

# ASSESSING “CYBER HYGIENE” IN THE U.S.

QUANTITATIVE RESEARCH ON AMERICANS’ CYBERSECURITY PRACTICES AND  
CREATION OF A RISK INDEX

FEBRUARY 2020



# TABLE OF CONTENTS

## SECTION

## SLIDE

PURPOSE OF RESEARCH

3

RESEARCH METHODOLOGY

4

KEY FINDINGS

5

BASELINE UNDERSTANDING OF RISK

11

CYBER HYGIENE RISK INDEX

14

RISK INDEX METRICS

20

DEMOGRAPHICS DRIVING THE RISK INDEX

32

HOME-BASED VERY SMALL BUSINESSES

40

USE AND SECURITY OF WORK DEVICES

44

APPENDIX

51

APPENDIX A: CYBER HYGIENE RISK INDEX – BREAKOUTS

52

APPENDIX B: CURRENT STATE OF CYBER HYGIENE

58

APPENDIX C: CYBER HYGIENE BEHAVIORS

61

APPENDIX D: ADDITIONAL CLASSIFICATION BREAKOUTS

69

# PURPOSE OF RESEARCH

---

Wakefield Research partnered with Webroot to conduct an online quantitative research study among U.S. consumers to:

- Better understand attitudes, perspectives, and behaviors related to cyber hygiene
- Based on this data, create a risk index (“Cyber Hygiene Risk Index”) to assess the risks associated with susceptibility to cybercrime in each state, ranking the states to determine the riskiest and least risky states in the U.S.
- Further analyze respondents’ susceptibility to risk by using a series of custom demographic and psychographic metrics to get a more nuanced understanding of what is behind cyber-hygiene levels

# RESEARCH METHODOLOGY

Wakefield Research fielded an online survey to 10,000 U.S. consumers, ages 18+, with 200 interviews in each of the 50 U.S. states. This survey was conducted between January 28<sup>th</sup> and February 10<sup>th</sup>, 2020, using an email invitation and an online survey instrument.



## Sub-audience analysis across the following demographics:


- Age/Generation (Gen Z, Millennial, Gen X, Boomer)
- Region (Rural, Suburban, Urban)
- Education, Income, Home Ownership, Investments
- Employment, Work Industry, Size of Company, Self-Employment
- Relationship and Parent Status

## As well as behavioral/psychographics:

- Electronic Device Ownership
- News Consumption and Hobbies / Interests
- Use of Mobile Banking and Auto Bill Pay
- Social Media Usage
- Online Password Management

The margin of error is +/- 0.98 percentage points for the total audience of this study and +/- 6.9 percentage points for each state at the 95% confidence level.

# KEY FINDINGS

**CARBONITE**  **+** **WEBROOT**  
an openstack company an openstack company

## KEY FINDINGS

**Almost all Americans say they are taking steps to protect themselves and their data online. However, while most are familiar with common cyber attacks like malware and phishing, few admit they could explain what those actually are. This lack of understanding and a closer review of online behaviors suggests Americans may be more confident than warranted in their approach to cybersecurity.**

Almost all (89%) Americans say they're taking appropriate steps to protect themselves online, and the majority are familiar with malware (78%) and phishing scams (68%). However, only 35% feel confident they can explain what phishing is and only 32% feel confident they can explain what malware is to someone else. This gap raises questions of Americans' readiness against cybersecurity threats.

A large majority of Americans use anti-virus software (83%) and regularly backup their data (80%), however a deeper look at practices reveals opportunities for security breaches. For example, only half know if their backup is in an encrypted format, and only 18% backup their data online and offline. A review of online activity reveals almost half (49%) of Americans use the same password across multiple accounts and only 37% keep social media accounts private. Americans should be taking greater precautions for threat protections for their electronic devices, their data, and their identity.

# KEY FINDINGS

The reality of Americans not being secure in their online behavior comes into greater focus with our 2020 Cyber Hygiene Risk Index. Most Americans receive a failing grade of “F” and only a quarter achieve an “A” or a “B” grade.

The Cyber Hygiene Risk Index quantifies the extent to which Americans take preventable risks with their online data and identify. The average American scored an “F” rating, or 58%. A small minority – only 11% of the total population, scored an “A” (90% or higher).

The state-by-state risk index scores have a wide spread of 15 points between the riskiest state (New York, 52%) and least risky state (Nebraska, 67%), though even with that spread all states score either a “D” or an “F”.

CYBER HYGIENE GRADE	% OF AMERICANS OVERALL <i>N=10,000</i>
A	11%
B	13%
C	16%
D	15%
F	45%

<u>RISKIEST STATES</u>	<u>LEAST RISKY STATES</u>
1. New York	50. Nebraska
2. California	49. New Hampshire
3. Texas	48. Wyoming
4. Alabama	47. Oregon
5. Arkansas	46. New Jersey

## KEY FINDINGS

---

A deeper review of the data reveals there is a direct relationship between a better risk index score and progressing through life markers such as increased education, daily news consumption, and home ownership. Somewhat surprisingly, there is also an inverse relationship between “tech-savviness” and risk index scores, meaning the more tech-savvy Americans are, the riskier their online behavior.

The least risky Americans are those who have progressed through certain life markers, such as having a college degree, owning a home, and engaging with the world by reading or watching the news everyday. This “Mile Marker” sub-audience tends to be, but are not necessarily, older in age, parents, and high-income earners. As Americans take on more responsibilities in life, they become more responsible online as well.

The most risky Americans exhibit greater tech-savviness and either work in IT or take a personal interest in IT through coding or web design. These Americans frequently (but not always) demonstrate their “tech savviness” by owning a smart device, using mobile banking, and their work and personal activities in technology. This “Tech Expert” sub-audience has a worse risk index score. Compared to Americans overall, Tech Experts’ tech savviness, greater awareness and knowledge of specific cyber attacks, and greater investments in identity protection services may make them more confident in taking riskier behavior.

## KEY FINDINGS

---

**Home-based Very Small Businesses (VSBs) are more likely to go their own way on technology issues rather than work with a dedicated IT consultant or team. As a result, they are more likely to use their personal devices for work and share passwords for their business and personal accounts.**

While many Americans are self-employed (including working as independent contractors), 5% are small business owners of a home-based business, classified as a “Very Small Business” (VSB). VSB owners regularly blur the lines between personal and work devices, and are more likely than most Americans to be the sole decision-maker over IT issues in their home and business.

While they exhibit a level of tech-savviness, they also have greater exposure and vulnerability. Around 80% of VSB owners use the same device for both work and personal use. In addition, 71% use the same password for their personal and business accounts, putting both their personal life and company at risk.

## KEY FINDINGS


---

In addition to devices Americans own for personal use, there is a hidden vulnerability in their work devices. Among those who are not self-employed and receive a work device from their employer, a slight majority (55%) also use their work device for personal use. Almost half (48%) have never looked into the security of their work devices, and only a third have taken any steps to improve its security.

It is common for the majority (55%) of Americans to use their employer-provided work device for personal use and over one-third (38%) consider an employer-provided work device to be their “primary” device for use at home. Even with using these devices for work and occasionally for personal use, almost half this group (48%) has never looked into the security of their work devices.

Despite this, only around a quarter (26%) believe their personal devices are more secure than their work devices. This suggests that non self-employed Americans, and in particular those who work at larger firms (over 1,000) simply assume their work devices are secure, or at least that they cannot or don’t know how to improve its security. This represents another vulnerability facing Americans that they may not have considered when assessing their cybersecurity habits.

# BASELINE UNDERSTANDING OF RISK

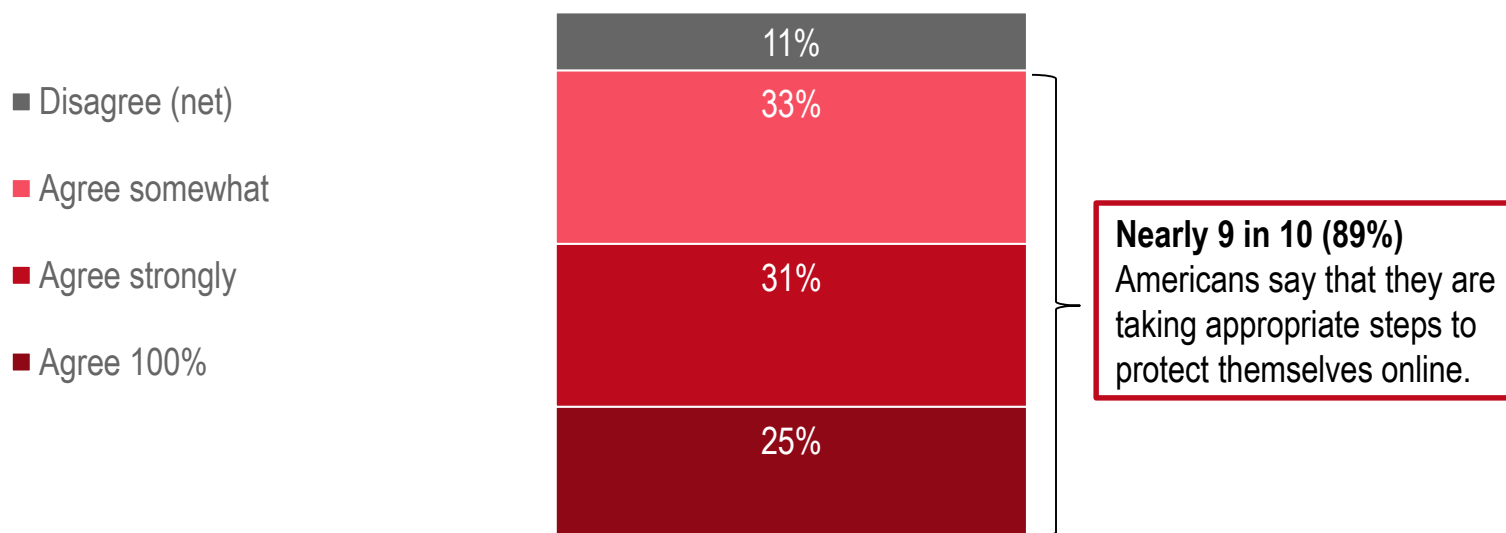
**CARBONITE**  **+** **WEBROOT**  
an openstack company an openstack company

# AMERICANS SAY THEY TAKE STEPS TO PROTECT THEMSELVES ONLINE

An overwhelming majority (89%) of Americans with a work and/or personal device say that they are taking the appropriate steps to protect themselves from cyber-related attacks, including a quarter (25%) who agree 100%.

## % WHO AGREE THAT THEY ARE TAKING STEPS TO PROTECT THEMSELVES FROM CYBER ATTACKS

AMONG THOSE WHO HAVE A WORK AND/OR PERSONAL DEVICE, *n*=9,978



## INSIGHTS BY SUB-GROUPS

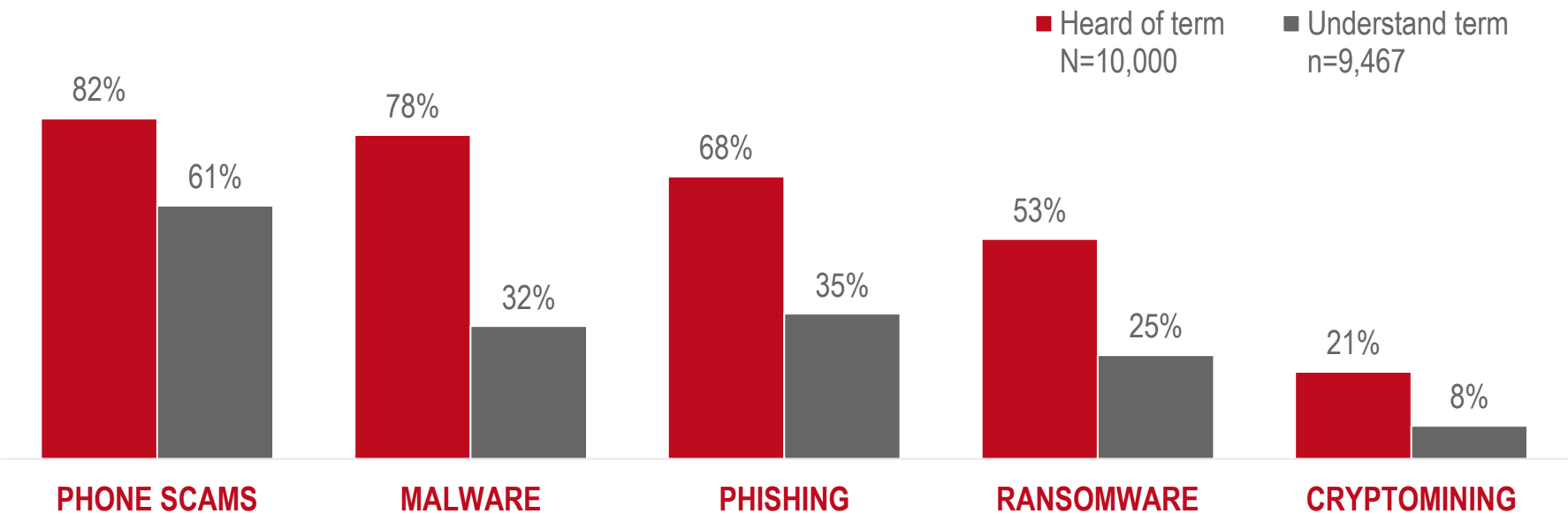
- **Industry:** Compared to 56% overall, Americans working in IT (89%), banking (75%), insurance (74%), and accounting (74%) agree 100% or strongly that they're taking appropriate steps to protect themselves.
- **Own Smart Home Hubs:** Americans with smart hubs with devices (71%) are more likely than those with smart hubs with no devices (53%) and those with no smart hubs or devices (51%) to agree 100% or strongly.

Among those who have a work and/or personal device: To what extent do you agree or disagree with the following statement - I am taking the appropriate steps to protect myself from cyber-related attacks.

# AMERICANS HAVE LIMITED UNDERSTANDING OF CYBER-RELATED ATTACKS

There is a gap between awareness and real understanding of cyber-related attacks. Most Americans can confidently explain phone scams, but are not as equipped to explain malware or phishing. This indicates that Americans may not be as prepared to confront risks as they think.

CYBER-RELATED ATTACKS AMERICANS HAVE HEARD OF VS. THOSE THEY UNDERSTAND




## INSIGHTS BY SUB-GROUPS

- Industry:** Nearly all (96%) Americans working in IT can confidently explain at least one term to someone else, including two-thirds (67%) who can confidently explain malware.
- News Consumption:** Americans who never read the news are far less likely to recognize (70%) or be able to confidently explain (51%) at least one term.
- Type of News Read:** Nine in ten (89%) Americans who consistently consume technology news can confidently explain at least one term, including over half (53%) who can confidently explain malware.

Which of the following cyber-related attacks, if any, have you heard of before today? / Among those who have heard of a cyber-related attack before today: Now, which of these terms, if any, would you be able to confidently explain to someone else (define and provide examples of)

# CYBER HYGIENE RISK INDEX

**CARBONITE**  **+** **WEBROOT**<sup>®</sup>  
an openstack company an openstack company

# 2020 CYBER HYGIENE RISK INDEX

The 2020 Cyber Hygiene Risk Index was constructed using the following 10 survey metrics. These metrics use a pass/fail format:

## 10 BENCHMARK CYBER HYGIENE RISK INDEX METRICS

1. Do they backup their data?
2. Have they avoided losing a device or discarding a device without wiping the data first?
3. Have they not had their ID stolen?
4. Have their devices not been impacted by malware?
5. Have they avoided being a victim of phishing?
6. Do they use anti-virus software?
7. Do they avoid sharing passwords with others?
8. Do they avoid reusing passwords?
9. Do they keep their social media accounts private?\*
10. Do they follow at least five cybersecurity best practices?

**INDEX SCORE**  
**X%**

### INDEX SCORES:

*Throughout this presentation, each of the 10 Cyber Hygiene Risk Index metrics will be attributed an Index Score. This score represents the % of overall Americans who pass each of these metrics.*

\*In a change from 2019, respondents who do not have any social media accounts received one point for this metric.

# CYBER HYGIENE RISK INDEX "GRADES"

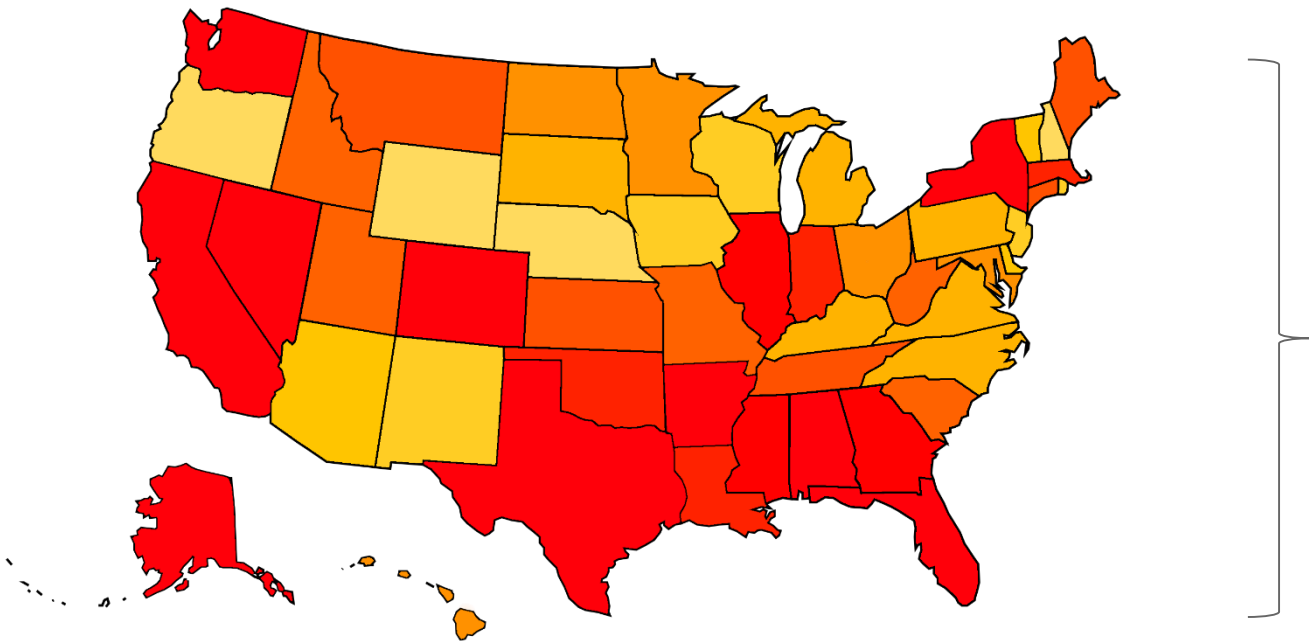
Few Americans practice all 10 benchmark metrics needed to protect themselves from cyber attacks. Among our total sample of 10,000 consumers, the average American scored a 58% on our index ("F" grade). Only 11% scored 90% or higher ("A" grade).

CYBER HYGIENE GRADE	% OF AMERICANS OVERALL <i>N=10,000</i>
A (90-100%)	11%
B (80-89%)	13%
C (70-79%)	16%
D (60-69%)	15%
F (0-59%)	45%

The average American  
scored a **58% (F Grade)**  
on our index.

# STATE-BY-STATE ASSESSMENT OF RISK IN AMERICA

Though there is a wide spread of risk across the United States, with a 15 point difference between the riskiest state (New York, 52%) and least risky state (Nebraska, 67%), no state scores a “C” grade or higher.



## TOP 5 RISKIEST STATES

1	NEW YORK
2	CALIFORNIA
3	TEXAS
4	ALABAMA
5	ARKANSAS

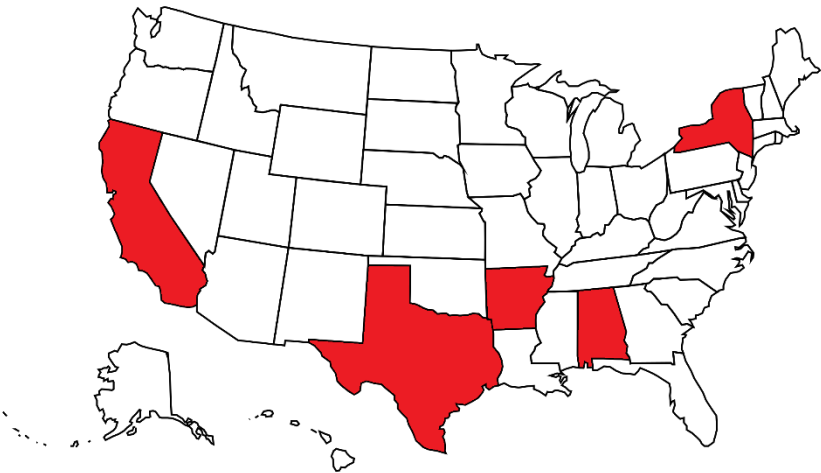


## TOP 5 LEAST RISKY STATES

50	NEBRASKA
49	NEW HAMPSHIRE
48	WYOMING
47	OREGON
46	NEW JERSEY

# RISKIEST STATES SCORECARD

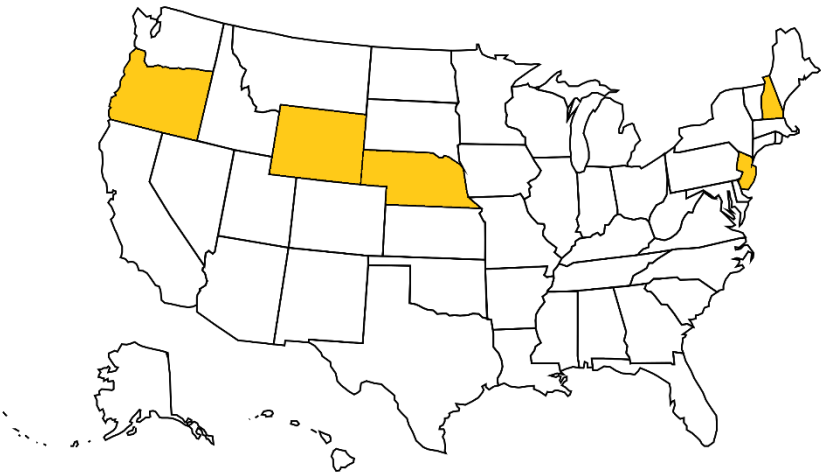
The average scores across our five riskiest states ranged from 52% to 57%.



CYBER HYGIENE GRADE	NEW YORK (#1)	CALIFORNIA (#2)	TEXAS (#3)	ALABAMA (#4)	ARKANSAS (#5)
A (90-100%)	6%	8%	9%	7%	8%
B (80-89%)	6%	8%	14%	9%	10%
C (70-79%)	16%	14%	10%	19%	18%
D (60-69%)	13%	13%	15%	19%	16%
F (0-59%)	60%	57%	52%	47%	49%
AVERAGE GRADE	52% (F)	52% (F)	55% (F)	56% (F)	57% (F)

# LEAST RISKY STATES SCORECARD

The average scores across our five least risky states ranged from 65% to 67%.









CYBER HYGIENE GRADE	NEBRASKA (#50)	NEW HAMPSHIRE (#49)	WYOMING (#48)	OREGON (#47)	NEW JERSEY (#46)
A (90-100%)	20%	18%	17%	15%	17%
B (80-89%)	21%	16%	15%	16%	19%
C (70-79%)	16%	18%	24%	22%	19%
D (60-69%)	14%	17%	13%	17%	14%
F (0-59%)	29%	31%	30%	30%	31%
AVERAGE GRADE	67% (D)	66% (D)	66% (D)	65% (D)	65% (D)

# RISK INDEX METRICS

**CARBONITE**  **+** **WEBROOT**  
an openstack® company an openstack® company

## 2020 CYBER HYGIENE RISK INDEX METRICS

					
BACKING UP DATA	LOST OR STOLEN DEVICES	IDENTITY THEFT	MALWARE, PHISHING, & AV SOFTWARE	PASSWORD PRACTICES	ONLINE BEHAVIOR
<ul style="list-style-type: none"> <li>• Methods of backing up, including online and offline options</li> <li>• Encryption cloud storage</li> </ul>	<ul style="list-style-type: none"> <li>• Quantify the % of Americans who in the past year have not lost a device without being able to find or recover it OR have given away a device without first resetting the factory settings</li> </ul>	<ul style="list-style-type: none"> <li>• Quantify the % of Americans who have not had their identity stolen</li> </ul>	<ul style="list-style-type: none"> <li>• Quantify the % of Americans who in the past year who have avoided being infected with malware or fallen victim to a phishing attempt</li> <li>• Quantify the % of Americans who use anti-virus software</li> </ul>	<ul style="list-style-type: none"> <li>• Quantify the % of Americans who don't share passwords</li> <li>• Quantify the % of Americans who are not reusing passwords across multiple accounts</li> </ul>	<ul style="list-style-type: none"> <li>• Quantify the % of Americans who have kept their social media accounts private</li> <li>• Gauges how many common cybersecurity best practices Americans are following</li> </ul>

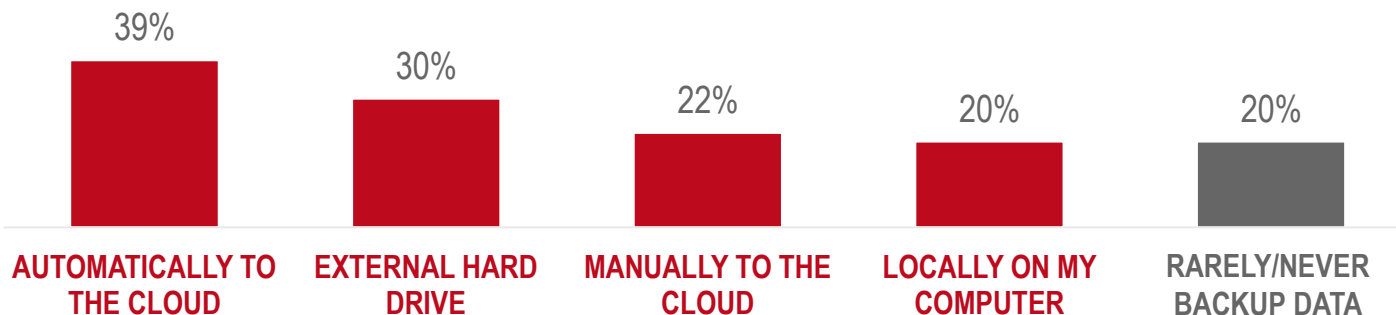
# WHILE MOST AMERICANS BACK UP THEIR DATA, THEY ONLY DO SO EITHER ONLINE OR OFFLINE, NOT BOTH



Four out of five (80%) Americans back up their data. The most common way to back up data is automatically to the cloud (39%). However, only 18% back up to both online and offline, while another 20% rarely or never back up their data at all.

## TOP WAYS AMERICANS ARE BACKING UP THEIR DATA

AMONG THOSE WHO HAVE A WORK AND/OR PERSONAL DEVICE, *n*=9,978



INDEX SCORE  
80%

60% of Americans are only backing up their data to either an online or offline source, rather than both.

## INSIGHTS BY SUB-GROUPS

- Generation:** Millennials (88%), Gen Zers (88%), and Gen Xers (85%) are more likely to backup their data than Boomers (70%).
- News Consumption:** Americans who read, watch, or listen to the news every day (21%) are more likely to backup their data to both an online and offline source than those who don't follow news (6%).
- Own Smart Home Hubs:** A third (33%) of Americans with smart hubs with devices backup their data to both an online and offline source, compared to just 13% of those with no smart hubs or devices.

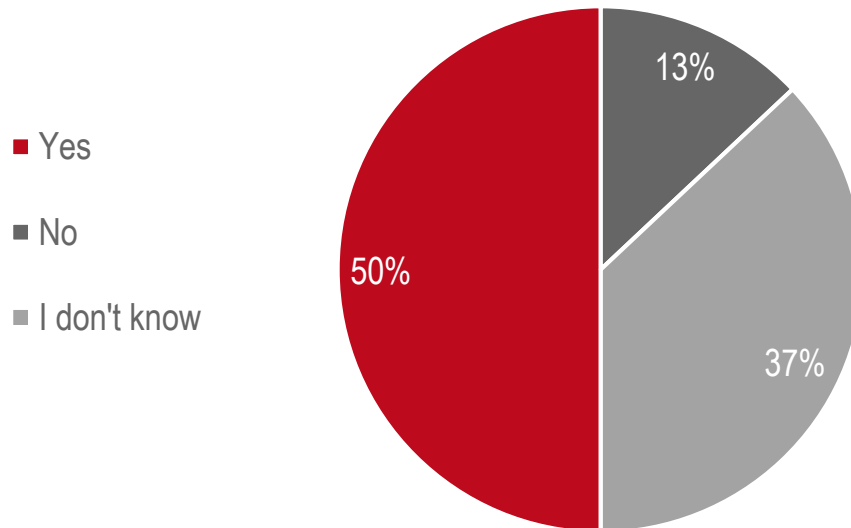
Among those who have a work and/or personal device: Which of the following methods, if any, do you regularly use to backup data on your computer?

# HALF OF THOSE BACKING UP DATA TO THE CLOUD SAY IT IS STORED IN AN ENCRYPTED FORMAT



While half of Americans say their online backups are encrypted, 37% aren't sure one way or another.

**% WHOSE INFORMATION IS STORED IN AN ENCRYPTED FORMAT  
AMONG THOSE WHO REGULARLY BACKUP DATA AUTOMATICALLY  
OR MANUALLY TO THE CLOUD, n=5,414**



## INSIGHTS BY SUB-GROUPS

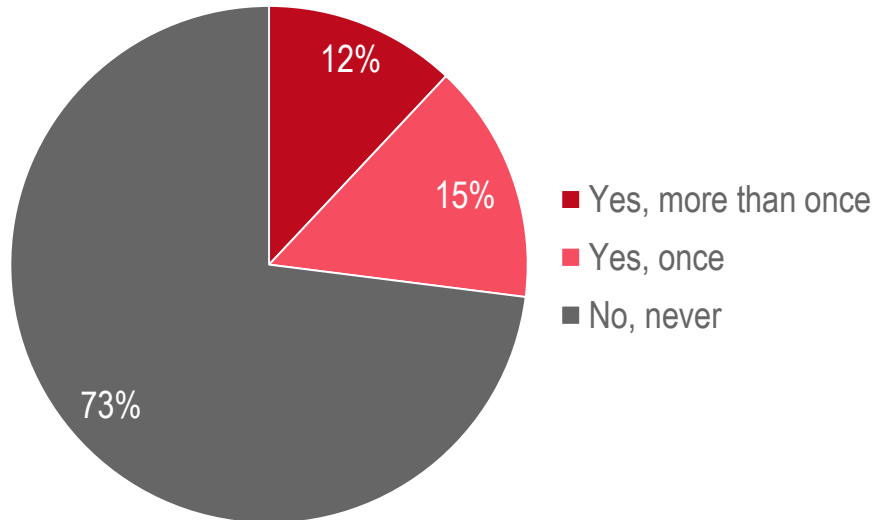
- **Industry:** Americans who work in IT (81%) and banking (74%) are very likely to store their information in an encrypted format when backing up their data to the Cloud.
- **Parents:** Parents (60%) are more likely to store their information in an encrypted format than Non-Parents (43%).
- **Type of News Read:** Nearly two-thirds (65%) of Americans who consistently consume technology news store their information in an encrypted format.

Among those who regularly backup data automatically or manually to the Cloud: When backing up your information to the Cloud, is your information stored in an encrypted format?

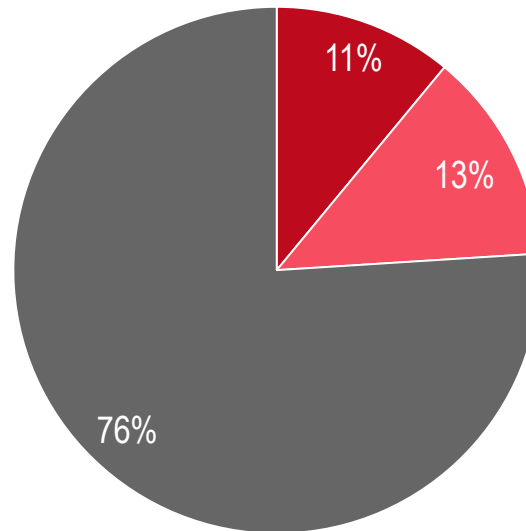
# MANY AMERICANS ARE LOSING OR DISCARDING DEVICES THAT STILL CONTAIN THEIR DATA

While most (72%) Americans have never lost a device without recovering it and never discarded a device without first wiping all of the data on the drives, a sizeable portion of the population have done either one or both of these unsafe data security behaviors.

LOST A DEVICE WITHOUT FINDING IT  
N=10,000



DISCARDED A DEVICE WITHOUT WIPING THE DATA  
N=10,000



INDEX SCORE  
72%

## INSIGHTS BY SUB-GROUPS

- **Generation:** Boomers are the least likely generation to say they lost a device they did not recover (10%) and discarded a device without first wiping all data from the drives (7%).
- **Parents:** Parents are more likely than Non-Parents to say they lost a device they did not recover (45% vs 19%) and discarded a device without first wiping all data from the drives (38% vs 17%).
- **Hobbies:** Two-thirds (66%) of Americans who consider web design a hobby admit losing a device they did not recover, and 58% say they've discarded a device without first wiping all data from the drives.

In the past year, have you ever, even once, lost a device containing your data that you were not able to find or recover? / In the past year, have you ever, even once, discarded a device containing your data without first wiping all data on all of the drives (such as hard drives, SD cards, etc.)?

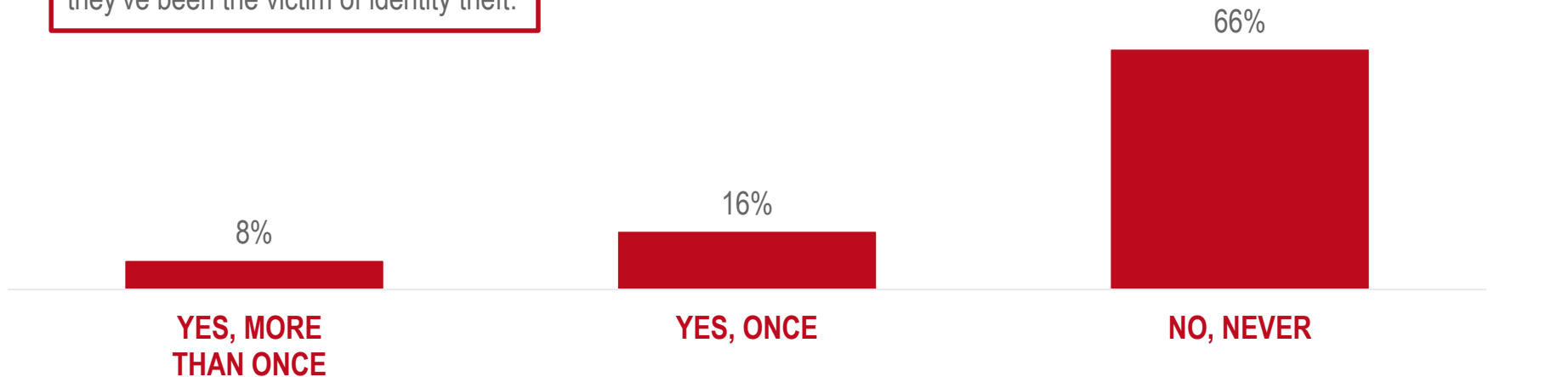
# A QUARTER OF AMERICANS REPORT HAVING THEIR IDENTITY STOLEN AT LEAST ONCE



A quarter (25%) of Americans have had their identity stolen, including 8% who have been a victim of identity theft more than once.

% WHO HAVE EXPERIENCED IDENTITY THEFT  
N=10,000

A quarter (25%) of Americans say they've been the victim of identity theft.



## INSIGHTS BY SUB-GROUPS

- **Industry:** Americans working in the IT (51%), banking (46%), and automotive (45%) industries are more likely to admit that they've had their identity stolen.
- **Mobile Banking:** Those who frequently conduct mobile banking on their phone (32%) are twice as likely to say they have had their identity stolen than those who don't bank on their mobile phone (15%).
- **Share Streaming Passwords:** Americans who share passwords for streaming services (38%) are twice as likely to say they have had their identity stolen than those who do not (18%).

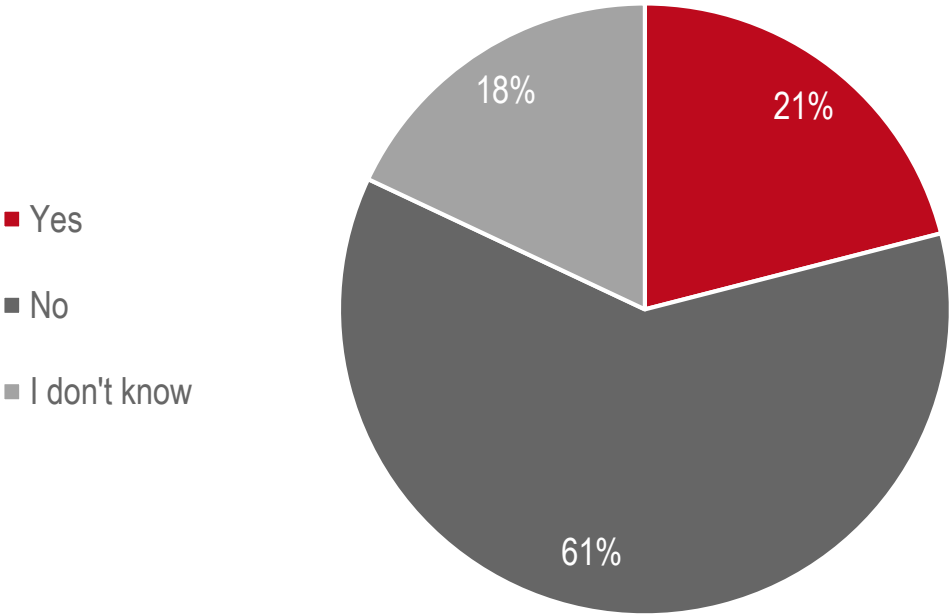
Have you ever, even once, had your identity stolen?

# ONE IN FIVE AMERICANS SAY THEY'VE BEEN IMPACTED BY MALWARE IN THE PAST YEAR



While most (61%) Americans say they've not been impacted, almost 1 in 5 (18%) aren't sure. As only 32% of Americans feel they understand malware well enough to explain it to a friend, it is likely that more Americans have been impacted and may not know it.

% WHOSE DEVICES HAVE BEEN IMPACTED BY MALWARE  
AMONG THOSE WHO HAVE A WORK AND/OR PERSONAL  
DEVICE, n=9,978



INDEX SCORE  
61%

## INSIGHTS BY SUB-GROUPS

- **Industry:** A majority of Americans working in banking (61%) and IT (53%) say they have had devices impacted by malware in the past year.
- **Gender:** Men (28%) are twice as likely to say they have had devices impacted by malware in the past year than women (14%).
- **Own Smart Home Hubs:** Over two in five (44%) Americans with smart hubs with devices say they have been impacted by malware in the past year, making them more likely to say this than those with smart hubs with no devices (19%) and those with no smart hubs or devices (12%).

Among those who have a work and/or personal device: To your knowledge, in the past year has your PC, tablet and/or smart phone been impacted as a result of malware?



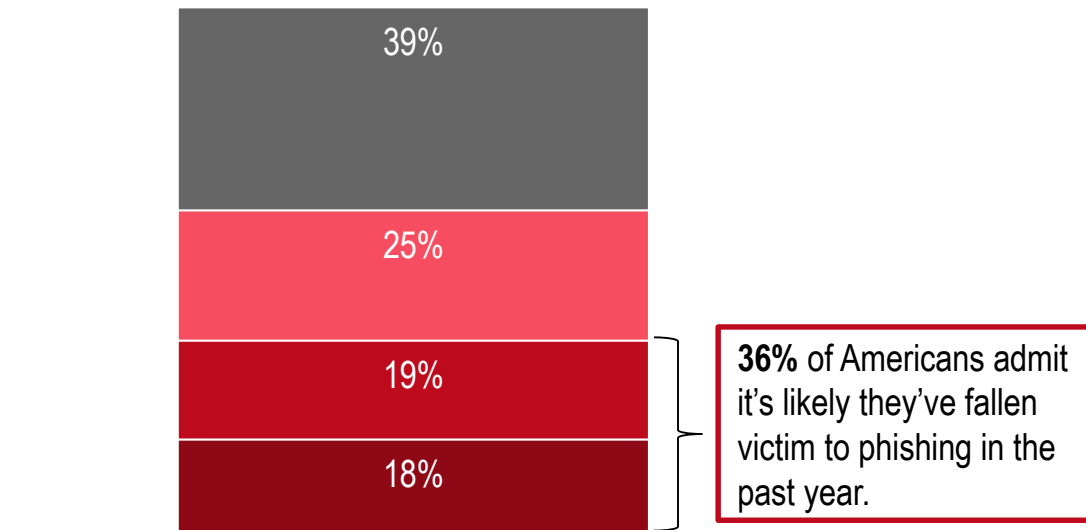
# A SIZABLE AMOUNT OF AMERICANS ARE AFFECTED BY PHISHING

Over one-third (36%) of Americans claim they have fallen victim to phishing in the past year. As only 35% of Americans feel they can explain what phishing is, it is possible that the real number of attacks is even higher.

## PROVIDED PERSONAL INFORMATION TO A PHISHING SCAM IN THE PAST YEAR

N=10,000

- No, definitely not
- Unsure, may or may not
- Probably
- Yes, definitely



INDEX SCORE  
39%

## INSIGHTS BY SUB-GROUPS

- **Generation:** Millennials (48%), Gen Zers (43%), and Gen Xers (41%) are more likely to say they have likely provided information to a phishing scam in the past year than Boomers (22%).
- **Auto Bill Pay:** About a third (31%) of Americans who automate all or almost all bill payments say they have likely provided information to a phishing scam in the past year, making them more likely to say this than those who automate one or some payments (15%) and those who automate no payments (10%).

Thinking about the past year, is it possible that you may have, even once, provided personal information through an email, text message, social media message, or phone call that you suspect could be phishing, based on the definition above?



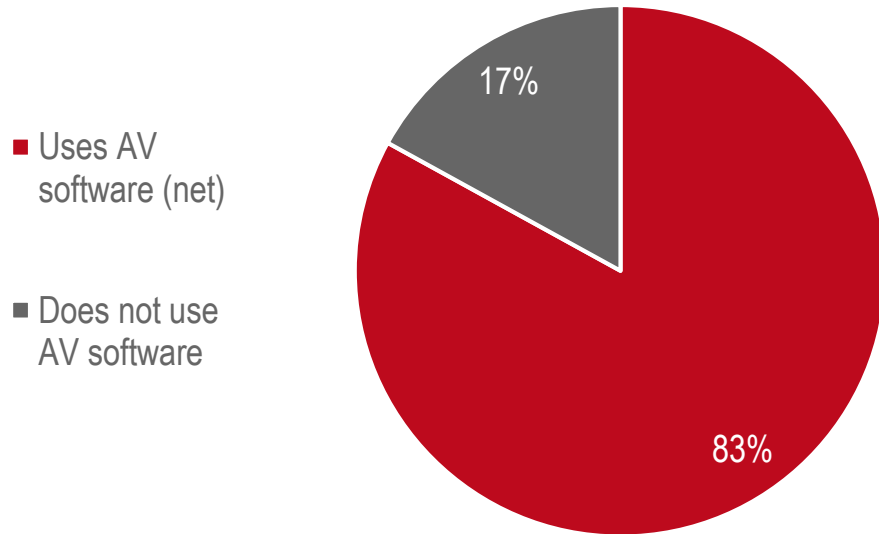
# MOST AMERICANS USE ANTI-VIRUS SOFTWARE

Most (83%) Americans have AV software on at least one of their personal devices – the top devices being Windows desktops or laptops (50%), Android phones (29%), and Apple phones (21%).

## INSIGHTS BY SUB-GROUPS

- **Industry:** Most Americans who work in the IT (96%), financial services (92%), construction (90%), and professional services (90%) industries say they use AV software on at least one personal device.
- **News Consumption:** Americans who read, watch, or listen to the news every day (87%) are more likely to say they use AV software than those who never follow the news (65%).
- **Type of News Read:** Americans who consistently consume technology (91%) and business (90%) news say they use AV software.

% WHO USE AV SOFTWARE ON PERSONAL DEVICE  
AMONG THOSE WHO HAVE A PERSONAL DEVICE, *n*=9,874



INDEX SCORE  
83%

PERSONAL DEVICES ANTI-VIRUS  
SOFTWARE IS USED ON  
AMONG THOSE WHO HAVE A PERSONAL  
DEVICE, *n*=9,874

	%
Windows laptop/desktop	50%
Android phone	29%
iOS (Apple) phone	21%
Mac (Apple) laptop (MacBook) / desktop (iMac)	11%
I don't use any anti-virus software on any device	17%

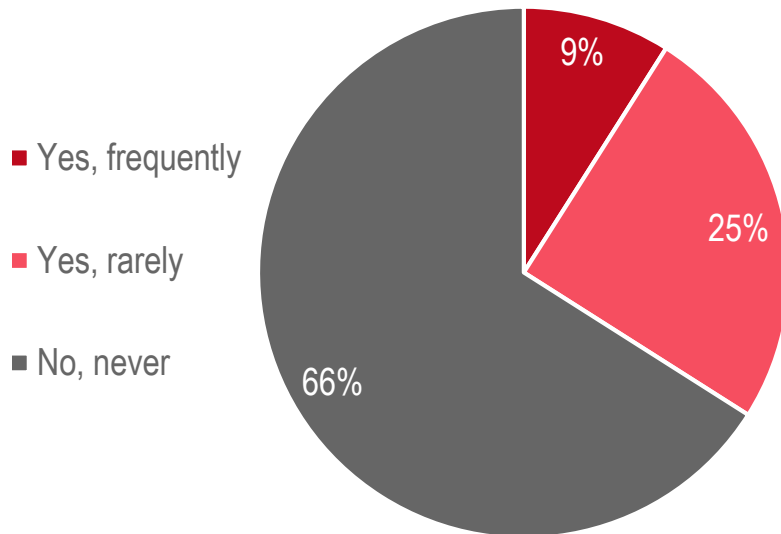
Among those who have a personal device: On which of your personal devices, if any, do you use antivirus (AV) software (Norton, McAfee, Webroot, Windows Defender, etc.)?



# A THIRD OF AMERICANS ARE SHARING PASSWORDS AND HALF REUSE PASSWORDS ACROSS ACCOUNTS

One-third (34%) of Americans are sharing passwords and other credentials with others. Furthermore, 49% have more accounts than passwords, which means they are reusing passwords across accounts.

% WHO SHARE PASSWORDS  
WITH OTHERS  
N=10,000



INDEX SCORE  
66%

# OF ACCOUNTS & # OF PASSWORDS  
N=10,000

10% have more  
passwords than accounts

**49% are reusing passwords  
across multiple accounts**

Americans have on average  
**10** passwords for **16** accounts

INDEX SCORE  
51%

## INSIGHTS BY SUB-GROUPS

- **Generation:** Gen Zers (56%) are most likely to share passwords, compared to 47% of Millennials, 33% of Gen Xers, and 19% of Boomers.

Boomers have an average of 19 online accounts that require a username and password, while Gen Xers have 15, Millennials have 14, and Gen Zers have 13.

- **Read Pop Culture News:** Over two in five (46%) Americans who consistently consume popular culture news have shared passwords with others, and three in ten (60%) reuse passwords across multiple accounts.

Have you ever, even once, shared your passwords or other access credentials with others? / How many separate passwords or passphrases do you maintain on a regular basis? / How many total online accounts do you have that require a username and password?

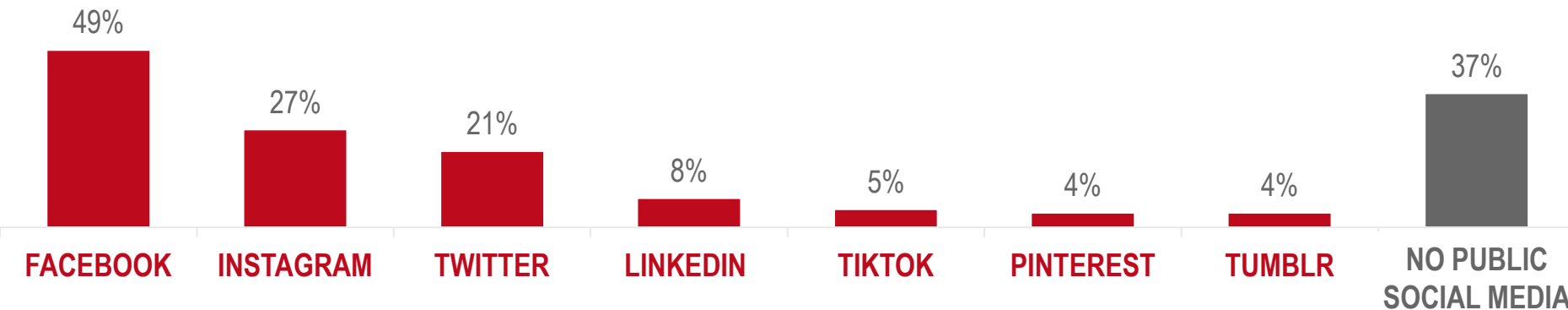
# MOST AMERICANS HAVE AT LEAST ONE SOCIAL MEDIA ACCOUNT KEPT PUBLIC WHERE ANYONE CAN SEE IT



Only a small percentage (37%) of Americans with social media have none of their social media accounts public. Facebook, Instagram, and Twitter are the most common public accounts.

% WHO HAVE KEPT SOCIAL MEDIA PUBLIC  
AMONG THOSE WHO HAVE SOCIAL MEDIA, *n*=8,827

INDEX SCORE  
37%



## INSIGHTS BY SUB-GROUPS

- **Generation:** Younger Americans are more likely to keep their social media accounts public, as 81% of Gen Zers have a public account versus only 48% of Boomers.
- **Home Ownership:** Americans who rent their housing (70%) are more likely to say they have kept a social media account public than those who own their housing (60%).
- **Share Streaming Passwords:** Americans who share passwords for streaming (78%) are more likely to say they have kept a social media account public than those who do not (56%).

Among those who have social media: Which of the following social media accounts have you ever, even once, kept public? Meaning, someone you don't know could find your posts or information by searching the internet.

# NEARLY HALF OF AMERICANS PRACTICE FIVE OR MORE BEST PRACTICES FOR ONLINE BEHAVIOR AND DATA SECURITY



Nearly half (45%) of Americans are regularly practicing at least five of the online habits they were presented with. Over half (56%) monitor their bank accounts, and about half (49%) take precautions before clicking on an email link and keep their software up to date.



% WHO REGULARLY... <i>N=10,000</i>	%
Monitor bank accounts	56%
Take precautions before clicking an email link	49%
Keep software up to date	49%
Monitor credit card statements	45%
Check credit reports	41%
Enable two-factor authentication	34%
Use an ad-blocking plug in (block pop-ups)	33%


CONTINUED: % WHO REGULARLY ... <i>N=10,000</i>	%
Limit online purchases	30%
Deactivate Bluetooth when not in use	27%
Use mobile payment	24%
Use a password manager	20%
Employ credit monitoring services	19%
Deactivate NFC when not using mobile payment	8%
I don't practice any of these habits	10%

## INSIGHTS BY SUB-GROUPS

- Industry:** The industries who are most likely to follow at least five best practices are entertainment (60%), insurance (58%), and IT (57%). The least likely are real estate (30%), hospitality (30%), and food service (33%).
- Home Ownership:** Americans who own their housing (50%) are more likely to follow at least five best practices than renters (37%).
- News Consumption:** Americans who read, watch, or listen to the news every day (51%) are more likely to practice five online habits than those who never follow the news (18%).

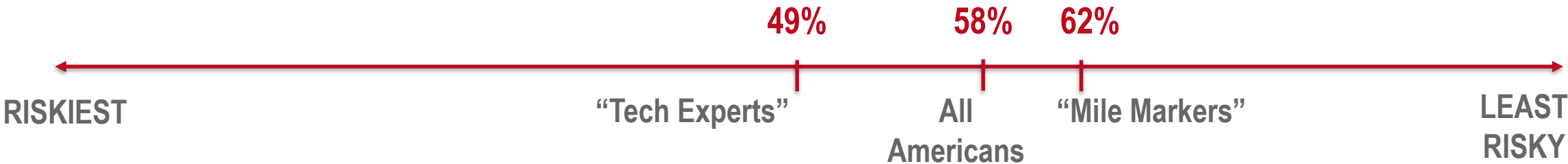
Which of the following online habits do you currently practice on a regular basis?

# DEMOGRAPHICS DRIVING THE RISK INDEX

**CARBONITE**  **+** **WEBROOT**<sup>®</sup>  
an openstack company an openstack company

# EXPLORING DEMOGRAPHIC IMPACTS ON THE RISK INDEX SCALE

## CYBER HYGIENE RISK INDEX SCALE



### Tech Experts

Those who work in IT or are coding or web design hobbyists – are among the riskiest populations.

*As Americans become more tech-savvy, they show riskier behaviors.*




### Mile Markers

Those who have progressed through certain life markers, including earning a college degree and owning a home, and who read or watch the news everyday.

*As Americans become more responsible in their lives, they tend to become more responsible in their cybersecurity habits as well.*

# TECH EXPERTS SNAPSHOT: THE MOST KNOWLEDGEABLE AND AWARE, BUT ONE OF THE RISKIEST GROUPS

<div></div> <div><b>Tech Experts</b></div> <div><i>Those who work in the IT industry or they code or web design as a hobby</i></div>	<div><b>Who They Are:</b></div> <ul style="list-style-type: none"><li>• More likely to be younger (under age 40)</li><li>• 71% male</li><li>• 59% live in cities</li><li>• 64% self-employed and/or contractors</li></ul>	<div><b>Attitudes and Behaviors</b></div> <ul style="list-style-type: none"><li>• 71% own smart home devices</li><li>• 81% use mobile banking</li><li>• 85% enroll in auto bill pay</li><li>• 65% follow technology news</li></ul>
	<div><b>Knowledge of Cyber-Security</b></div> <ul style="list-style-type: none"><li>• More likely to be able to explain phishing (47%) than Americans overall (35%), and more likely to be able to explain malware (57% compared to 32%).</li><li>• They are also more likely to say they've been the target of those attacks, which drives their Risk Index score down.</li></ul>	<div><b>Risk Index</b></div> <ul style="list-style-type: none"><li>• Have a lower risk index relative to the all Americans (49% vs. 58%)</li><li>• Fewer % have "A" ratings compared to all Americans (6% vs. 11%)</li></ul>

# TECH EXPERTS SCORE LOWER ON 7 OF THE 10 METRICS, BUT ALSO ARE MORE LIKELY TO SCORE POSITIVELY ON 3 BEHAVIOR METRICS

On Risk Index metrics that ask about recall (losing a device, malware, phishing, and stolen ID), Tech Experts are more likely to say yes than average Americans. They are also more likely to share and re-use passwords and keep their social media accounts public. However, they are also more likely to follow data security and online best practices.

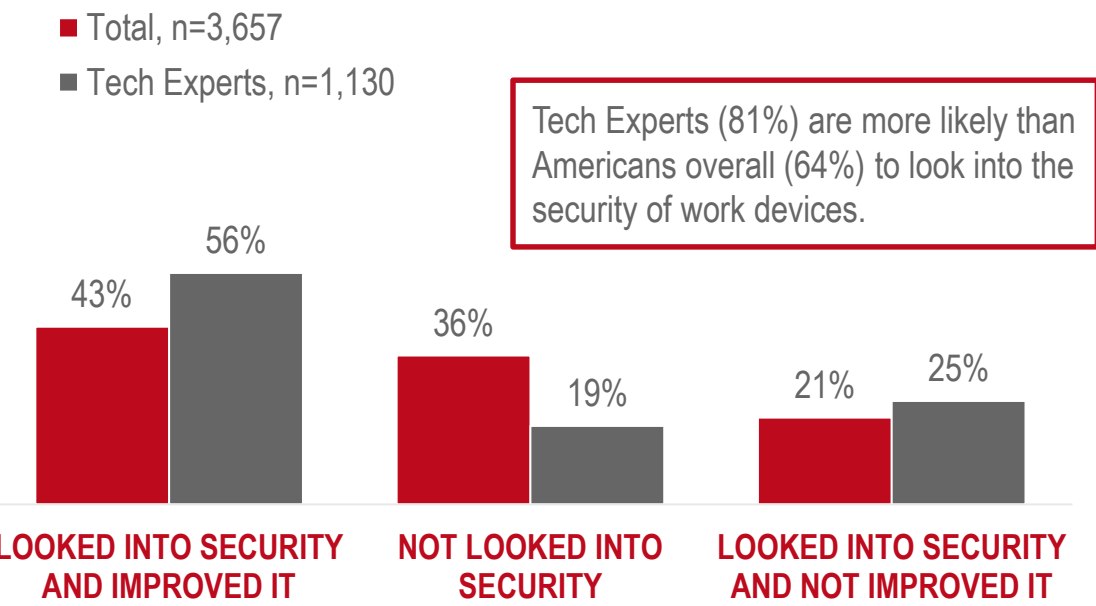
RISK INDEX METRICS WHERE IT EXPERTS SCORE <u>LOWER</u>	TOTAL N=10,000	TECH EXPERTS n=1,521
Have they avoided losing a device or discarding a device without wiping the data first?	72%	45%
Have they <u>not</u> had their ID stolen?	66%	48%
Have their devices <u>not</u> been impacted by malware?	61%	42%
Have they avoided being a victim of phishing?	39%	25%
Do they avoid sharing passwords with others?	66%	44%
Do they avoid reusing passwords?	51%	49%
Do they keep their social media private?	37%	15%

RISK INDEX METRICS WHERE IT EXPERTS SCORE <u>HIGHER</u>	TOTAL N=10,000	TECH EXPERTS n=1,521
Do they backup their data?	80%	96%
Do they use anti-virus software?	83%	93%
Do they follow at least five cybersecurity best practices?	45%	54%

# TECH EXPERTS ARE MORE LIKELY TO FOLLOW OTHER BEST PRACTICES BEYOND THE RISK INDEX METRICS

Tech Experts are more likely than Americans overall to be able to confidently explain a cyber-related attack term (92% vs 76%). They're nearly twice as likely to agree 100% that they are taking appropriate steps to protect themselves from cyber attacks (47% vs 25%) and twice as likely to say they use an identity protection service (60% vs 30%).

## SECURITY OF WORK DEVICES



## USE ID PROTECTION SERVICES



**Tech Experts: 60%**  
All Americans: 30%

## BACKUP DATA IN ENCRYPTED FORMAT



**Tech Experts: 75%**  
All Americans: 50%


## USE A PASSWORD MANAGER



**Tech Experts: 58%**  
All Americans: 30%

Which of the following online habits do you currently practice on a regular basis? / Among those who have a work and/or personal device: Do you use an identity protection service such as LifeLock, ID Watch Dog or others? / Among those who regularly backup data automatically or manually to the Cloud: When backing up your information to the Cloud, is your information stored in an encrypted format? / Among those who have a work and/or personal device: Do you use a password manager, or other software tool that assists in generating and retrieving complex passwords?

# MILE MARKERS SNAPSHOT: AMERICANS BECOME MORE RESPONSIBLE WITH CYBERSECURITY AS THEY PROGRESS THROUGH LIFE MARKERS

<div></div> <div><b>MILE MARKERS</b></div> <div><i>Those who have a college education, own a home, and read or watch the news every day.</i></div>	<div><b>Who They Are:</b></div> <ul style="list-style-type: none"><li>• 63% earning over \$100,000 a year</li><li>• 81% are married</li><li>• 41% have children under 18 living at home</li><li>• 47% live in the suburbs</li></ul>	<div><b>Attitudes and Behaviors</b></div> <ul style="list-style-type: none"><li>• 61% invest in the stock market</li><li>• 81% enroll in auto bill pay</li><li>• 51% are self-employed or contractor</li><li>• 79% follow the national news</li></ul>
	<div><b>More Aware of Cybersecurity</b></div> <ul style="list-style-type: none"><li>• More likely than all Americans to be able to explain phishing (54%) and malware (52%)</li><li>• 63% follow at least five best practices for online behavior and cybersecurity</li></ul>	<div><b>Risk Index</b></div> <ul style="list-style-type: none"><li>• Have a lower risk index relative to all Americans (62% vs. 58%)</li><li>• Higher % have “A” ratings compared to all Americans (17% vs. 11%)</li></ul>

# PROGRESSING THROUGH MILE MARKERS CORRESPONDS MOST WITH FOLLOWING NUMEROUS BEST PRACTICES

Those who have a college degree, own a home, and read the news everyday are largely in-line with Americans overall on most of the Risk Index questions. However, on data security and especially on practicing five or more examples of good online behavior, they are far less risky than most Americans.

RISK INDEX METRICS WHERE MILE MARKERS SCORE ABOUT EVEN	TOTAL N=10,000	MILE MARKERS n=1,515	RISK INDEX METRICS WHERE MILE MARKERS SCORE <u>HIGHER</u>	TOTAL N=10,000	MILE MARKERS n=1,515
Have they avoided losing a device or discarding a device without wiping the data first?	72%	75%	Do they backup their data?	80%	87%
Have they <u>not</u> had their ID stolen?	66%	59%	Do they use anti-virus software?	83%	90%
Have their devices <u>not</u> been impacted by malware?	61%	61%	Do they follow at least five cybersecurity best practices?	45%	63%
Have they avoided being a victim of phishing?	39%	42%			
Do they avoid sharing passwords with others?	66%	63%			
Do they avoid reusing passwords?	51%	49%			
Do they keep their social media private?	37%	36%			

# BEYOND THE RISK INDEX, MILE MARKERS FOLLOW THROUGH ON OTHER DATA SECURITY BEST PRACTICES

Over six in ten (63%) Mile Markers practice five or more good cybersecurity behaviors, compared to less than half (45%) of Americans overall. They are also more likely to use ID protection services (47% vs 30%), backup data in an encrypted format (64% vs 50%), and use a password manager (37% vs 30%).

REGULARLY FOLLOW BEST PRACTICES TOP RESPONSES SHOWN	TOTAL N=10,000	MILE MARKERS n=1,515
Monitor bank accounts	56%	68%
Take precautions before clicking a link in an email	49%	61%
Keep software up to date	49%	62%
Monitor credit card statements	45%	65%
Check credit reports	41%	53%
Enable two-factor authentication	34%	45%
Use an ad-blocking plug in (block pop-ups)	33%	40%
Five or more practices (net)	45%	63%

## USE ID PROTECTION SERVICES



**Mile Markers: 47%**  
All Americans: 30%

## BACKUP DATA IN ENCRYPTED FORMAT



**Mile Markers: 64%**  
All Americans: 50%


## USE A PASSWORD MANAGER




**Mile Markers: 37%**  
All Americans: 30%

Among those who have a work device: Have you taken any steps to learn about or improve upon the security of your work devices? / Among those who have a work and/or personal device: Do you use an identity protection service such as LifeLock, ID Watch Dog or others? / Among those who regularly backup data automatically or manually to the Cloud: When backing up your information to the Cloud, is your information stored in an encrypted format? / Among those who have a work and/or personal device: Do you use a password manager, or other software tool that assists in generating and retrieving complex passwords?

# HOME-BASED VERY SMALL BUSINESSES

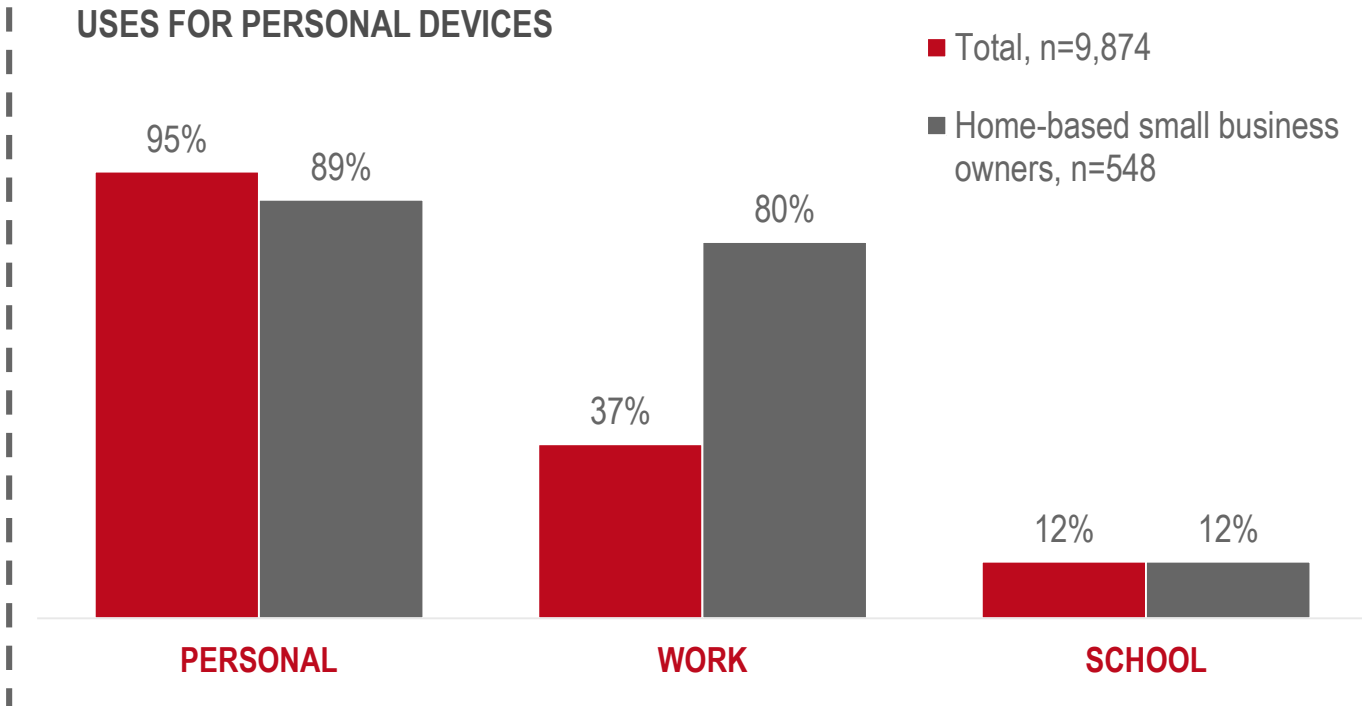
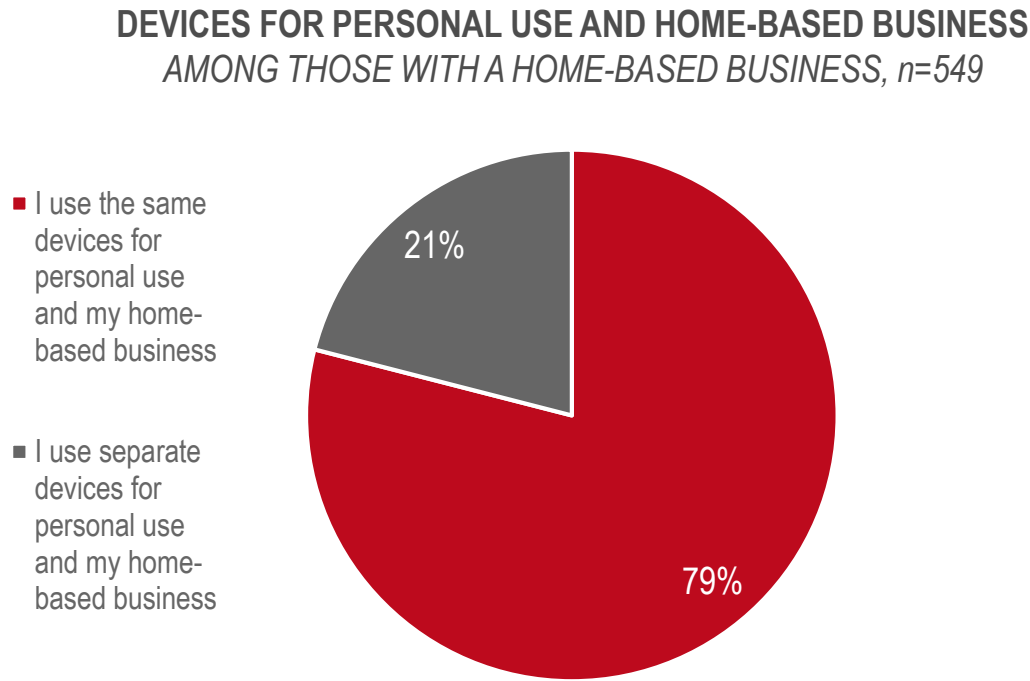
**CARBONITE**  **+** **WEBROOT**<sup>®</sup>  
an openbit company an openbit company

# HOME-BASED VERY SMALL BUSINESS OWNERS SNAPSHOT

<div></div> <div><b>HOME-BASED VERY SMALL BUSINESS OWNERS</b></div> <div><i>Self-employed SBOs (either as a primary or side job) whose VSB is home-based.</i></div>	<b>Who They Are:</b> <ul style="list-style-type: none"><li>• 73% of VSBs are their primary job</li><li>• 46% live in cities</li><li>• 49% are college-educated</li><li>• Top industries: IT (13%), Professional Services (9%), Construction (9%)</li></ul>	<b>Attitudes and Behaviors</b> <ul style="list-style-type: none"><li>• 50% invest in the stock market</li><li>• 75% conduct mobile banking</li><li>• 81% enroll in auto bill pay</li><li>• 52% have smart home devices</li></ul>
	<b>How They Operate:</b> <ul style="list-style-type: none"><li>• 73% of owners are solely responsible for cybersecurity</li><li>• 91% backup their data (compared to 80% for all Americans)</li><li>• 69% encrypt their backups (compared to 50% for all Americans)</li></ul>	<b>Risk Index</b> <ul style="list-style-type: none"><li>• Have a lower risk index relative to the total (54% vs. 58%)</li><li>• About equal % have “A” ratings relative to the total (10% vs. 11%)</li></ul>

# VSB OWNERS BLUR THE LINES BETWEEN PERSONAL AND WORK DEVICES

Four out of five VSB owners say they use the same devices for both personal use and work use. This compares to just 37% of Americans who report using their personal devices for work purposes.



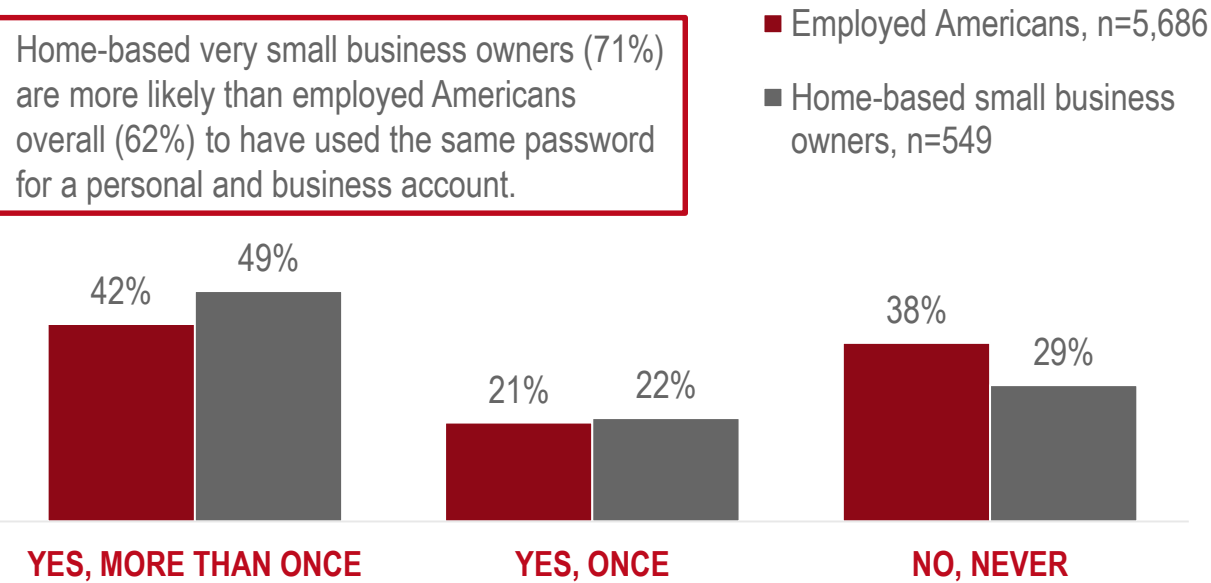
Among those with a home-based business: Which of the following best describes the electronic devices you use for your home-based business? / Among those who have any personal devices: For which of the following reasons do you use the personal electronic devices that you own?

# ALMOST THREE-FOURTHS OF VSB OWNERS MIX PERSONAL AND BUSINESS ACCOUNT PASSWORDS

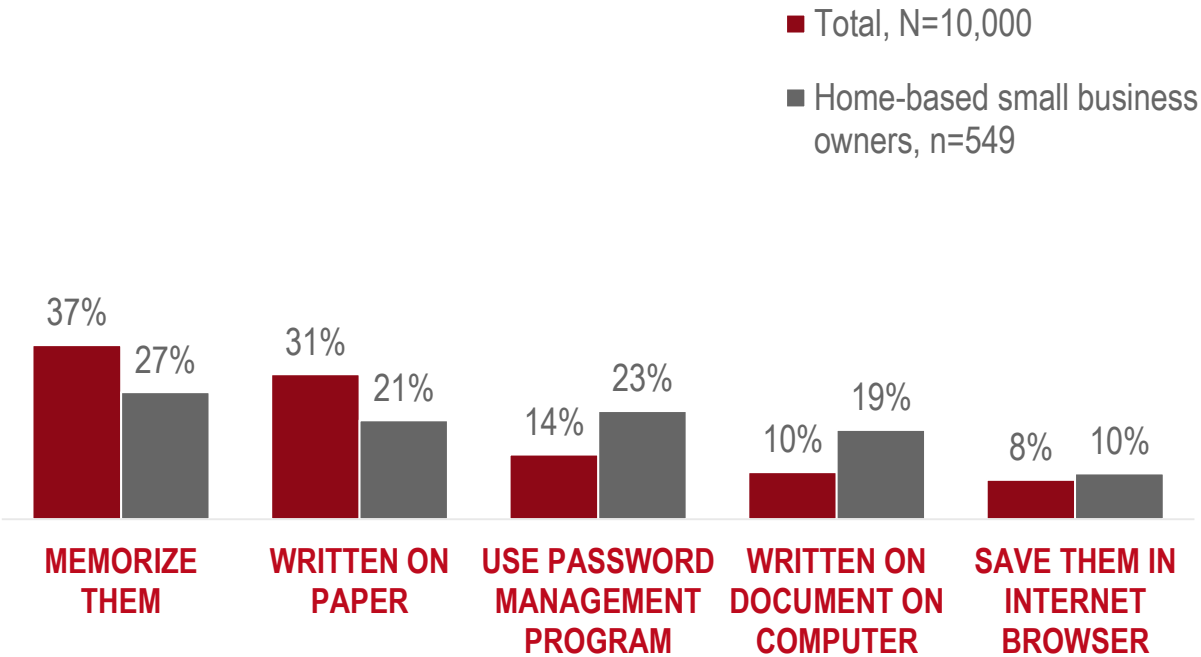
More VBS (71%) owners use the same password for a personal and business accounts, and half of VSB owners have done this more than once. However, VSB owners are more likely to use a password management program or a document on their computer, rather than relying on memory or written out on a sheet of paper.

% WHO USE SAME PASSWORD FOR A PERSONAL AND BUSINESS ACCOUNT

Home-based very small business owners (71%) are more likely than employed Americans overall (62%) to have used the same password for a personal and business account.




WAYS OF KEEPING TRACK OF PASSWORDS



Have you ever, even once, shared your passwords or other access credentials with others? / Among those who are employed: Have you ever, even once, used the same password for a personal and business account?

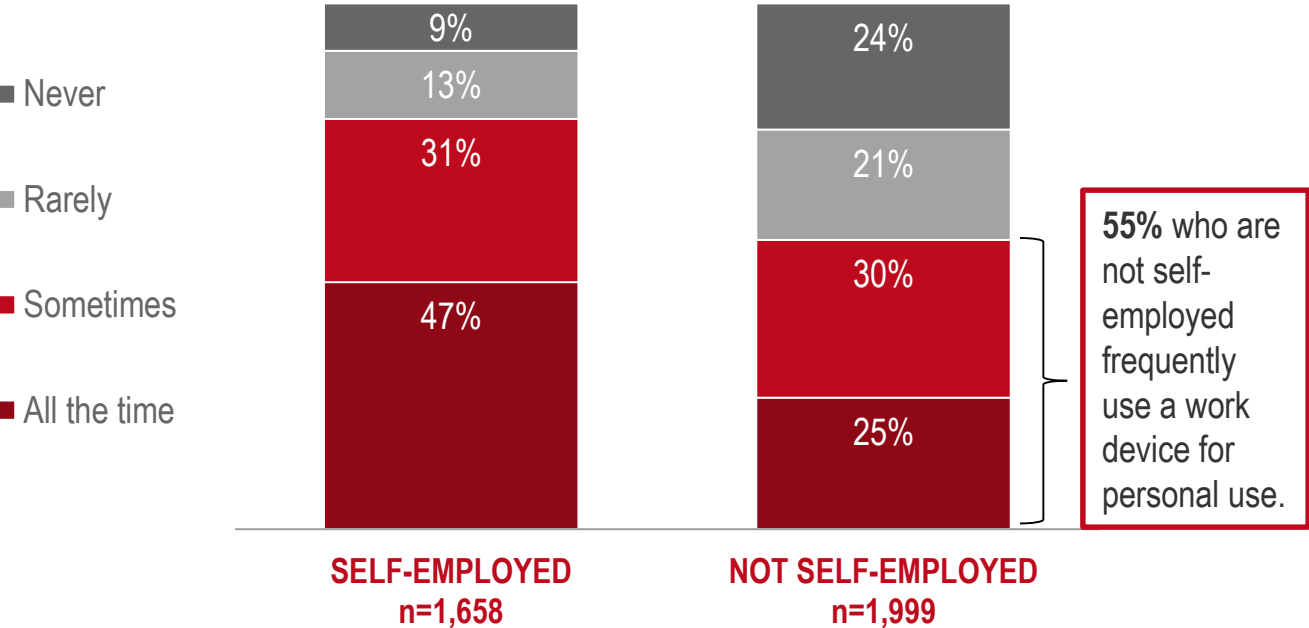
# USE AND SECURITY OF WORK DEVICES

**CARBONITE**  **+** **WEBROOT**  
an openstack company an openstack company

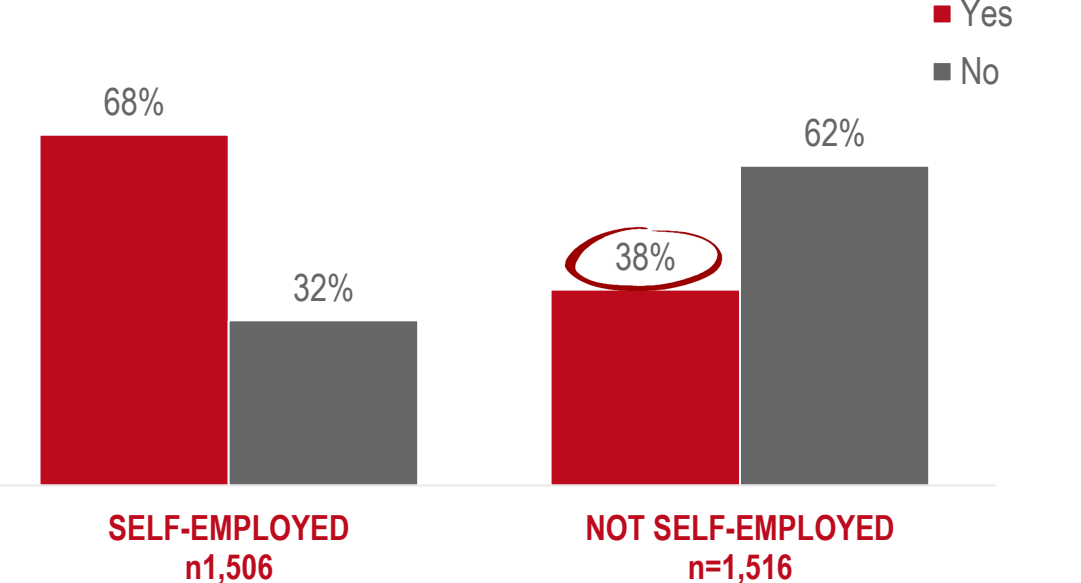
# WORK DEVICES ARE OFTEN USED FOR PERSONAL USE AND ARE SLIGHTLY MORE LIKELY TO BE SEEN AS THE PRIMARY DEVICE AT HOME

Slightly more than half (55%) of non self-employed workers use their assigned work devices for personal use, including 25% who do this all the time. In addition, almost 40% who use their work device for personal use actually consider their work device to be their “primary” device for using it at home.

**FREQUENCY OF USING WORK DEVICE FOR PERSONAL USE**  
*AMONG THOSE WHO HAVE A WORK DEVICE*



**% WHO CONSIDER THEIR WORK DEVICE TO BE THEIR PRIMARY DEVICE FOR USE AT HOME**  
*AMONG THOSE WHO HAVE A WORK DEVICE THAT THEY USE FOR PERSONAL USE*

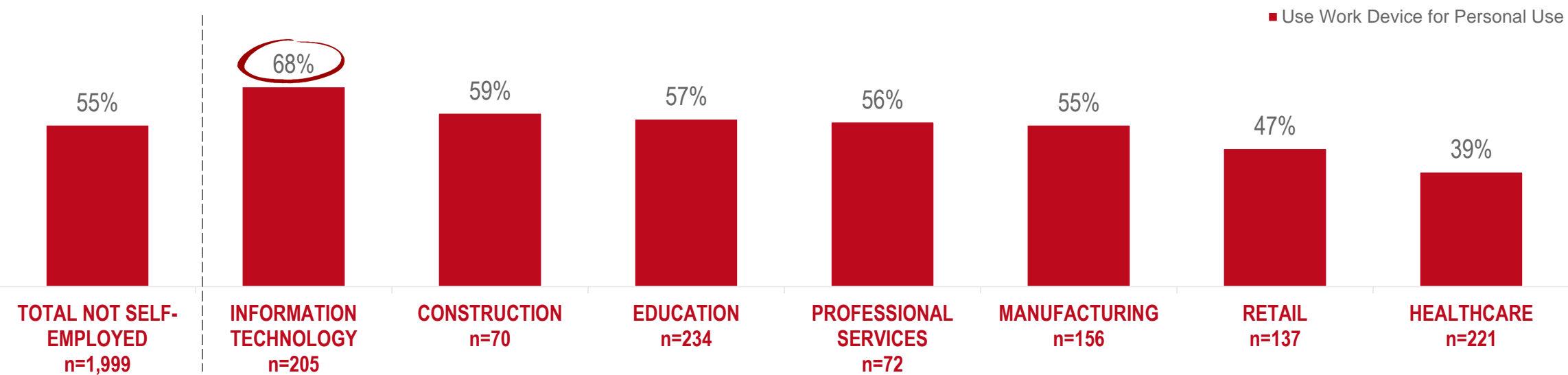


Among those who have a work device: How often, if ever, do you use your work devices, such as a work phone or laptop, for personal use? / Among those who have a work device that they use for personal use: Would you consider any of your work devices to be your primary device for use at home?

# AMONG WORKERS WHO AREN'T SELF-EMPLOYED, IT WORKERS ARE THE MOST LIKELY TO USE THEIR ASSIGNED WORK DEVICE FOR PERSONAL USE

Among those who are not self-employed, two-thirds (68%) of IT professionals frequently use work devices for personal use. A majority of workers in Construction, Education, Professional Services, and Manufacturing also do the same.

FREQUENCY OF USING WORK DEVICE FOR PERSONAL USE  
AMONG THOSE WHO ARE NOT SELF-EMPLOYED AND HAVE A WORK DEVICE

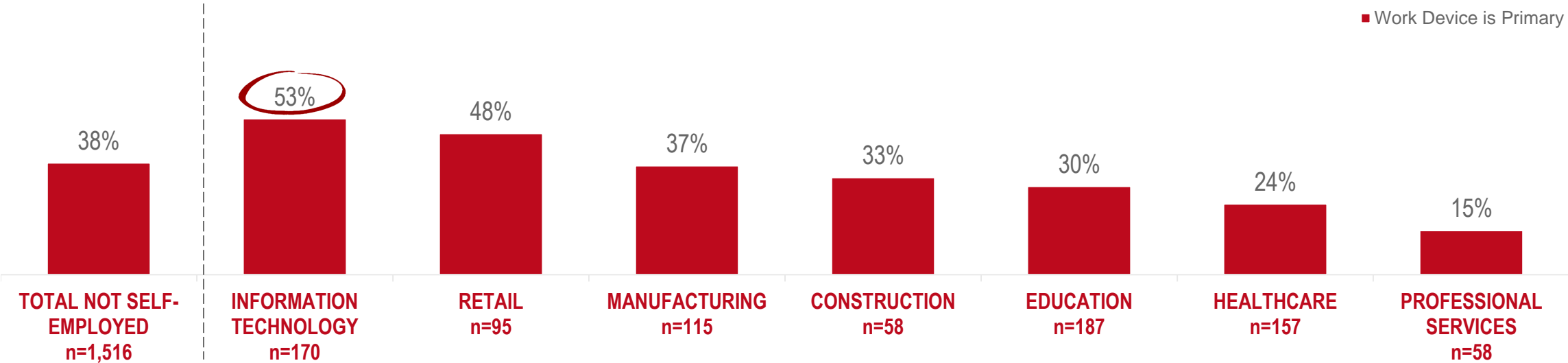


Among those who have a work device: How often, if ever, do you use your work devices, such as a work phone or laptop, for personal use?

# IN MOST PROFESSIONS, A MAJORITY OF EMPLOYEES DO NOT CONSIDER THEIR ASSIGNED WORK DEVICE TO BE THEIR “PRIMARY” DEVICE AT HOME

While IT professionals are the only profession where a majority (53%) consider their assigned work device to be their primary one at home, substantial percentages of other industries also do the same.

% WHO CONSIDER THEIR WORK DEVICE TO BE THEIR PRIMARY DEVICE FOR USE AT HOME  
AMONG THOSE WHO ARE NOT SELF-EMPLOYED AND HAVE A WORK DEVICE THAT THEY USE FOR PERSONAL USE

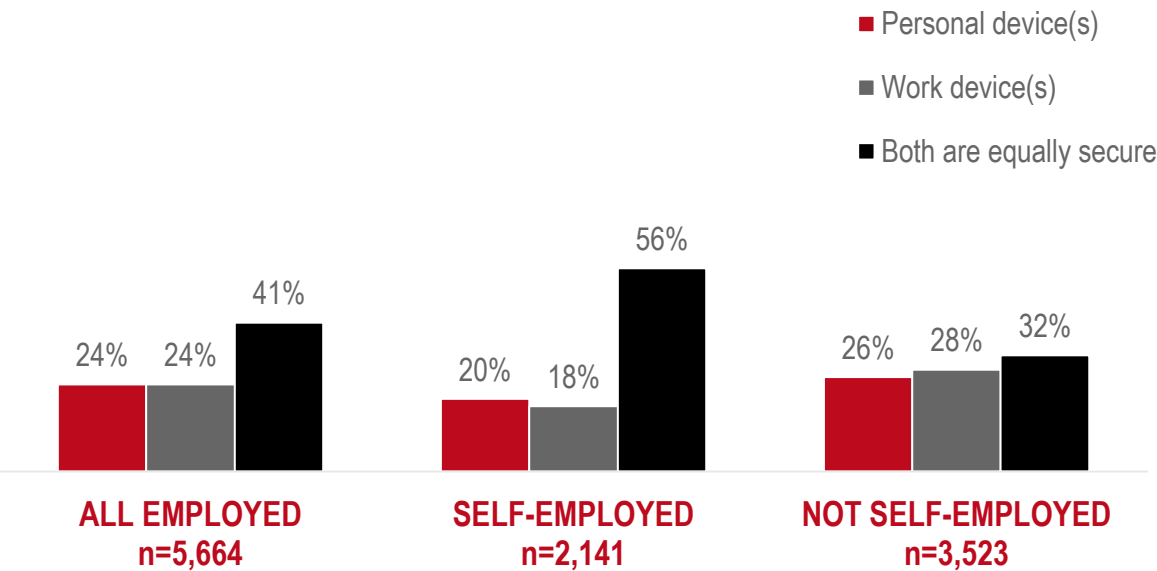


Among those who have a work device that they use for personal use: Would you consider any of your work devices to be your primary device for use at home?

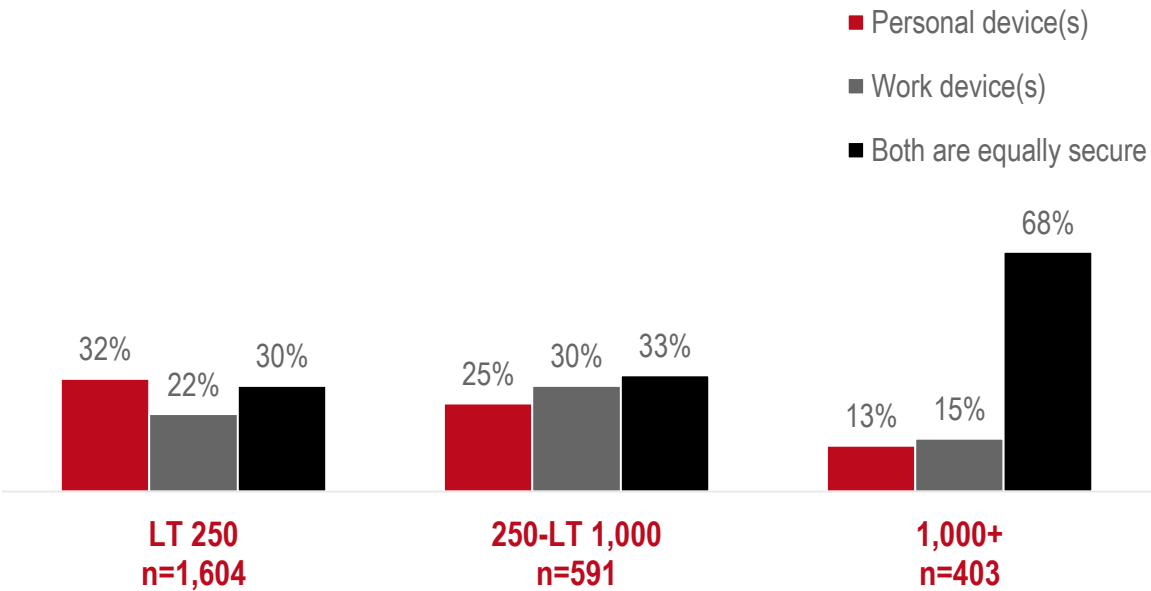
# ASSIGNED WORK DEVICES ARE NOT CONSIDERED TO BE LESS SECURE THAN PERSONAL DEVICES

Only around a quarter of employed Americans (24%) and not self-employed Americans (26%) feel their personal device is more secure than their work device. The rest either feel both devices are secure or their work device is more secure; or they aren't sure either way. Any of those suggests a belief that their work device is secure. This belief is strongest among those who work at larger companies (1,000+).

MORE SECURE DEVICE(S) BETWEEN WORK AND PERSONAL



MORE SECURE DEVICE(S) BETWEEN WORK AND PERSONAL  
AMONG THOSE WHO ARE NOT SELF-EMPLOYED

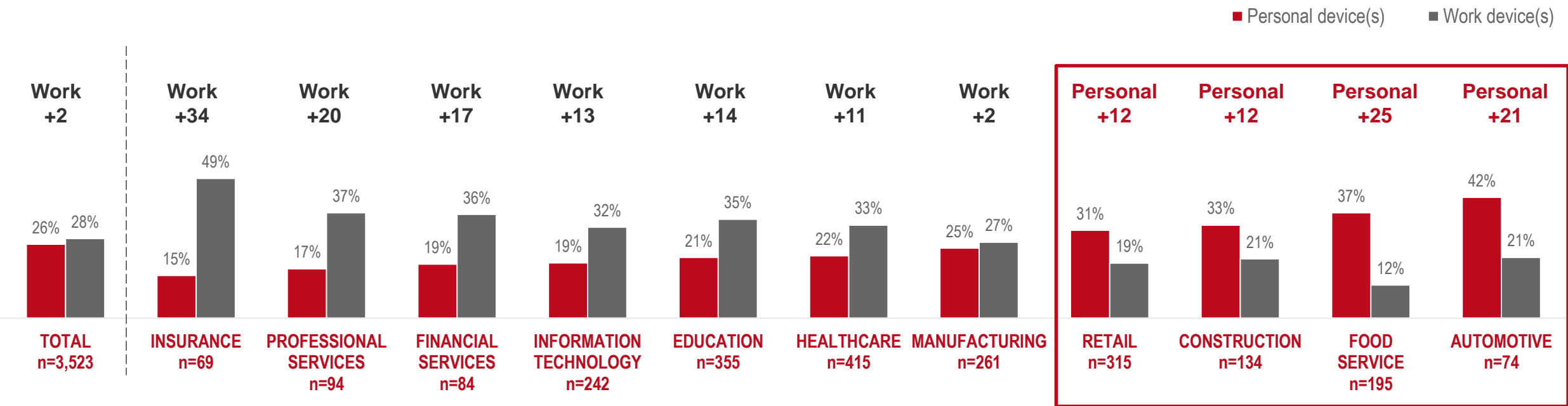


Among those who have a work and/or personal device: Do you believe your work device(s) or your personal device(s) are more secure?

# IN SEVERAL INDUSTRIES, NON SELF-EMPLOYED AMERICANS SAY THEIR WORK DEVICES ARE MORE SECURE THAN THEIR PERSONAL DEVICES

Those in Insurance (49%), Professional Services (37%), and Financial Services (36%) are the most likely to say their work devices are more secure than their personal devices.

## MORE SECURE DEVICE(S) BETWEEN WORK AND PERSONAL *AMONG THOSE WHO ARE NOT SELF-EMPLOYED AND HAVE A WORK AND/OR PERSONAL DEVICE*

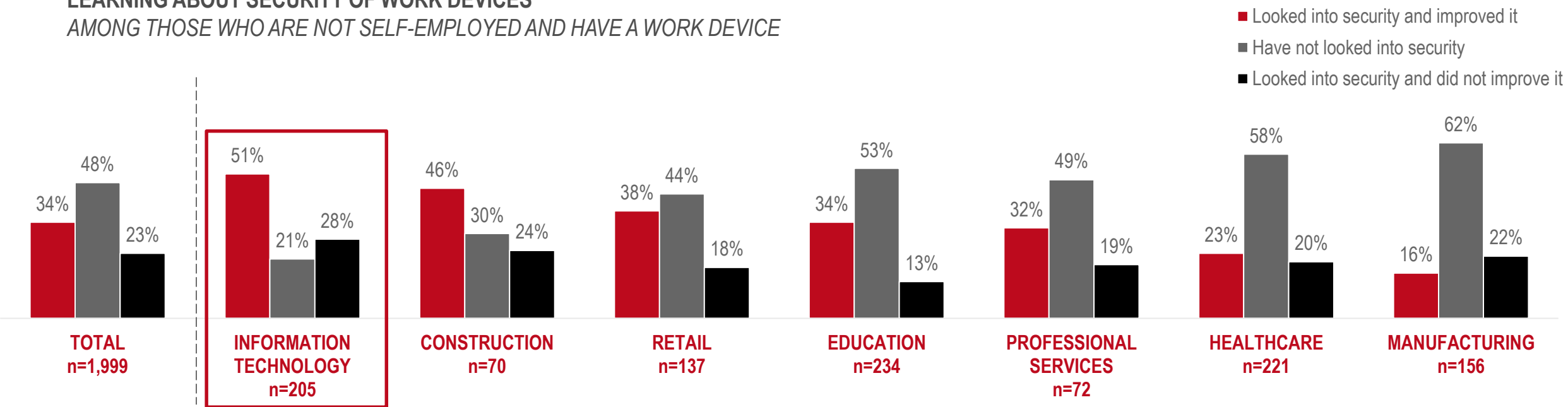


Among those who have a work and/or personal device: Do you believe your work device(s) or your personal device(s) are more secure?

# ALMOST HALF OF EMPLOYEES DO NOT REVIEW THE SECURITY SETTINGS ON THEIR EMPLOYER-PROVIDED DEVICES


Employees take for granted security settings on their work devices – close to half (48%) have not taken any steps to improve their data and identity protection on their work devices. Perhaps given their natural inclinations and type of work, employees in the IT industry (51%) are far more likely to personally improve their work device security compared to employees overall (34%).

LEARNING ABOUT SECURITY OF WORK DEVICES  
AMONG THOSE WHO ARE NOT SELF-EMPLOYED AND HAVE A WORK DEVICE



Among those who have a work device: Have you taken any steps to learn about or improve upon the security of your work devices?

# APPENDIX

**CARBONITE**  **+** **WEBROOT**  
an openstack company an openstack company

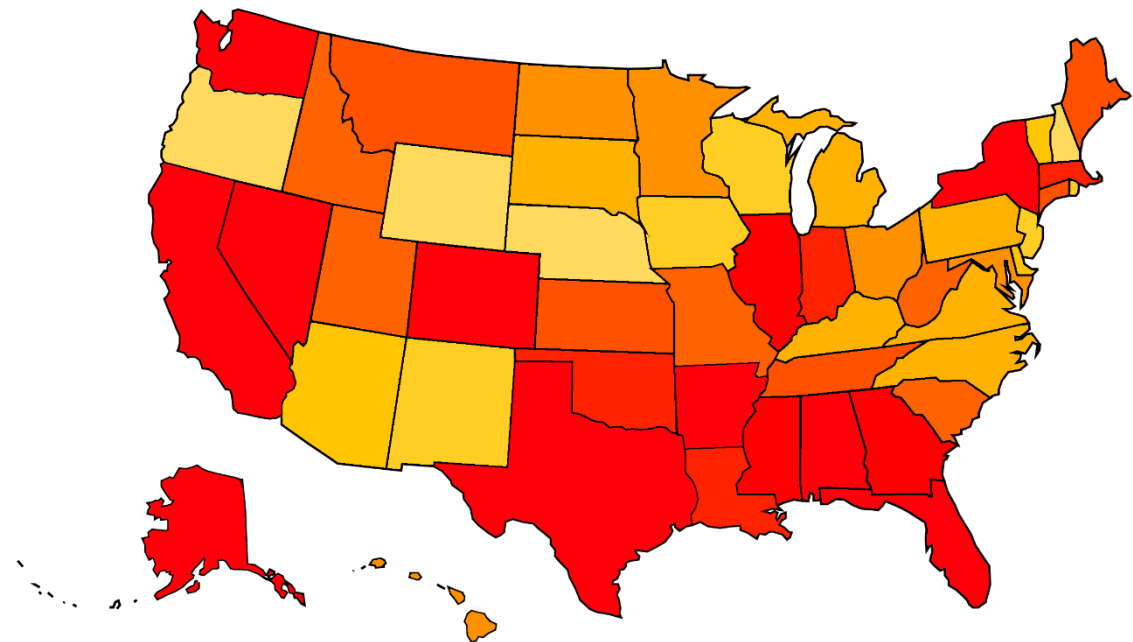
# APPENDIX A: CYBER HYGIENE RISK INDEX – BREAKOUTS



# % PASSING EACH CYBER HYGIENE RISK INDEX METRIC

% PASSING EACH CYBER HYGIENE RISK INDEX METRIC	%
DO THEY BACKUP THEIR DATA?	80%
HAVE THEY AVOIDED LOSING A DEVICE OR DISCARDING A DEVICE WITHOUT WIPING THE DATA FIRST?	72%
HAVE THEY NOT HAD THEIR ID STOLEN?	66%
HAVE THEIR DEVICES NOT BEEN IMPACTED BY MALWARE?	61%
HAVE THEY AVOIDED BEING A VICTIM OF PHISHING?	39%
DO THEY USE ANTI-VIRUS SOFTWARE?	83%
DO THEY NOT SHARE PASSWORDS WITH OTHERS?	66%
DO THEY AVOID REUSING PASSWORDS?	51%
DO THEY KEEP THEIR SOCIAL MEDIA PRIVATE?	37%
DO THEY FOLLOW AT LEAST FIVE CYBERSECURITY BEST PRACTICES?	45%

# STATE RISK INDEX – MOST TO LEAST RISKY



State Risk Index - Most to Least Risky		
1	New York	
2	California	
3	Texas	
4	Alabama	
5	Arkansas	
6	Washington	
7	Florida	
8	Alaska	
9	Nevada	
10	Colorado	
11	Georgia	
12	Illinois	
13	Mississippi	
14	Louisiana	
15	Oklahoma	
16	Indiana	
17	Massachusetts	
18	Connecticut	
19	Tennessee	
20	Kansas	
21	Montana	
22	Maine	
23	Utah	
24	South Carolina	
25	Idaho	
26	West Virginia	
27	Missouri	
28	Ohio	
29	Maryland	
30	Hawaii	
31	North Dakota	
32	Minnesota	
33	North Carolina	
34	South Dakota	
35	Virginia	
36	Michigan	
37	Pennsylvania	
38	Kentucky	
39	Arizona	
40	Delaware	
41	Vermont	
42	Rhode Island	
43	Iowa	
44	Wisconsin	
45	New Mexico	
46	New Jersey	
47	Oregon	
48	Wyoming	
49	New Hampshire	
50	Nebraska	

# CYBER HYGIENE RISK INDEX GRADE BREAKOUTS BY STATE – MOST TO LEAST RISKY

CYBER HYGIENE GRADE	NY #1	CA #2	TX #3	AL #4	AR #5	WA #6	FL #7	AK #8	NV #9	CO #10	GA #11	IL #12	MS #13	LA #14	OK #15	IN #16	MA #17
A (90-100%)	6%	8%	9%	7%	8%	11%	7%	12%	7%	13%	7%	11%	13%	20%	13%	9%	11%
B (80-89%)	6%	8%	14%	9%	10%	13%	18%	10%	13%	13%	16%	12%	17%	12%	11%	18%	16%
C (70-79%)	16%	14%	10%	19%	18%	12%	12%	17%	18%	12%	20%	19%	17%	11%	18%	15%	18%
D (60-69%)	13%	13%	15%	19%	16%	16%	21%	15%	17%	19%	17%	18%	11%	15%	22%	27%	17%
F (0-59%)	60%	57%	52%	47%	49%	48%	43%	45%	45%	43%	39%	40%	42%	41%	36%	31%	37%

# CYBER HYGIENE RISK INDEX GRADE BREAKOUTS BY STATE – MOST TO LEAST RISKY

CYBER HYGIENE GRADE	CT #18	TN #19	KS #20	MT #21	ME #22	UT #23	SC #24	ID #25	WV #26	MO #27	OH #28	MD #29	HI #30	ND #31	MN #32	NC #33	SD #34
A (90-100%)	15%	14%	14%	13%	12%	12%	16%	13%	13%	11%	16%	15%	13%	16%	11%	13%	12%
B (80-89%)	16%	16%	14%	10%	16%	18%	14%	10%	19%	16%	9%	15%	14%	13%	17%	21%	15%
C (70-79%)	13%	17%	15%	24%	16%	19%	13%	25%	18%	24%	24%	20%	20%	13%	19%	21%	26%
D (60-69%)	20%	16%	21%	16%	18%	12%	18%	21%	9%	16%	12%	13%	23%	22%	18%	12%	13%
F (0-59%)	35%	37%	36%	36%	38%	38%	39%	31%	41%	33%	39%	37%	30%	36%	34%	33%	34%

# CYBER HYGIENE RISK INDEX GRADE BREAKOUTS BY STATE – MOST TO LEAST RISKY

CYBER HYGIENE GRADE	VA #35	MI #36	PA #37	KY #38	AZ #39	DE #40	VT #41	RI #42	IA #43	WI #44	NM #45	NJ #46	OR #47	WY #48	NH #49	NE #50
A (90-100%)	17%	15%	15%	17%	17%	18%	15%	14%	12%	13%	18%	17%	15%	17%	18%	20%
B (80-89%)	11%	16%	14%	20%	17%	15%	17%	20%	16%	24%	15%	19%	16%	15%	16%	21%
C (70-79%)	21%	14%	20%	11%	13%	14%	19%	13%	20%	16%	17%	19%	22%	24%	18%	16%
D (60-69%)	13%	21%	17%	17%	17%	21%	16%	21%	23%	15%	18%	14%	17%	13%	17%	14%
F (0-59%)	38%	34%	33%	35%	35%	33%	33%	32%	29%	33%	32%	31%	30%	30%	31%	29%

# APPENDIX B: CURRENT STATE OF CYBER HYGIENE



# AMERICANS NAME THE MOST DAMAGING CYBER-RELATED ATTACKS TODAY

## MOST DAMAGING CYBER-RELATED ATTACKS TODAY

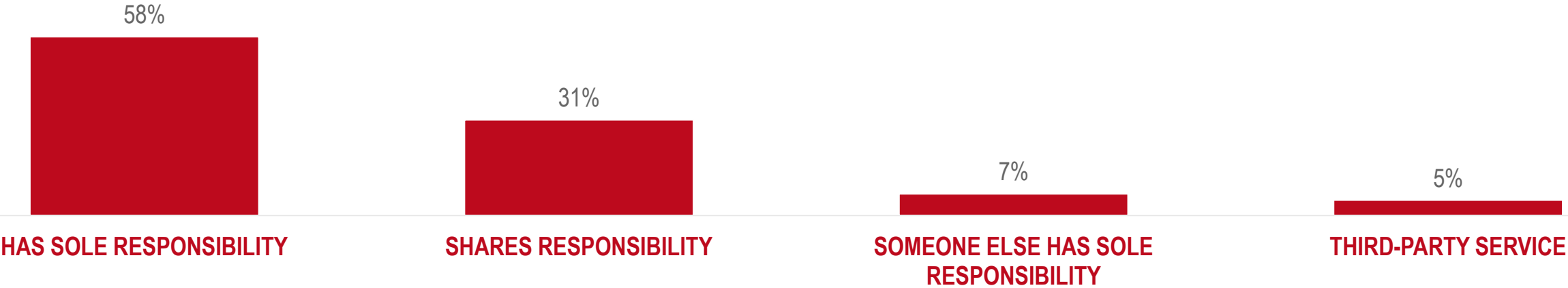
*N=10,000*

	%
Virus / Malware (computer worm, ransomware, adware, drive-by, etc.)	27%
Identity theft / Personal information (theft)	26%
Hacking (General)	16%
Finance / Banking / Credit or debit card (theft)	14%
Phishing	13%
Cyberbullying	7%
Attack on institution (government, business, hospital, etc.)	5%
DoS / DDoS attack	4%
Data breach	4%
Spam / Spamware	3%
Social media	3%
Software (spyware, keystroke logging)	2%
Attack on elections	2%
Healthcare (records hacked, fraud, etc.)	2%
Attack on utilities	2%
Man-in-the-middle attack	1%
Attack by foreign country	1%
Non-specific response (personal, computer, email, etc.)	12%
Other	14%
I don't know / None	19%

What types of cyber-related attacks do you think are most damaging today? Please think of up to 3 cyber-related types of attacks.

# RESPONSIBILITY FOR CYBERSECURITY DECISION-MAKING

RESPONSIBILITY FOR CYBERSECURITY DECISION-MAKING  
*N=10,000*



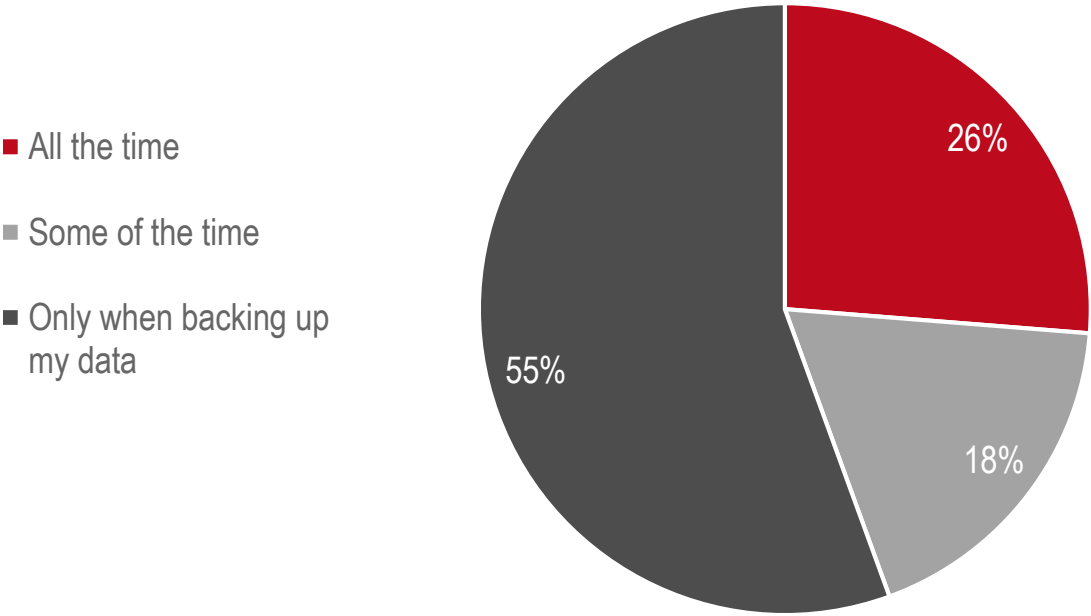
Who is responsible for the cybersecurity decision-making in your household or home-based business?

# APPENDIX C: CYBER HYGIENE BEHAVIORS



# FREQUENCY OF KEEPING EXTERNAL HARD DRIVE PLUGGED INTO COMPUTER

FREQUENCY OF KEEPING EXTERNAL HARD DRIVE PLUGGED INTO COMPUTER  
AMONG THOSE WHO REGULARLY BACKUP DATA TO AN EXTERNAL HARD DRIVE, n=3,018



Among those who regularly backup data to an external hard drive: When do you have your external hard drive plugged into your computer?

# CONSEQUENCES OF IDENTITY THEFT

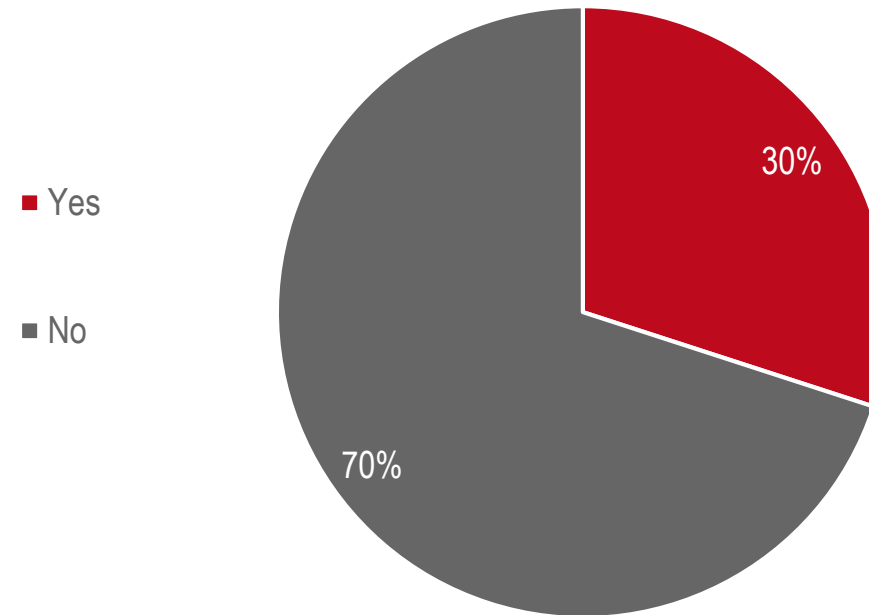
CONSEQUENCES OF IDENTITY THEFT AMONG THOSE WHO HAVE HAD THEIR IDENTITY STOLEN, n=2,459	%
Misuse of credit card or debit card / ATM card	48%
Private information was stolen	35%
Social media accounts were misused	27%
Creation of new debt such as a loan or mortgage	19%
Criminal took control of bank accounts	19%
Credit (FICO) scores declined	18%
Tax returns were stolen	16%
Medical records were stolen	14%
Other	3%
None of the above	2%
Don't know	2%

Among those who have had their identity stolen: What were the main consequences of the identity theft incident(s)?

## % WHO USE AN IDENTITY PROTECTION SERVICE

---

**% WHO USE AN IDENTITY PROTECTION SERVICE**  
*AMONG THOSE WHO HAVE A WORK AND/OR PERSONAL DEVICE, n=9,978*



Among those who have a work and/or personal device: Do you use an identity protection service such as LifeLock, ID Watch Dog or others?

# FREQUENCY OF ALLOWING COMPUTER OR MOBILE DEVICE TO SAVE PASSWORD

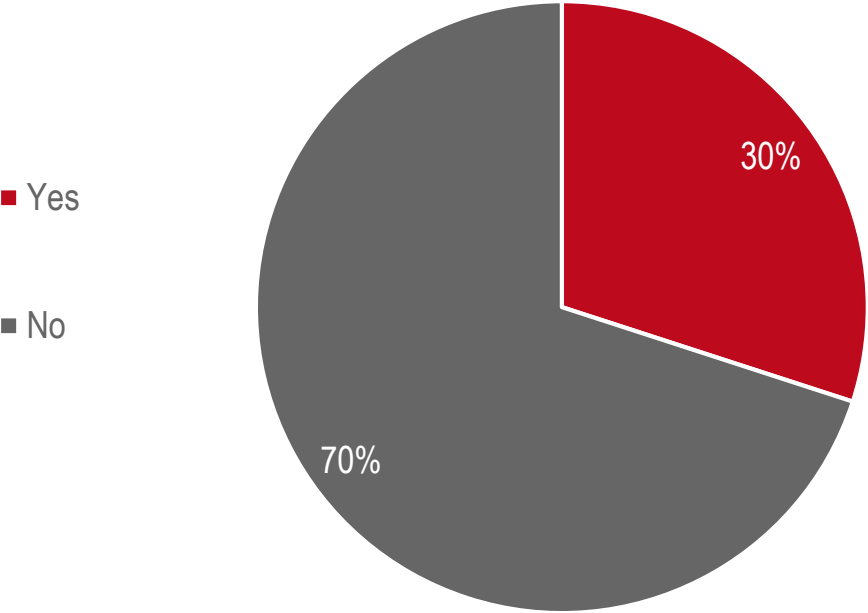
<b>FREQUENCY OF ALLOWING COMPUTER OR MOBILE DEVICE TO SAVE PASSWORD</b> <i>AMONG THOSE WHO HAVE A WORK AND/OR PERSONAL DEVICE, n=9,978</i>	<b>%</b>
All the time	19%
Majority of the time	23%
About half the time	15%
Occasionally / rarely	19%
I never have my device save login information	24%

Among those who have a work and/or personal device: When you are able, how often, if ever, do you allow your computer or mobile device to save your password for an online account? Meaning, your device will automatically populate the username and password the next time you sign-in.

# % WHO USE A PASSWORD MANAGER

---

**% WHO USE A PASSWORD MANAGER**  
*AMONG THOSE WHO HAVE A WORK AND/OR PERSONAL DEVICE, n=9,978*

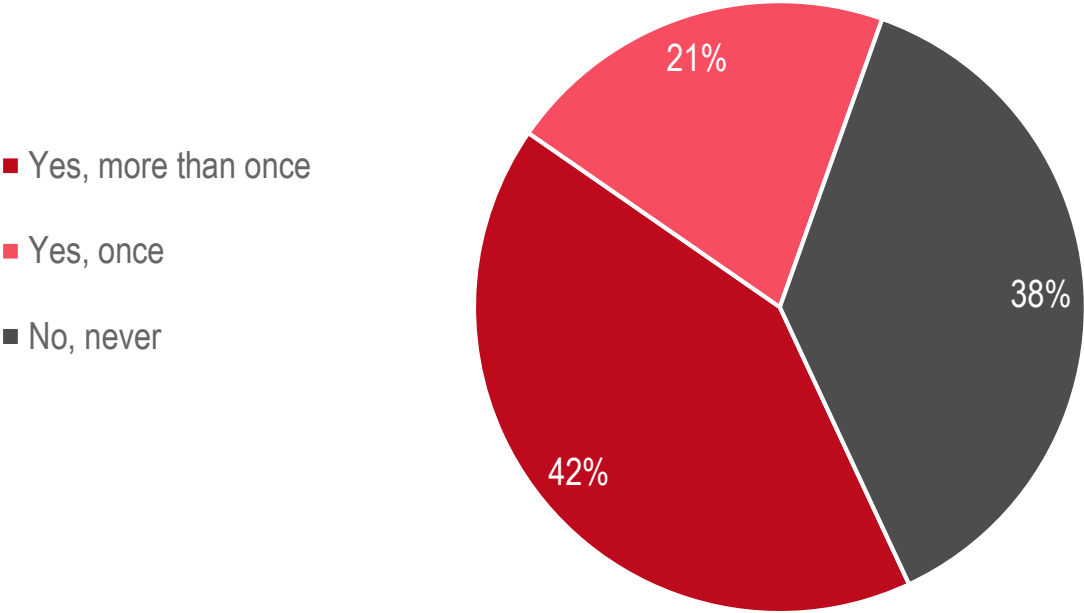


Among those who have a work and/or personal device: Do you use a password manager, or other software tool that assists in generating and retrieving complex passwords?

# % WHO HAVE EVER USED THE SAME PASSWORD FOR A PERSONAL AND BUSINESS ACCOUNT

---

**% WHO HAVE EVER USED THE SAME PASSWORD FOR A PERSONAL AND BUSINESS ACCOUNT**  
*AMONG THOSE WHO ARE EMPLOYED, n=5,686*



Among those who are employed: Have you ever, even once, used the same password for a personal and business account?

# CHANGES MADE TO ONLINE BEHAVIOR AFTER CYBER-RELATED ATTACK

CHANGES MADE TO ONLINE BEHAVIOR AFTER CYBER-RELATED ATTACK <i>N=10,000</i>	%
Regularly monitor bank accounts	24%
Take precautions before clicking a link in an email	21%
Regularly monitor credit card statements	18%
Keep software up to date	18%
Regularly check credit reports	17%
Enable two-factor authentication	15%
Use an ad-blocking plug in (block pop-ups)	10%
Limit online purchases	10%
Deactivate Bluetooth when not in use	9%
Regularly use a password manager	9%
Use mobile payment, such as Apple Pay, Google Pay or Samsung Pay	8%
Regularly employ credit monitoring services	7%
Deactivate NFC (near field communication) when not using mobile payment	3%
I don't know anyone who was a victim of a cyber-attack	27%
None of these	19%

Which of the following changes, if any, did you make to your online behavior as a result of you or someone you know being negatively affected by a cyber-related attack?

# APPENDIX D: ADDITIONAL CLASSIFICATION BREAKOUTS



# AMERICANS WHO HAVE SUFFERED FROM IDENTITY THEFT ARE LIKELY TO CHANGE THEIR ONLINE BEHAVIOR

---

Americans shouldn't wait until they have been impacted by a cyber-related attack to change their online behavior. However, those who have had their identity stolen are very likely to have changed their online behavior due to their own or someone else's experience.

- Over three-quarters (78%) of those who have had their identity stolen have made changes to their online behavior as a result of them or someone they know being negatively affected by a cyber-related attack, while less than half (47%) of those who have not had their identity stolen have changed their online behavior.
- Among those who know someone who was a victim of a cyber-related attack, 88% of Americans who have had their identity stolen have changed their online behavior, compared to 70% of Americans who have not had their identity stolen.
- Those who have had their identity stolen are more likely than those who have not to perform any of the changes listed, including regularly monitoring bank accounts (31% vs 22%), regularly monitoring credit card statements (26% vs 16%), keeping software up to date (26% vs 16%), and regularly checking credit reports (25% vs 15%).
- Americans who have had their identity stolen (88%) are more likely than those who have not (79%) to regularly backup data.
- Nearly three-quarters (73%) of employed Americans who have had their identity stolen have looked into the security of their work devices, while 59% of those who have not say the same thing.
- Those who have lost a device (71%) or discarded a device without wiping the data (71%) are the next most likely to have experienced or know someone who has experienced a cyber-attack and made a change to their online behavior.

# SOCIAL MEDIA ACCOUNTS CURRENTLY USED

SOCIAL MEDIA ACCOUNTS CURRENTLY USED <i>N=10,000</i>	%
Facebook	77%
Instagram	46%
Twitter	37%
Pinterest	33%
Snapchat	30%
LinkedIn	27%
TikTok	13%
Tumblr	9%
Other	1%
I don't have any social media accounts	12%

Which of the following social media accounts, if any, do you currently have?

# SELF-EMPLOYMENT

<b>SELF-EMPLOYMENT STATUS</b> <i>AMONG THOSE WHO ARE EMPLOYED, n=5,686</i>	<b>%</b>
Yes, as a freelancer	20%
Yes, as the owner of a business	18%
No	62%

<b>SELF-EMPLOYMENT AS PRIMARY OR SIDE JOB</b> <i>AMONG THOSE WHO OWN A BUSINESS, n=1,027</i>	<b>%</b>
Primary job	79%
On the side from my primary	21%

Among those who are employed: Are you self-employed? That is, you do work for yourself as a freelancer or as the owner of a business? This can include full-time or part-time work. / Among those who own a business: For the work you do as the owner of a business, is this your primary job or part-time on the side from your primary job?

# HOME-BASED BUSINESS

LOCATION OF BUSINESS AMONG THOSE WHO OWN A BUSINESS, n=1,027	%	ELECTRONIC DEVICES USED IN HOME-BASED BUSINESS AMONG THOSE WHO OWN A BUSINESS THAT IS BASED OUT OF THEIR HOME, n=549	%
My business is based out of my home	53%	I use the same devices for personal use and my home-based business	79%
My business is located in an office space or commercial setting	47%	I use separate devices for personal use and my home-based business	21%

Among those who own a business: Which of the following best describes where the business you own is located? / Among those who own a business that is based out of their home: Which of the following best describes the electronic devices you use for your home-based business?

# PERSONAL DEVICES OWNED, USES FOR PERSONAL DEVICES OWNED, AND WINDOWS OPERATING SYSTEMS USED

PERSONAL DEVICES OWNED <i>N=10,000</i>	%
Windows laptop/desktop	56%
Android phone	50%
iOS (Apple) phone	44%
Mac (Apple) laptop (MacBook) / desktop (iMac)	17%
Other	5%
I don't have any personal electronic devices	1%
USES FOR PERSONAL DEVICES OWNED <i>AMONG THOSE WHO OWN A PERSONAL DEVICE, n=9,874</i>	%
Personal use	95%
Work	37%
School	12%
Other	1%

WINDOWS OPERATING SYSTEMS USED <i>AMONG THOSE WHO OWN A PERSONAL WINDOWS DEVICE, n=5,647</i>	%
Windows 10	79%
Windows 7	14%
Windows XP	10%
Windows 8	8%
Windows Vista	3%
Other	1%

Which of the following personal electronic devices, if any, do you own? / Among those who own a personal device: For which of the following reasons do you use the personal electronic devices that you own? / Among those who own a personal Windows device: Which of the following Windows operating systems do you use?

# INDUSTRY OF EMPLOYMENT

INDUSTRY OF EMPLOYMENT AMONG THOSE WHO ARE EMPLOYED, n=5,686	%
Accounting	3%
Agriculture	1%
Automotive	2%
Banking	3%
Consumer Products	1%
Construction	6%
Education	8%
Entertainment	2%
Energy	1%
Financial Services	2%
Food Service	6%
Healthcare	9%
Hotel and Hospitality	2%
Insurance	2%
Information Technology	11%
Law	1%
Manufacturing	6%
Professional Services	4%
Real Estate	1%
Retail	8%
Utilities	1%
Other	19%

Among those who are employed: In which of the following industries do you currently work in?

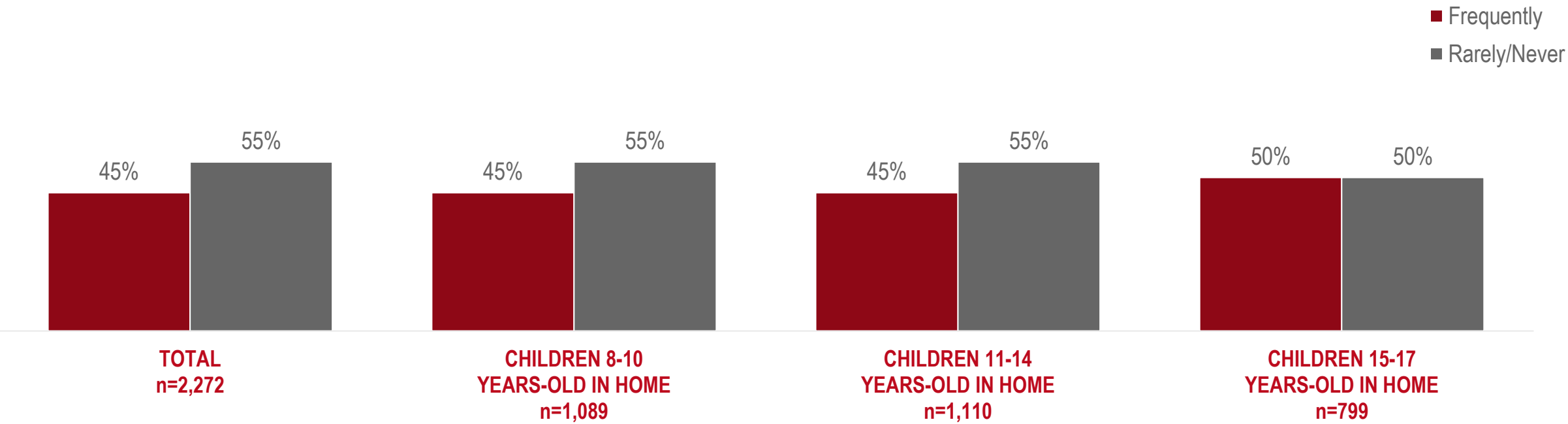
# DEVICES PROVIDED BY EMPLOYER

DEVICES PROVIDED BY EMPLOYER <i>AMONG THOSE WHO ARE EMPLOYED, n=5,686</i>	%
Windows laptop/desktop	38%
Android phone	22%
iOS (Apple) phone	20%
Mac (Apple) laptop (MacBook) / desktop (iMac)	15%
Other	1%
My company does not provide me with any electronic device	36%

Among those who are employed: Which of the following electronic devices, if any, does your company or employer provide for you?

# FREQUENCY OF DEPENDING ON CHILDREN FOR KNOWLEDGE AND HELP WITH ONLINE CYBERSECURITY

FREQUENCY OF DEPENDING ON CHILDREN FOR KNOWLEDGE AND HELP WITH ONLINE CYBERSECURITY  
AMONG PARENTS WHO HAVE CHILDREN OVER SEVEN YEARS-OLD



Among parents who have children over seven years-old: How often, if ever, do you depend on your child(ren) for knowledge and help with online cybersecurity?

# HOME OWNERSHIP STATUS AND ACTIVELY INVESTING IN STOCK MARKET

HOME OWNERSHIP STATUS <i>N=10,000</i>	%
I own my house or townhouse	56%
I rent my house or townhouse	13%
I own my condo	2%
I rent my apartment	16%
I live with someone else and do not pay rent	11%
Other	1%

ACTIVELY INVESTING IN STOCK MARKET <i>N=10,000</i>	%
Yes	31%
No	69%

What is your home ownership status? / Do you actively invest money in the stock market?

# ACTIVITIES AND INTERESTS

ACTIVITIES AND INTERESTS <i>N=10,000</i>	%
Video gaming	35%
Gardening	33%
Board games/card games	31%
Outdoors recreation – solo	24%
Photography	24%
Outdoors recreation – team or group	20%
Collectables	15%
Painting	15%
Web design	9%
Coding or programming	7%
None of these	20%

Which of the following activities and interests, if any, do you do regularly?

# FREQUENCY OF NEWS CONSUMPTION AND TYPES OF NEWS CONSUMED

<b>FREQUENCY OF NEWS CONSUMPTION</b> <i>N=10,000</i>	<b>%</b>
Every day consistently	45%
Several times a week	29%
Once a week	8%
A few times a month	5%
Occasionally	9%
Never	5%

<b>TYPES OF NEWS CONSUMED</b> <i>AMONG THOSE WHO READ, WATCH OR LISTEN TO THE NEWS, n=9,546</i>	<b>%</b>
National	58%
Local/metro	51%
Sports	39%
International	35%
Technology	30%
Business	27%
Arts/entertainment	25%
Travel/leisure	25%
Popular culture	22%
Product reviews	19%
Opinion/editorial	18%
Other	3%

How often, if ever, do you read, watch, or listen to the news? / Among those who read, watch, or listen to the news: Which types of news do you consistently read, watch, or listen to?

# FREQUENCY OF CONDUCTING MOBILE BANKING ON PHONE AND USE OF AUTOMATED PAYMENTS FOR BILLS

FREQUENCY OF CONDUCTING MOBILE BANKING ON PHONE <i>N=10,000</i>	%
All the time	29%
Sometimes	27%
Rarely	12%
Never	31%

USE OF AUTOMATED PAYMENTS FOR BILLS <i>N=10,000</i>	%
Yes, for all or almost all of my payments	24%
Yes, for some of my payments	34%
Yes, for one of my payments	8%
No, for none of my payments	33%

How often, if at all, do you conduct mobile banking on your phone? / When you pay for certain bills, such as your utility bill or your rent or mortgage, are your payments automated? Meaning, without taking any action other than the set-up, you automatically pay a bill periodically.

# SHARE PASSWORDS FOR STREAMING VIDEO SERVICES AND WAYS OF KEEPING TRACK OF PASSWORDS

SHARE PASSWORDS FOR STREAMING VIDEO SERVICES <i>N=10,000</i>	%
Yes, several	15%
Yes, one	16%
No, none	69%

WAYS OF KEEPING TRACK OF PASSWORDS <i>N=10,000</i>	%
I memorize them	37%
I have them written on paper	31%
I use a password management program	14%
I have them written on a document on my computer	10%
I save them in the internet browser	8%

Do you share passwords, or use someone else's password, for streaming video services, such as Netflix, Hulu, or HBO? / Which of the following ways best describes how you keep track of your passwords, such as for websites, social media, or email accounts?

# SMART DEVICES/SMART HUB IN HOME, SMART HOME STATUS, AND ATTITUDE TOWARDS DEVICES THAT MAY HAVE A MICROPHONE

SMART DEVICES/SMART HUB IN HOME <i>N=10,000</i>	%
No, I do not have smart devices/a smart hub in my home	62%
Yes, I have smart devices/a smart hub in my home	38%

SMART HOME STATUS <i>AMONG THOSE WHO HAVE SMART DEVICES OR A SMART HUB IN THEIR HOME, n=3,754</i>	%
I have some smart devices (like a Nest thermostat or lights) connected to a phone or smart hub	66%
I have a smart hub but have not connected any devices to it	34%

ATTITUDE TOWARDS DEVICES THAT MAY HAVE A MICROPHONE <i>N=10,000</i>	%
I try to avoid being around devices that may have a microphone	51%
I don't mind being around devices that may have a microphone	49%

Do you have smart devices or a smart hub in your home, like an Amazon Echo or Google Home? / Among those who have smart devices or a smart hub in their home: Which of the following best describes your home? / Which of the following best describes you:

# **WAKEFIELD**

[WAKEFIELDRESEARCH.COM](https://wakefieldresearch.com)

Copyright ©2020 Wakefield Research. All rights reserved.  
All information contained herein is confidential and proprietary to Wakefield Research.

