2024

CONSUMER CYBER READINESS REPORT

Cyber Civil Defense Initiative

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

Introduction

The Third Annual Consumer Cyber Readiness Report reviews consumer attitudes toward digital privacy and security practices. Together, Consumer Reports, Aspen Digital, and Global Cyber Alliance have reviewed findings from Consumer Reports' recent nationally representative surveys and connected with thought leaders to understand consumers' behaviors to improve their own digital privacy and security. In addition to our year-over-year findings on cybersecurity behavior, this year we've included data based on new survey questions designed to give us insight into consumer scams and their attack vectors.

Our findings indicate that while consumers do take steps to improve their cybersecurity online, the adoption of practices and tools has remained flat. Cyberattacks and digital scams continue to pose a serious threat, and many Americans are affected.

Improving our nation's cyber civil defense is a team effort. While consumers can take steps to improve their cyber hygiene, government and industry also have a role to play. In particular, companies can lift the burden from consumers by designing products with a secure-by-default, secure-by-design approach and by utilizing best practices such as data minimization. Regulators need to take action against companies that fail to use reasonable safeguards to protect data and systems from attack. This involves enacting clearer protections and investing resources in enforcing existing laws that are often ignored due to chronic underenforcement.

We have analyzed our survey findings and provided recommendations to improve both consumer behavior and the ecosystem at large. We have also enlisted commentary from leaders in cybersecurity, who provided insights on the behavioral trends identified in this report and suggested ways that industry, government, and consumers can continue to improve our nation's cyber civil defense.

> "Everyone needs to protect themselves, their families, and the whole country against ongoing for-real cyber threats. The 2024 Consumer Cyber Readiness Report reminds us that we all need to work together to better address real, everyday attacks on us all. As cyber threats become more sophisticated, we need to get real serious about education, innovation, and collaboration. It's not just about individual actions anymore—we need a collective approach to cybersecurity that involves consumers, industry, and government working in tandem.

CRAIG NEWMARK
Founder of craigslist, Philanthropist, and Lead of the #CyberCivilDefense initiative

Key Findings

Among the security habits surveyed, consumer privacy and security practices remain flat. There were no significant changes from the survey we conducted in 2023. This year we added new questions to give us insight into the scams to which people are susceptible.

DIGITAL SCAMS

A cyberattack or digital scam is 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 any deceptive tactics to commit a crime.

VULNERABILITY TO FRAUD VIA SOCIAL MEDIA

Two-thirds of social media users (67 percent) say they have received friend requests from people they don't know. Roughly half say they have received direct messages that seemed to be part of a scam or fraud attempt. And roughly half say they have received direct messages on social media from people they don't know.

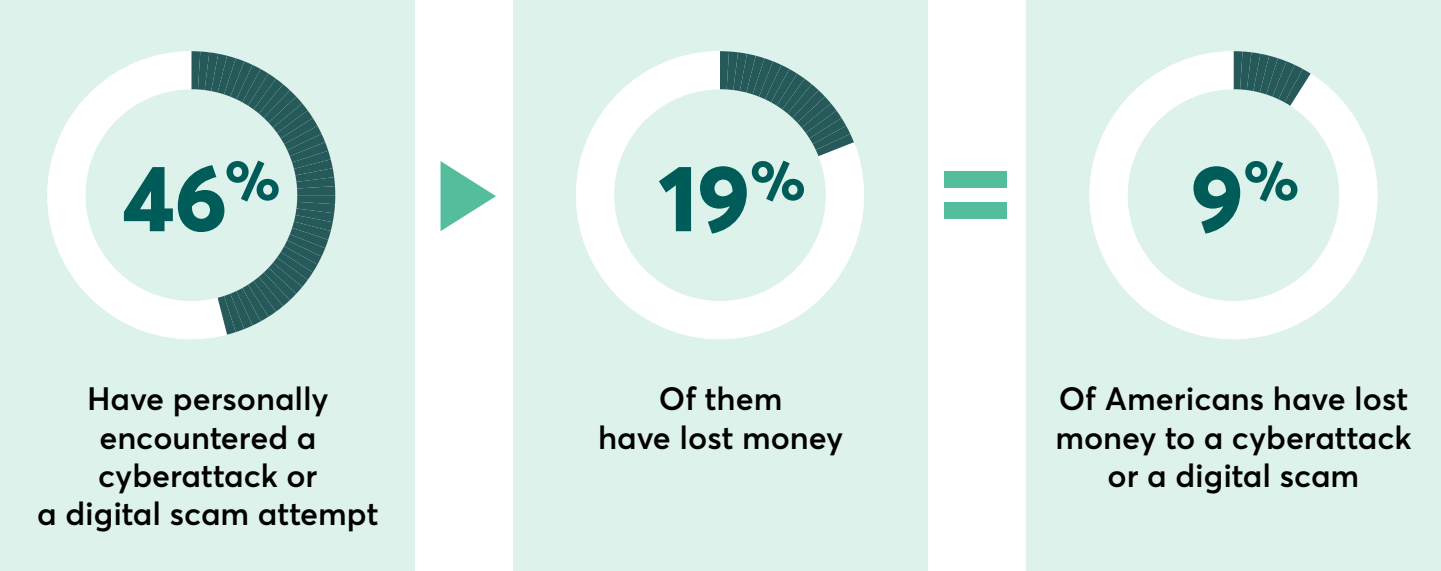
FINDING 1	Have You Had Any of the Following Experiences on Any Social Media Site or App in the Past 12 Months?	2024
Received friend requests on social media from people you don't know		67%
Received direct messages on social media that seemed to be part of a scam or fraud attempt		48%
Received direct messages on social media from people you don't know		47%
Bought a product by clicking through an ad on social media		22%
Bought a product through a social media platform like Facebook Marketplace*		21%
Responded to requests for donations that came directly from an organization on social media*		7%
I have not experienced any of these in the past 12 months		15%

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

Source: Consumer Reports 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 say they have personally encountered a scam or cyberattack—or about 1 in 10 Americans—say they lost money to the scam.



Base: All respondents, or as indicated.

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

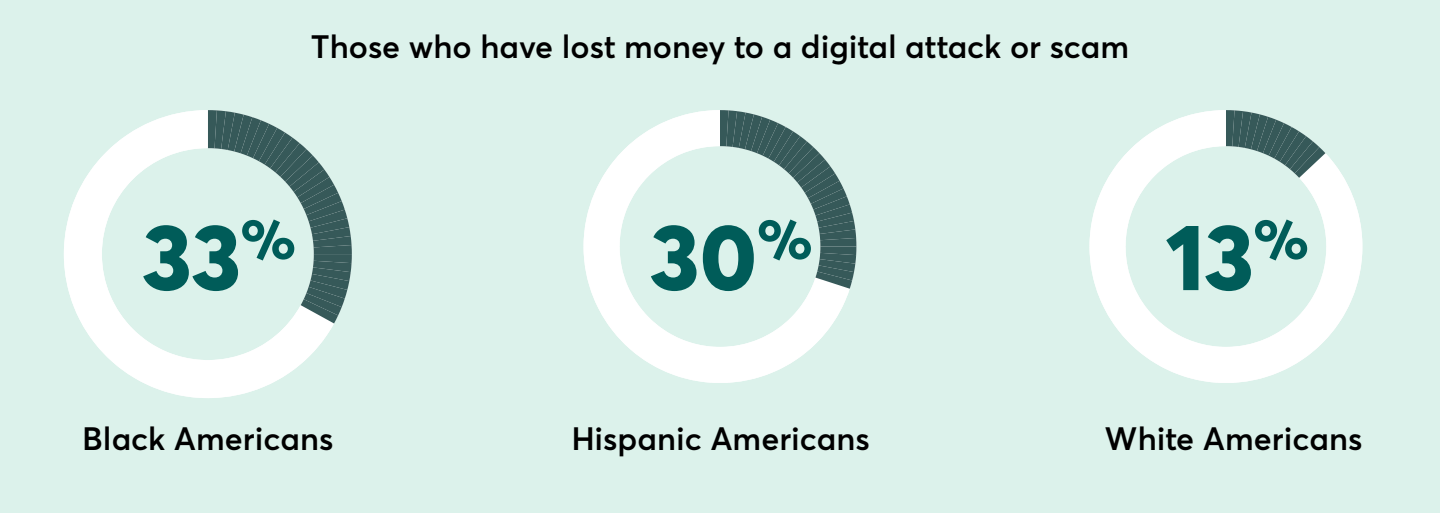
> *The figures in this report are deeply concerning. Unfortunately, they are in line with global trends. We estimate $1 trillion was lost last year in scams and a quarter of the global population has been approached by a scammer. More action is required on both the national and international level to protect consumers.*

JORIJ ABRAHAM
Managing Director,
Global Anti-Scam Alliance

> *Scams are becoming increasingly difficult to recognize and are having an alarming financial impact on Americans. Through strong public private partnerships and continued innovation with emerging technologies, we are helping to improve detection and prevention of scams while taking steps to teach consumers how to spot them.*

MICHAEL LASHLEE
Chief Security Officer,
Mastercard

Among Americans who have personally encountered a cyberattack or digital scam attempt, Black and Hispanic Americans are twice as likely to have lost money to a digital attack or scam as white Americans: Thirty-three percent of Black Americans and 30 percent of Hispanic Americans who have encountered such an attack say they have lost money to a digital attack or scam, compared with just 13 percent of white Americans.



Base: Respondents who have personally encountered a cyberattack or a digital scam attempt.
Asian, multiracial, other, and unknown race were present in the data in insufficient numbers to report.
Race and Hispanic ethnicity were recorded in separate questions; people who identified as Hispanic are reported as Hispanic here, regardless of what race(s) they selected.

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

The difference between racial/ethnic groups on having lost money to a cyberattack or scam was found to be statistically significant in a logistic regression controlling for gender, age, household income, educational attainment, region, urbanicity, and political leaning. It's not clear why this disparity exists, but several other studies, including a 2016 report by the Federal Trade Commission, "Combating Fraud in African American and Latino Communities," note that communities of color are more likely to become victims of fraud and are more likely to lose money when they are victims of fraud.

A 2021 FTC report "Serving Communities of Color" noted that communities of color filed more reports that included paying for services and things using debit cards, cash, cryptocurrency, and money orders, which have fewer fraud protections when compared with credit cards. By contrast, white Americans reporting fraud said they used credit cards more often. That report also noted that the government relies on widespread reports of fraud to understand trends in scams and to educate consumers about the types of fraud active in their communities. However, Latino communities (as extrapolated from demographic data on ZIP codes where fraud was reported) submitted fewer fraud reports than white-dominated ZIP codes. Black communities filed more reports than both white and Latino communities, so reporting fraud cannot be the sole reason that Black and Latino communities are disproportionately likely to lose money in a digital scam.

Regardless, the disparities are so substantial that we're calling for more research to understand why Black and Latino Americans are so much more likely to lose money from digital attacks or scams. Everyone should have the opportunity to be safe on the internet.

> *This report reveals a disturbing digital divide. Black Americans losing money to cyber scams at twice the rate of white Americans is unacceptable. We must act swiftly to close this gap through targeted education, stronger consumer protections, and increased investment in digital awareness for our communities.*

STEVEN HORSFORD
Representative (Nevada 4th District), Chair of the Congressional Black Caucus

> *The disproportionate impact of digital scams on Hispanic Americans is alarming. This disparity underscores the urgent need for tailored cybersecurity education, enhanced consumer safeguards, and policies addressing language barriers. We must ensure our community has equal protection and resources in the digital landscape.*

NANETTE BARRAGÁN
Representative (California 44th District), Chair of the Congressional Hispanic Caucus

PLATFORMS WHERE DIGITAL SCAMS BEGIN

The majority of scam attempts that Americans have experienced began on email, social media, or text messages, or through a messaging app.

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

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

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

DIGITAL SCAMS METHODS

We wanted more insight on the methods that had been used in the attacks people experienced, while noting that people can, of course, report only on the methods of which they are aware. The most common type of scam or attack people say they experienced was phishing, where scammers trick you into giving them your personal information, such as a password or credit card number. Other common types of scams or attacks involved impersonation, where scammers pretend to be, for example, the consumer's bank, a tech support person, or even someone they know personally.

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

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

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

> *Although stories about AI-generated deepfakes dominate the news, most cybercrime and fraud attempts rely on less sophisticated approaches. Well-known social engineering techniques, such as phishing emails or smishing texts, are much more common and affect far more people than cutting-edge AI tools. Traditional techniques continue to work, at least for now.*

J. MICHAEL DANIEL
President and CEO,
Cyber Threat Alliance

> *Creating a unified mission to address global cybersecurity challenges requires collaboration on a worldwide scale. Despite increased phishing awareness, the high rate of account takeovers indicates that recognition alone isn't sufficient. To effectively counter evolving threats, we must enhance global cooperation and advocate for updated legislation to foster comprehensive, collective defense strategies.*

CHRIS GIBSON
CEO, Forum of Incident Response and Security Teams (FIRST)

ACCOUNT TAKEOVERS

Two in 10 Americans who experienced a cyberattack or a digital scam say a social media account had been taken over, and roughly 1 in 10 say they had an email account taken over.

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

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

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

RECOMMENDATION FOR (INDUSTRY) MANUFACTURERS/COMPANIES

Make it easier to get accounts back after they're hacked/taken over (email and social).
Social media companies should provide sufficient dedicated staff to help consumers whose accounts have been taken over. These contact centers should be easily accessible by the public, and their existence should be prominently promoted.

PASSWORDS AND PASSKEYS

How Consumers Protect Their Personal Data When It Comes to Passwords

Another nationally representative CR survey, this one of 2,022 U.S. adults in May 2024, examined Americans' digital security habits. The most common precaution Americans say they take to protect their passwords is using a strong password to protect their home WiFi network. Most also require a password, PIN, or other method to unlock their smartphone, and a majority use multifactor authentication (MFA), which requires a password plus another piece of information to log in to an online account. Roughly a third of Americans do not use unique passwords across accounts, even though doing so can limit the damage when a single password is compromised (such as in a data breach) and even though threat actors use username and password combinations to try to access additional accounts. Using a password manager makes it extremely easy to generate and store strong, unique passwords for each account, but adoption of password managers remains low among consumers.

Passkeys are an emerging tool to help consumers protect access to their accounts without using passwords. Passkeys enable consumers to use a physical device such as their phone, a security key, or even the password manager from their web browser to sign into a service. Major web platforms started rolling out passkeys last year, and the ultimate goal is to end reliance on passwords.

However, the rollout of passkeys has been uneven. Not all platforms are offering consumers the opportunity to use passkeys. Some platforms allow passkeys on the web, but not on mobile devices. Additionally, for users who switch between mobile devices or platforms, passkeys may not transfer. Today, the best advice is for consumers to pick one device or browser to store their passkeys and use that in as many places as they can.

The user experience is not seamless for all consumers, but the benefits of passkeys are undeniable. We expect web platforms, operating system providers, and services to continue adopting passkeys. As the user experience gets easier, we encourage consumers to adopt them.

FINDING 6	When It Comes to Passwords, Do You ...?	MAY 2024	MAY 2023
	Use a strong password, often defined as at least 8 characters long, including upper and lowercase letters, numbers, and symbols, to access your home WiFi network	89%	86%
	Require a password, PIN, or other method, such as touch or face ID, to unlock your smartphone	86%	83%
	Use multifactor authentication, a feature that requires a password plus another piece of information to log in to any of your online accounts	80%	76%
	Use a unique password across your different accounts	65%	67%
	Change default passwords on devices, such as routers, modems, "smart" appliances, and so on	61%	59%
	Use a password manager that automatically creates and stores a very strong password for each of your online accounts	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 2,022 U.S. adults (May 2024) and Consumer Reports nationally representative American Experiences Survey of 2,000 U.S. adults (May 2023).

> *The vulnerability of passwords is clear in the 4,000+ password attacks we block each second at Microsoft alone. That's why we believe everyone should switch to passkeys as soon as they can, other MFA when passkeys aren't available, and—if forced to rely on passwords—password managers can help ensure unique, strong passwords to help reduce risk.*

ALEX WEINERT
VP Director of Identity Security, Microsoft

> *The rollout of passkeys, and even U2F [Universal 2nd Factor] before it, has been clunky and slow. In fact, the technology is actually moving faster than organizations can adopt, causing fragmentation and uncertainty. The single biggest problem with passkeys is the lack of a good user experience when trying to migrate or add passkeys to other devices.*

BRET JORDAN
Vice Chair of the Board of Directors, OASIS

MULTIFACTOR AUTHENTICATION

We sought to understand whether Americans use multifactor authentication to protect their personal devices, as well as what types of multifactor authentication they use, noting that it's possible to use more than one type. As we found in a similar nationally representative survey of 2,000 U.S. adults in May of last year, most Americans who use multifactor authentication use SMS or text-based authentication, and about half of Americans who use multifactor authentication use apps such as Google Authenticator or Duo Mobile. Although physical security keys (small USB keys or wireless dongles) are the most secure method of authentication, usage among consumers remains extremely low.

FINDING 7	Which, If Any, of the Following Types of Multifactor Authentication Do You Use?	MAY 2024	MAY 2023
	SMS or text-based: You get a code texted to you that you enter to log in	83%	82%
	Multifactor authentication apps, like Google Authenticator or Duo Mobile	54%	50%
	Phone call authentication, that is, you get a call and answer or press a particular key to log in	25%	26%
	Physical security key: You plug in a USB-C or other small device when logging on	5%	6%
	Other (please specify)	1%	2%

Base: Respondents who use multifactor authentication.
(Respondents could select multiple responses.)
**See links below for full language.*

Sources: 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).

> *"CISA has aptly cited FIDO Certified Security Keys as the gold standard for authentication security. These convenient devices provide consumers and employees with a portable authentication mechanism that mitigates the constantly evolving threat landscape, including increasingly sophisticated AI-driven social engineering and phishing attacks.*

ANDREW SHIKIAR
Executive Director and CEO,
FIDO Alliance

RECOMMENDATION FOR CONSUMERS

Migrate from text-based MFA to more secure versions. You can lose access to text-based MFA if you lose a phone or are removed from a phone plan (such as a work phone or plan, or a family phone plan), and text-based MFA is a bit less secure than MFA apps and is certainly less secure than security keys.

PRIVACY PROTECTION TOOLS

Around 7 in 10 Americans say that they implement software updates as soon as they are available on the personal electronic device they use the most—also the most common response last year—and a majority also say they use software from a company like McAfee or Norton that is designed to prevent malware or viruses. Of all the tools we asked about, Americans are least likely to say they have encryption software installed on their devices. About a quarter of Americans say they are unsure whether they have a firewall installed on their device, and almost as many are unsure whether they use a tracker-blocking browser extension, such as Privacy Badger or uBlock Origin.

FINDING 8	When It Comes to Privacy Protection Tools Installed on Your Device, Do You ...?	2024	2023	2024	2023	2024	2023
		Yes		No		Unsure	
Implement software updates as soon as they are available		71%	67%	22%	24%	7%	9%
Have software that prevents malware or viruses*		54%	56%	35%	30%	12%	14%
Have a firewall		42%	46%	32%	28%	26%	26%
Have a "virtual private network," or VPN, for accessing the internet		32%	33%	51%	51%	17%	16%
Have a browser extension that blocks trackers*		25%	27%	53%	52%	23%	22%
Have identity theft protection services*		28%	26%	63%	62%	9%	12%
Have software to encrypt files on your device, so no one else can use them*		10%	12%	75%	73%	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 2,022 U.S. adults (May 2024) and Consumer Reports nationally representative American Experiences Survey of 2,000 U.S. adults (May 2023).

> *"The U.S. Cyber Trust Mark will give consumers greater peace of mind about the internet of things products they bring into their homes. It will provide an easy way for shoppers to identify internet of things products that meet critical cybersecurity standards while creating incentives for manufacturers to make products more secure.*

U.S. CYBER TRUST MARK

JESSICA ROSENWORCEL
Chairwoman, Federal Communications Commission

> *Staying updated is the simplest and most effective step consumers can take to safeguard their digital lives. Regular software updates not only patch vulnerabilities but also ensure that your devices remain resilient against evolving threats. It's encouraging to see more Americans prioritizing this essential aspect of cybersecurity.*

TARAH WHEELER
CEO, Red Queen Dynamics

ENCRYPTED MESSAGING APPS

In CR's April 2024 survey, a majority of Americans (60 percent) say they use Facebook Messenger. After Facebook Messenger, iMessage—the default messaging app on iPhones—is the encrypted messaging app Americans are most likely to say they use, at 39 percent. A quarter say they use WhatsApp, and 22 percent say they use Google Messages, the default messaging app on Android phones.

FINDING 9	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?	2024
Facebook Messenger		60%
iMessage*		39%
WhatsApp		25%
Google Messages*		22%
Signal		4%
Threema		.04%
Another encrypted messaging app		2%
None of these		14%

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

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

RECOMMENDATION FOR MANUFACTURERS

Encrypt by default. Consumers are much more likely to use encryption if it's built into a tool they already use (such as Facebook or SMS) than to download a separate encryption tool. Create a visual reminder or an icon that can affirmatively indicate when a chat is encrypted.

RECOMMENDATION FOR CONSUMERS

Recognize that *group* chats on encrypted messaging tools may not be encrypted by default.

SETTINGS AND BEHAVIORS

In the May 2024 American Experiences Survey, more than 9 in 10 Americans say 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, with 84 percent saying they will either delete apps or not install them if they think the apps collect too much data or do not adequately protect data. The same percentage of Americans say they allow apps to access their location only while they are using the app. Four in 55 Americans adjust the permission settings of their smartphone apps to restrict access to their camera, location, or contacts when the app doesn't need them to function.

On the other hand, less than half of Americans regularly review their security settings, and just 22 percent encrypt their hard drive.

FINDING 10	Here Is a List of Actions People Might Take to Protect Their Privacy or Personal Data. Do You ...?	MAY 2024 AES	MAY 2023 AES
	Avoid clicking links in texts from people you don't know	94%	92%
	Avoid clicking links in emails from people you don't know	94%	91%
	Delete or choose not to install apps on your smartphone if you think they collect too much personal information*	84%	83%
	Adjust smartphone settings to only allow an app access to your location while you are using the app	84%	82%
	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%	79%
	Block or routinely delete some or all cookies on your web browser	70%	71%
	Adjust the privacy settings in your web browser	61%	63%
	Use "private" or "incognito" mode on your web browser*	57%	57%
	Review security settings at least once every six months	46%	47%
	Encrypt your hard drive	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 2,022 U.S. adults (May 2024) and Consumer Reports nationally representative American Experiences Survey of 2,000 U.S. adults (May 2023).

RECOMMENDATION FOR COMPANIES

All companies should strive to minimize the data they collect, use, and store to what is reasonably necessary to provide the service requested by a consumer.

Phone operating system manufacturers should offer periodic reminders to consumers to review their security and privacy settings. They should also make clear to consumers which apps collect sensitive data, especially if the apps have not been used or if the apps can collect data even when they are not being used.

RECOMMENDATION FOR APP DEVELOPERS

Because consumers do not want to install or use apps that collect too much data or that do not adequately protect data, developers should explain (using clear language) why their app collects sensitive data such as location data. And, in accordance with data minimization principles, when an app is done using sensitive data, the data should be deleted.

RECOMMENDATION FOR CONSUMERS

Consumers should recognize that applications often share and sell their data. This is especially likely to be true of supposedly free apps, which often generate their revenue by monetizing customer data. Consumers should generally seek to understand the relationship between their privacy and business models of the companies with which they are interacting.

> *Encrypting your hard drive is like locking the front door to your digital life. In a world where data breaches and thefts are increasingly common, protecting personal information with encryption ensures that even if your device is lost or stolen, your sensitive data remains private, secure, and inaccessible to criminals.*

DAVID BRUMLEY
CEO of Mayhem Security and
Professor at Carnegie Mellon University

CONSUMER CONFIDENCE

Also in May 2024, 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. Consumer confidence has not meaningfully changed since 2022.

Overall, a majority of Americans (53 percent) are very or somewhat confident; nevertheless, nearly half (47 percent) are not very or not at all confident. That split suggests companies have a great deal of work to do to make Americans feel more confident about how their data is being used.

FINDING 11	Americans' Confidence That Their Personal Data Is Private and Not Distributed Without Their Knowledge	MAY 2024	MAY 2023	JUNE 2022
Very confident		8%	10%	7%
Somewhat confident		45%	46%	45%
Not too confident		32%	31%	34%
Not confident at all		15%	14%	13%

Base: All respondents.

Sources: 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 Third Annual Consumer Readiness Report shows that although consumers are taking some steps to reduce their risk online, there is much work yet to be done.

While consumers can take some additional steps to improve their security, industry and government also have important roles to play. Policymakers should advocate for, and companies should adhere to, secure-by-design principles such as data minimization and encryption by default, both of which reduce the burden on consumers.

Although there has not been a statistically significant improvement in consumer cyber readiness over the past year, there is a silver lining: Consumers continue to focus on using strong passwords and multifactor authentication, and on keeping their software and devices updated. These continue to be the most effective measures available to consumers and can make a major difference in their security posture.

INDUSTRY TIP

Industry must do more to step up when security measures break down. When a consumer loses access to an account because of an account takeover, for example, companies must provide the tools, staff, and clear procedures to make it easy for consumers to report the incident and get effective help.

And if companies do not act on their own, policymakers will need to step in. In March, for example, the attorneys general of 41 states wrote a joint letter asking Meta, the parent company of Facebook, to increase its investment in account takeover mitigation tactics and to respond quickly to users whose accounts were taken over.

Closing

The last year has again brought home the risks businesses face from online threats, including ransomware. Less attention is paid to the scams and attacks aimed directly at consumers, but they merit equal attention. While we work to ensure internet technology is secure by design, there are simple steps consumers can take to be safer. It's great to see some of those steps becoming even more popular, even if slowly.

PHILIP REITINGER
President and CEO,
Global Cyber Alliance

Nearly half of consumers have faced cyberattacks or digital scams—threats disproportionately hurting Black and Hispanic Americans. We must improve cybersecurity skills, but our defense can't rest on consumers alone. Companies must ensure products are secure by design, and government must enact clear guardrails. Together, we can protect our nation's data, systems, and consumers.

MARTA TELLADO
President and CEO,
Consumer Reports

This year's report underscores the ongoing challenges in cybersecurity. As emerging technologies like AI reshape the digital landscape, it's crucial that we adapt our approach to consumer protection. We must foster a culture of cyber resilience that spans from individual awareness to collective action.

VIVIAN SCHILLER
Executive Director,
Aspen Digital

Thank You

AUTHORS

YAEL GRAUER
STACEY HIGGINBOTHAM
Consumer Reports

DESIGN

CHRIS GRIGGS
Consumer Reports

SURVEY RESEARCH

NOEMI ALTMAN
DEBRA KALENSKY
TESS M. YANISCH
Consumer Reports

EDITING

SCOTT MEDINTZ
Consumer Reports

COPYEDITING

NOREEN BROWNE
WENDY GREENFIELD
Consumer Reports

GUEST CONTRIBUTORS

JORIJ ABRAHAM
Managing Director,
Global Anti-Scam Alliance

NANETTE BARRAGÁN
Representative (California 44th District), Chair of the Congressional Hispanic Caucus

DAVID BRUMLEY
CEO of Mayhem Security and Professor at Carnegie Mellon University

J. MICHAEL DANIEL
President and CEO,
Cyber Threat Alliance

CHRIS GIBSON
CEO, Forum of Incident Response and Security Teams (FIRST)

STEVEN HORSFORD
Representative
(Nevada 4th District), Chair of the Congressional Black Caucus

BRET JORDAN
Vice Chair of the Board of Directors, OASIS

MICHAEL LASHLEE
Chief Security Officer,
Mastercard

CRAIG NEWMARK
Founder of craigslist, Philanthropist, and Lead of the #CyberCivilDefense initiative

PHILIP REITINGER
President and CEO,
Global Cyber Alliance

JESSICA ROSENWORCEL
Chairwoman, Federal Communications Commission

VIVIAN SCHILLER
Executive Director,
Aspen Digital

ANDREW SHIKIAR
Executive Director and CEO,
FIDO Alliance

MARTA TELLADO
President and CEO,
Consumer Reports

ALEX WEINERT
VP Director of Identity Security,
Microsoft

TARAH WHEELER
CEO, Red Queen Dynamics

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 empowers policymakers, civic organizations, companies, and the public to be responsible stewards of technology and media in the service of an informed, just, and equitable world. This program, part of the Aspen Institute, shines a light on urgent global issues across cybersecurity, the information ecosystem, emerging technology, the industry talent pipeline, tech and communications policy, and innovation. It then turns ideas to action and develops human solutions to these digital challenges.

Global Cyber Alliance is an international nonprofit focused on delivering a secure, trustworthy internet that enables social and economic progress for all. The Global Cyber Alliance builds communities to deploy tools, services, and programs that provide cybersecurity at global scale.

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