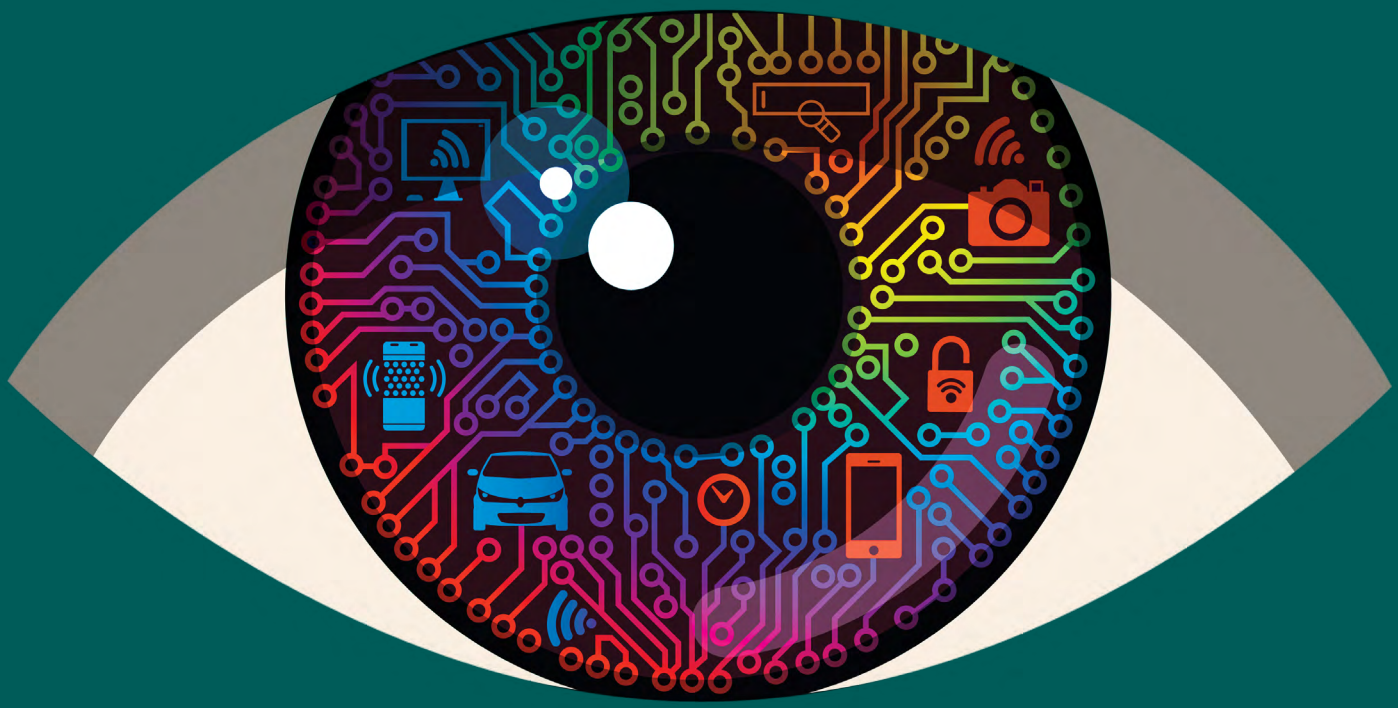
2022

CONSUMER CYBER READINESS REPORT



Consumer Reports

ASPEN DIGITAL
aspen institute

Intro

The Consumer Cyber Readiness Report reviews consumer attitudes towards digital privacy and security practices online. Together, Consumer Reports and Aspen Digital have reviewed findings across CR's recent nationally representative surveys and connected with thought leaders to understand the changes in consumer cybersecurity behaviors.

Though an understanding of consumer cybersecurity practices has increased over the years resulting in positive changes in behaviors, consumer attitudes towards adopting practices and tools to secure themselves online have moved at a slower pace. In an effort to secure networks, data, and devices, it is critical that consumers feel confidence in securing information online and within platforms to prevent harm in light of future threats.

It is also important to examine ways to empower consumers with changes in behavior online, while weighing the responsibilities of governments and industry to reduce systemic cybersecurity risks.

In addition to examining the survey findings, we have enlisted commentary from cybersecurity leaders to provide thoughts and reflections in regards to the various trends that have surfaced.

> *"Measuring consumer attitudes on cybersecurity is an important step to understanding how effective efforts across government, industry, and civil society have been in moving us all towards a more empowered and secure democratic society. It also informs where we should spend more time and resources to continue moving in the right direction.*

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

Key Findings

Among the security habits surveyed, consumer privacy and security practices have increased over the years as consumers have made changes to update and protect themselves and their personal information or data.

These increases vary depending on each practice. Since 2019, a large number of individuals have adapted the use of multi-factor authentication versus a stagnant change in individuals who use a password manager or virtual private network.

Security Habits Consumers say they Currently Do	2022	2019
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	88%	74%
Require a password, PIN, or other method, such as touch or face ID, to unlock your smartphone	85%	69%
Adjust your smartphone settings to only allow an app access to your location while you are using the app	81%	65%
Delete or choose to not install apps on your smartphone if you think they collect too much personal information or do not protect it adequately	80%	71%
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	78%	60%
Use multi-factor* authentication, a feature that requires a password plus another piece of information (such as a code sent in a text message) to log in to any of your online accounts	77%	50%
Block or routinely delete some or all cookies on your web browser	67%	63%
Adjust the privacy settings in your web browser	60%	Not Asked
Use "private" or "incognito" mode on your web browser when you want to keep your browsing or search history from being saved or seen by others	51%	47%
Use a password manager that automatically creates and stores a very strong password for each of your online accounts	39%	36%
Use a "virtual private network," or VPN, to ever access the internet on your devices, for instance your laptop, smartphone or tablet	35%	34%

June 2022 Consumer Reports nationally representative American Experiences Survey of 2,103 US adults.
June 2019 Consumer Reports nationally representative Privacy: Risk/Benefit Survey of 1,004 US adults.

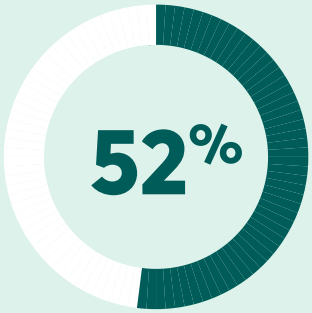
- Base: All respondents; excludes those who said "Not applicable" or "Don't know"
- The 2019 survey was conducted via phone mode only; 2022 was via web and phone.
* Multi-factor item was described in 2019 as "two-factor."
- Results between the two survey administrations may not be fully comparable due to these differences.

> *MFA is the single biggest step individuals can take to secure their devices and privacy, which is why the Administration made it a priority, including requiring it for the federal government as part of the President's Executive Order on Improving the Nation's Cybersecurity. I'm thrilled by this progress, and to know that more Americans are secure today than even a few years ago.*

ANNE NEUBERGER
Deputy National Security Advisor
for Cyber and Emerging Technology

Given the increase in security and privacy behaviors, consumers are more likely to adjust permission settings for their data across platforms and products. Many are confident that digital tools are not distributing their personal information without their consent. Though many consumers still express concerns over how their personal data is being stored online, over 50% of individuals have some trust in consensual data sharing practices of their most sensitive information.

Consumer Confidence That Personal Data, Such As Social Security Number, Health History And Financial Information, Is Private And Not Distributed Without Their Knowledge	**2022**
Very Confident	7%
Somewhat Confident	45%
Not Too Confident	34%
Not Confident At All	14%



At least somewhat confident personal data is private

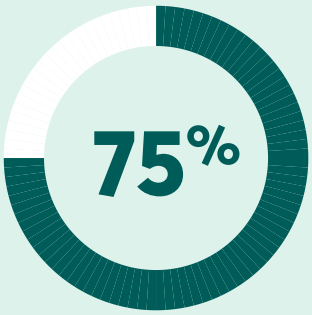
June 2022 Consumer Reports nationally representative American Experiences Survey of 2,103 US adults.

> *Cybersecurity and data protection has been one of my top priorities since becoming Deputy Secretary of the Treasury. Over the last year, we've undertaken a department-wide modernization effort to shore up our cyber defenses with tools like multi-factor authentication and encryption that will help keep our critical systems secure.*

WALLY ADEYEMO
Deputy Secretary,
US Department of the Treasury

With the growing knowledge of cybersecurity issues and their coverage in major news outlets, three out of four consumers say they are concerned with how companies collect and store data about them. This can be attributed to the increase in data breaches or presence of third-party trackers or emerging digital threats. Many consumers have concerns about how the companies collect or store their personal data, which suggests they believe it is vulnerable to attacks or may be sold for corporate profit.

Related To Online Activities, Consumer Concern About The Privacy Of Their Personal Data That Companies Collect And Store About Them	**2022**
Very Concerned	24%
Somewhat Concerned	51%
Not Too Concerned	20%
Not Concerned At All	3%
I Didn't Know They Collect Data About Me	2%



At least somewhat concerned about privacy of personal data collected online

June 2022 Consumer Reports nationally representative American Experiences Survey of 2,103 US adults.

> *This isn't a surprise. Surveys consistently demonstrate that people are concerned about their privacy in the face of both governments and corporations. The reason people don't often act on those concerns is that they feel powerless. There are often no easy ways people have to protect the privacy of their personal data, nor are there reasonable alternatives to the tech monopolies that make surveillance their business model.*

BRUCE SCHNEIER
Fellow and Lecturer,
Harvard Kennedy School

For consumers who expressed that they aren't too concerned, if at all, about the privacy and security of their personal data, the most commonly stated reasons why not are that it's just not something they worry about, they haven't experienced any issues, or don't have anything worth stealing. Some consumers also believe that their increase in cybersecurity behaviors would protect them if potential issues arise.

Reasons Consumers Are Not Concerned About The Privacy Of Their Personal Data Collected Online	**2022**
It's just not something I worry about	42%
I've never had any issues related to the security and privacy of my personal data	33%
I don't have anything worth stealing	30%
There's nothing I can do about it anyway	24%
I take all of the privacy precautions that I can so I believe my personal data is secure and private	18%
I take all of the privacy precautions that I can so I believe the security and privacy of my personal data is out of my hands	18%
Even if there is a breach in security and privacy of my personal data, it is fixable	16%
The benefit of my online activities is worth the risk of potential privacy-related issues	11%
Though my online data might be shared without my knowledge or consent, what I don't know can't hurt me	8%
Data breaches are rare	7%
Other	3%
Unsure	7%

June 2022 Consumer Reports nationally representative American Experiences Survey of 2,103 US adults.

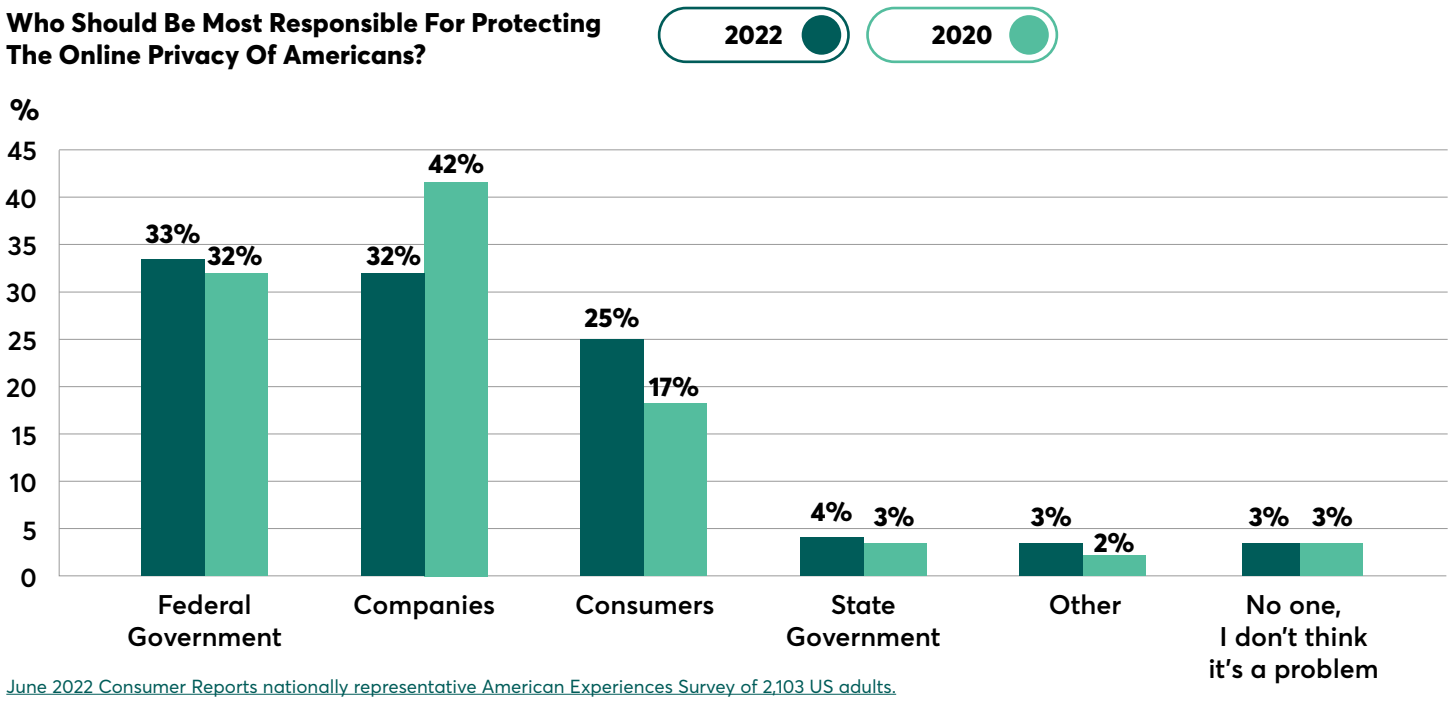
- Base: Respondents who are not too concerned or not concerned at all about the privacy of their personal data that companies collect about them online
- Respondents were able to select all that apply (Note: the two response options that start "I take all the privacy precautions that I can…" could not both be selected together).

> *Every individual is a potential target of cyber criminals and other malicious actors. As such, every individual should take action to protect their information and expect reasonable security measures to be available in the technologies they use every day. If your email service, bank, or other critical provider doesn't offer basic security measures like multi-factor authentication by default, consider choosing another company – it's your information that's at risk.*

ERIC GOLDSTEIN
Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency (CISA)

As consumers have increased their own accountability in staying safe online in recent years, 2022 data showed a decreased percentage of consumers who felt companies held primary responsibility to protect the privacy of consumers and an increase in consumers taking responsibility for their own online privacy. Now, equal parts place accountability on companies as they do on the federal government to protect consumers online. In the 2022 survey, individuals who selected 'other' commonly voiced accountability be shared equally across the stakeholders listed.

Who Should Be Most Responsible For Protecting The Online Privacy Of Americans?



June 2022 Consumer Reports nationally representative American Experiences Survey of 2,103 US adults.
February 2020 Consumer Reports nationally representative Privacy Front and Center Survey of 5,085 US adults.

> *All of us have a part to play in cybersecurity. The Biden-Harris Administration is working hard to expand cybersecurity awareness and education so that everyone has access to the tools and skills they need to safely thrive in the digital ecosystem. We still have a lot of work to do, but the progress is inspiring. We will continue the fight to ensure that our Nation does not fall victim to collective ambivalence in cyberspace.*

KEMBA WALDEN
Principal Deputy
National Cyber Director

> *These survey results are a promising sign that government and private sector collaboration to improve security and security awareness is having positive impact. In its long history of bringing people together to improve cybersecurity, NIST has seen that open and transparent collaboration is key to making a difference.*

LAURIE E. LOCASCIO
Under Secretary of Commerce
for Standards and Technology
and National Institute of Standards
and Technology (NIST) Director

Closing

Across the last 60 years, there have been monumental shifts in consumer behavior based on who bears the responsibility for risk and how much information consumers have as they make risk-based decisions. From seatbelts to nutrition labels, consumers have gained more information about products entering their lives and homes. For cybersecurity, all of these risks can be immediate and serious given the speed and convenience of the digital world.

With the constant evolution of the cybersecurity threat landscape, it is important to examine which risks are placed into the hands of consumers and what tools are at their disposal to combat rampant threats, ranging from malicious actors seeking financial gain through ransomware to nation states undermining key levers of societal function, all from the connected devices consumers use knowingly (or unknowingly) everyday.

> *Consumers are increasingly vulnerable to cyber threats, and current options to secure their data are often complicated. We must give people the cybersecurity tools to protect themselves and demand action and accountability from industry and government.*

MARTA TELLADO
President and CEO, Consumer Reports

> *With cybersecurity incidents on the rise, consumer awareness of online threats become more critical. In this interconnected world, governments, industry, and civil society must work together to drive safer cybersecurity.*

VIVIAN SCHILLER
Executive Director, Aspen Digital

Thank You

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 policy-makers, 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 Aspen Institute program 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.

AUTHORS

AMIRA DHALLA
Consumer Reports

KATIE BROOKS
Aspen Digital

DESIGN

CHRIS GRIGGS
Consumer Reports

SURVEY RESEARCH

DEBRA KALENSKY
JANE MANWEILER
KRISTEN PURCELL
TESS YANISCH
Consumer Reports

GUEST CONTRIBUTORS

WALLY ADEYEMO
Deputy Secretary,
US Department of the Treasury

ERIC GOLDSTEIN
Executive Assistant Director for Cybersecurity, Cybersecurity and Infrastructure Security Agency (CISA)

JEFF GREENE
Senior Director, Cybersecurity Programs, Aspen Digital

LAURIE E. LOCASCIO
Under Secretary of Commerce for Standards and Technology and National Institute of Standards and Technology (NIST) Director

ANNE NEUBERGER
Deputy National Security Advisor for Cyber and Emerging Technology

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

VIVIAN SCHILLER
Executive Director of Aspen Digital

BRUCE SCHNEIER
Fellow and Lecturer, Harvard Kennedy School

MARTA TELLADO
President and CEO of Consumer Reports

KEMBA WALDEN
Principal Deputy National Cyber Director

Visit securityplanner.org to find information on staying safer online