

# WAKEFIELD RESEARCH: CYBER HYGIENE RISK INDEX

Assessment of Americans' Cybersecurity Practices

ANALYSIS OF RESULTS

MARCH 2019



# TABLE OF CONTENTS

---

## SECTION

## SLIDE

PURPOSE OF RESEARCH

3

RESEARCH METHODOLOGY

4

KEY FINDINGS

5

CYBER HYGIENE RISK INDEX

10

CYBER HYGIENE SUPERSTARS

17

DETAILED RESEARCH FINDINGS

19

APPENDIX

38

# PURPOSE OF RESEARCH

---

Wakefield Research conducted an online quantitative research study to:

- Better understand attitudes, perspectives, and behaviors related to cyber hygiene
- Enhance the Cyber Hygiene Risk Index to assess on the risks associated with susceptibility to cybercrime in each state

# RESEARCH METHODOLOGY

Wakefield fielded an online survey to 10,000 U.S. consumers (ages 18+) with 200 interviews in each of the 50 US states.



This survey was conducted between February 11<sup>th</sup> and February 25<sup>th</sup>, 2019, using an email invitation and an online survey instrument.

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

**WEBROOT®**  
Smarter Cybersecurity™

## KEY FINDINGS

---

**Despite lacking the basic knowledge needed to protect themselves from cyber-threats, today's Americans are overestimating their levels of cyber hygiene.**

Americans are overconfident in the perceived protection they're getting now. Nearly 9 in 10 (88%) feel that they are currently taking the appropriate steps to protect themselves from cyber-related attacks, but this confidence is misplaced.

Instead, Americans have only a surface-level understanding of the most common types of cyber threats. They can recognize some of the names of the most common cyber-attacks such as malware (79%) or phishing (70%), but for most, that's where their knowledge ends. Very few (less than 1 in 3) actually know what these common cyber-attacks are or what they do.

# KEY FINDINGS

The Cyber Hygiene Risk Index reveals a lack of cyber security preparedness among American consumers. And while there is some gradation in risk, poor levels of cyber hygiene are realized country-wide.

Scores among American consumers ranged from 100% (A+) to 0% (F). However, the average consumer scored a grade of 60%, with only 10% of the total population scoring a 90% or higher (Grade A).

Mississippi and New Hampshire headline our riskiest and least risky states, respectively. And while there is some slight variation in risk levels state to state, our highest performing state (New Hampshire) only scored a 65% (D Grade).

CYBER HYGIENE GRADE	% OF AMERICANS OVERALL N=10,000
A	10%
B	14%
C	17%
D	19%
F	40%

<u>MOST RISKY STATES</u>	<u>LEAST RISKY STATES</u>
1. Mississippi	46. Kentucky
2. Louisiana	47. Idaho
3. California	48. Ohio
4. Alaska	49. North Dakota
5. Connecticut	50. New Hampshire

## KEY FINDINGS

---

**Less than half of Americans have yet to adopt cyber hygiene practices that are now considered the bare minimum when it comes to keeping themselves protected. And among those who have, many are not doing so effectively.**

In an era where cyber threats are becoming more complex with no signs of disappearing, less than half of Americans are refraining from reusing passwords across multiple accounts (37%), making sure their social media accounts are private (36%), and ensuring they are not falling victim to phishing attempts (47%).

Even for those who are adopting basic cyber hygiene, such as backing up their data or using anti-virus software, very few are doing so properly. Instead, the majority are still leaving themselves susceptible to risk by only backing up their data using one method or allowing their anti-virus software to become outdated.



## KEY FINDINGS

---

**Despite low cyber hygiene levels overall, there does exist a finite group of Cyber Hygiene Superstars who are going above and beyond. And these Superstars exist in every state.**

While only reflecting 5% of Americans today, Cyber Hygiene Superstars are embedded in every state. As a group, they score high marks on the benchmark Cyber Hygiene Risk Index, but they are also doing more. Superstars are taking additional steps such as backing up their data using multiple methods, using AV software that is paid for and kept up to date, and using tools like personal VPNs and password managers to ensure that their information is protected.

There is opportunity to use these Superstars as the new blueprint for which every U.S. consumer needs to aspire to. And only when someone adopts the behaviors of these Superstars, are they really practicing the cyber hygiene required to keep them safe today.

# CYBER HYGIENE SUPERSTARS SNAPSHOT

A **Cyber Hygiene Superstar** is someone who is not only taking all of the basic steps necessary in protecting oneself in our Cyber Hygiene Risk Index, but unlike the majority of Americans, they are going above and beyond. Today, Cyber Hygiene Superstars represent only 5% of Americans overall.

## WHO WE ARE



Cyber Hygiene  
Superstars

### Compared to the overall, we are:

- More likely to be Boomers
- More likely to be married or in a relationship
- More likely to live in the suburbs
- Less likely to be parents

### We are:

- Spread across 100% of U.S. states
- The highest Cyber Hygiene Risk Index performers

## OUR CYBER HYGIENE BEHAVIOR

### Compared to the overall, we are:

- Regularly backup data in multiple ways
- Keeps their reliable AV software up to date
- Uses VPN, ID protection & password management services

### Compared to the overall, we are:





- Less likely to fall victim to phishing attempts
- Less likely to lose our identities
- Less likely to use work devices for personal use

# CYBER HYGIENE RISK INDEX

**WEBROOT®**  
Smarter Cybersecurity™

# CYBER HYGIENE RISK INDEX METHODOLOGY

Wakefield created a new benchmark to provide Webroot with an objective and intuitive assessment of risk. Below, we outline key points of differentiation from last year’s risk index:

2019 CYBER HYGIENE RISK INDEX		2018 RISK INDEX
	<b>Uses a Pass / Fail grade for each metric</b> This is a straight-forward, intuitive assessment of risk.	Used as weighted / points-based system. This point-based allocation approach was subjective and not defensible.
	<b>Contains the 10 key metrics</b> Simplifies measurement of risk by focusing on the 10 baseline metrics on cyber hygiene all Americans should be practicing.	Key areas of risk left out or contained extraneous information the Webroot team deemed unnecessary.
	<b>Quantifiable large-scale analysis at the state level</b> Total sample of 10,000 Americans, including 200 in each state. Study achieves statistically significant findings at the state level.	A survey of 4,290 Americans, with varying sample sizes at the state level (from 40 to 195 interviews/state). Majority of states below 100 total interviews (does not meet statistical significant threshold).
	<b>Introduces a grading system</b> Intuitive, creative approach for media generation.	Not applicable.

# 2019 CYBER HYGIENE RISK INDEX

The 2019 Cyber Hygiene Risk Index was constructed using the following 10 survey metrics. These metrics all follow a pass/fail (yes/no) format:

## 10 BENCHMARK CYBER HYGIENE RISK INDEX METRICS



1. Do they backup their data?
2. Have they lost a device without recovering it or given away a device without wiping memory?
3. Have they had their ID stolen?
4. Have they been impacted by Malware?
5. Have they been a victim of phishing?
6. Do they use AV software?
7. Do they share passwords with others?
8. Do they reuse passwords?
9. Do they keep their social media public?
10. Do they practice good online behavior?

**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.*

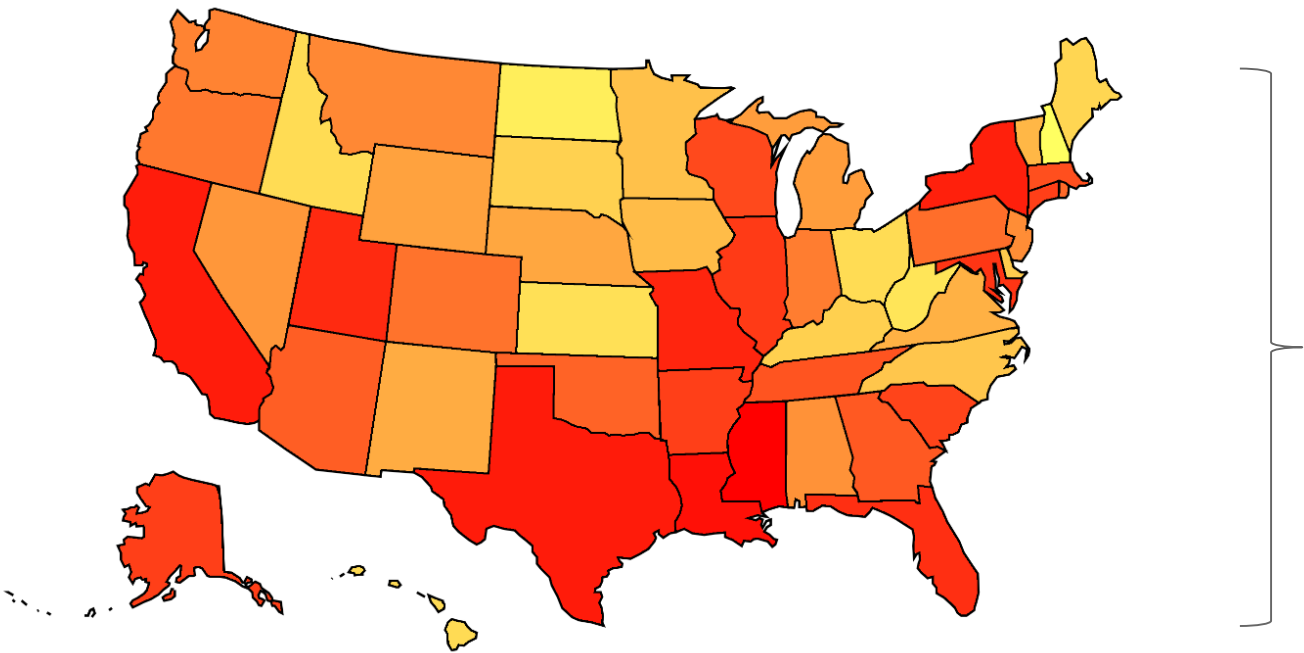
# OVERALL AMERICANS RISK SCORECARD

Few Americans are practicing all of the 10 benchmark metrics needed to protect themselves from cybercrime. Among our total sample of 10,000 general population consumers, the average American scored a 60% on our index, and only 10% scored a mark of 90% or higher (Grade A).

CYBER HYGIENE GRADE	% OF AMERICANS OVERALL N=10,000
A (90-100%)	10%
B (80-89%)	14%
C (70-79%)	17%
D (60-69%)	19%
F (0-59%)	40%

The average American scored a **60% (D)** on our index.

# RISKIEST STATES IN AMERICA



## TOP 5 MOST RISKY STATES

1	MISSISSIPPI
2	LOUISIANA
3	CALIFORNIA
4	ALASKA
5	CONNECTICUT

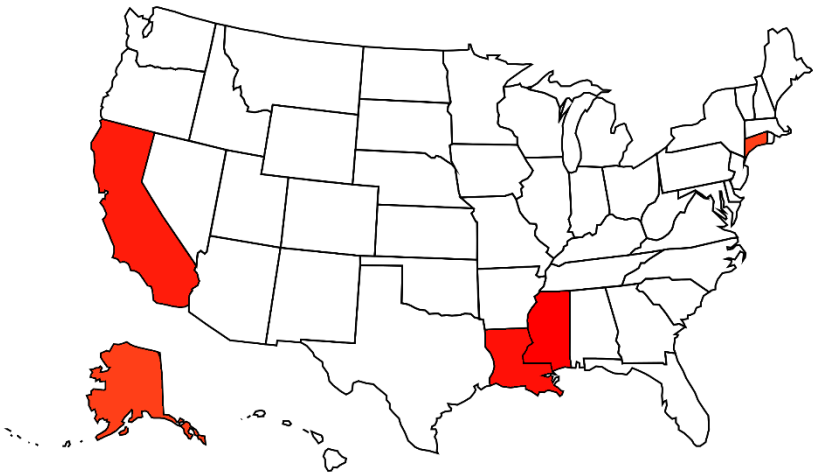


## TOP 5 LEAST RISKY STATES

46	KENTUCKY
47	IDAHO
48	OHIO
49	NORTH DAKOTA
50	NEW HAMPSHIRE

# MOST RISKY STATES SCORECARD

Average scores across our riskiest states ranged from 55% - 57%.

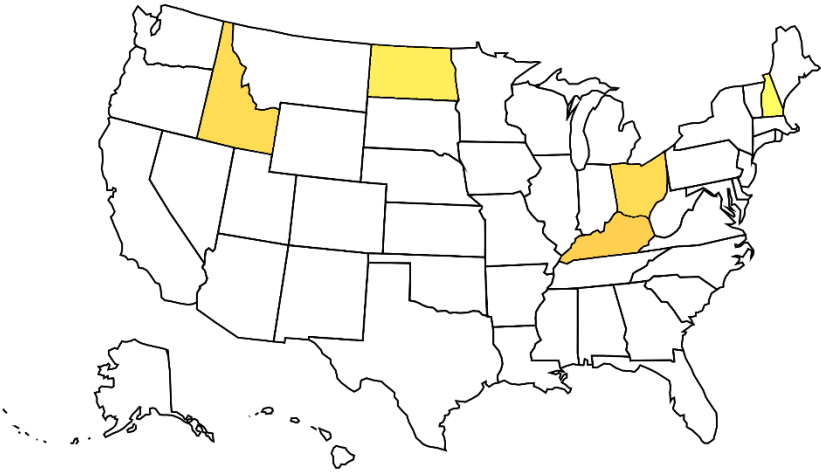


CYBER HYGIENE GRADE	MISSISSIPPI (#1)	LOUISIANA (#2)	CALIFORNIA (#3)	ALASKA (#4)	CONNECTICUT (#5)
A (90-100%)	6%	5%	8%	11%	6%
B (80-89%)	11%	9%	10%	13%	16%
C (70-79%)	15%	19%	16%	12%	13%
D (60-69%)	16%	18%	20%	15%	19%
F (0-59%)	53%	51%	48%	50%	46%
AVERAGE GRADE	55% (F)	56% (F)	56% (F)	56% (F)	57% (F)



# LEAST RISKY STATES SCORECARD

Average scores across our least risky states ranged from 62% - 65%.



CYBER HYGIENE GRADE	NEW HAMPSHIRE (#50)	NORTH DAKOTA (#49)	OHIO (#48)	IDAHO (#47)	KENTUCKY (#46)
A (90-100%)	18%	14%	16%	10%	11%
B (80-89%)	19%	14%	15%	15%	16%
C (70-79%)	13%	20%	18%	21%	20%
D (60-69%)	17%	22%	21%	22%	19%
F (0-59%)	33%	31%	32%	33%	35%
AVERAGE GRADE	65% (D)	64% (D)	64% (D)	62% (D)	62% (D)

# DETAILED RESEARCH FINDINGS

**WEBROOT®**  
Smarter Cybersecurity™

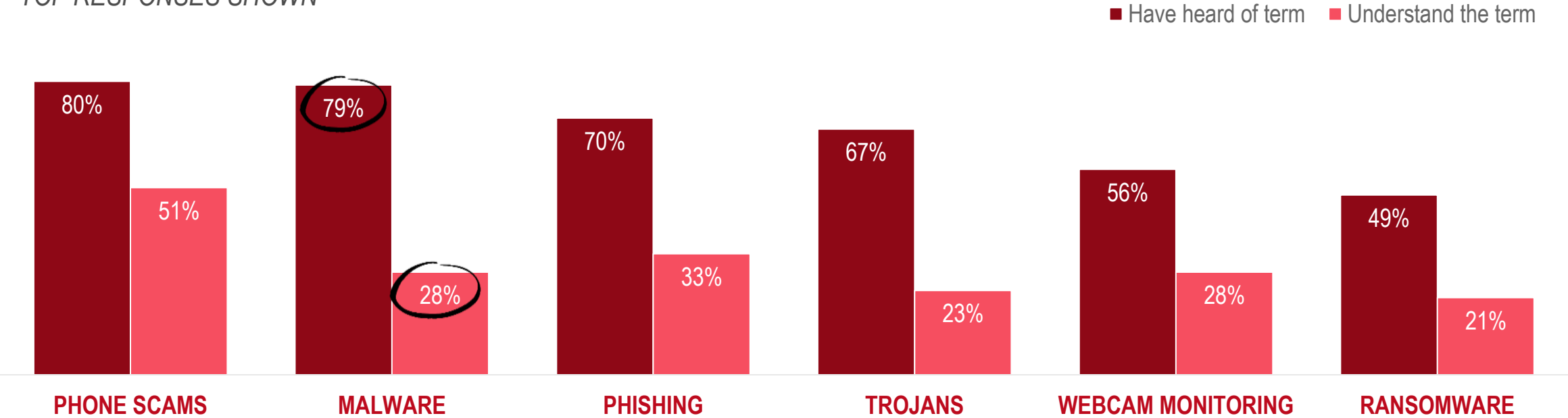
# THE CURRENT STATE OF CYBER HYGIENE

**WEBROOT®**  
Smarter Cybersecurity™

# AMERICANS DON'T UNDERSTAND WHAT COMMON CYBER-ATTACKS REALLY ARE

While Americans indicate that they've heard of some of the most common cyber-attack terms when prompted, very few actually understand what those cyber-attacks are. Malware has the largest discrepancy, where 79% of Americans have heard of this term, but only 28% can confidently explain what it is.

CYBER-ATTACKS AMERICANS HAVE HEARD OF VS. THOSE THEY UNDERSTAND  
TOP RESPONSES SHOWN

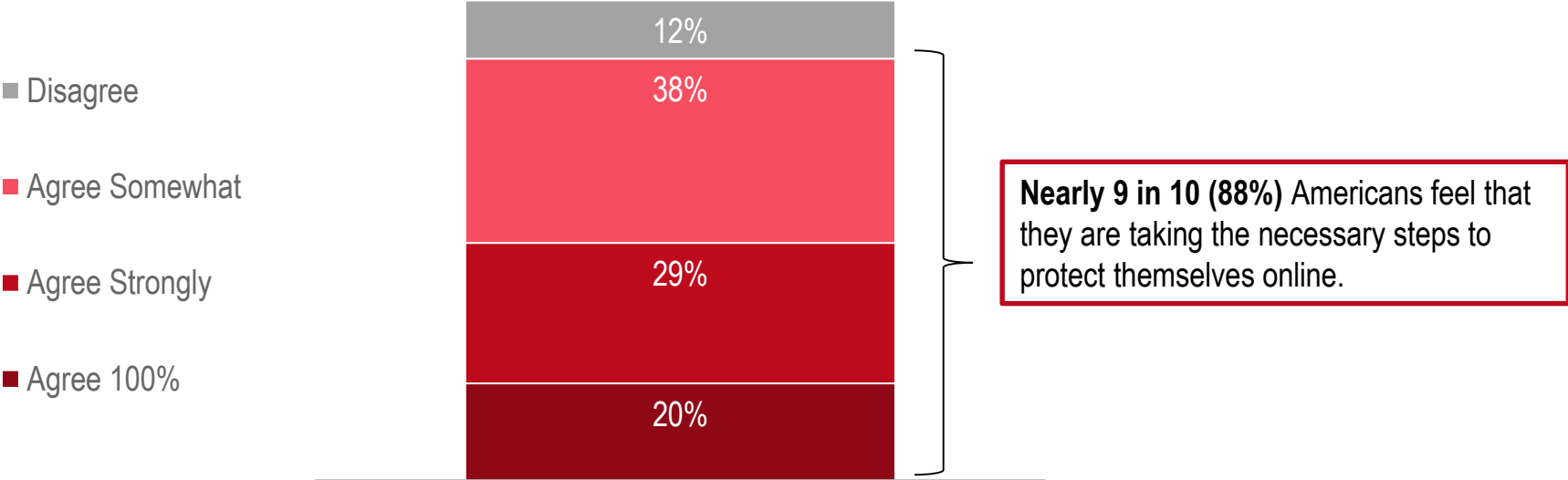


Which of the following cyber-related attacks, if any, have you heard of before today? Now, which of these terms, if any, would you be able to confidently explain to someone else (define and provide examples of).

# AMERICANS OVERESTIMATE THEIR CURRENT LEVELS OF CYBER HYGIENE

Despite admitting a lack of basic knowledge in this area, Americans are overestimating their current levels of cyber hygiene. Roughly 9 in 10 (88%) Americans agree that they're taking the appropriate steps to protect themselves from cyber-related attacks, including half (49%) who agree strongly or agree 100%.

## HOW STRONGLY AMERICANS BELIEVE THEY ARE PROTECTING THEMSELVES ONLINE









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.

# CYBER HYGIENE BEHAVIORS

**WEBROOT**<sup>®</sup>  
Smarter Cybersecurity<sup>™</sup>

# CYBER HYGIENE BEHAVIORS

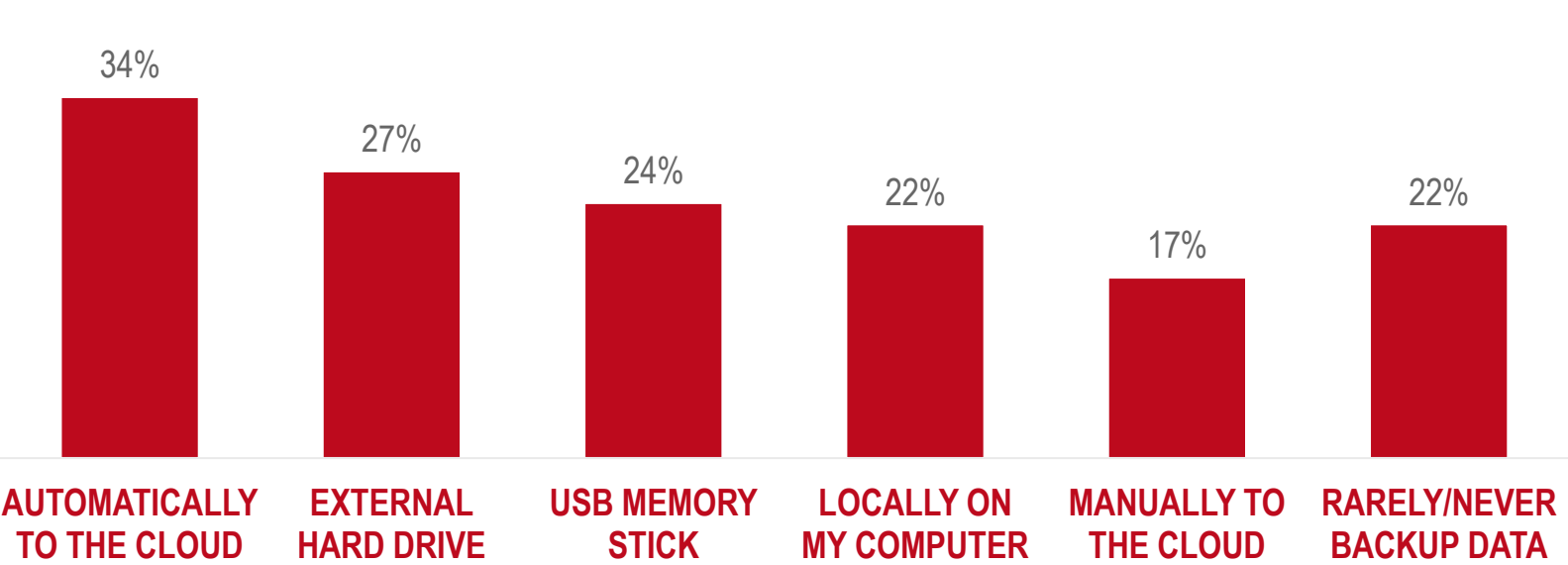
					
BACKING UP DATA	LOST OR STOLEN DEVICES	IDENTITY THEFT	MALWARE, PHISHING & AV SOFTWARE	PASSWORD PRACTICES	ONLINE BEHAVIOR
<ul style="list-style-type: none"> <li>Methods of backing up, including online and offline options</li> <li>Encryption cloud storage</li> </ul>	<p>Quantify the % of Americans who in the past year have lost a device without being able to find or recover it – or – have given away a device without first resetting the factory settings</p>	<ul style="list-style-type: none"> <li>Quantify the % of Americans who have had their identity stolen</li> <li>Frequency in which Americans have had their identity stolen in the past year</li> <li>Main consequences of identity theft</li> </ul>	<ul style="list-style-type: none"> <li>Quantify the % of Americans who in the past year may have been infected with Malware or fallen victim to a phishing attempt</li> <li>AV software use, including free vs. paid services</li> <li>Frequency in which AV software is updated</li> </ul>	<ul style="list-style-type: none"> <li>Quantify the % of Americans who share passwords</li> <li>Quantify the % of Americans who are reusing passwords across multiple accounts</li> <li>Quantify the % of Americans who use a password manager tool</li> </ul>	<ul style="list-style-type: none"> <li>Quantify the % of Americans who use public WiFi without a VPN</li> <li>Quantify the % of Americans who have left their social media accounts public</li> <li>Online habits practiced regularly</li> </ul>

# FEW AMERICANS ARE PROPERLY BACKING UP THEIR IMPORTANT INFORMATION



Today, more than 3 in 4 (78%) of Americans are backing up their data using one of the methods below. However, most of them (57%) are still leaving themselves susceptible to risk by only backing up using one method, rather than backing up online (cloud) and offline (external hard drive, USB memory, etc.).

## TOP WAYS AMERICANS ARE BACKING UP THEIR DATA



**INDEX SCORE**  
**78%**

**57%** of Americans are *only* backing up their data to either an online or offline source, rather than both.

Which of the following methods, if any, do you regularly use to backup your important documents or other sensitive information contained on your PC, tablet, smart phone or other data-bearing devices?



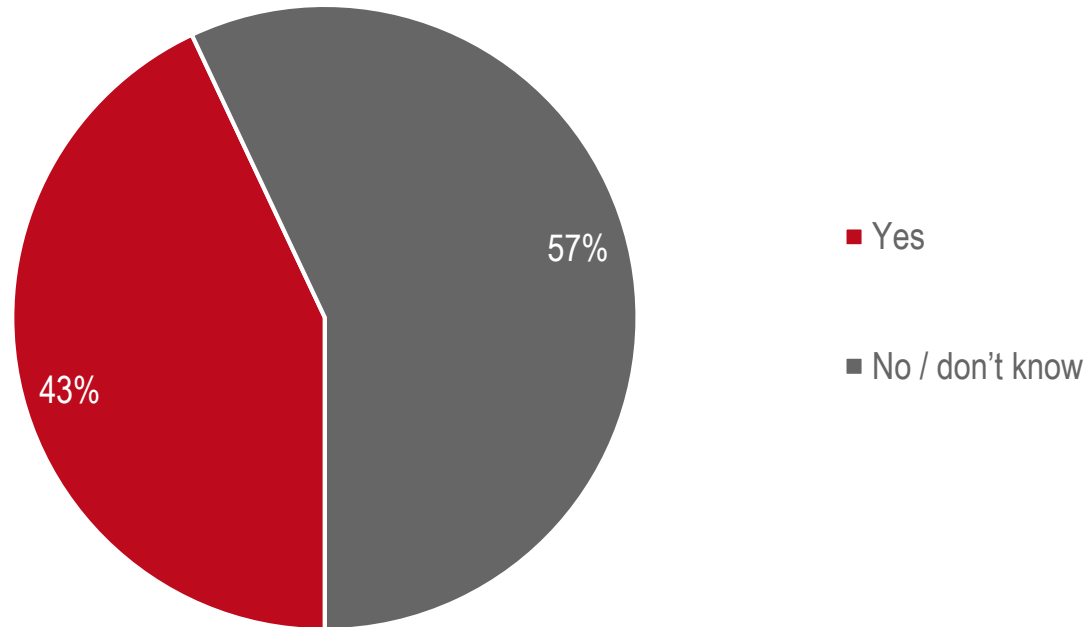


## MANY ARE UPLOADING INFORMATION TO THE CLOUD UNPROTECTED

Among those who are backing up their information by uploading it to the cloud, only 2 in 5 (43%) are taking the extra step in ensuring that it's stored in an encrypted format.

**PERCENTAGE WHO STORE THEIR DATA ENCRYPTED**  
*AMONG THOSE WHO BACKUP DATA TO THE CLOUD, n=4,519*

**80%** of Cyber Hygiene Superstars know that their data is stored encrypted, compared to just 43% of Americans overall.



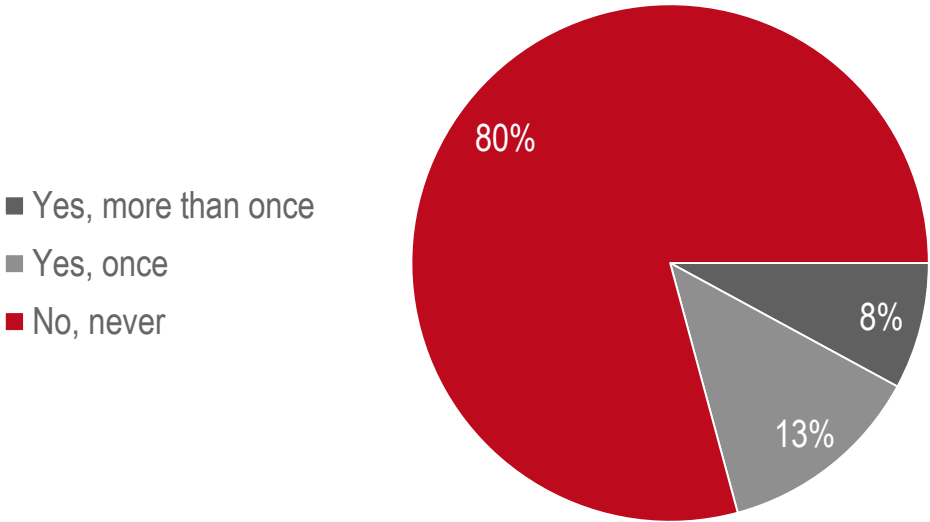
When backing up your information to the Cloud, is your information stored in an encrypted format?

# AMERICANS ARE LOSING THEIR DEVICES OR GIVING THEM AWAY WITHOUT CLEARING THEIR MEMORY

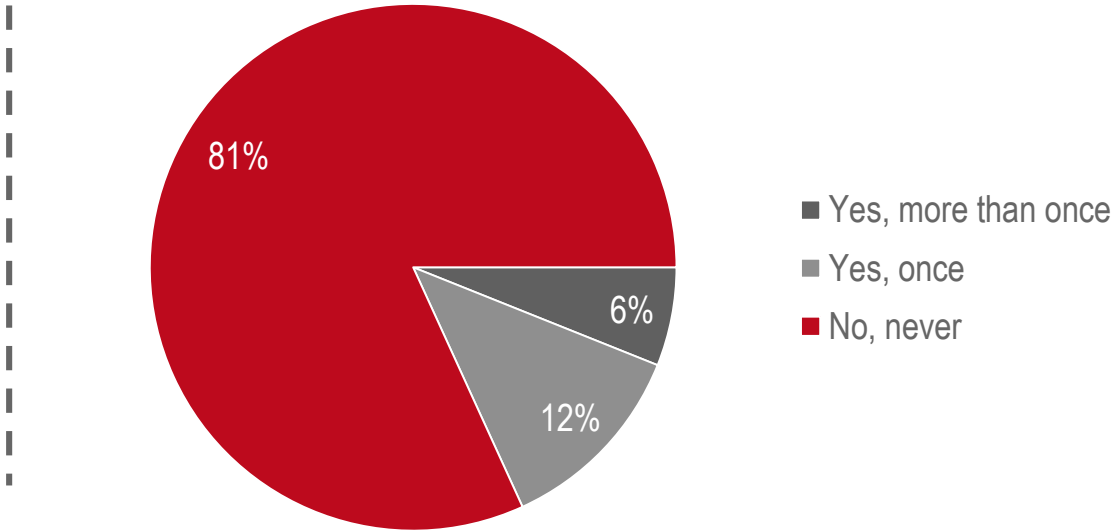


In the past year, only 72% of Americans can say that they have not lost a device without being able to recover it or given one away without first resetting it's factory settings. Roughly 4 in 5 (80-81%) have either done one or the other.

LOST A DEVICE WITHOUT FINDING IT



GAVE AWAY A DEVICE WITHOUT WIPING THE MEMORY



**INDEX SCORE**  
72%

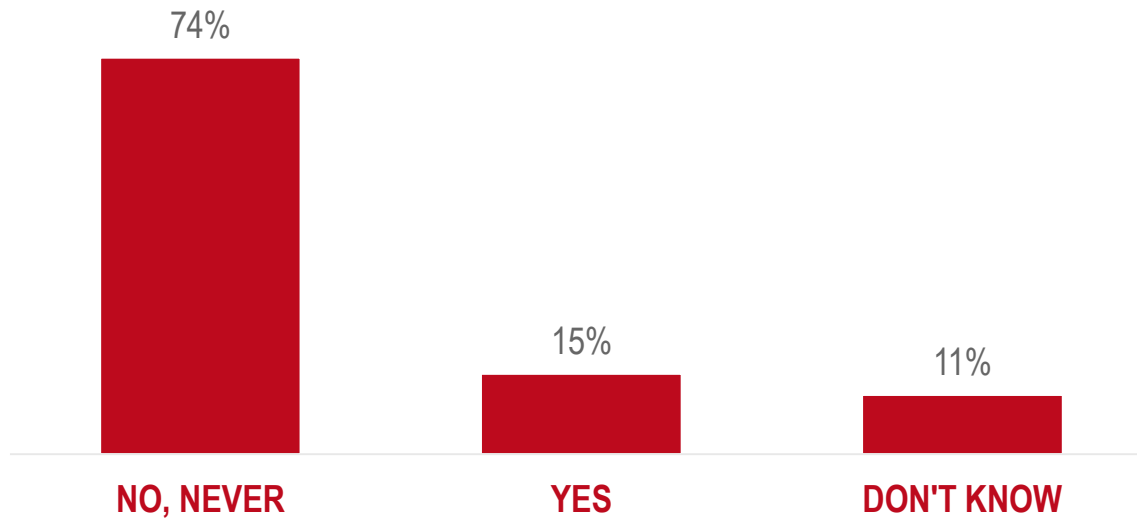
In the past year, have you lost a PC, tablet, smart phone or USB memory stick that you were not able to find or recover?  
In the past year, have you retired, traded in, sold, gave away or recycled a PC, tablet, smartphone or USB memory stick without first resetting the factory settings?



# IDENTITY THEFT IS OPENING UP AMERICANS TO CYBER RISK

Today, only 74% of Americans can say that they have never had their identity stolen.

## PERCENTAGE WHO HAVE EXPERIENCED IDENTITY THEFT



INDEX SCORE  
74%

**6%** of Americans indicate that they were a victim of identity theft **in the past year**.

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

# AMERICANS ARE ADOPTING THE USE OF AV SOFTWARE TO PROTECT THEMSELVES

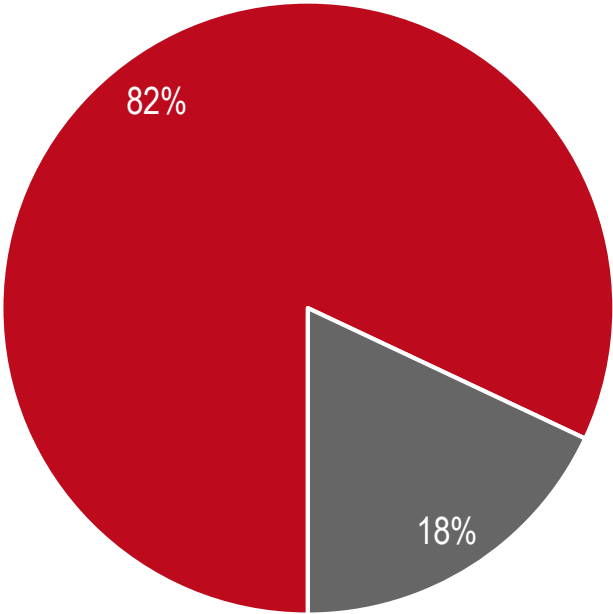


Today, more than 4 in 5 (82%) Americans are using some sort of AV software on their personal devices.

INDEX SCORE  
82%

PERCENTAGE WHO USE AV SOFTWARE

100% of Cyber Hygiene Superstars use AV software, compared to 82% of Americans overall.



- Uses AV software
- Does not use AV software

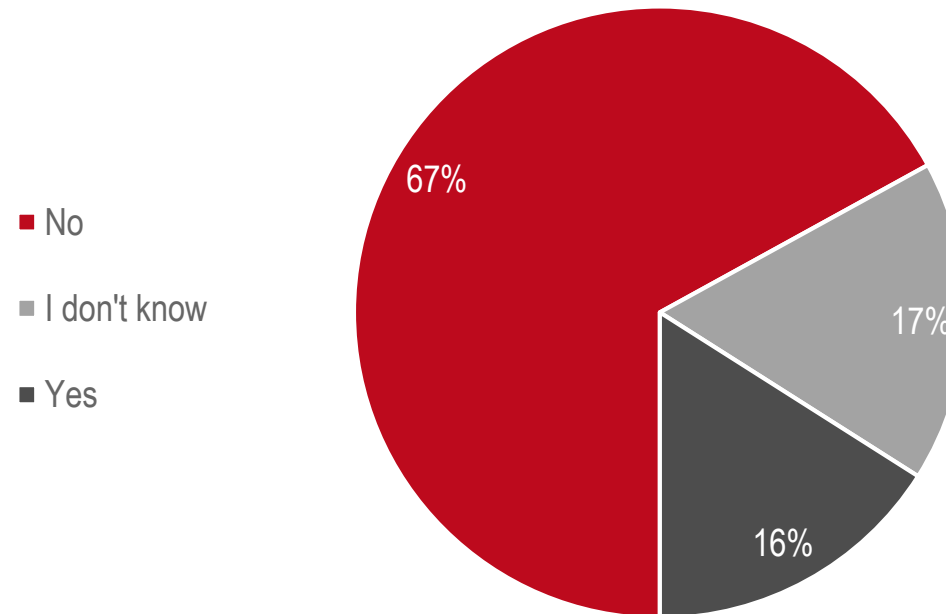
On which of your personal devices, if any, do you use antivirus (AV) software (Norton, McAfee, Webroot, etc.)?



# WITH INCREASED AV SOFTWARE USE, MALWARE IS LESS OF A THREAT

In the past year, 67% of Americans have not been negatively impacted by malware.

PERCENTAGE WHOSE DEVICES HAVE BEEN NEGATIVELY IMPACTED BY MALWARE



INDEX SCORE  
67%

To your knowledge, in the past year has your PC, tablet and/or smart phone been negatively impacted as a result of malware?

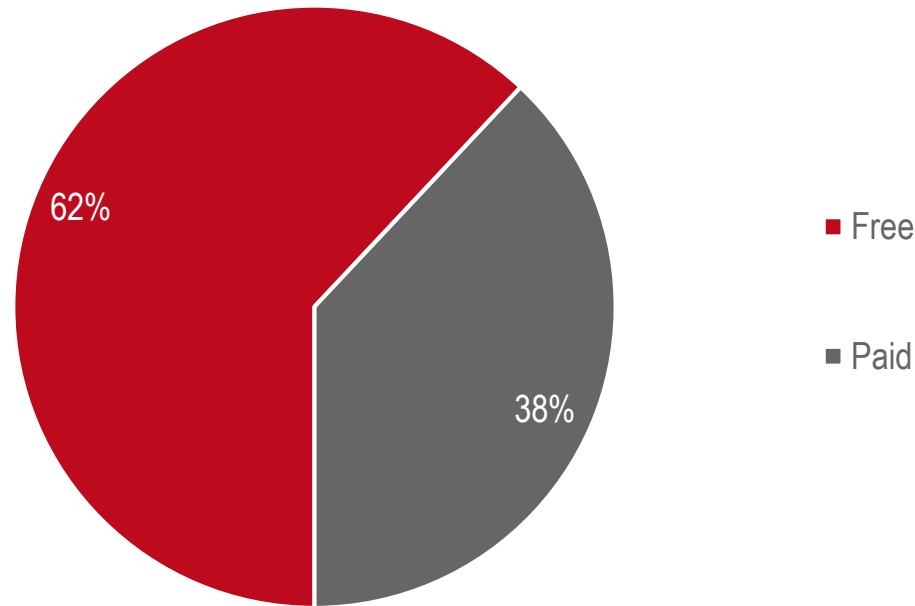
# HOWEVER, MOST AMERICANS ARE USING LESS SECURE, FREE SOFTWARE SERVICES



While the majority of Americans are using AV software, most (62%) are turning to free services for protection. Cyber Hygiene Superstars recognize the benefits of paying for better protection.

TYPE OF AV SOFTWARE USED  
AMONG THOSE WHO USE AV SOFTWARE,  $n=8,139$

75% of Cyber Hygiene Superstars use Paid AV software, compared to 38% of Americans overall.



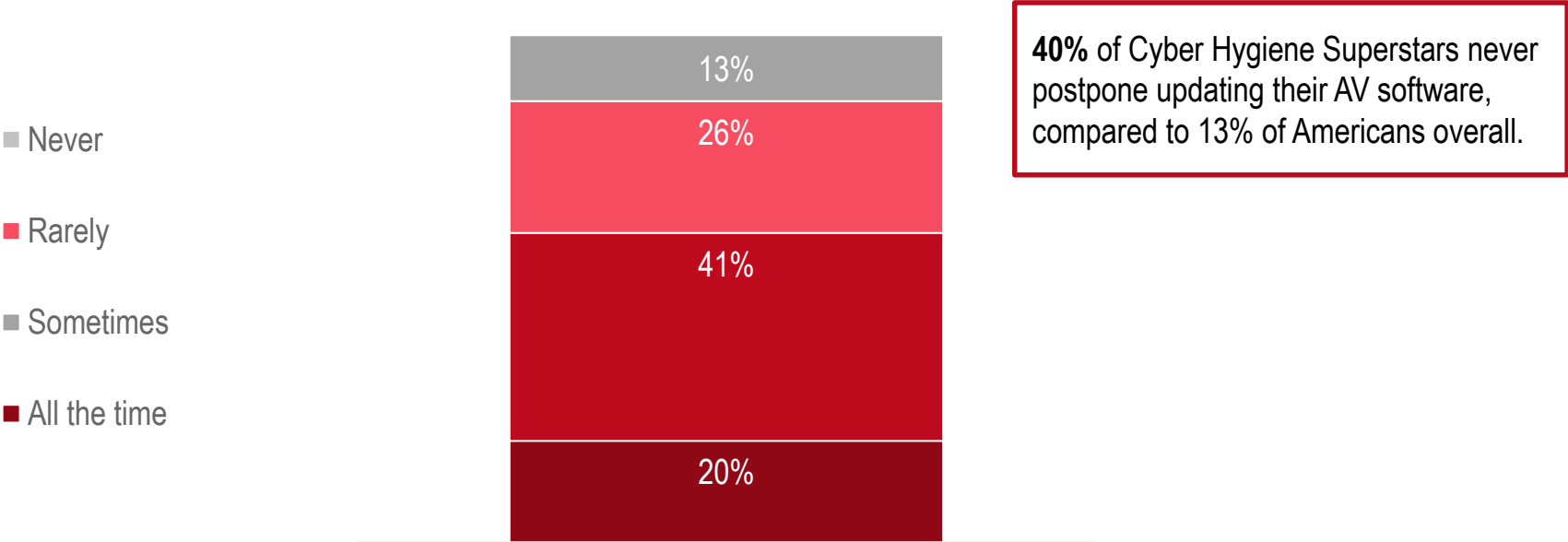
Do you use paid or free AV software?

# THOSE WHO ARE USING AV SOFTWARE ARE NOT KEEPING THEM UP TO DATE



Regardless of what type of AV software is used (free vs. paid), Americans are not doing a good enough job in keeping them up to date. Only 20% of Americans are updating their AV software each time they are prompted, rather than postponing it.

## FREQUENCY OF POSTPONING AV SOFTWARE UPDATES WHEN PROMPTED



AMONG THOSE WHO USE AV SOFTWARE n=8,139

In general, when your AV software or computer prompts you that it needs to be updated, how often do you postpone or select “ask me at a later time”?



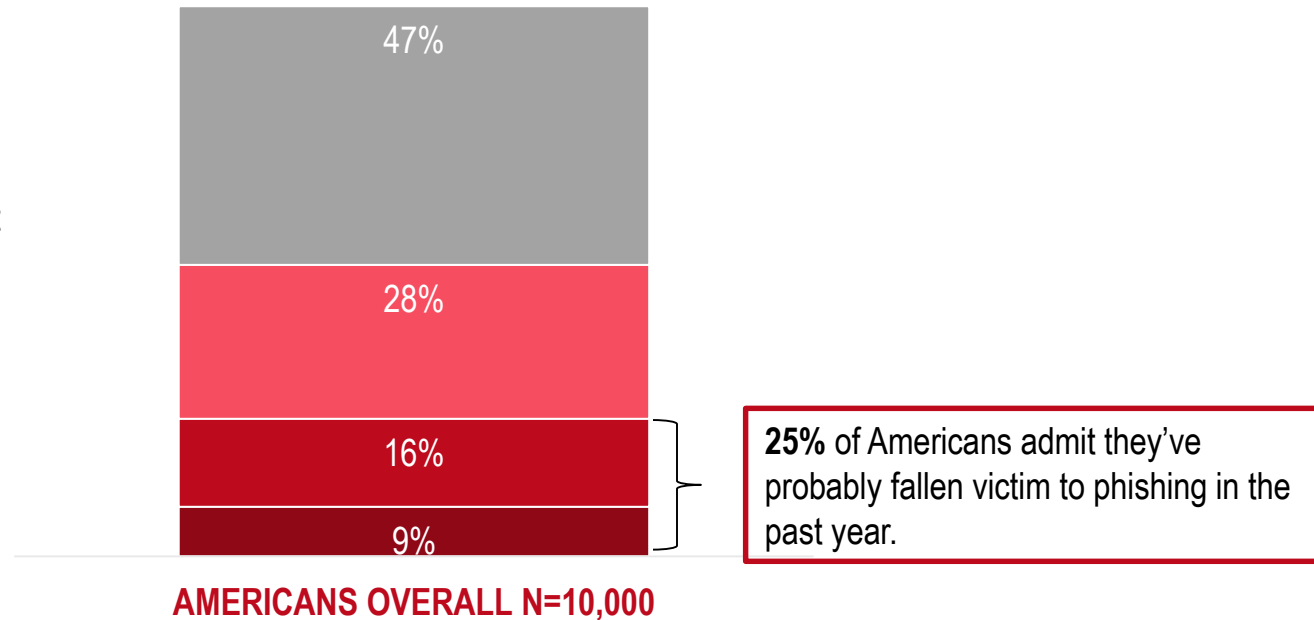
# PHISHING ATTACKS ARE STILL CLAIMING VICTIMS OF NAIVE AMERICANS

Less than half (47%) of Americans can say confidently that they have not fallen victim to a phishing attempt in the past year. On the other hand, 1 in 4 (25%) feel that they probably have.

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

**INDEX SCORE**  
47%

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



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

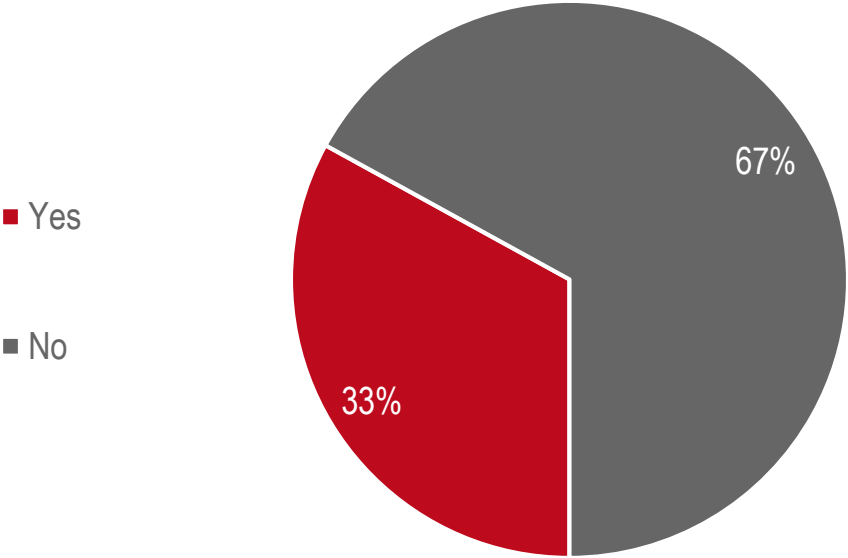




# MANY AMERICANS ARE STILL SHARING THEIR PASSWORDS WITH OTHERS

Only 2 in 3 (67%) Americans are not sharing their passwords with others. To make matters worse, only 37% of Americans are refraining from reusing passwords across multiple accounts.

PERCENTAGE WHO HAVE SHARED  
PASSWORDS WITH OTHERS



INDEX SCORE  
67%

INDEX SCORE  
37%

Only 9% have more passwords  
than accounts

63% are reusing passwords  
across multiple accounts

Americans have on average  
9 passwords for 17 accounts

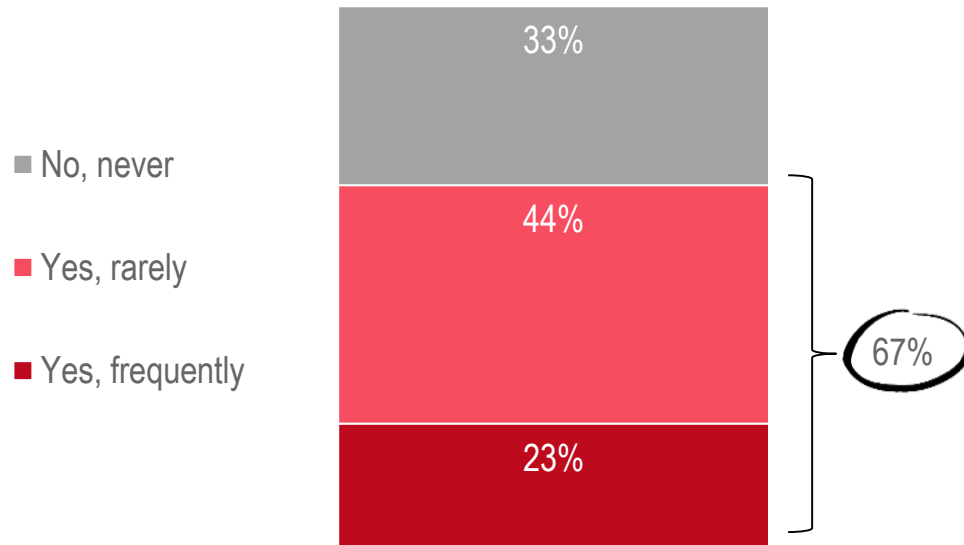
Have you ever, even once, shared your passwords or other access credentials with others? How many separate passwords or passphrases do you maintain on a regular basis? How many total online accounts do you have that require a username and password?



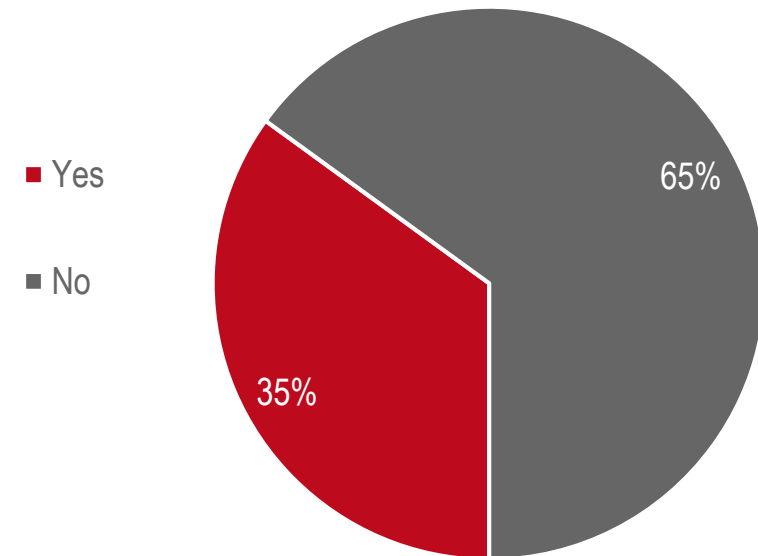
# AMERICANS ARE USING PUBLIC WIFI WHILE UNPROTECTED

While 2 in 3 (67%) Americans are using public WiFi when they're out and about, only 1 in 3 (35%) are taking the extra step in protecting themselves by using a VPN.

PERCENTAGE WHO USE PUBLIC WIFI



PERCENTAGE WHO OWN A PERSONAL VPN



Do you use public WiFi when traveling for business or leisure? For example in an airport, library or coffee shop?  
Do you use a personal virtual private network (VPN) service (such as Webroot WiFi Security, ExpressVPN, or NordVPN) when connecting to the Internet?

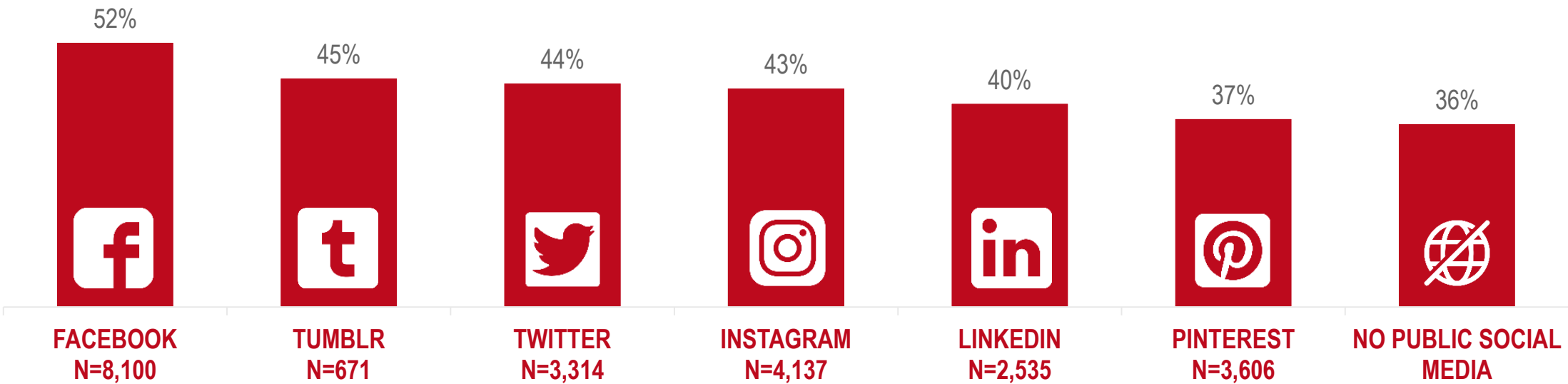
# RISKIEST AMERICANS ARE NOT MAKING THEIR SOCIAL MEDIA ACCOUNTS PRIVATE



Only 36% of Americans who use social media are making sure that all of their accounts are private. The most common social media platform that Americans have kept public is Facebook (52%).

PERCENTAGE WHO HAVE KEPT SOCIAL MEDIA PUBLIC  
AMONG THOSE WHO USE EACH SOCIAL MEDIA PLATFORM

INDEX SCORE  
36%



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.

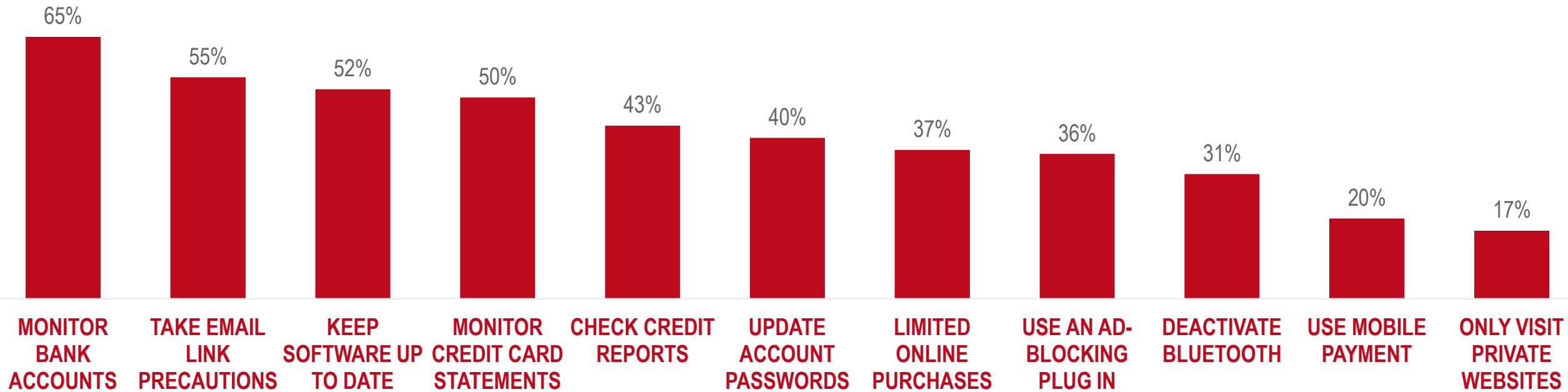
# MOST AMERICANS ARE NOT REGULARLY PRACTICING HABITS THAT ARE CRITICAL TO PROTECTION ONLINE



Most Americans are not yet adopting some of the key online habits that help ensure proper cyber hygiene. Less than half (49%) are regularly practicing at least 5 of the online habits shown below.

PERCENTAGE REGULARLY PRACTICING THE FOLLOWING CYBER-HYGIENE HABITS

INDEX SCORE  
49%



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

# APPENDIX

**WEBROOT®**  
Smarter Cybersecurity™

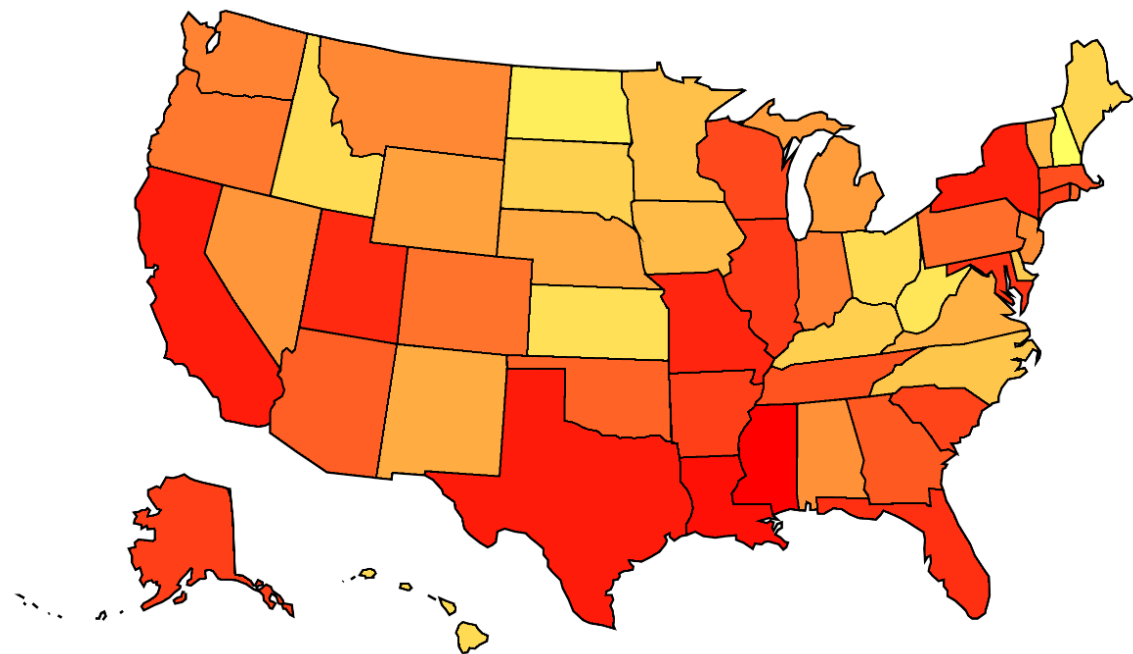
# CYBER HYGIENE RISK INDEX – BREAKOUTS

**WEBROOT**<sup>®</sup>  
Smarter Cybersecurity<sup>™</sup>

# PERCENTAGE PASSING EACH CYBER HYGIENE RISK INDEX METRIC

PERCENTAGE PASSING EACH CYBER HYGIENE RISK INDEX METRIC	%
DO THEY BACKUP THEIR DATA?	78%
HAVE THEY LOST A DEVICE WITHOUT RECOVERING IT OR GIVEN AWAY A DEVICE WITHOUT WIPING MEMORY?	72%
HAVE THEY HAD THEIR ID STOLEN?	67%
HAVE THEY BEEN INFECTED WITH MALWARE?	67%
HAVE THEY BEEN A VICTIM OF PHISHING?	47%
DO THEY USE AV SOFTWARE?	82%
DO THEY SHARE PASSWORDS WITH OTHERS?	67%
DO THEY REUSE PASSWORDS?	37%
DO THEY KEEP THEIR SOCIAL MEDIA PUBLIC?	36%
DO THEY PRACTICE GOOD ONLINE BEHAVIOR?	49%

# STATE RISK INDEX – MOST TO LEAST RISKY



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



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

CYBER-HYGIENE GRADE	MS #1	LA #2	CA #3	AK #4	CT #5	TX #6	NY #7	MO #8	UT #9	FL #10	MD #11	IL #12	AR #13	SC #14	WI #15	MA #16	TN #17
A (90-100%)	6%	5%	8%	11%	6%	9%	9%	7%	9%	11%	8%	9%	10%	11%	8%	7%	11%
B (80-89%)	11%	9%	10%	13%	16%	13%	11%	16%	13%	9%	12%	12%	14%	12%	13%	14%	12%
C (70-79%)	15%	19%	16%	12%	13%	17%	18%	14%	17%	18%	19%	18%	20%	19%	16%	16%	18%
D (60-69%)	16%	18%	20%	15%	19%	18%	22%	17%	15%	17%	14%	20%	16%	13%	24%	21%	21%
F (0-59%)	53%	51%	48%	50%	46%	44%	42%	47%	48%	46%	47%	42%	42%	47%	40%	43%	40%

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

CYBER-HYGIENE GRADE	GA #18	AZ #19	OK #20	RI #21	PA #22	CO #23	OR #24	IN #25	WA #26	MT #27	NJ #28	AL #29	NV #30	MI #31	WY #32	NE #33	NM #34
A (90-100%)	10%	10%	9%	7%	8%	8%	7%	10%	13%	10%	10%	9%	9%	12%	10%	12%	12%
B (80-89%)	11%	14%	15%	13%	14%	14%	15%	14%	15%	16%	11%	13%	12%	17%	17%	11%	17%
C (70-79%)	21%	20%	16%	18%	19%	22%	18%	19%	14%	15%	18%	18%	22%	14%	15%	17%	14%
D (60-69%)	20%	16%	18%	22%	22%	18%	21%	18%	19%	22%	25%	22%	15%	19%	17%	23%	16%
F (0-59%)	39%	42%	43%	41%	39%	39%	40%	40%	41%	37%	37%	39%	43%	39%	41%	38%	42%

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

CYBER-HYGIENE GRADE	VA #35	VT #36	IA #37	MN #38	NC #39	DE #40	SD #41	ME #42	HI #43	KS #44	WV #45	KY #46	ID #47	OH #48	ND #49	NH #50
A (90-100%)	13%	10%	10%	9%	13%	12%	13%	9%	12%	10%	14%	11%	10%	16%	14%	18%
B (80-89%)	13%	13%	16%	16%	14%	27%	16%	16%	15%	14%	15%	16%	15%	15%	14%	19%
C (70-79%)	21%	20%	18%	20%	18%	17%	16%	22%	19%	22%	18%	20%	21%	18%	20%	13%
D (60-69%)	19%	24%	21%	20%	19%	19%	17%	16%	22%	21%	17%	19%	22%	21%	22%	17%
F (0-59%)	36%	35%	37%	36%	37%	37%	38%	38%	34%	34%	41%	35%	33%	32%	31%	33%

# CURRENT STATE OF CYBER HYGIENE

**WEBROOT®**  
Smarter Cybersecurity™

# AMERICANS NAME THE MOST DAMAGING CYBER-RELATED ATTACKS TODAY

TOP RESPONSES TO THE MOST DAMAGING CYBER-RELATED ATTACKS TODAY	%
IDENTITY THEFT	21%
PHISHING	13%
FINANCE / BANKING (THEFT)	13%
VIRUS	13%
PERSONAL INFORMATION (THEFT)	11%
HACKING (GENERAL)	11%
MALWARE	10%
NON-SPECIFIC RESPONSE (GOVERNMENT, PERSONAL, COMPUTER, ETC.)	9%
CYBERBULLYING	8%
DEBIT / CREDIT CARD THEFT	8%
RANSOMWARE	5%
ONLINE / PHONE SCAMS	4%
TROJANS	4%

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

# CYBER HYGIENE BEHAVIORS

**WEBROOT**<sup>®</sup>  
Smarter Cybersecurity<sup>™</sup>



# FREQUENCY OF IDENTITY THEFT

NUMBER OF IDENTITY THEFTS IN PAST YEAR AMONG THOSE WHO HAVE HAD THEIR ID STOLEN	%
1 TIME	25%
2-3 TIMES	11%
4-5 TIMES	2%
6-7 TIMES	0%
8-10 TIMES	1%
HAVE NOT HAD ID STOLEN IN PAST YEAR	60%

How many times in the past year were you a victim of identity theft?



# CONSEQUENCES OF IDENTITY THEFT

CONSEQUENCES OF IDENTITY THEFT AMONG THOSE WHO HAVE HAD THEIR ID STOLEN	%
PRIVATE INFORMATION STOLEN	45%
CREDIT/DEBIT CARD MISUSE	33%
CREDIT (FICO) SCORES DECLINED	22%
LOST CONTROL OF BANK ACCOUNTS	22%
CREATED NEW DEBT	18%
SOCIAL MEDIA WAS MISUSED	18%
TAX RETURNS WERE STOLEN	12%
MEDICAL RECORDS STOLEN	8%
OTHER	8%
NONE OF THE ABOVE	5%
DON'T KNOW	4%

What were the main consequences of the identity theft incident(s)?





## PERCENTAGE WHO USE AN IDENTITY PROTECTION SERVICE

PERCENTAGE WHO USE AN IDENTITY PROTECTION SERVICE	%
YES	24%
NO	76%

Do you use an identity protection service such as LifeLock, ID Watch Dog or others?

# FREQUENCY AMERICANS ALLOW THEIR DEVICE TO REMEMBER THEIR PASSWORDS



FREQUENCY AMERICANS ALLOW THEIR DEVICE TO REMEMBER THEIR PASSWORDS	%
NEVER HAVE DEVICE SAVE LOGINS	22%
OCCASIONALLY / RARELY	24%
ABOUT HALF THE TIME	18%
MAJORITY OF THE TIME	20%
ALL THE TIME / WHENEVER ABLE	16%

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.



# PERCENTAGE WHO USE A PASSWORD MANAGER

PERCENTAGE WHO USE A PASSWORD MANAGER	%
YES	25%
NO	75%

Do you use a password manager, or other software tool that assists in generating and retrieving complex passwords?

# ONLINE BEHAVIOR OF CYBER HYGIENE SUPERSTARS VS. AMERICANS OVERALL



PERCENTAGE PRACTICING THE FOLLOWING CYBER-HYGIENE PRACTICES	AMERICANS OVERALL	SUPERSTARS
MONITOR BANK ACCOUNTS	65%	76%
TAKE PRECAUTIONS BEFORE CLICKING A LINK IN AN EMAIL	55%	76%
KEEP SOFTWARE UP TO DATE	52%	83%
MONITOR CREDIT CARD STATEMENTS	50%	68%
CHECK CREDIT REPORTS	43%	64%
UPDATE ONLINE ACCOUNT PASSWORDS	40%	68%
LIMITED ONLINE PURCHASES	37%	54%
USE AN AD-BLOCKING PLUG IN (BLOCK POP-UPS)	36%	58%
DEACTIVATE BLUETOOTH WHEN NOT IN USE	31%	46%
USE MOBILE PAYMENT, SUCH AS APPLE PAY	20%	17%
ONLY VISIT WEBSITES THAT ARE PRIVATE (HTTPS INSTEAD OF HTTP)	17%	35%
I DON'T PRACTICE ANY OF THESE HABITS	8%	2%

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

# PERCENTAGE WHO ADOPTED THE FOLLOWING CYBER HYGIENE PRACTICES AS A RESULT OF A CYBER-RELATED ATTACK



PERCENTAGE WHO ADOPTED THE FOLLOWING CYBER HYGIENE PRACTICES	%
REGULARLY MONITOR BANK ACCOUNTS	26%
TAKE PRECAUTIONS BEFORE CLICKING A LINK IN AN EMAIL	22%
REGULARLY MONITOR CREDIT CARD STATEMENTS	19%
KEEP SOFTWARE UP TO DATE	18%
STARTED USING RELIABLE ANTIVIRUS SOFTWARE	18%
REGULARLY CHECK CREDIT REPORTS	17%
REGULARLY UPDATE ONLINE ACCOUNT PASSWORDS	14%
USE AN AD-BLOCKING PLUG IN (BLOCK POP-UPS)	11%
LIMITED ONLINE PURCHASES	10%
DEACTIVATE BLUETOOTH WHEN NOT IN USE	9%
STARTED USING A PASSWORD MANAGEMENT TOOL	6%
PURCHASED A PERSONAL VPN	6%
ONLY VISIT WEBSITES THAT ARE PRIVATE (HTTPS INSTEAD OF HTTP)	5%
USE MOBILE PAYMENT, SUCH AS APPLE PAY	5%
I DON'T KNOW ANYONE WHO WAS A VICTIM OF A CYBER-ATTACK	24%
NONE OF THESE	22%

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?

# ADDITIONAL CLASSIFICATION BREAKOUTS

**WEBROOT**<sup>®</sup>  
Smarter Cybersecurity<sup>™</sup>



# DEVICES USING AV SOFTWARE

PERCENTAGE OF EACH PERSONAL DEVICE TYPE USING AV SOFTWARE	%
WINDOWS LAPTOP	40%
WINDOWS DESKTOP/PC	33%
ANDROID PHONE	27%
TABLET (NOT APPLE PRODUCT)	14%
IOS (APPLE) PHONE	12%
IPAD	8%
MAC (APPLE) LAPTOP	6%
MAC DESKTOP (IMAC)	3%
OTHER	1%
I DON'T USE ANY ANTI-VIRUS SOFTWARE ON ANY DEVICE	18%

On which of your personal devices, if any, do you use antivirus (AV) software (Norton, McAfee, Webroot, etc.)?



# SOCIAL MEDIA USE BY PLATFORM

PERCENTAGE WHO USE EACH SOCIAL MEDIA PLATFORM	%
FACEBOOK	81%
INSTAGRAM	41%
PINTEREST	36%
TWITTER	33%
SNAPCHAT	26%
LINKEDIN	25%
TUMBLR	7%
OTHER	2%
NOT ON SOCIAL MEDIA	9%

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





## PERCENTAGE WHO HAVE PUBLIC SOCIAL MEDIA ACCOUNTS

PERCENTAGE WHO HAVE PUBLIC SOCIAL MEDIA ACCOUNTS	AMONG THOSE ON SOCIAL MEDIA, n=9,136
ON SOCIAL MEDIA	63%
NOT ON SOCIAL MEDIA	36%

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.

# FREQUENCY AMERICANS USE THEIR WORK DEVICE FOR PERSONAL USE

FREQUENCY AMERICANS USE THEIR WORK DEVICE FOR PERSONAL USE	AMONG THOSE EMPLOYED WITH A WORK DEVICE n=3,310
NEVER	22%
RARELY	22%
SOMETIMES	33%
ALL THE TIME	24%

How often, if ever, do you use your work devices, such as a work phone or laptop, for personal use?

# USES A WORK DEVICE AS THEIR PRIMARY DEVICE AT HOME

PERCENTAGE USING A WORK DEVICE AS THEIR PRIMARY PERSONAL DEVICE AT HOME	AMERICANS OVERALL	SUPERSTARS	5 SAFEST STATES	5 RISKIEST STATES
YES	34%	19%	25%	41%
NO	66%	81%	75%	59%

Would you consider any of your work devices to be your primary device for use at home?

The Wakefield Research logo, featuring a red square icon with three white vertical bars of increasing height, followed by the word "WAKEFIELD" in a red, sans-serif, uppercase font.The Wakefield Research logo, featuring a red square icon with three white vertical bars of increasing height, followed by the word "WAKEFIELD" in a red, sans-serif, uppercase font.The Webroot logo, featuring the word "WEBROOT" in a bold, green, sans-serif, uppercase font, with a registered trademark symbol (®) to its upper right. Below it, the tagline "Smarter Cybersecurity" is written in a smaller, green, sans-serif font, with a trademark symbol (™) to its upper right.

[WAKEFIELDRESEARCH.COM](http://WAKEFIELDRESEARCH.COM)

Copyright ©2019 Wakefield Research. All rights reserved.  
All information contained herein is confidential and proprietary to Wakefield Research.

