regulations: Around a third of Americans who said the most recent scam attempt they encountered began with a phone call also said that it had been customized using their personal details. That is notably higher than those whose scam attempt began using a different contact method.

The good news is that 13 percent of Americans have a code word or safeword with family members to confirm if a call or message is really from them, which could help thwart personalized phone scams that use AI to mimic a loved one's voice. Agreed-upon safewords could work for text messages as well.

Percentage of most recently encountered scam attempts that were customized to respondents' personal details by platform where the attack began



Base: Respondents whose most recently encountered cyberattack or scam attempt began on each platform. "Dating app or website" not shown due to low sample size. Respondents were given the following additional instruction: "Remember, please answer only for the most recent scam attempt you have encountered."

*See link below for full language.

Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.

Risk Factors: PAYMENT METHODS

For the Americans who fell prey to a scam (17 percent), how they paid the scammer mattered when it came to how likely they were to get their money back. People who paid the scammer by credit card were most likely to get their money back—61 percent of them said they recovered their funds—followed by debit card users, 45 percent of whom got their money back. This is likely because credit cards have more robust anti-fraud protection due to federal law. For those using peer-to-peer payment services such as Zelle or Venmo, which are not subject to the same standards, only 15 percent got their money back.

When trying to avoid monetary loss after a scam, payment methods are important. We asked Americans to identify the two most common ways they pay in daily life, whether online or in person. Fortunately, 57 percent of Americans use a credit card as one of the top two payment methods they use most often and 44 percent use a debit card (the method with the next-highest percentage getting their money back).

Risk Factors: ONLINE SHOPPING AND SOCIAL MEDIA USE

Given that many scams begin on social media platforms or involve some form of online shopping, it's unsurprising that people who use social media were more likely to say they have been scammed (20 percent vs. 12 percent, compared to 17 percent overall). And the

more often a person shops online, the more likely they were to say they had fallen victim to a digital scam (from 25 percent of those who buy products online daily to 17 percent of those who do so less often than once a month).

Do you currently use
any social media?

Yes

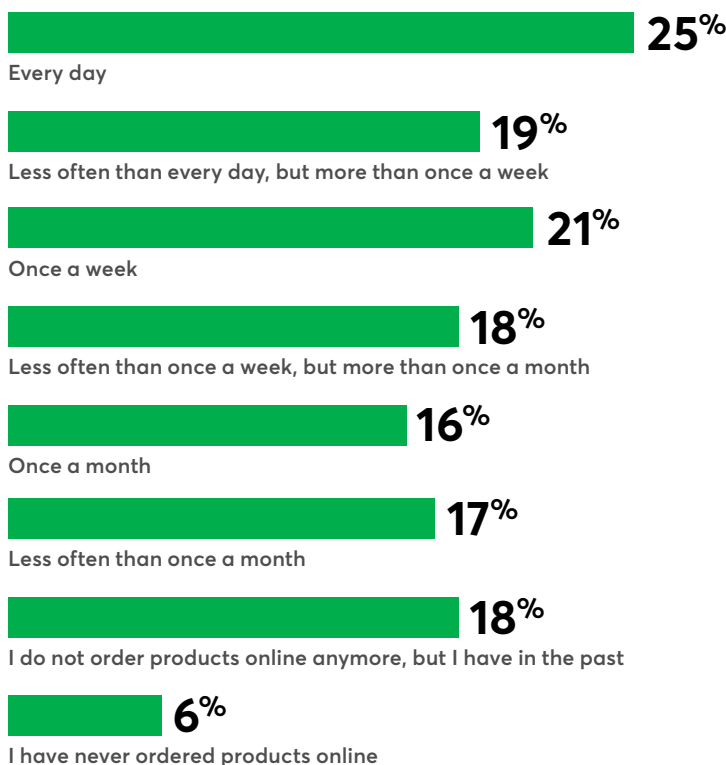
No

Percentage
Scammed

20%

12%

Percentage scammed by frequency of ordering products online



Base: All respondents. Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults

KEY FINDINGS



Whose job is it to prevent scams?

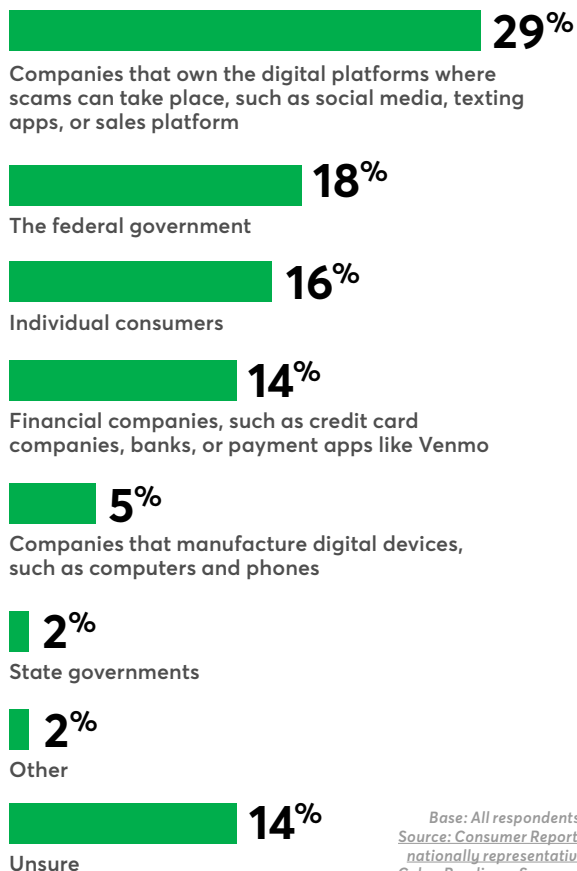
Existing on the Internet almost guarantees you will encounter a scam. But there are plenty of policies that can reduce the number of scams people encounter and help when they do encounter them. Consumer Reports supports legislation that would impose obligations on platforms and Artificial Intelligence tool providers to take basic steps to prevent abuse. For social media platforms, this would include implementing know-your-customer obligations for social media advertisers and social media sites actively monitoring their platforms for misuse.

Platforms should also make it easier for consumers to report fraud and make humans available to help when they do. This would help address scams at their start and also raise the cost of making a platform easily accessible to scammers, giving the companies operating those platforms an incentive to monitor for scams more closely. Today, social media platforms, phone providers, and others earn revenue from scammers attempting to reach consumers on their platforms, yet provide little assistance to those who lose money. But while it would be nice to see platforms step up to reduce scams, it's clear that government regulation is necessary.

When it comes to phone scams, the need for government intervention has become so obvious that the Federal Communications Commission has started several rulemakings. Many focus on mandating better know-your-customer requirements and increasing the penalties associated with letting scammers onto the voice network. Consumer Reports has also supported federal and state legislation that would impose these mandates, including the bipartisan [SCAM Act](#).

For this survey we asked all respondents, regardless of their personal experience, who they think should be most responsible for protecting Americans from digital scams. The most common response, by far, was companies that own the digital platforms where scams can take place (29 percent), followed by the federal government (18 percent).

Who do you think should be MOST responsible for protecting Americans from digital scams?



Base: All respondents.
Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.



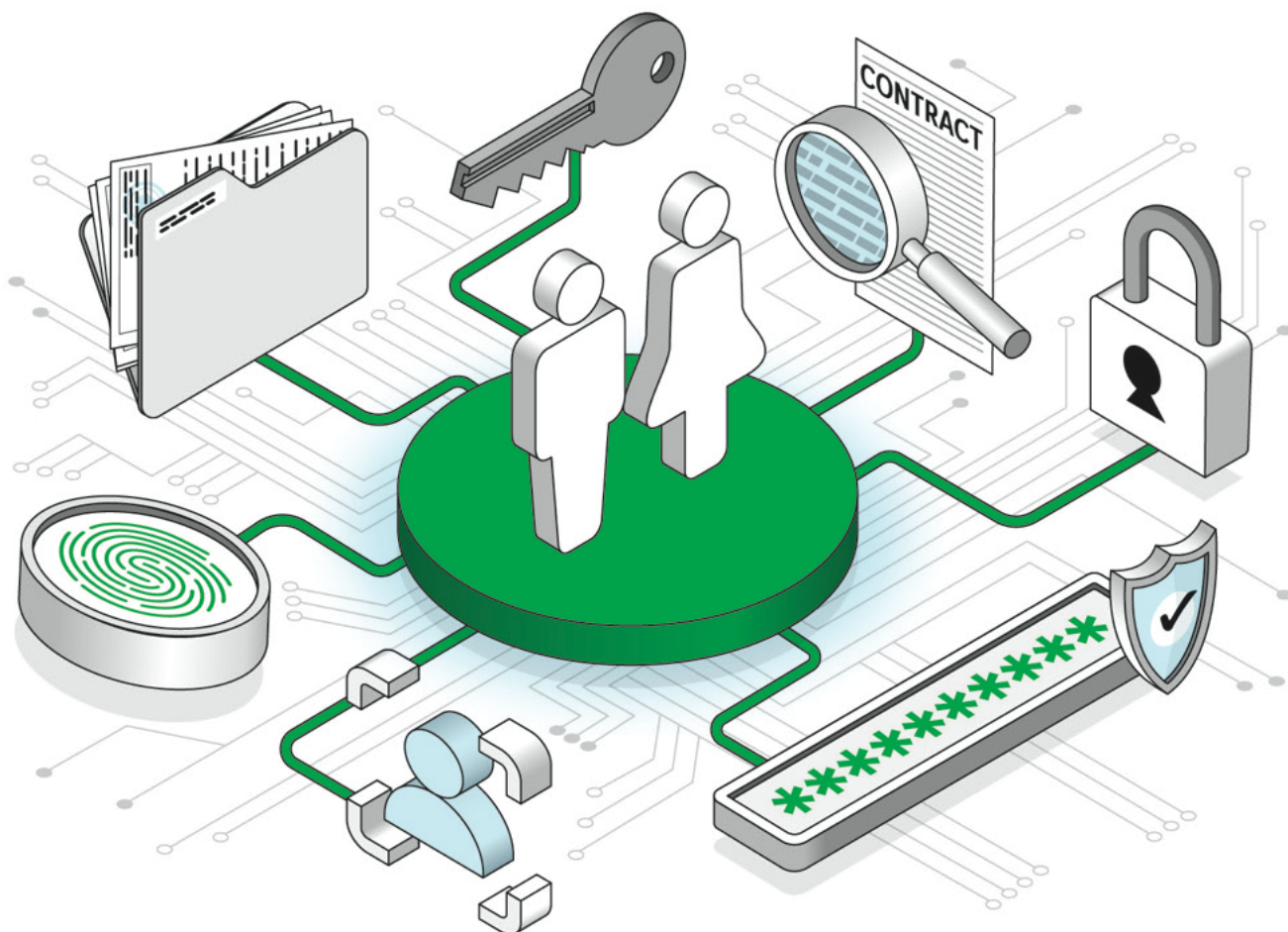
AI is making it easier than ever for scammers to impersonate people we trust, deceive consumers, and steal their money. Education and strong cybersecurity habits are critical, but we can't put the sole burden on consumers to defend against increasingly sophisticated threats. Companies need to be accountable, and governments must enact strong guardrails to keep consumers safe and secure online.



PHIL RADFORD
President and CEO
Consumer Reports



How consumers are trying to stay safe



Today it's still very much a consumer's responsibility to guard against scams, along with other digital precautions. With that in mind, we asked consumers a few questions about their online habits and the security precautions they take.

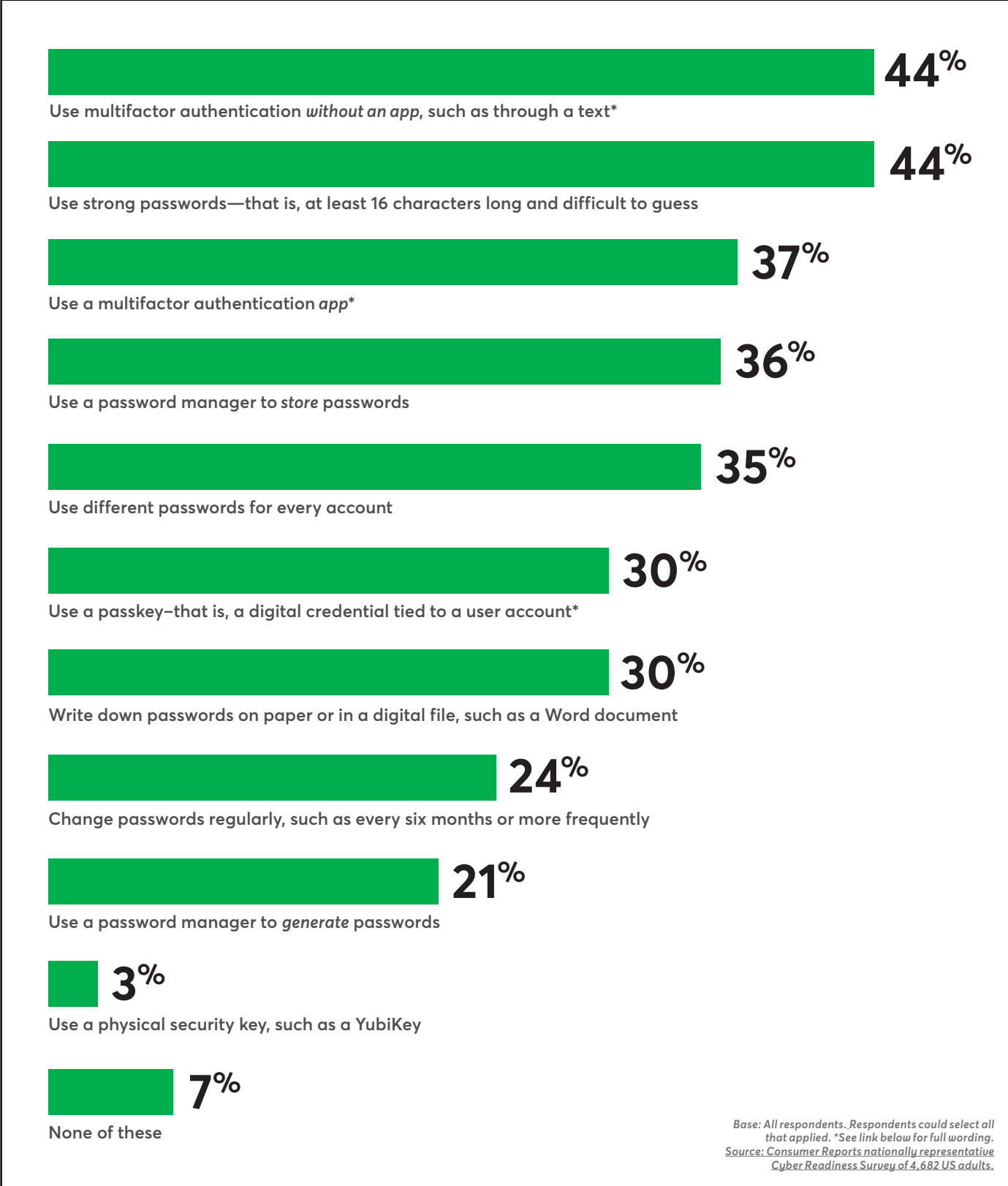
Overall, good password hygiene, using multifactor authentication, updating devices promptly, and inspecting emails and texts closely before clicking links or opening attachments are all precautions consumers are taking.

One question dealt specifically with passwords and login information. The most common precautions people said they take around passwords are using some type of multifactor authentication (60 percent) and using strong passwords (44 percent).

We defined strong passwords as being at least 16 characters long and difficult to guess. Also, four in 10 Americans use password managers in some fashion.

It's worth noting that some of Americans' password precautions rely on businesses supporting these options. A business can require consumers to use multifactor authentication to access their bank account, for example, and reject weak passwords. Notably, however, some businesses do not provide an option for consumers who might want to use multifactor authentication. We believe that businesses dealing with sensitive information such as financial data, health data, or even airline miles or rewards programs should provide multifactor authentication and push consumers to use it.

Which, if any, of the following do you do regarding passwords and logging in to *any* of your online accounts, like bank accounts, social media profiles, or email accounts?



Base: All respondents. Respondents could select all that applied. *See link below for full wording.
Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults.

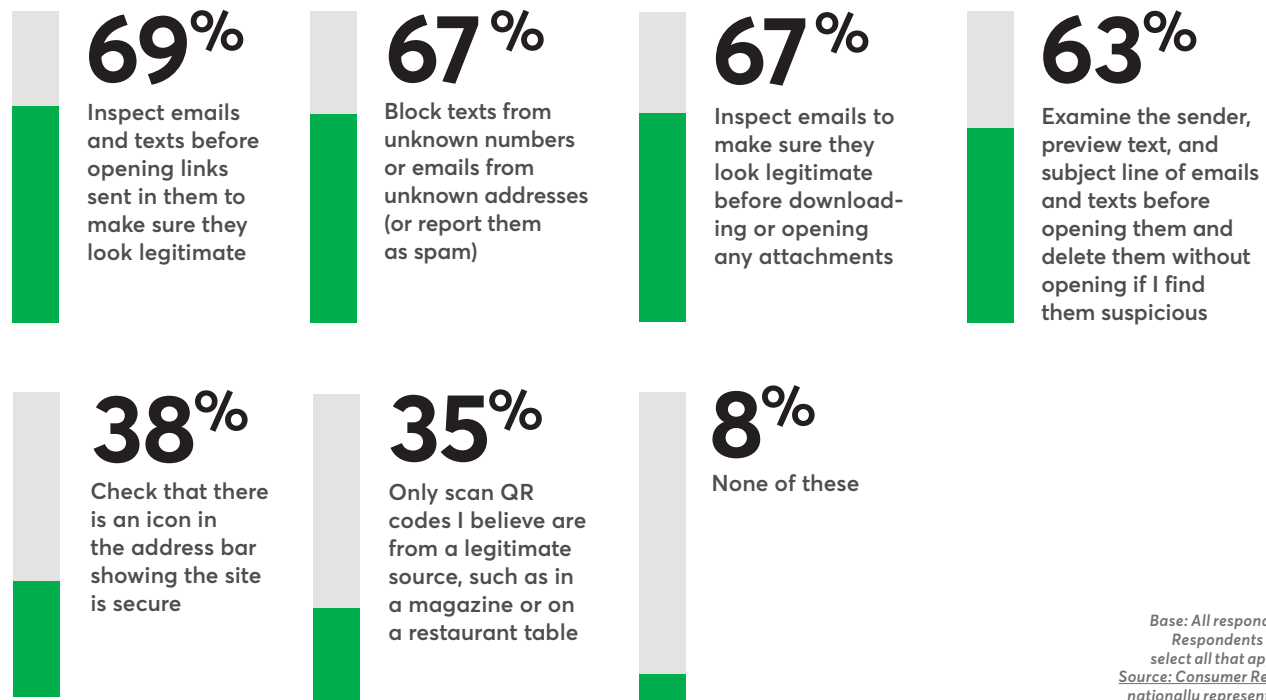
WHEN IT COMES TO keeping their devices secure, about half of Americans (48 percent) said they turn on automatic software updates for at least some programs. Almost as many (46 percent) said they use antivirus software. About one in three said they accept and run software updates individually—again, for at least some types of updates (35 percent)—and that, when devices come with default passwords, they change them (also 35 percent).

A good way to avoid scams is to make sure any links you click, text messages you open, or websites you

visit are legitimate. We also asked some questions about what people do to ensure legitimacy. We should note that while we asked if consumers are checking for an icon in the address bar of their web browser, most browsers no longer show the padlock icon used to indicate that a site's traffic is encrypted.

Consumers may also want to set up transaction alerts in their online banking accounts and mobile banking apps to automatically send text messages regarding any payments made above a certain threshold, such as \$250 or \$500.

Which, if any, of the following do you do to make sure that you only interact with *legitimate links, messages, or websites*?



Base: All respondents. Respondents could select all that applied.
Source: Consumer Reports nationally representative Cyber Readiness Survey of 4,682 US adults



KONSTANZE FRISCHEN
Executive Director (acting), Aspen Digital, The Aspen Institute



The [Take9](#) campaign encourages consumers to slow down online for a safer digital experience and also gives them actionable tips to spot possible threats and stay protected. It's great to see consumers taking effective actions, and as scams become more sophisticated and targeted, we have to ensure they stay informed of the latest cybersecurity trends and alerts.



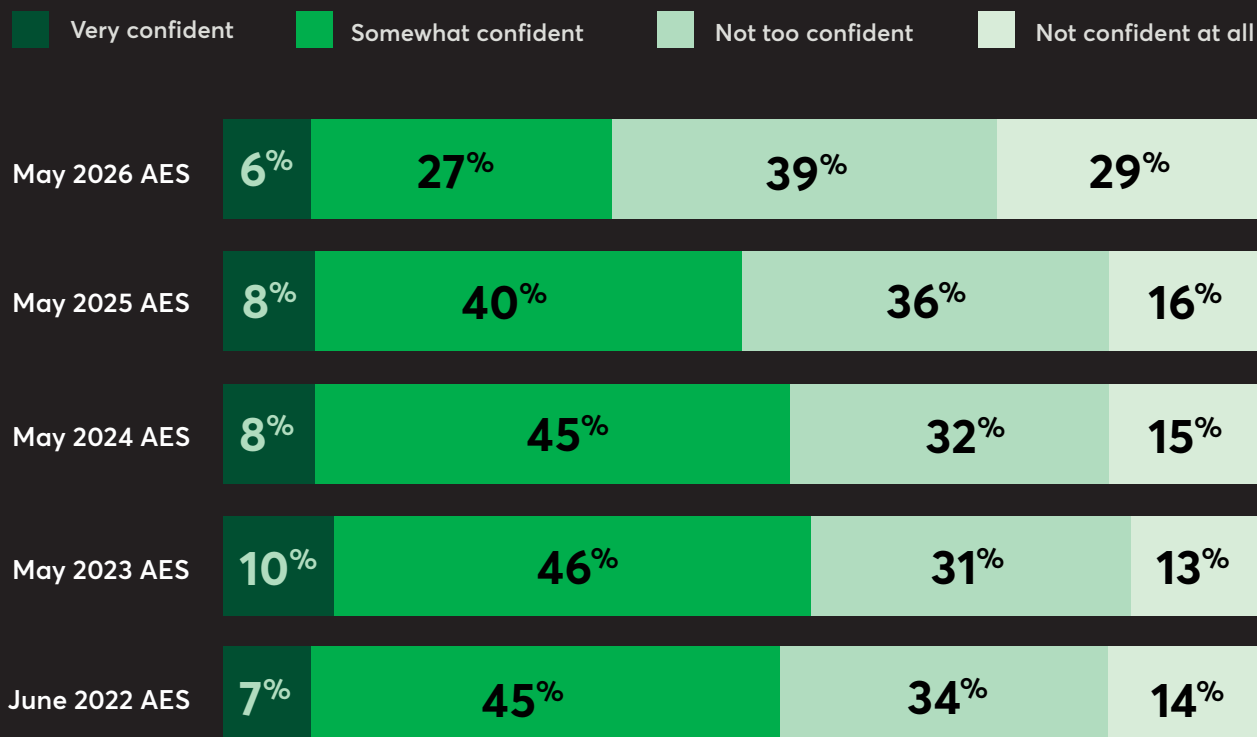
A final note on privacy

IN ADDITION TO asking about fraud and scams, we also conducted a second nationally representative survey to ask trending questions about privacy and cybersecurity. We asked Americans, “How confident are you that your personal data, such as Social Security number, health history, and financial information, is private and not distributed without your knowledge?” four times over the past four years.

When we asked that question again in May 2026, there was a dramatic drop from the prior year.

Only around a third of Americans (32 percent) said they were at least somewhat confident that their personal data was private—down from about half (48 percent) last year. Meanwhile, the percentage that said they were “not confident at all” nearly doubled, from 16 percent to 29 percent.

How confident are you that your personal data, such as Social Security number, health history, and financial information, is private and not distributed without your knowledge?

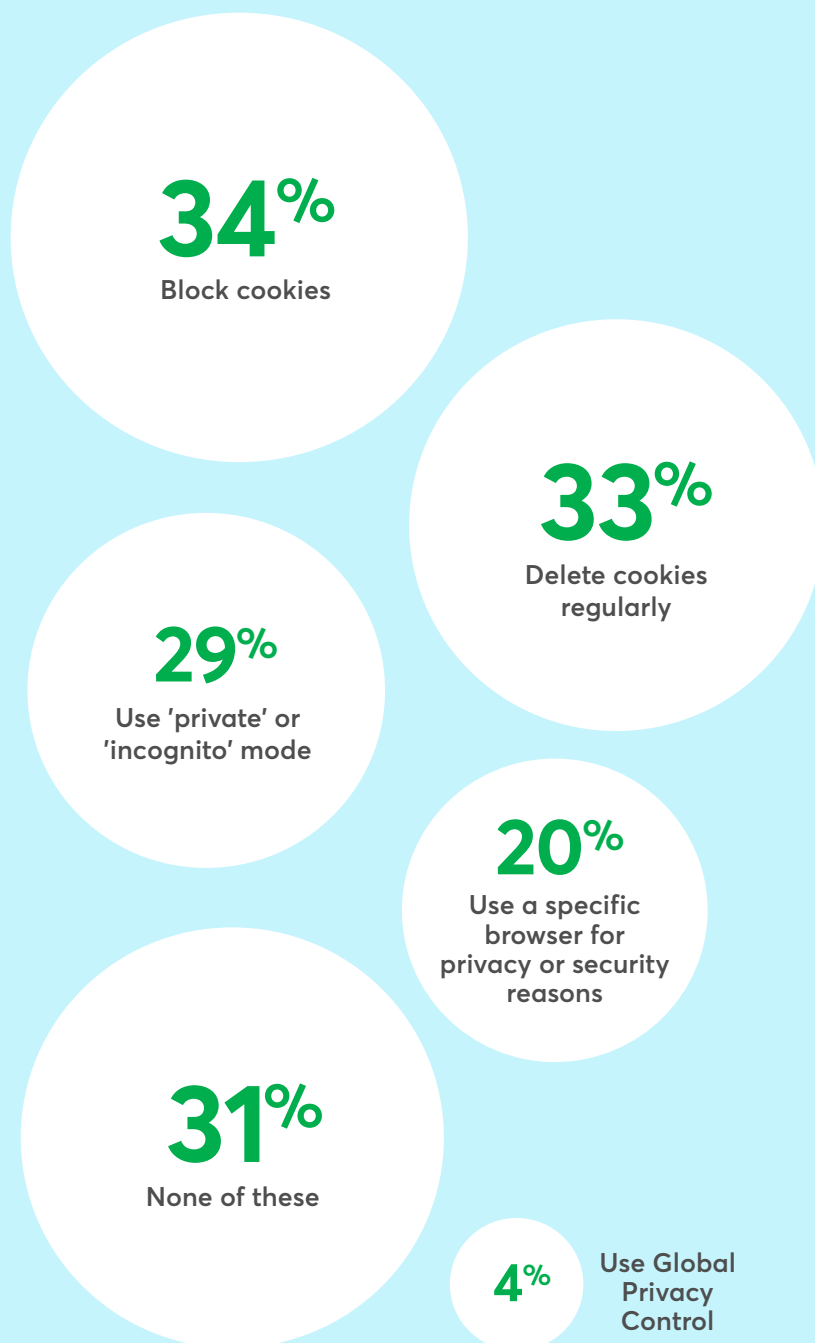


Base: All respondents. Sources: [Consumer Reports nationally representative American Experiences Survey of 2,082 US adults \(May 2026\)](#); [Consumer Reports nationally representative American Experiences Survey of 2,333 US adults \(May 2025\)](#); [Consumer Reports nationally representative American Experiences Survey of 2,022 US adults \(May 2024\)](#); [Consumer Reports nationally representative American Experiences Survey of 2,000 US adults \(May 2023\)](#); and [Consumer Reports nationally representative American Experiences Survey of 2,103 US adults \(June 2022\)](#).

WHEN IT COMES TO keeping communications private, we asked Americans if they use encrypted apps and which encrypted apps they use to communicate with others. As in previous surveys ([April 2025](#) and [April 2024](#)), a little more than one in 10 Americans say they do not use any encrypted texting apps. We moreover noted that the use of Facebook Messenger was shrinking compared to 2025 levels, while the use of Signal had risen slightly.

We also asked whether consumers were using ad blockers and how they might act to keep their data more private while browsing the web. A majority of Americans, 59 percent, said they do not think they have an ad- or tracker-blocking browser extension on the device they use most often. (This could be because many people's most commonly used devices are smartphones, where browser extensions work differently than on computers.) Another 15 percent said they have an adblocker, but don't know what it is. The most common ones that people knew they had were AdBlock Plus and DuckDuckGo; each was selected by just 8 percent of Americans. However, around seven in 10 Americans in our May survey reported taking some measures to protect their personal data while using a web browser on the personal device they use most often (see chart to the right).

Here are some actions people might take to protect their privacy or personal data when using a web browser, such as Chrome or Firefox. Which, if any, of the following do you do on the personal device you use most often?



Base: All respondents. Respondents could select all that applied.
Source: May 2026 CR nationally representative survey of 2,082 US adults.

Closing

In the past five years, as part of this report, we shared multiple actions that consumers can take to protect their digital lives. We have emphasized good password hygiene, the use of multifactor authentication, and more recently, passkeys. We have also drawn attention to the prevalence of scams affecting low-income Americans and younger Americans.

But it's clear that consumers taking action is not enough. Businesses should enable tools such as multifactor authentication and encourage its use along with good password hygiene. And it can't stop there. Social media platforms should do more to hold scammers accountable on their platforms while also making it easier for consumers to report scams and reach human beings when they think a scam has occurred.

Governments have a role to play, too. Enacting proposed laws such as the bipartisan [SCAM Act](#) or New York's False Social Media Advertising Prevention Act would hold social media platforms accountable for turning their sites into a playground for scammers and make it easier for consumers to report fraudulent and scammy activity. In addition, the Federal Trade Commission and state Attorneys General can investigate and [bring enforcement actions](#) against social media platforms under the FTC Act and state laws that already prohibit unfair and deceptive practices.

Thank you

AUTHORS

CONSUMER REPORTS:

Chuck Bell
Stacey Higginbotham
Tess M. Yanisch

DESIGN

Kim Gray

SURVEY RESEARCH

CONSUMER REPORTS:

Noemi Altman
Debra Kalensky
Tess M. Yanisch

EDITING AND COPYEDITING

Carolyn Pritchard

CREDITS: Cover and page 16 illustrations by Pete Sucheski; page 4, invoice icon created by arkan studio from Noun Project; page 7, unlock icon created by Lin Qiye from Noun Project; page 9, questions icon created by Gregor Cresnar by Noun Project; page 10, quote icon created by Tyler Gobberdiel from Noun Project; page 12, scam icon by Moch Rizki Eko Waluyo; page 13, risk factor icon by New River; page 15, government icon created by Larea; page 19, key icon created by Chandra Mohan Singh from Noun Project



Founded in 1936, CR has a mission to create a fair and just marketplace for all. Widely known for our rigorous research and testing of products and services, we also survey millions of consumers each year, report extensively on marketplace issues, and advocate for consumer rights and protections around safety as well as digital rights, financial fairness, and sustainability. CR is independent and nonprofit.



The Global Cyber Alliance (GCA) is a global 501(c)3 nonprofit that makes the Internet safer by reducing widespread cyber risk. We bring together partners across sectors to strengthen the Internet's core infrastructure and put practical cyber protections in the hands of the organizations and communities most at risk. As the threat landscape evolves at a pace unmatched in speed and scale, GCA is at the forefront, studying the problem, convening the right people and organizations, and delivering solutions that work.



Aspen Digital, a program of the Aspen Institute, convenes thinkers and does to anticipate how our world is changing in the age of AI. We find signal in the noise, elevate thoughtful ideas, and inspire collaboration across industry, government, and civil society to shape solutions that work for all. To learn more, visit aspendigital.org or email aspendigital@aspeninstitute.org.