

CHUBB®


Chubb Personal Risk Services

# Fifth Annual Study on Personal Cyber Risk

2022







## Fifth annual study on personal cyber risk: progress, yes, but more to do.

It's been four years since Chubb released its first cyber report examining consumer perceptions of cyber risks. To date, our annual survey has found a common theme: while people care a great deal about their privacy and cyber threats, too many aren't doing enough to protect their personal information. The findings of our 2022 survey, however, offer new evidence of progress: more people than ever before are taking concrete steps to protect their personal data and information.

For example, in 2022, more than half of Americans and Canadians (51%) reported using multi-factor authentication to log into their online accounts, which is twice the level found in our survey a year earlier. Three out of four respondents report updating the password for their primary bank or financial account in the last 12 months. Nearly as many (70%) have voluntarily updated a password for a digital account without being required to by the provider.

This is progress, and it's encouraging. But poor cyber-security practices are still far too common. To cite one survey nugget: half of consumers in the U.S. and Canada are continuing to use the name of their pet, or a similarly identifiable name or date, for their new password. Remarkably, the wealthiest people – those who are most vulnerable to a cyber-crime that involves money – are continuing to use such identifiable terms or dates as passwords.

Looking across all 2022 survey data, one compelling narrative emerges: awareness of cyber threats is high and growing. Consumers admit to annoyance and frustration in taking actions to protect themselves online. But, finally, the gap between awareness and action that we've observed for years has started to narrow.

The question is why. Could it be heightened awareness of cyber risks that came with the pandemic? The rise of high-profile ransomware attacks? Growing comfort with the actions more businesses are requiring, such as multi-factor authentication? Increased public attention on the threat of a large-scale, catastrophic attack against infrastructure? The proliferation of internet-connected devices?

Each of these factors likely played a role. The job of this study is to raise awareness for these risks, understand how consumers perceive them, and, we hope, drive greater adoption of the actions and behaviors that can help people keep themselves, and their families, more secure.

Chubb commissioned Dynata, a leading global provider of consumer and professional data, to conduct this public opinion poll. The survey was fielded between August 29-September 19, 2022. The results are based on 1,605 completed surveys of consumers in the U.S. and Canada. The margin of error is +/- 2%. For more information on methodology, see page 19.

## Executive summary

### ■ Concern about cyber breaches is high – and growing.

More than nine out of 10 consumers (92%) are concerned about a cyber breach exposing their personal information or identity. That's up from 80% in 2019. The intensity of concern is also higher. In 2022, 56% of respondents said they were "very concerned," versus 39% in 2019.

### ■ Consumers are worried about breaches of data on their devices, on the internet and from the companies they do business with.

A significant majority (81%) are concerned that the proliferation of internet-connected devices is a threat to their privacy. Nearly one in three are very concerned about this risk. Less than half of consumers are confident their personal data is secure on the internet. Only 18% strongly believe this.

### ■ People are worried about catastrophic cyber-attacks.

People are concerned about the threat of large-scale cyber-attacks that could cause widespread damage and chaos. Nearly nine in 10 (87%) are concerned that there will be a significant cyber-attack on the power grid in the U.S. Large majorities are worried about the threat of a cyber-attack waged by a hostile foreign country (85%) and cyber-attacks on a nuclear power plant, chemical factory or water supply (84%).

### ■ Consumers are getting better about protecting themselves from cyber risks - but more can be done.

Our survey found that Americans are increasingly taking proactive steps to protect themselves online. For example,

in 2022, more than half of respondents (51%) reported using multi-factor authentication to log into their online accounts, which is twice the level found in our survey last year. Adoption of password protection apps is growing too, with 35% using them this year, versus 19% a year ago. However, while adoption of these good cyber habits is growing, most people are still not taking these actions.

### ■ People are pretty sure their devices are eavesdropping on them.

Nearly four out of five respondents (79%) believe their virtual assistants and streaming devices can listen to their conversations. Another 11% aren't sure. In addition, two out of three (67%) believe they have received an advertisement based on a conversation they've had that was captured by a virtual assistant or streaming device. Wealthy and affluent Americans and Canadians are most likely to believe this.

### ■ The wealthy are most likely to be the target of a cyber-attack involving money.

In the last year, nearly 30% of high-net worth Americans and Canadians reported falling victim to a cyber-attack that involved their money. That's twice the average for all income groups and seven times the frequency cited by middle-class respondents. Compared to other income groups, wealthy respondents are twice as likely to have had their personal information breached in the last 12 months, and four times more likely than those in the middle class.

### ■ The most feared breach: loss of financial information.

More than half (53%) said the breach of their financial information was the most concerning type of cyber breach. In all, 78% of respondents named this among their top three concerns. The loss of personal information to a breach ranked second.

### ■ Americans understand that not all cyber risks are equal.

90% of respondents believe the app from their primary bank is secure. That's much higher than for personal finance (68%) or peer-to-peer payment apps (70%). Less than half of consumers are confident in the security of other apps, such as social media (48%), fitness (48%), and online dating (40%).

### ■ Personal cyber insurance is becoming more common.

About two in five (39%) currently have a personal cyber insurance policy. Wealthy consumers are much more likely to have this coverage. But an equal share of people are unfamiliar with personal cyber insurance, including 19% who are not at all familiar with the protections that personal cyber coverage offers individuals and families.

### ■ People with personal cyber insurance may have *too much* peace of mind.

Personal cyber policyholders are less likely to take precautions to protect themselves compared to those without a policy, such as conducting business while using a wi-fi hot spot, posting personal information on social media or regularly clearing their browser history.



## Executive summary

### Focus on Passwords

#### ■ Consumers like multi-factor authentication.

Nearly 80% say they prefer to use multi-factor authentication when logging into their digital accounts.

#### ■ People have trouble keeping track of their passwords and are annoyed when they have to change them.

Three in five (61%) report having trouble keeping track of their passwords. A similar share (63%) gets annoyed when they are forced to update their passwords.

#### ■ The good news:

Despite the annoyance factor, people are changing their passwords in high numbers. Three out of four respondents report updating the password for their primary bank or financial account in the last 12 months. Nearly as many – 70% – have voluntarily updated a password for a digital account without being required to by the provider.

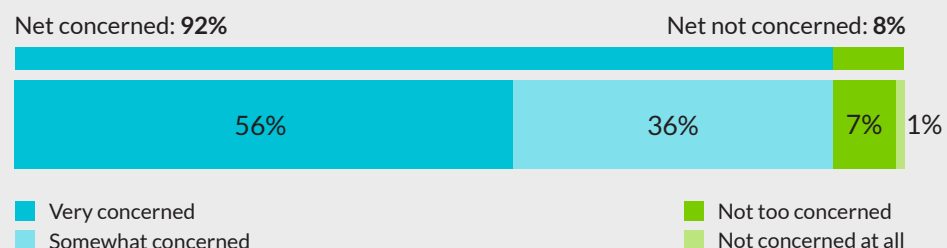
#### ■ The bad news:

People may be changing their passwords, but half are still including the name of their pet or other identifiable name or date in the new password. Nearly 85% of high-net worth Americans and Canadians use such identifiable terms of dates in their passwords – more than three times the rate of middle-class respondents (27%). Across the generations, Millennials are most likely to have a password that consist of a family or pet name, important date, etc. (69%). Baby Boomers are the least likely (23%).

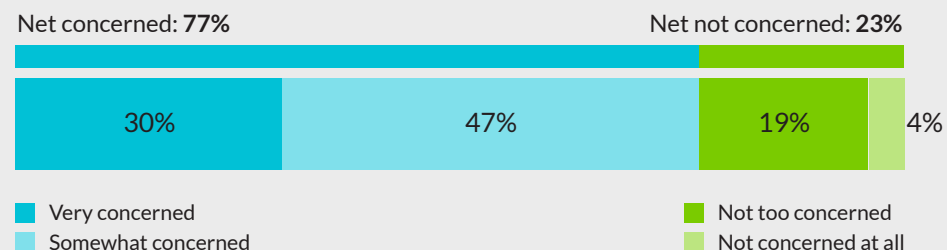
## Concern about cyber breaches is high – and growing.

- More than nine out of 10 consumers (92%) are concerned about a cyber breach exposing their personal information or identity. That's up from 80% in 2019.
- The intensity of concern is also higher. In 2022, 56% of respondents said they were “very concerned,” versus 39% in 2019. In 2022, two out of three Millennials say they are “very concerned” – the highest level among the generations. That compares to 50% of Gen Z and 45% of Baby Boomer respondents.
- More than three out of four consumers (77%) are concerned that businesses they interact with do not protect or adequately store their digital data. About one in three are very concerned.

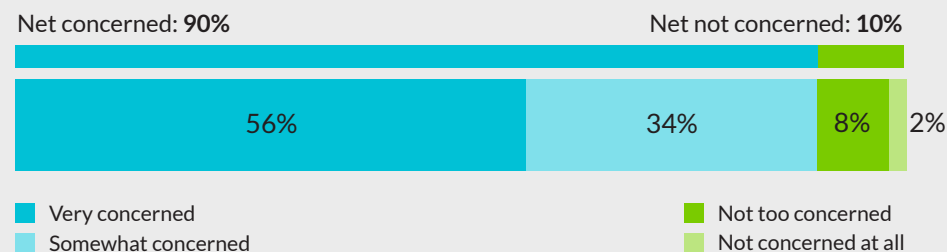
### ► How concerned are you about a cyber breach exposing your personal information or identity?



### ► I am concerned that many businesses I interact with do not protect or adequately store my personal electronic data

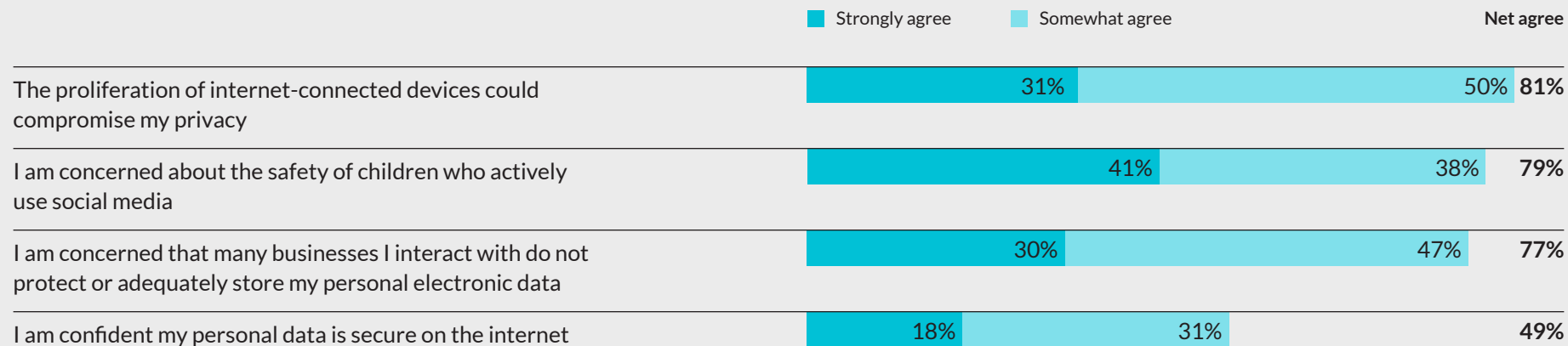


### ► Personal privacy is important to me



Concern about cyber security is broad:  
Consumers are worried about breaches of data on their devices, on the internet and from the companies they do business with.

- A significant majority of respondents (81%) is concerned that the proliferation of internet-connected devices is a threat to their privacy. Nearly one in three are very concerned about this risk.
- Less than half of consumers are confident their personal data is secure on the internet. Only 18% strongly believe this.
- More than three in four are concerned that the companies they do business with are not adequately protecting their personal data.



## People are worried about large-scale, catastrophic cyber-attacks.

- People are overwhelmingly concerned about a cyber breach that affects them individually. They are also concerned about the threat of large-scale cyber-attacks that could cause widespread damage and chaos.
- 87% are concerned that there will be a significant cyber attack on the power grid in the U.S.
- 85% recognize the threat of a cyber-attack waged against the U.S. by a hostile foreign country.
- Nearly as many (84%) are worried about cyber-attacks on a nuclear power plant, chemical factory, the water supply and other significant infrastructure.
- More than three in four (77%) fear a cyber-attack could affect the community where they live.
- Nearly four out of five respondents (78%) are concerned that their local government or school could suffer a cyberattack.

► How concerned are you with each of the following?	Very concerned	Somewhat concerned	Not too concerned	Not at all concerned
A significant cyber-attack on the power grid in the U.S.	46%	41%	11%	2%
A significant cyber-attack on infrastructure, such as a nuclear power plant, chemical plant or the water supply, that causes major damage	46%	38%	13%	3%
A cyber-attack in the U.S. launched by a hostile foreign power	44%	41%	11%	4%
A large-scale cyber-attack on my community	37%	40%	20%	3%
A cyber-attack on my local government or school	34%	44%	19%	3%

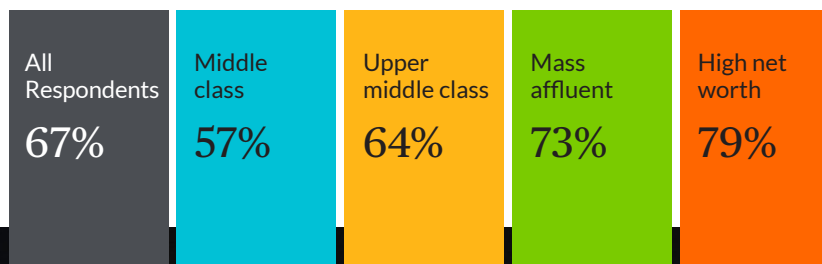
## People are getting better about protecting themselves from cyber risks.

- Our survey found that Americans and Canadians are increasingly taking proactive steps to protect themselves online. While adoption of these good cyber habits is growing, however, most people are still not taking these actions.
- In 2022, more than half of respondents (51%) reported using multi-factor authentication to log into their online accounts, which is twice the level found in our survey last year.
- About half (48%) of respondents cleared their browser history in the past 12 months. That compares to just 28% in 2021.
- Usage of cybersecurity software has increased – 38% in 2022 versus 25% last year.
- Adoption of password protection apps is growing too, with 35% using them this year, versus 19% a year ago.

▶ Which of the following actions have you taken in the last 12 months?	2022	2021
Used multi-factor authentication to log into my digital accounts	51%	28%
Cleared my browser history	48%	28%
Used cybersecurity software, such as malware protection	38%	25%
Used a password protection app (e.g. Google Password Manager, iCloud Keychain, etc.)	35%	19%
Used a pop-up blocker	39%	25%



Listening in: people believe their devices are eavesdropping on them.



I've received a digital ad based on a conversation.

**79%** Nearly four out of five respondents believe their virtual assistants and streaming devices can listen to their conversations. Another 11% aren't sure. Only 12% say that isn't happening.

**67%** Two out of three people believe they have received an advertisement based on a conversation they've had that was captured by a virtual assistant or streaming device. Wealthy and affluent Americans are most likely to believe this.

## Taking a page from Willie Sutton: Wealthy people are most likely to be the target of a cyber-attack involving money.

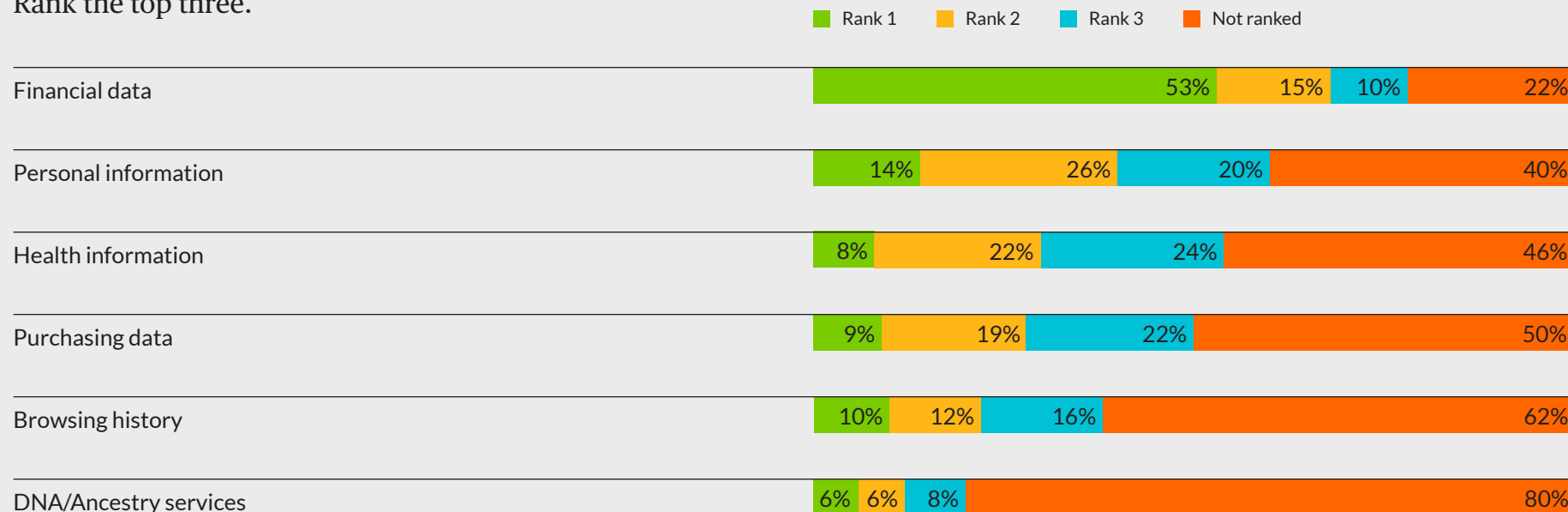
- When asked why he robbed banks, Willie Sutton famously said, “Because that’s where the money is.” Today’s cyber criminals appear to be taking Sutton’s lead: wealthy people are the most likely income group to be the victim of a cyber-attack that involves money.
- In the last year, nearly 30% of high-net worth Americans and Canadians reported falling victim to a cyber-attack that involved their money. That’s twice the average for all income groups and seven times the frequency cited by middle-class respondents.
- Compared to other income groups, wealthy respondents are twice as likely to have had their personal information breached in the last 12 month, and four times more likely than those in the middle class.
- Mass affluent and high-net worth consumers were about twice as likely as members of the middle class to have fraudulent charges made on their credit card.

► In the past 12 months, which of the following has occurred to you or a member of your household?	All respondents	High net worth	Mass affluent	Upper middle class	Middle class
Fraudulent charges were made on credit card	25%	35%	33%	23%	16%
Victim of a cyber-attack that involved the breach of personal information	18%	35%	24%	14%	8%
Contacted by a credit card company about a suspicious transaction	31%	34%	39%	29%	24%
Victim of a cyber-attack that involved money	13%	28%	21%	8%	4%

## Ranking risk: The top concern among consumers is a breach of their financial information.

- The survey asked respondents to rank the type of cyber breaches they are most worried about. Not surprisingly, financial data was ranked first by far. More than half (53%) said the breach of their financial information was the most concerning type of breach. In all, 78% of respondents named this among their top three concerns.
- The loss of personal information to a breach ranked second. Some 60% ranked the loss of personal information as one of their top three concerns. Fourteen percent ranked it first.
- Perhaps surprisingly, only about half of consumers (54%) considered the breach of their health information to be among their top three concerns.
- Exactly 20% of consumers ranked the breach of their DNA as a top three concern.

### ► Which of the following types of breaches of personal data or information most concern you? Rank the top three.





## Password hygiene: Does it pass muster?

- To gauge the current state of password hygiene, we surveyed respondents on several different behaviors. The results suggest an interesting dynamic: many people have trouble keeping track of their passwords (61%) and are annoyed when they are forced to update them (63%). At the same time, however, big majorities are willingly engaging in proactive practices that can help them protect their data.
- Three out of four consumers report updating the password for their primary bank or financial account in the last 12 months.
- Nearly as many – 70% – have voluntarily updated a password for a digital account without being required to by the provider.
- Perhaps surprisingly, nearly 80% of respondents say they prefer to use multi-factor authentication when logging into my digital accounts.
- Only 13% admit to sharing a password with others.

### ► Which of the following have you done in the last 12 months?

Voluntarily updated a password for a digital account without being required to by the provider	70%
Updated the password for your primary bank or financial account	75%
Shared a password with others	13%
Used the same password for multiple accounts	35%

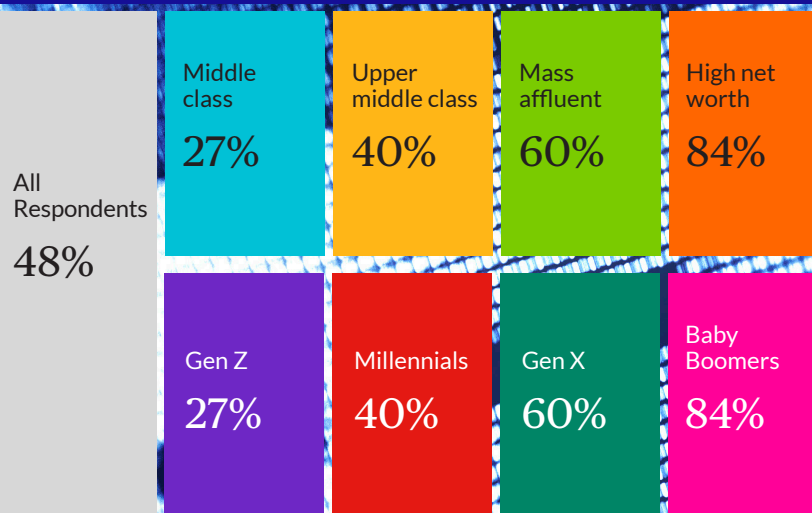
### ► Please indicate the extent to which you agree or disagree with the following statements

	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
I have trouble keeping track of my passwords	27%	34%	20%	17%
I get annoyed when I am forced to update my password on a digital account	23%	40%	20%	15%
I prefer to use multi-factor authentication when logging into my digital accounts	39%	40%	15%	4%

## Password pet names

- Cyber security 101 advises consumers not to use potentially identifiable words or dates in a password. Our survey data shows progress over last year. But it's still common – especially among the wealthy.
- A large majority of high-net worth Americans and Canadians (84%) use such identifiable terms of dates in their passwords – more than three times the rate of middle class respondents (27%).
- Across the generations, Millennials are most likely to have a password that consists of a family or pet name, important date, etc. (69%). Baby Boomers are the least likely (23%).
- Here's the good news: on average 48% have these less-than-optimal passwords. That's down from 57% last year.

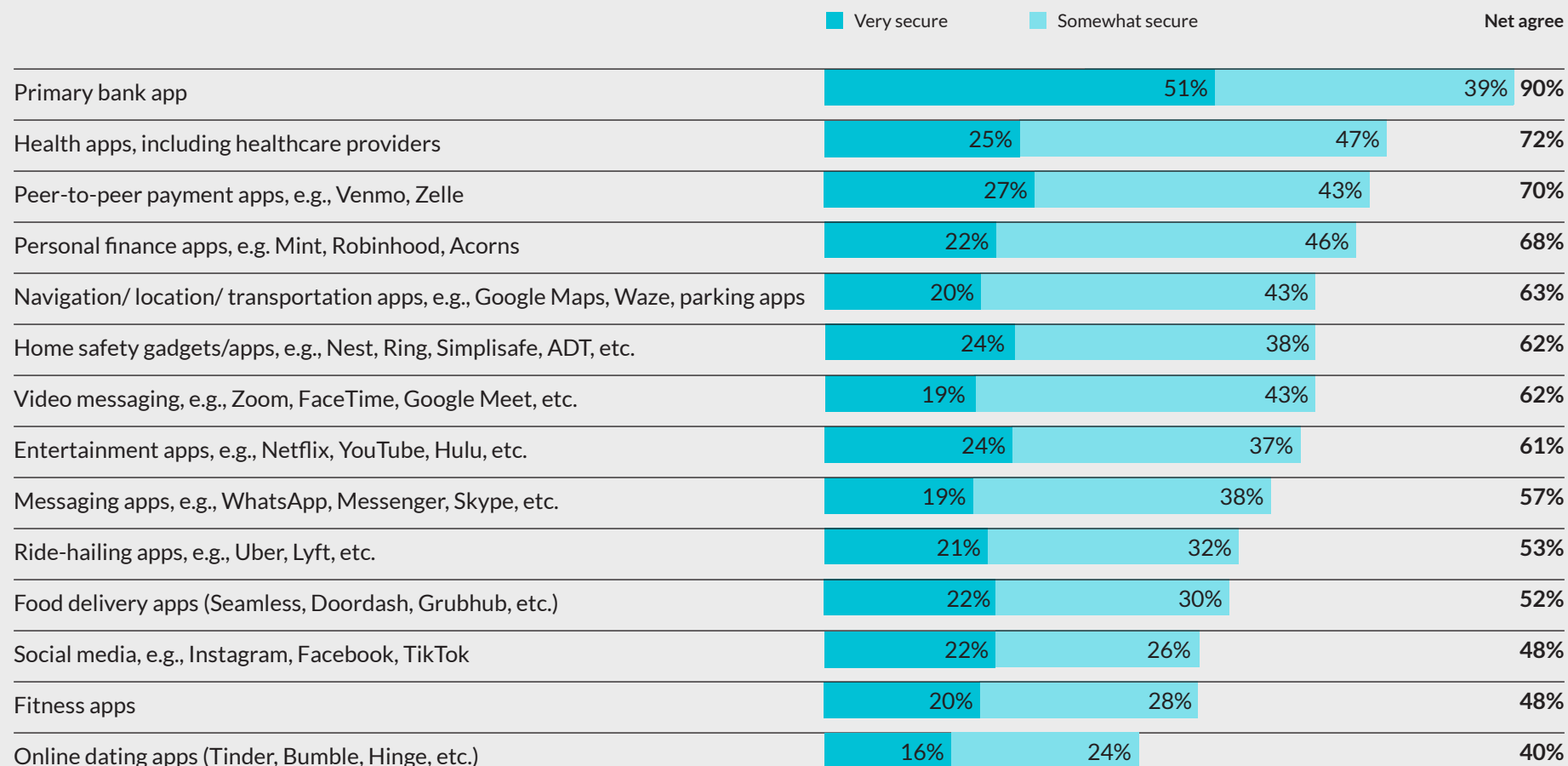
Think back to the last time you created or updated a username or password for an online/internet-based account. Did the new username or password consist of any of the following: family or pet name, birthday/important date, previous credentials, or current/previous address?



## People understand that not all cyber risks are equal: Part one

- 90% of respondents believe the app from their primary bank is secure. That's much higher than for personal finance (68%) or peer-to-peer payment apps (70%).
- 72% of consumers believe health apps are secure.
- Less than half of consumers are confident in the security of other apps, such as social media (48%), fitness (48%), and online dating (40%).

### ► Consumer's level of confidence in the security of apps





## People understand that not all cyber risks are equal: Part two

- Our survey finds that consumers are mindful that the level of cyber risk can vary by digital channel or the type of business they are interacting with.
- Consumers say that the security of their personal data is at greater risk if their cell phone is connected to a rental car rather than their own vehicle.
- Respondents believe that large companies are better equipped to protect their personal information than small businesses.

► Please indicate the extent to which you agree or disagree with the following statements

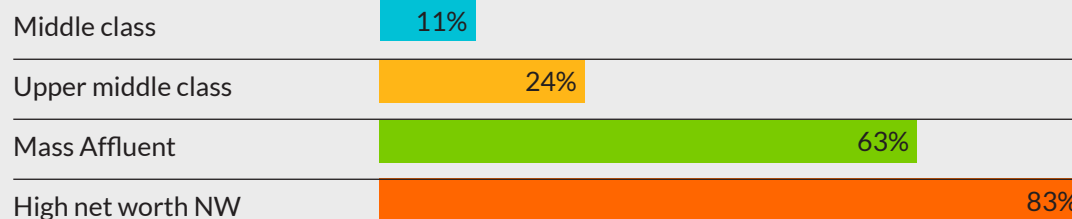
	Strongly/ somewhat agree	Strongly/ somewhat disagree	NA
My personal data is at risk when my cell phone is connected to my car	58%	32%	10%
My personal data is at risk when my cell phone is connected to a rental car	67%	21%	12%
Small businesses are well prepared to protect my personal information	60%	40%	—
Large companies are well prepared to protect my personal information	74%	26%	—

## Spotlight on personal cyber insurance

Personal cyber insurance is becoming more common, but many consumers are still unfamiliar with this sort of coverage.

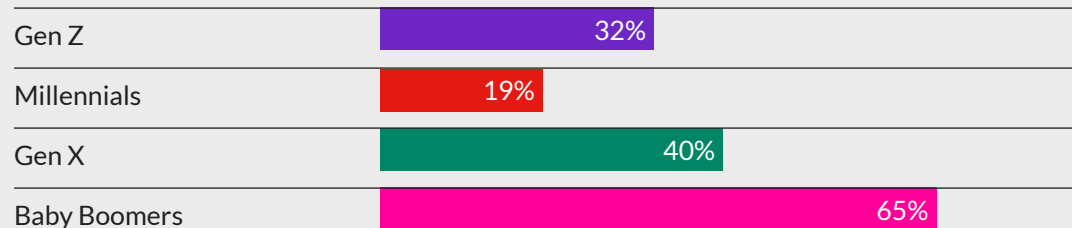
**39%** Currently have a personal cyber insurance policy. Wealthy consumers are much more likely to have this coverage.

By income:



**39%** Are unfamiliar with personal cyber insurance, including 19% who are not at all familiar with the protections that personal cyber coverage offers individuals and families. Awareness is higher among younger respondents.

Share of each generation that is not familiar with cyber insurance:



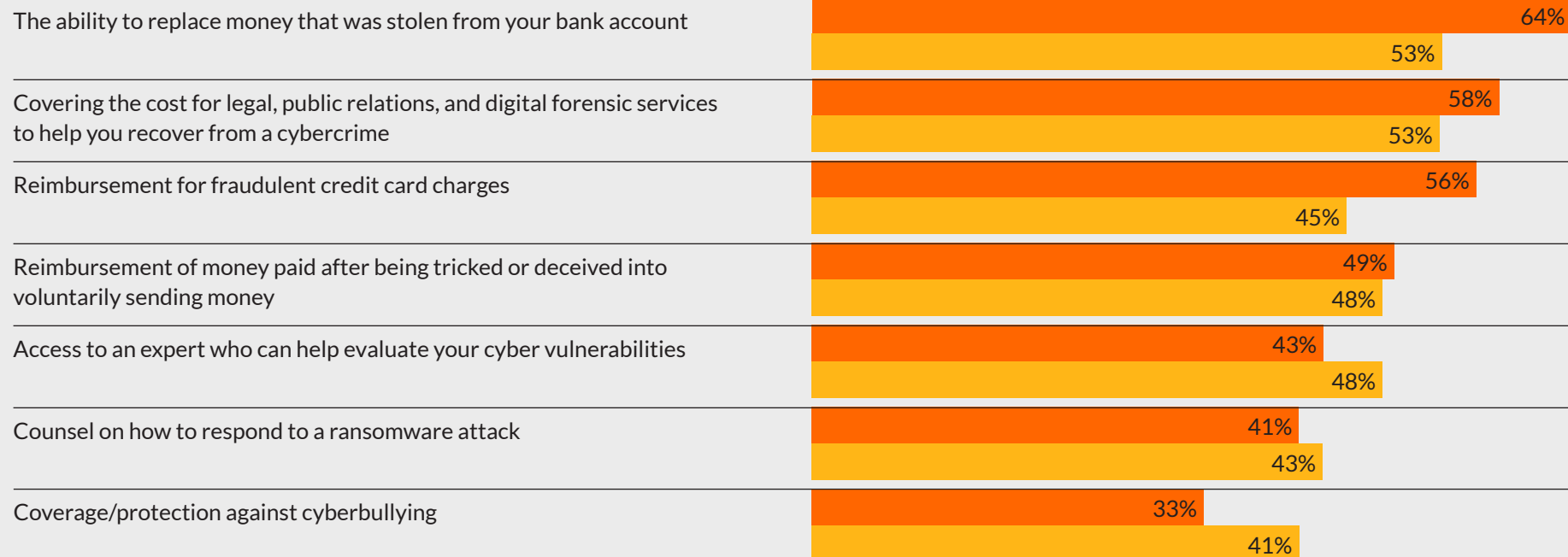
## What coverage do consumers value when they suffer a breach?

- Personal cyber insurance offers a range of coverages for individuals and families. Our survey gauged which protections consumers believe have the most value in the event of a cyber-attack or breach.
- Consumers want to feel comfortable knowing stolen funds would be replaced, legal costs would be covered, and fraudulent credit cards would be reimbursed.
- While only one third of all survey respondents say they would value coverage/protection against cyberbullying, this number jumps to 41% among those who currently have a policy, and 42% among those with young children at home.

### ► Which cyber insurance coverage do you see value in having?

■ All respondents

■ Currently have policy





## Do personal cyber policyholders have *too much* peace of mind?

- Nearly three quarters (72%) of respondents who currently have a personal cyber insurance policy feel their personal data is secure on the internet, more than twice that of those without a policy (34%). Policyholders are also more likely to use a password protection app (41% versus 31%) and subscribe to a cyber monitoring service (38% vs 10%) than those without a policy.
- Current personal cyber policyholders are also less likely to take precautions to protect themselves compared to those without a policy, such as conducting business while using a wi-fi hot spot, posting personal information on social media or regularly clearing their browser history.

▶ Which of the following have you done in the last 12 months?	Have a cyber policy	Do not have a cyber policy
Conducted business online while using a public wi-fi hotspot	79%	35%
Accepted a friend request on social media from someone you didn't recognize	30%	10%
Posted potentially sensitive personal information, such as your location or personally identifiable photos, etc., on social media	32%	15%
Avoided opening an attachment or link because the sender was unknown or suspicious	40%	66%
Used multi-factor authentication to log into my accounts (when applicable)	40%	59%
Periodically cleared my browser history and tracking cookies	34%	57%
Password contained family or pet name, birthday/important date, previous credentials, address	84%	57%

## Methodology

This is the fifth survey by Chubb measuring consumer approaches and behaviors toward cyber risk. Conducted by Dynata, a leading global provider of first-party consumer and professional data, the online survey was fielded in the U.S. and Canada from August 29-September 19, 2022. To qualify for the study, respondents were screened to be 18 years of age or older, have a minimum household income of \$50,000, and use at least one internet connected device.

The results are based on 1,605 completed interviews. A full demographic breakdown is at right.

Gender	Age	Socioeconomic Status	Region
Male: 50% Female 50%	18-24 (6%) 25-34 (25%) 35-44 (23%) 45-54 (16%) 55-64 (13%) 65 or older (17%)	<b>Middle Class:</b> \$50,000 - <\$100,000 (24%) <b>Upper Middle Class:</b> \$100,000 - <\$500,000 (40%) <b>Mass Affluent:</b> \$500,000 - <\$1M (18%) HNW: \$1M+ (18%)	Northeast (20%) South (22%) Midwest (16%) West (20%) Canada (22%)

## Cyber best practices cheat sheet

Taking the right steps to protect your personal data doesn't have to be a hard or daunting task. By following the below guide, we can all get most of the way to being cyber secure:



### 1 Keep your software up-to-date

- Use anti-virus protection and cyber security software
- Install software and app updates ("patches") as soon as possible, or turn on automatic updates



### 2 Change your passwords regularly and always use strong passwords

- Do not share your passwords with others
- Do not use the same password for multiple accounts
- Use a password manager app



### 3 Manage your credit profile

- Review your credit report periodically
- Sign-up for credit monitoring service
- Freeze your credit with all 3 bureaus



### 4 Manage your data

- Don't store compromising electronic data about yourself that someone could use against you
- Back-up data you can't afford to lose both in the cloud and on an offline storage device (like an external hard drive)



### 6 Use a personal VPN, even on a private network



### 5 Use multi-factor authentication to log into accounts



### 7 Be wary of social media

- Don't accept social media "friend" requests from strangers
- Don't share sensitive or personal information on social media



### 8 Watch what you click

- Don't click links from unknown or suspicious senders
- Don't click sale or digital coupon links in emails



### 9 Purchase a Chubb cyber insurance policy



CHUBB®

Chubb is the marketing name used to refer to subsidiaries of Chubb Limited providing insurance and related services. For a list of these subsidiaries, please visit our website at [www.chubb.com](http://www.chubb.com). Insurance provided by ACE American Insurance Company and its U.S. based Chubb underwriting company affiliates. This document is advisory in nature and is offered for informational purposes only as a resource to be used together with your professional insurance advisors in maintaining a loss prevention program. The information contained in this document is not intended as a substitute for legal, technical, or other professional advice. This presentation is solely for informational purposes. No liabilities or warranties are assumed or provided by the information contained in this document. Chubb, 202 Hall's Mill Road, Whitehouse Station, NJ 08889-1600.

Chubb. Insured.<sup>SM</sup>