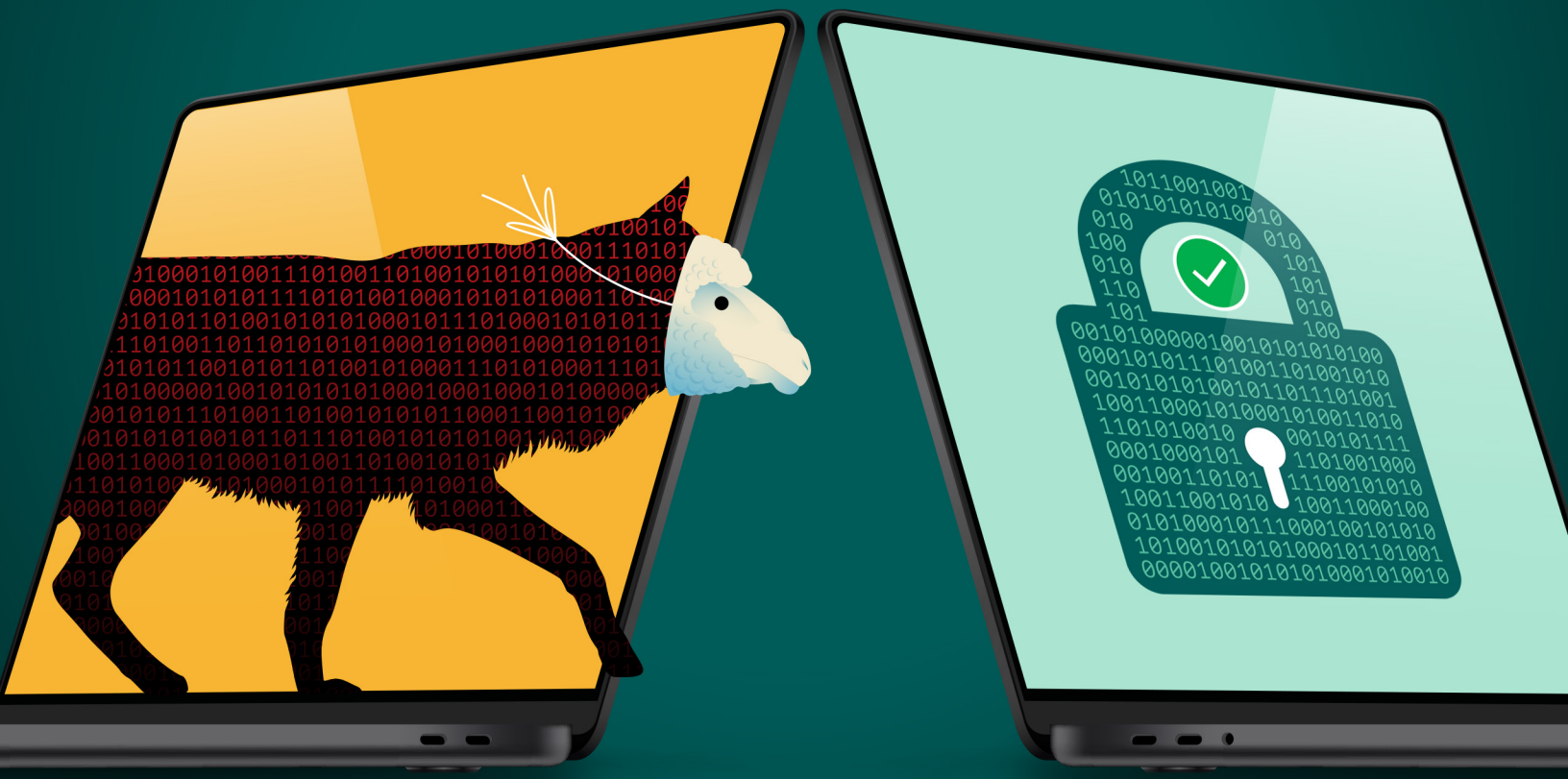
2025

CONSUMER CYBER READINESS REPORT



Cyber Civil Defense Initiative

Consumer Reports | Aspen Digital, aspen institute | Global Cyber Alliance

Introduction

The Fourth Annual Consumer Cyber Readiness Report examines how consumers view and manage their digital privacy and security. Together, Consumer Reports, Aspen Digital, and the Global Cyber Alliance have reviewed findings from Consumer Reports' recent nationally representative surveys to understand the steps people are taking to improve their digital privacy and security. In addition to our year-over-year trends on cybersecurity behavior, consumer scams, and their attack vectors, this year we've included sidebars to contextualize the insights from our findings. We've also provided explainers, consumer guidance, and perspectives from thought leaders.

This year's findings show that Americans are less confident than they were last year that their personal data is private and not distributed without their knowledge.

We continue to observe a racial disparity in money lost in response to scams: Black Americans who encountered a scam were nearly two and a half times as likely as white Americans to report losing money. We also found a difference by household income: Americans with the highest household incomes were less likely to have lost money to a digital scam than other household income groups.

Additionally, we have included a question about passkeys for the first time this year and saw a surprisingly high adoption rate of this technology, which can provide robust protection against phishing attacks.

This year's survey data also demonstrated an increase in text-based scams as a share of all scams encountered—especially among the youngest adults.

Because improving our nation's cyber civil defense is a team effort, we have continued to include tips for ways consumers can improve their cyber hygiene, but we recognize that government and industry also have a role to play.

Historically, many of our consumer protection agencies have been underfunded. Consumers' confidence in the privacy of their data is down, and federal efforts to rein in data brokers and boost security have been rolled back.

Companies do not need to wait for government regulation to take action. They, too, can lift the burden of consumers by making products with security built in—by design and by default—and by utilizing best practices such as data minimization.

Consumers also have a role to play. They can reduce their risk by educating themselves in cyber readiness with resources such as Security Planner and Take9.

About The Surveys

In April 2025, Consumer Reports conducted a nationally representative multimode American Experiences Survey. NORC at the University of Chicago administered the survey from April 10 to 21, 2025, through its AmeriSpeak Panel to a nationally representative sample of 2,158 U.S. adults.

We conducted an additional nationally representative multimode American Experiences Survey administered by NORC at the University of Chicago from May 8 to 19, 2025, to a representative sample of 2,333 U.S. adults.

Both of these surveys included trending questions–that is, 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 to 21, 2022); May 2023 (administered to 2,000 U.S. adults from May 5 to 16, 2023); April 2024 (administered to 2,042 U.S. adults from April 5 to 15, 2024); and May 2024 (administered to 2,022 U.S. adults from May 9 to 20, 2024).

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. More details on the surveys' methodology can be found in the links above.

Key Findings

Our April 2025 survey included questions about cyberattacks and digital scams.

DIGITAL SCAMS

A cyberattack or digital scam occurs when bad actors use technology to harm, steal from, or deceive people over the internet. This can include hacking into systems to access private data, tricking people into revealing personal information, spreading viruses, or using deceptive tactics to commit a crime.

VULNERABILITY TO FRAUD VIA SOCIAL MEDIA

We asked social media users (84 percent of Americans) whether they had certain types of experiences on social media, each of which may pose a risk of cyberattack or digital scam. Nearly two-thirds of social media users (64 percent) said they had received friend requests from people they don't know. About half (48 percent) said they had received direct messages that seemed to be part of a scam or fraud attempt, and roughly half (46 percent) said they had received direct messages on social media from people they don't know. These numbers are unchanged from last year.

Have You Had Any of the Following Experiences on Any Social Media Site or App in the Past 12 Months?	2025	2024
Received friend requests on social media from people you don't know	64%	67%
Received direct messages on social media that seemed to be part of a scam or fraud attempt	48%	48%
Received direct messages on social media from people you don't know	46%	47%
Bought a product by clicking through an ad on social media	21%	22%
Bought a product through a social media platform like Facebook Marketplace or Nextdoor	21%	21%
Responded to requests for donations that came directly from an organization on social media*	6%	7%
I have not experienced any of these in the past 12 months	16%	15%

Base: Respondents who use social media.
(Respondents could select multiple response options.)
**See link below for full language.*

Sources: Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults (April 2025) and CR nationally representative American Experiences Survey of 2,042 U.S. adults (April 2024).

MONEY LOSS DUE TO DIGITAL SCAMS

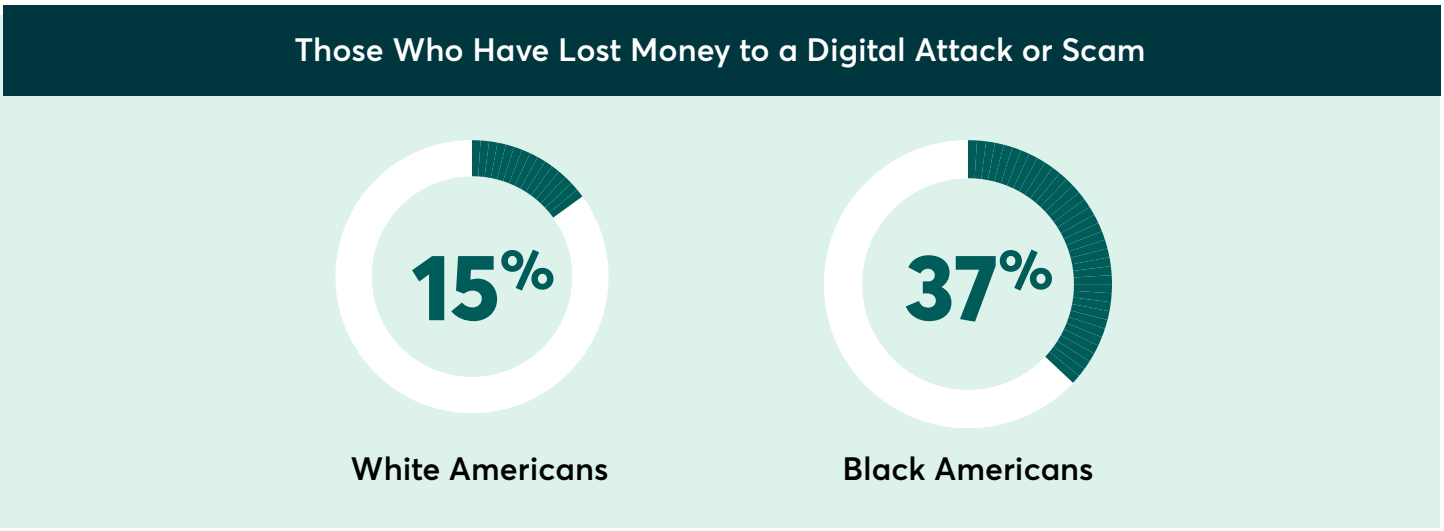
When we asked Americans whether they had ever personally encountered a cyberattack or a digital scam, nearly half said they had. Alarmingly, 1 in 5 of those who said they had personally encountered a digital scam or cyberattack—or about 1 in 10 Americans—said they lost money to the scam. These numbers are unchanged from last year.

Base: All respondents, or as indicated.

Source: Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults (April 2025).

MONEY LOSS DUE TO DIGITAL SCAMS BY RACE

Our survey data revealed demographic differences in Americans who lost money to a scam, as it did last year. Once again, we found that Black Americans who had encountered a scam attempt were more likely to have lost money than white Americans who had encountered a scam attempt: Thirty-seven percent of Black Americans who had encountered a scam attempt lost money, compared with 15 percent of white Americans.



Base: Respondents who have personally encountered a cyberattack or a digital scam attempt.

Source: Consumer Reports nationally representative American Experiences Survey of 2158 U.S. adults (April 2025).

> **The continued reality that Black Americans lose money to digital scams at more than twice the rate of white Americans is unacceptable—and it's not improving. These disparities reflect systemic inequities in financial protections, targeted scam tactics, and access to digital safeguards. Every person—regardless of race, income, or ZIP code—deserves to be safe, empowered, and secure in our digital world.**

YVETTE D. CLARKE
Representative (New York 9th District), Chair of the Congressional Black Caucus

RACIAL DISPARITIES IN SCAMS

Our survey found that there continues to be an enormous disparity between white Americans (15 percent) and Black Americans (37 percent) who reported financial loss after encountering a scam. A 2021 Federal Trade Commission report titled "Serving Communities of Color" suggests one reason for the disparity: People living in communities of color filed a higher percentage of reports that included payments using debit cards, cash, cryptocurrency, and money orders, all of which provide fewer fraud protections than credit cards. By contrast, white Americans filed a higher percentage of reports that included payments using credit cards.

The FTC report also found evidence that scams centered around student loan forgiveness, false business opportunities, and pyramid schemes disproportionately impacted Black or Latino communities. Recently, the FBI found that many of these scams are investment related: The agency reported a 300 percent increase in "ramp-and-dump" stock scams through messaging platforms.

To stay safe, consumers should use secure payment methods, such as credit cards offered by financial institutions that are legally required to have fraud protection and investigation policies in place.

These policies limit the liability of consumers who are victims of fraud. Cryptocurrencies or digital payment apps like Cash App and Venmo are not required to have these policies in place and often shift the responsibility to handle disputes to banks and consumers.

There is a need for more research on the causes of this disparity both by government and civil society, and more work to address and prevent it on the side of platforms where the scams are originating.

MONEY LOST DUE TO DIGITAL SCAMS BY HOUSEHOLD INCOME

This year's data also revealed that the likelihood of losing money due to a digital scam increases as household income decreases. Among those who had encountered a scam attempt, the group with household incomes of $100,000 or more were the least likely to have lost money to a scam among income groups. One in 10 (10 percent) among the highest income group who had encountered a scam lost money, compared with, for example, 3 in 10 (29 percent) among the lowest income group.

Base: Respondents who have personally encountered a cyberattack or digital scam attempt.

Source: Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults (April 2025).

PLATFORMS WHERE DIGITAL SCAMS BEGIN

Three out of 4 scam attempts (74 percent) that Americans have experienced began through email, on social media, in text messages, or through a messaging app.

In a change from last year's survey, scams that began in a text message or a messaging app have become more commonly reported. Three in 10 of those who had experienced a cyberattack or digital scam said it began over a text message or a messaging app, while only 20 percent said that last year. The percentage who said their scam began over email, 27 percent, has not meaningfully changed. Social media scams have decreased somewhat, to 17 percent in this year's survey from 23 percent last year.

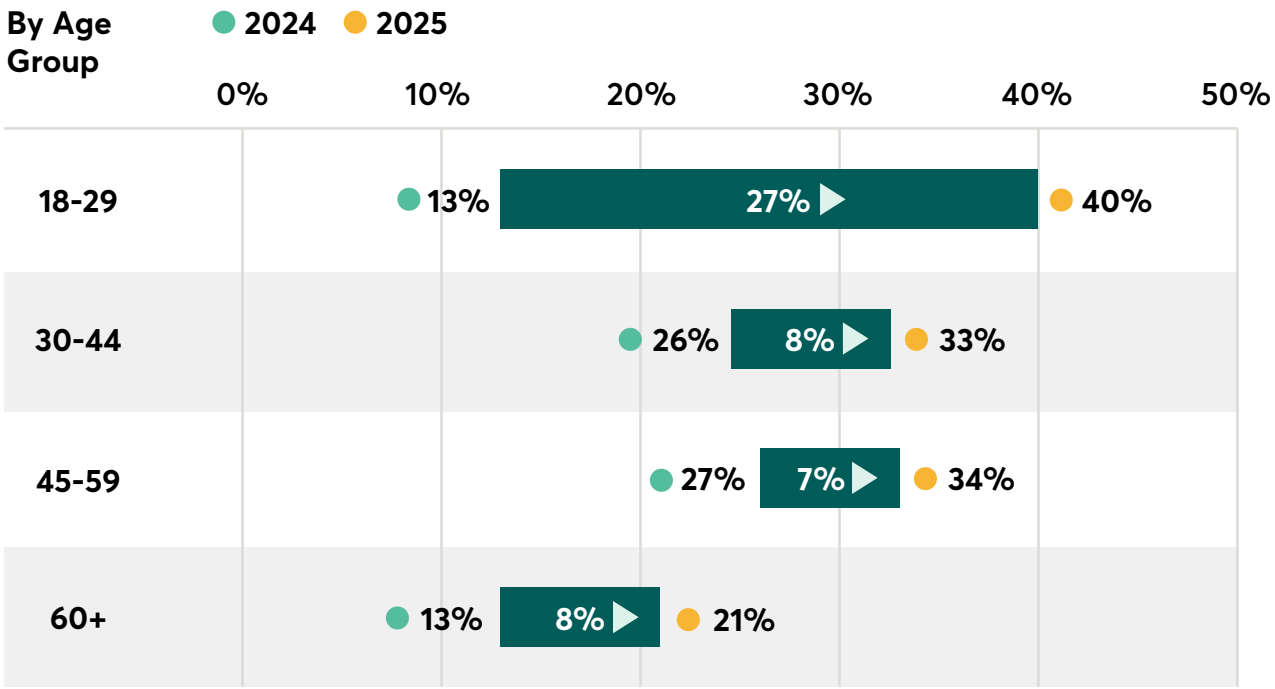
What Type of Platform Did the Cyberattack or Scam Begin On?	2025	2024
A text message or messaging app like iMessage, WhatsApp, or Facebook Messenger	30%	20%
Email	27%	30%
Social Media	17%	23%
A phone call	11%	9%
A dating app or website	3%	3%
Other	6%	7%
Unsure	5%	9%

Base: Respondents who have personally encountered a cyberattack or a digital scam attempt.

Sources: Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults (April 2025) and Consumer Reports nationally representative American Experiences Survey of 2,042 U.S. adults (April 2024).

We saw an increase in text scams as a proportion of scams encountered. Text scams have meaningfully increased in the past year for all age groups, but while older age groups saw increases of 7 or 8 percentage points, the youngest age group experienced a 27 percentage-point increase in encountering text scams.

Percentage Increase in Reported Scam Attempts That Began In a Text Message or a Messaging App



Percentages are rounded to whole numbers. As a result, they may not appear to sum precisely.

> **Gen Z is falling victim to record levels of text scams due to three colliding trends. First, texting is their primary communication channel, with hundreds of daily messages creating a perfect opening for scammers. Second, they tend to be in large group messaging threads with unknown contacts, making it easy to mistake a scammer's number for a friend's number. Third, they have less experience spotting scams but instant access to money on their phones, reducing friction for scams to succeed. For many, especially with small-dollar scams, the experience has become so common that it feels almost normal!**

JASON DORSEY
President and Lead Gen Z Researcher, The Center for Generational Kinetics

PREVENTING TEXTING OR MESSAGING SCAMS

Texting or messaging scams have increased in the last year, with 30 percent of those who experienced a cyberattack or digital scam saying it began over a text message or a messaging app, compared with 20 percent who reported the same the year prior. Whether it's WhatsApp, iMessage on Apple or Google Messages, consumers are fielding more scams via messaging applications.

While there's currently no way to eliminate the spam and scam texts you receive, the major smartphone makers and three biggest cell phone service providers all offer tools that can reduce their incidence.

SMARTPHONES

Apple iPhones: With iOS 26, Apple's iMessage messaging service allows users to block unknown numbers, filter and report spam messages, block unwanted messages, and turn off business alerts. To turn these settings on, you will need to click on the hamburger menu in Messages and click on Manage Filtering. In a section called Screen Unknown Senders, you will have the option to turn the setting on. Then you have the option on how you want to handle notifications from unknown senders. You can hide notifications from unknown senders and move those messages into an unknown senders list. You will also be able to manage notification alerts across different categories of notifications. For example, turning on Time Sensitive notifications will allow you to receive those that are time sensitive, such as alerts, account verification codes, or urgent messages. Turning on Transactions allows order updates, receipts and confirmations to come through. Apple also has a feature called Text Message Filter that uses on-device machine learning to filter messages from unknown senders into the Transactions or Promotions categories, which can help users organize their texts and make spam filtering a bit more useful. Apple has Text Message Filter turned on by default, but users can turn it off.

Samsung phones: Samsung has its own messaging app, Samsung Messages, but is transitioning to Google Messages on its handsets. If you are still using Samsung Messages, you can block numbers that deliver spam by selecting them and choosing "block" from the option menu. The app also gives you the option to report a message as spam.

Android phones: These handsets usually use the Google Messages app by default, which actively filters out suspected spam and also offers users the option to block or mark messages as spam on their own. When it encounters a suspicious message it will offer the user an alert and let them click to indicate whether the message is or is not spam. Unlike the other services mentioned here, Google Messages looks at the content of unencrypted messages, among other data, to determine if something is likely spam. Google uses RCS, an industry-standard messaging protocol: Messages between two users that use RCS-based chats are always encrypted at the transport layer, and Google also employs end-to-end encryption, which means they are encrypted at the server as well. Note that many iPhone users are not yet using RCS, which means texts between Android and many iPhone users are not encrypted. Only iPhone users who have iOS 18 or later and who have manually turned on RCS are using it. We recommend that iPhone users turn on RCS messaging if they are able.

CELL PHONE SERVICE PROVIDERS

Cell service providers have joined together to create the Secure Messaging Initiative, which provides a clearinghouse for information about suspected scam messages. Suspicious activity can include information such as the originating IP address, abnormalities in the message headers, and time and volume of messages. Carriers then tag these messages and shunt them to a suspected spam filter or block them.

To help stop spam from reaching your phone, forward spam texts to 7726 (SPAM), which shares the sender with your cell phone service provider.

AT&T offers ActiveArmor, which has both free and paid tiers. To use it, consumers must download the AT&T ActiveArmor mobile application and keep it running. The free version of the ActiveArmor app allows users to block callers and messages and attempts to block spam texts and calls. If customers upgrade to the $3.99 per month paid service, AT&T says the app "Detects and blocks harmful website links to protect you from malware and phishing attempts."

Verizon provides an in-depth discussion of how it works behind the scenes to prevent unwanted texts and provides a mobile app called Call Filter that blocks unwanted numbers and filters spam calls. A $3.99 per month upgrade lets users block entire categories of calls, such as those from telemarketers or politicians, as well as create customized blocking lists.

T-Mobile provides identification and blocking services that it calls Scam ID and Scam Block. It also offers an app called T-Life that comes in a free and a $4 per month paid version. Scam ID displays "Scam Likely" and uses mechanisms beyond the telephone number to help reject spoofed numbers. T-Mobile also labels some calls as telemarketing, political, and potential scam before they reach your phone and shows that label to customers. Scam Block will automatically block any calls the app determines are likely scams. If a customer wants to also block whole categories of calls, such as political or telemarketing, they have to upgrade to a paid version of T-Life. Prepaid T-Mobile customers can dial #662# to enable Scam Block and #436# to enable Caller ID.

As a final note, it's important that you do not reply to any scam messages that do make it through. Do not text STOP or try to engage a scammer via text. Replies confirm that your number is in use and scammers will continue to target it or sell it as part of a list of working numbers. Block the number sending the suspicious text or mark it as spam and forward the text to 7726 to cover all of your bases.

PREVENTING SOCIAL MEDIA SCAMS

Consumers report being affected by digital scams as much this year as the previous year. Federal Trade Commission (FTC) research shows that fraud on social media platforms is often related to product advertisements. In 2023, the FTC also investigated social media companies' efforts to combat fraudulent products and scams advertised to users on their platforms.

Digital payment apps like CashApp, Venmo, and Zelle generally offer fewer protections than credit cards, and should be used to pay only friends, family, and people you trust. Make sure that you are not sending money to an impersonator. These apps may reimburse some consumers in some cases, but they are not legally required to provide the same protections against fraud that traditional financial institutions are.

All payment platforms should take proactive efforts to strengthen consumer protections and reach underrepresented communities. Education to increase awareness around popular scamming techniques can also help. For example, do not respond to unsolicited requests for payment. If someone you know reaches out in an "emergency," connect on a different platform with them to get the real story; there's a possibility their account was hacked. Scammers often try to create a false sense of urgency. If they are pushing you to act immediately, that could be a sign of a scam, so assess the situation instead of immediately reacting.

Social media companies make money from fraudulent advertisements while arguing that they have no legal duty to users to combat these scams. With over a dozen federal agencies making efforts to combat online scams, there is a pressing need for a comprehensive, government-wide strategy to protect consumers, and for continued support for consumer-facing agencies like the Federal Trade Commission and the Consumer Financial Protection Bureau. Meanwhile, social media platforms that profit from advertising networks utilized by scammers must invest more resources in enforcing fraud policies and providing support for victims of scams. Until this happens, the burden will continue to fall unfairly on consumers to learn how to protect themselves from scams.

DIGITAL SCAM METHODS

We found no meaningful change from last year when we asked about the methods that had been used in the attacks that people experienced. Phishing was still the most common type of scam or attack that people experienced, with 39 percent of those who had experienced an attack or scam saying that they had received messages or emails purporting to be from a legitimate source asking for personal information. One in 4 of this group said that scammers had pretended to be their bank, and 1 in 4 said the scammers pretended to be tech support. SIM swapping (where criminals get your phone number assigned to their device and use it, for example, to sign in to your bank account or other sensitive accounts) and deepfake video (where a person's face or body is digitally altered so they appear to be someone else) were selected by just 4 percent and 3 percent of this group, respectively, although it might be particularly difficult to be aware of those attacks. Of course, people could report only on the methods of which they were aware. The starred methods in the chart below were defined for the respondents, but those definitions have been omitted here for brevity.

Which, If Any, of the Following Methods Did the Attack or Scam Use?	2025	2024
Phishing*	39%	38%
Pretending to be your bank or credit card company	25%	27%
Pretending to be tech support	25%	27%
Impersonating someone you know	17%	17%
Catfishing*	14%	16%
Stalkerware or spyware*	7%	5%
Impersonating a famous person	6%	4%
Ransomware*	4%	7%
SIM swapping*	4%	3%
Deepfake video	3%	2%
Other	14%	12%
No response	1%	3%

Base: Respondents who have personally encountered a cyberattack or a digital scam attempt.
(Respondents could select multiple responses.)
**See links below for full language.*

Sources: Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults (April 2025) and Consumer Reports nationally representative American Experiences Survey of 2,042 U.S. adults (April 2024).

ACCOUNT TAKEOVERS

Lastly, we asked the people who had experienced a cyberattack or a digital scam if they had ever had an online account taken over by scammers. Once again, we did not find any significant change from last year. Two out of 3 (69 percent) said that had never happened to them. Seventeen percent said they had a social media account taken over, and 12 percent said they had an email account taken over.

Have You Ever Had One of Your Online Accounts Hacked or Taken Over by a Scammer?	2025	2024
No	69%	65%
Yes, a social media account	17%	22%
Yes, an email account	12%	11%
Yes, another type of account	5%	5%

Base: Respondents who have personally encountered a cyberattack or a digital scam attempt. (Respondents could select multiple responses.)

Sources: Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults (April 2025) and Consumer Reports nationally representative American Experiences Survey of 2,042 U.S. adults (April 2024).

PASSWORDS AND PASSKEYS

Our May 2025 nationally representative survey examined Americans' digital security habits.

The most common precautions Americans said they take to protect their privacy and personal data are using a strong password to protect their home WiFi network and requiring a password, PIN, or other method to unlock their smartphone. Almost as many, around 4 in 5, use multifactor authentication (MFA) to log in to at least one account. These were also the most common responses last year.

People were slightly more likely to say they used password managers this year than last year, rising from 36 percent last year to 42 percent this year. However, this was still the least common response.

When It Comes to Passwords, Do You ...?	MAY 2025	MAY 2024	MAY 2023
Use a strong password to access your home WiFi network	86%	89%	86%
Require a password, PIN, or other method to unlock your smartphone	86%	86%	83%
Use multifactor authentication to log in to any of your online accounts	81%	80%	76%
Use a unique password across your different accounts	65%	65%	67%
Change default passwords on devices, such as routers, modems, "smart" appliances, and so on	65%	61%	59%
Use a password manager that automatically creates and stores a very strong password for each of your online accounts	42%	36%	37%

Base: Respondents who did not say "not applicable."
**See links below for full language.*

Sources: Consumer Reports nationally representative American Experiences Survey of 2,333 U.S. adults (May 2025); Consumer Reports nationally representative American Experiences Survey of 2,022 U.S. adults (May 2024); and Consumer Reports nationally representative American Experiences Survey of 2,000 U.S. adults (May 2023).

MULTIFACTOR AUTHENTICATION

We sought to understand whether Americans use multifactor authentication as well as what types of multifactor authentication they use, noting that it's possible to use more than one type. Most of the 81 percent of Americans who use multifactor authentication said they used SMS or text-based authentication, as they did last year and the year before. Just over half use an app like Google Authenticator or Duo Mobile, also similar to last year. As was true the last few years, about a quarter of respondents who use MFA get a phone call that instructs them to press a certain key to log in, and 5 percent use a physical security key (small USB key or wireless dongle), the most secure method of authentication.

This year we added a new response option, passkeys, which we defined as a digital credential tied to a user account, usually used instead of a password. A third of Americans who use multifactor authentication said they use a passkey.

Which, If Any, of the Following Types of Multifactor Authentication Do You Use?	MAY 2025	MAY 2024	MAY 2023
SMS or text-based: You get a code texted to you that you enter to log in	83%	83%	82%
Multifactor authentication apps, like Google Authenticator or Duo Mobile	55%	54%	50%
Passkey, a digital credential tied to a user account, usually used instead of a password	33%	—	—
Phone call authentication, that is, you get a call and answer or press a particular key to log in	24%	25%	26%
Physical security key: You plug in a USB-C or other small device when logging on	5%	5%	6%
Other (please specify)	1%	1%	2%

Base: Respondents who use multifactor authentication.
(Respondents could select all that applied.)
**See links below for full language.*

Sources: Consumer Reports nationally representative American Experiences Survey of 2,333 U.S. adults (May 2025); Consumer Reports nationally representative American Experiences Survey of 2,022 U.S. adults (May 2024); and Consumer Reports nationally representative American Experiences Survey of 2,000 U.S. adults (May 2023).

PASSKEYS

Passkeys, one of the newest digital security tools, were introduced in 2022 and provide a way to securely access websites without using a password. They are based on public key encryption technology, which uses a pair of digital "keys," one stored on the website or service you want to access and the other stored on your device or in the cloud. Both keys must be used to verify your identity. The key stored on your device can be accessed only by you, usually by using a passcode or biometric data, such as a face scan or fingerprint. Passkeys are more secure than traditional passwords because they cannot be shared with malicious sites or during a phishing attempt.

Consumer Reports' May 2025 American Experiences Survey data show that 33 percent of consumers who use any type of multifactor authentication are using a passkey, a noteworthy figure in part because passkeys are so new.

THE INTRODUCTION OF PASSKEYS HAS BEEN CONFUSING

While passkeys are easier to use than passwords and offer superior security, they have their own drawbacks that need to be ironed out. For example, they do not transfer seamlessly between password managers maintained by various devices or ecosystems. So, if you have a passkey that is stored in Apple's iCloud Keychain on your MacBook but not synced with the cloud, it may not be available on your Google Android phone. Or if you use Google's Chrome browser to manage your passwords and then try to access a passkey created on an iPhone using Safari, it won't work.

An additional layer of confusion exists when consumers expect a passkey to run across all of the services associated with a particular company, but the company has yet to implement passkeys everywhere. When Facebook implemented passkeys on mobile devices in June, it allowed users to log in to the site using a passkey on their phones. But the company waited a few months before letting those same mobile users log in to Facebook Messenger on the phone. Similarly, U.S. consumers can be tripped up when a company has rolled out passkeys first in North America and a consumer travels to a country where the company has not yet implemented passkeys.

Some of these rollout delays will be resolved over time, and the upcoming implementation of the FIDO Alliance's Credential Exchange Protocol and the Credential Exchange Format will enable the secure transfer of passkeys from password manager to password manager. Andrew Shikiar, the executive director and CEO at the FIDO Alliance, says he expects these problems to be resolved in the next couple of years. Credential Exchange is supported for those in the Apple ecosystem beginning with iOS 26.

WHAT YOU SHOULD DO

Despite the confusion, Consumer Reports recommends that people adopt passkeys as a more secure way to manage access to their services and devices. To make it easy to manage your passkeys across multiple ecosystems and services, we think the best practice in 2025 is to use an independent password manager such as Bitwarden, 1Password, or LastPass. Install one of these managers on your primary devices, and when prompted to create a passkey, set up the passkey and store it in your independent password manager.

If you happen to be all in on one ecosystem, such as Apple or Google, feel free to use its password manager for your passkeys, but be aware that if you want to transition to another ecosystem in the near term, you will need to set up new passkeys. After the Credential Exchange Protocol is widely implemented, moving between password managers should be relatively seamless.

When setting up a passkey, it is essential that consumers understand the recovery method and then take whatever steps are necessary to use that recovery method in a time of need. For instance, if you lose access to your phone and can't enter your fingerprint to access a site, are there other recovery mechanisms that you can access? Some sites let users enter an alternative recovery email address, use an alternative device, or even print out a code or series of codes to use in case they lose access to one of their passkeys.

PRIVACY AND SECURITY TOOLS

We asked about privacy and security tools that people have installed on the personal device they use the most. About 2 in 3 Americans said they install software updates on the personal electronic device they use the most as soon as they are available—also the most common response in the past two years. A majority also said they use software from a company such as McAfee or Norton that is designed to protect against malware or viruses.

This year's respondents were more likely than last year's to say they had identity theft protection (33 percent vs. 28 percent), browser extensions that block trackers such as Privacy Badger or uBlock Origin (29 percent vs. 25 percent), and file encryption software (14 percent vs. 10 percent).

Of all the tools we asked about, Americans were least likely to say they have encryption software installed on their devices. A quarter of Americans said they were unsure whether they have a firewall installed on their device, and 19 percent were unsure whether they use a tracker-blocking browser extension.

When It Comes to Privacy Protection Tools Installed on Your Device, Do You ...?	Yes			No			Unsure		
	2025	2024	2023	2025	2024	2023	2025	2024	2023
Implement software updates as soon as they are available	68%	71%	67%	23%	22%	24%	9%	7%	9%
Have software that prevents malware or viruses*	53%	54%	56%	35%	35%	30%	12%	12%	14%
Have a firewall	45%	42%	46%	30%	32%	28%	25%	26%	26%
Have a "virtual private network," or VPN, for accessing the internet	34%	32%	33%	52%	51%	51%	15%	17%	16%
Have identity theft protection services*	33%	28%	26%	55%	63%	62%	11%	9%	12%
Have a browser extension that blocks trackers*	29%	25%	27%	52%	53%	52%	19%	23%	22%
Have software to encrypt files on your device, so no one else can use them*	14%	10%	12%	71%	75%	73%	15%	15%	15%

Base: Respondents who did not say "not applicable."
(Respondents could select multiple responses.)
**See links below for full language.*

Sources: Consumer Reports nationally representative American Experiences Survey of 2,333 U.S. adults (May 2025); Consumer Reports nationally representative American Experiences Survey of 2,022 U.S. adults (May 2024); and Consumer Reports nationally representative American Experiences Survey of 2,000 U.S. adults (May 2023).

ENCRYPTED MESSAGING APPS

End-to-end encrypted messaging protects private communication from being accessed in transit or when stored by the provider. In Consumer Reports' April 2025 survey, a solid majority of Americans (57 percent) said they use Facebook Messenger. After Facebook Messenger, iMessage—the default messaging app on iPhones—is the encrypted messaging app Americans were most likely to say they use, at 39 percent, while 27 percent said they use WhatsApp and 23 percent said they use Google Messages, the default messaging app on Android phones. These percentages are consistent with last year's findings.

The Following Apps Use Digital Encryption to Protect Your Communications and Keep Them Private. Which, If Any, of These Apps Do You Use to Communicate With Other People?	2025	2024
Facebook Messenger	57%	60%
iMessage*	39%	39%
WhatsApp	27%	25%
Google Messages*	23%	22%
Signal	4%	4%
Threema	.5%	.4%
Another encrypted messaging app	1%	2%
None of these	14%	14%

Base: All Respondents.
(Respondents could select multiple responses.)
**See link below for full language.*

Sources: Consumer Reports nationally representative American Experiences Survey of 2,158 U.S. adults (April 2025) and Consumer Reports nationally representative American Experiences Survey of 2,042 U.S. adults (April 2024).

SETTINGS AND BEHAVIORS

In May, we asked about a list of actions people may take to protect their data and privacy. Like last year, more than 9 in 10 Americans said they avoid clicking on links in texts or emails from people they do not know. And most Americans continue to be wary of how much data smartphones collect; most said they will either delete apps or avoid installing them in the first place if they think the apps collect too much data or do not adequately protect it. Moreover, most Americans allow apps to access their location only while they're using said apps. Similarly, 4 in 5 Americans adjust the permissions settings of their smartphone apps to restrict access to their camera, location, or contacts when the app does not need them to function. This helps minimize companies collecting that data in a way that doesn't provide any real benefit to the consumer.

On the other hand, fewer than half of Americans regularly review their security settings, which can help assure that they reflect their current preferences to avoid unwanted data sharing, and just 24 percent encrypt their hard drives, which protects their data in the case of theft when the hard drives are not already encrypted by default.

Here Is a List of Actions People Might Take to Protect Their Privacy or Personal Data. Do You ...?	MAY 2025	MAY 2024	MAY 2023
Avoid clicking links in texts from people you don't know	94%	94%	92%
Avoid clicking links in emails from people you don't know	93%	94%	91%
Delete or choose not to install apps on your smartphone if you think they collect too much personal information*	86%	84%	82%
Adjust smartphone settings to only allow an app access to your location while you are using the app	83%	84%	83%
Set permissions for apps on your smartphone to block access to things like your camera, location, or contacts if they aren't needed for the app to function*	80%	80%	79%
Block or routinely delete some or all cookies on your web browser	72%	70%	71%
Adjust the privacy settings in your web browser	63%	61%	63%
Use "private" or "incognito" mode on your web browser*	60%	57%	57%
Review security settings at least once every six months	48%	46%	47%
Encrypt your hard drive	24%	22%	22%

Base: Respondents who did not say "not applicable."
(Respondents could select multiple responses.)
**See links below for full language.*

Sources: Consumer Reports nationally representative American Experiences Survey of 2,333 U.S. adults (May 2025); Consumer Reports nationally representative American Experiences Survey of 2,022 U.S. adults (May 2024); and Consumer Reports nationally representative American Experiences Survey of 2,000 U.S. adults (May 2023).

USEFUL SECURITY TOOLS

Consumers are increasing their use of some security tools and software to protect themselves online. Americans' confidence that their personal data is private and not distributed without their knowledge has dropped each year in our survey since 2023. This, combined with continued education and outreach efforts through tools such as Security Planner, as well as a focus on usability by security tool designers, may have led to the increase in the use of these tools. The tools include the following.

Password managers: Reusing passwords is a widespread security risk. More consumers are using password managers, which create and store strong, unique passwords for online accounts. These tools make it easy and convenient for users to protect themselves online. Security experts advise users to create unique passwords for each account they have; password managers remove the need to memorize them all and simplify the process of securely logging in to accounts.

Third-party tracker blockers: Consumers are also increasing their use of free browser extensions like Privacy Badger or uBlock Origin, which block third-party trackers. This makes it difficult for advertisers and companies to track consumers across multiple websites and reduces the digital footprint consumers generate with both regular and sensitive online activities. They also have additional benefits, such as reducing the number of advertisements—including malicious "malvertisements" that can infect devices with viruses—and can even reduce website load times. Third-party tracker blockers benefit consumers greatly, yet tech companies like Google (which has been fined repeatedly for illegally tracking users) are intentionally disabling the usability of sites like YouTube for users who have these browser extensions. Consumers and regulators must push back against this.

File encryption software: Most modern computer operating systems offer file encryption software by default through programs like BitLocker or FileVault (note that file encryption programs often need to be enabled). This encrypts the content of the device's hard drive so that it cannot be read if it is accessed by an unauthorized user, and it protects the files and personal information on the device if it is lost or stolen. While more consumers report that they are encrypting their devices, many remain unsure. More research is needed to see how many consumers are actually benefiting from file encryption software without being aware of it because some manufacturers encrypt hard drives by default.

Identity theft protection services: Consumers are turning to identity theft protection services like Experian, Aura, or LifeLock at higher rates than in 2024, possibly due to frequent news coverage of massive data breaches. These services help consumers respond to identity theft by covering some financial damages, providing credit alerts, monitoring potential future scams, and providing assistance in recovering from identity theft. The U.S. Government Accountability Office found that government entities and private businesses often offer identity theft services to individuals affected by data breaches, but that the usefulness of such services was limited to helping consumers after identity theft occurred, a conclusion Consumer Reports also reached. It is unclear if the increase in the use of identity protection services is the result of individual consumers deciding to subscribe to them or because they are being provided to consumers who have been affected by data breaches.

CONFIDENCE THAT PERSONAL DATE IS PRIVATE

We asked Americans how confident they are that their personal data, such as their Social Security number, health history, and financial information, is private and is not being distributed without their knowledge. Although consumer confidence was virtually unchanged in our surveys between 2022 and 2024, this year only 48 percent of Americans said they were at least somewhat confident that their personal data is private, down from 53 percent last year. While those who said they were very confident remained flat at 8 percent, those who were somewhat confident fell from 45 to 40 percent. Thirty-six percent were "not too confident," up from 32 percent in 2024, and 16 percent were not confident at all.

Although the survey responses do not indicate whether the diminishing confidence is due to government or industry shortcomings, it suggests that a great deal of work must be done to protect privacy and restore Americans' confidence about how their data is being used.

Americans' Confidence That Their Personal Data Is Private and Not Distributed Without Their Knowledge	MAY 2025	MAY 2024	MAY 2023	JUNE 2022
Very confident	8%	8%	10%	7%
Somewhat confident	40%	45%	46%	45%
Not too confident	36%	32%	31%	34%
Not confident at all	16%	15%	13%	14%

Base: All respondents.

Sources: Consumer Reports nationally representative American Experiences Survey of 2,333 U.S. adults (May 2025); Consumer Reports nationally representative American Experiences Survey of 2,022 U.S. adults (May 2024), Consumer Reports nationally representative American Experiences Survey of 2,000 U.S. adults (May 2023), and Consumer Reports nationally representative American Experiences Survey of 2,103 U.S. adults (June 2022).

Closing

The Fourth Annual Consumer Cyber Readiness Report shows that while consumers are taking additional steps to reduce their risk online by using password managers, third-party tracker blockers, file encryption software, and identity theft protection, there is much work yet to be done. We see consumer confidence in the privacy of their personal data dropping, and an increase in text messaging-based scams, especially in younger age brackets. Like last year, we note a racial disparity, where Black Americans who encounter scams are more likely to lose money. And this year, we see a financial disparity as well, with people in the highest income demographic less likely to have lost money to a scam than people in other income groups.

While consumers should take additional steps to improve their security, government and industry also have important roles to play. Policymakers and companies should advocate for or implement additional secure-by-design principles such as data minimization and encryption by default, both of which reduce the burden on consumers. Federal agencies have faced massive layoffs and funding cuts this year, but protecting consumers from scams is as important as ever. Furthermore, we need to reinvest in consumer protection agencies to go after criminals and fraudsters to hold them accountable and to return money stolen from consumers. Unfortunately, these agencies are seriously underfunded today, so the burden will fall more on consumers to adopt good cybersecurity practices to protect themselves from increasingly sophisticated scams and attacks.

Thank You

AUTHORS

YAEL GRAUER
STACEY HIGGINBOTHAM
JEFF LANDALE
Consumer Reports

LEAD CONTRIBUTORS

NOEMI ALTMAN
TESS M. YANISCH
Consumer Reports

CONTRIBUTORS

CHUCK BELL
JUSTIN BROOKMAN
Consumer Reports

DESIGN

CHRIS GRIGGS
Consumer Reports

SURVEY RESEARCH

NOEMI ALTMAN
TESS M. YANISCH
Consumer Reports

EDITING

KEVIN DOYLE
SCOTT MEDINTZ
Consumer Reports

COPYEDITING

JAMES BROCK
Consumer Reports

FACT-CHECKING

JONEA GURWITT
Consumer Reports

GUEST CONTRIBUTORS

YVETTE D. CLARKE
Representative (New York 9th District), Chair of the Congressional Black Caucus

JASON DORSEY
President and Lead Gen Z Researcher, The Center for Generational Kinetics

Consumer Reports works to create a fair and just marketplace for all. As a mission-driven, independent, nonprofit member organization, Consumer Reports empowers and informs consumers, incentivizes corporations to act responsibly, and helps policymakers prioritize the rights and interests of consumers in order to shape a truly consumer-driven marketplace.

Aspen Digital is a nonpartisan technology and information-focused organization that brings together thinkers and doers to uncover new ideas and spark policies, processes, and procedures that strengthen communities all over the world. This future-focused Aspen Institute program inspires collaboration among voices from industry, government, and civil society to ensure our interconnected world drives networked impact.

The Global Cyber Alliance is an international nonprofit organization focused on delivering a secure and trustworthy internet that enables social and economic progress for all. The Global Cyber Alliance mobilizes collective action to tackle the Internet's greatest challenges and build a safer digital world for everyone.

Go to securityplanner.org to find information on staying safer online.