



The Cyber Hygiene Index: Measuring the Riskiest States

Conducted by Ponemon Institute

Sponsored by Webroot

Publication Date: April 2018

The Cyber Hygiene Index: Measuring the Riskiest States

Ponemon Institute, April 2018

Part 1. Introduction

Ponemon Institute is pleased to presents the results of a U.S.-based survey of consumers located in all 50 states and Washington D.C. Survey findings were used to create the Cyber Hygiene Index (CHI) that attempts to measure consumers' ability to protect themselves from various criminal attacks, especially in the online environment. The CHI consists of a series of positive and negative survey questions weighted by the relative importance of each question for achieving a high level of readiness.¹

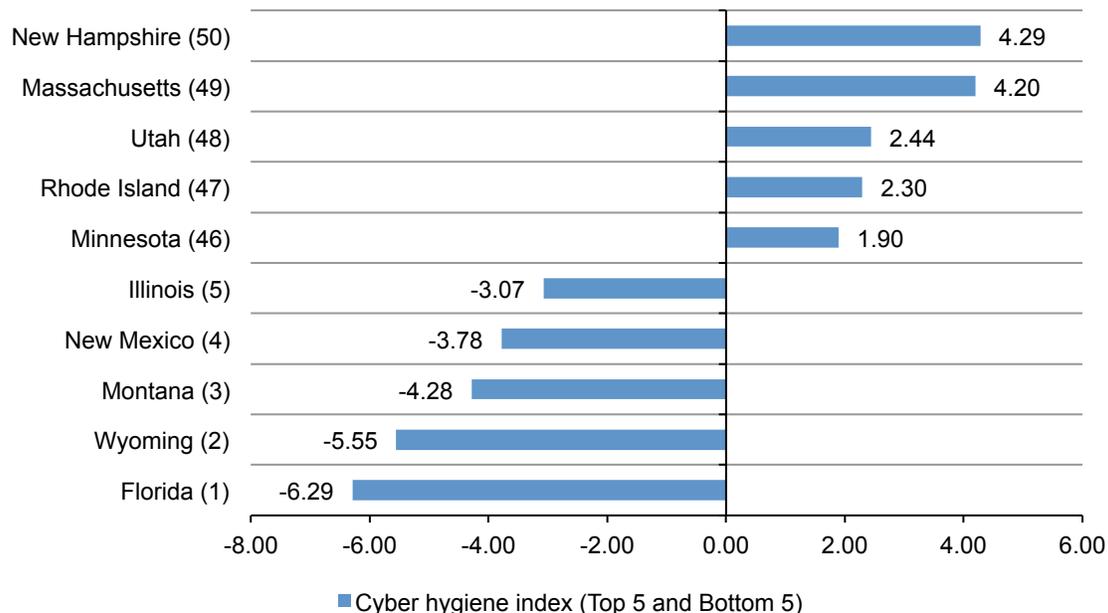
In the context of this research we define cyber hygiene as an individual's ability to maintain a high level of readiness in order to prevent, detect and respond to cyber-related attacks such as malware, phishing, ransomware and identity/credential theft. The index provides a score ranging from +37 points (highest possible CHI) to -39 points (lowest possible CHI).

A total of 4,290 respondents were surveyed, which represented a 3.2 percent response rate from a proprietary sampling frame of consumers located throughout the United States. A total of 553 surveys were removed from the final sample because of reliability failure. The state-by-state sample sizes varied from a low of 40 completed surveys in Wyoming to a high of 179 completed surveys in New York.

Table 1. Survey response	Freq	Pct
Total sampling frame (U.S. Consumers)	132,450	100.0%
Total returns	4,843	3.7%
Rejected surveys	553	0.4%
Final sample	4,290	3.2%

Figure 1 provides the CHI scores for the top 5 and bottom 5 U.S. states. The bracketed number next to each state is the relative ranking from the most positive score for New Hampshire (re: 4.29) to the most negative score for Florida (re: -6.29). The index score and rank for all 50 states plus D.C. is provided in Appendix 1.

Figure 1. Cyber Hygiene Index: top 5 and bottom 5 U.S. states



¹Webroot's subject matter experts provided the question weights used to construct this index.

Part 2. Survey findings

In this section, we provide an analysis of the CHI and survey findings. The figures summarize the results of our survey. Each chart provides the overall survey response compiled from our total sample of 4,290 U.S. consumers with comparison to the 100 individuals with the most risky responses. We call this group the Bottom 100.

The complete audited research results are presented in the Appendix of this report. We have organized the report according to the following topics:

- The impact of identity theft on cyber hygiene
- The impact of malware and phishing attacks on cyber hygiene
- The impact of a lost device on cyber hygiene
- The impact of password practices on cyber hygiene
- The impact of online behavior on cyber hygiene

The impact of identity theft on cyber hygiene

Figure 2 shows the percentage of respondents who said they experienced an identity fraud or another identity theft crime over the past 12 months. Our hypothesis is that consumers who experience an identity-related crime were less likely to have strong cyber hygiene at the time of the incident.

Figure 2. Over the past year, was your identity stolen?

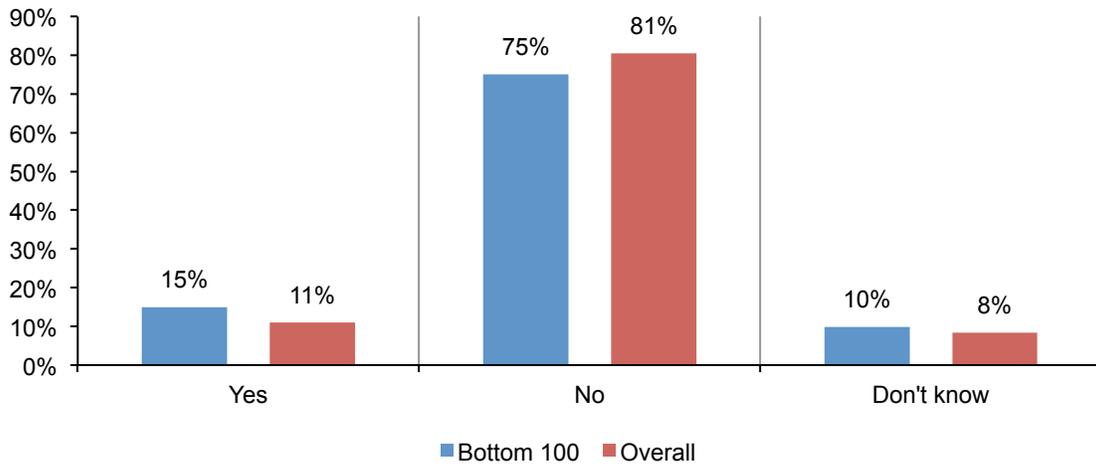


Figure 3 shows the immediate consequences of the identity theft. As can be seen, both the Overall and Bottom 100 show a similar pattern. The most significant consequence is the decline in credit because of a low FICO score, followed by the misuse or theft of the respondents' credit or debit cards.

Figure 3. What were the main consequences of the identity theft incident?

More than one response permitted

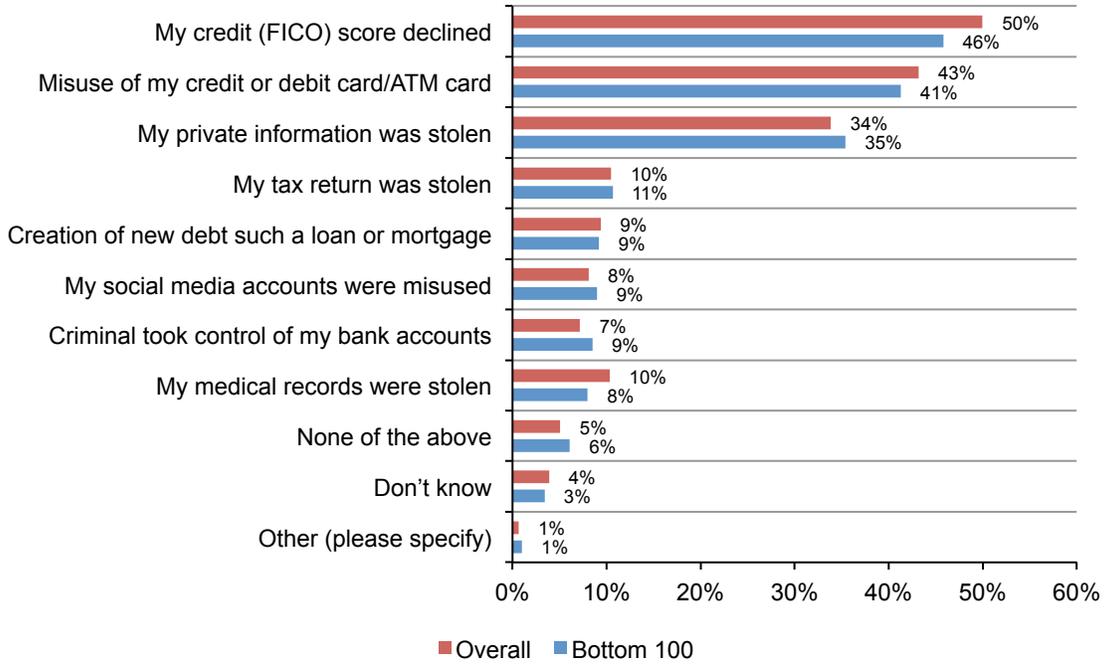


Figure 4 presents respondents' level of cautiousness resulting from the identity theft incident. As shown, 42 percent of respondents said the incident had a significant impact on their level of caution when connected to the Internet or when sharing their personal information. In sharp contrast, 60 percent of the Bottom 100 said the incident had no impact on their online behaviors.

Figure 4. Did the identity theft incident impact your level of cautiousness when connected to the Internet or when sharing your personal information

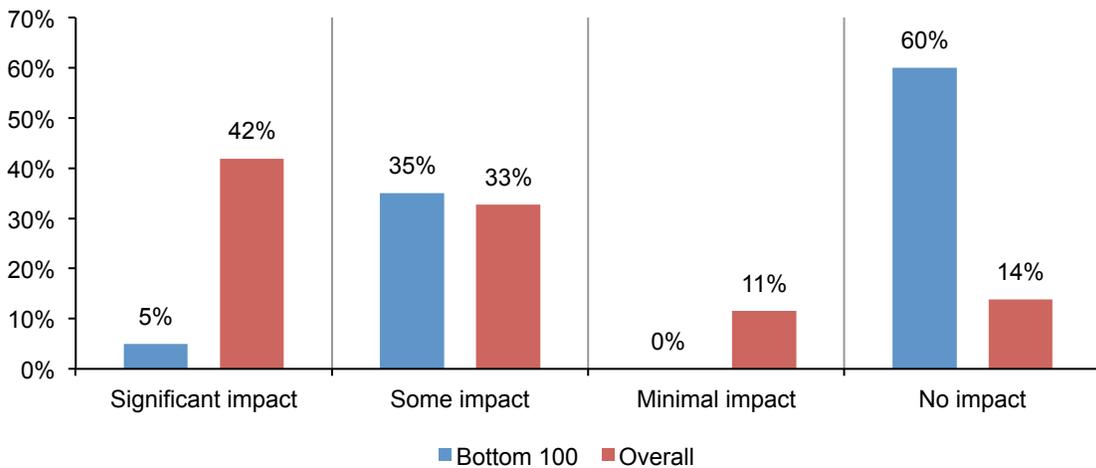
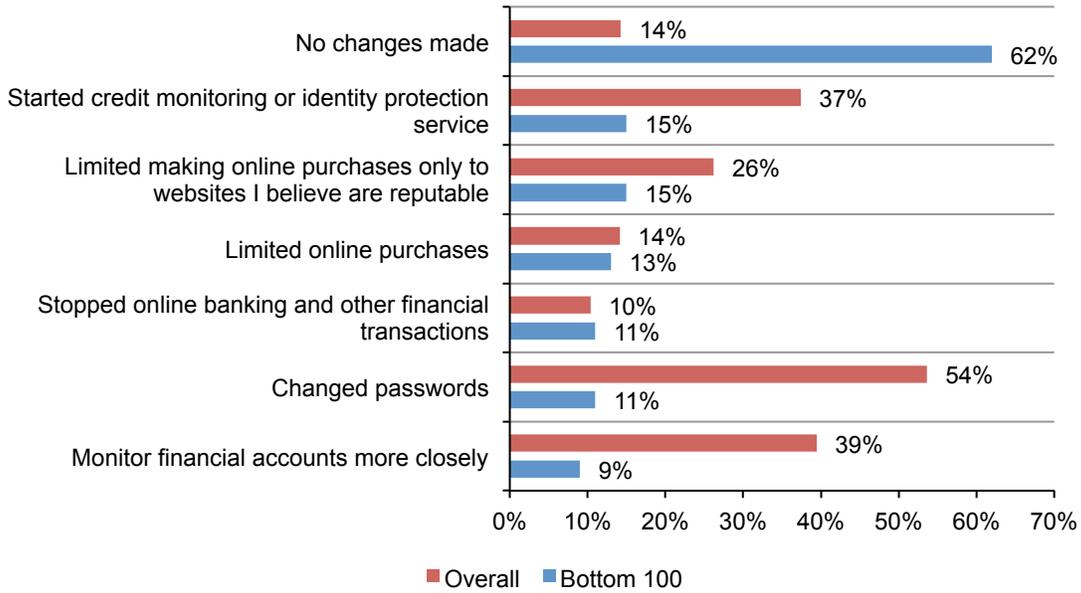


Figure 5 shows marked differences between the Overall and Bottom 100 subsample. Only 14 percent of the Overall sample versus 62 percent of the Bottom 100 subsample said their online behavior did not change after the identity theft. Fifty-four percent of the Overall sample, versus only 11 percent of the Bottom 100, changed passwords. Similarly, 39 percent of the Overall sample and 9 percent of the Bottom 100 sample said they now monitor online financial accounts more closely.

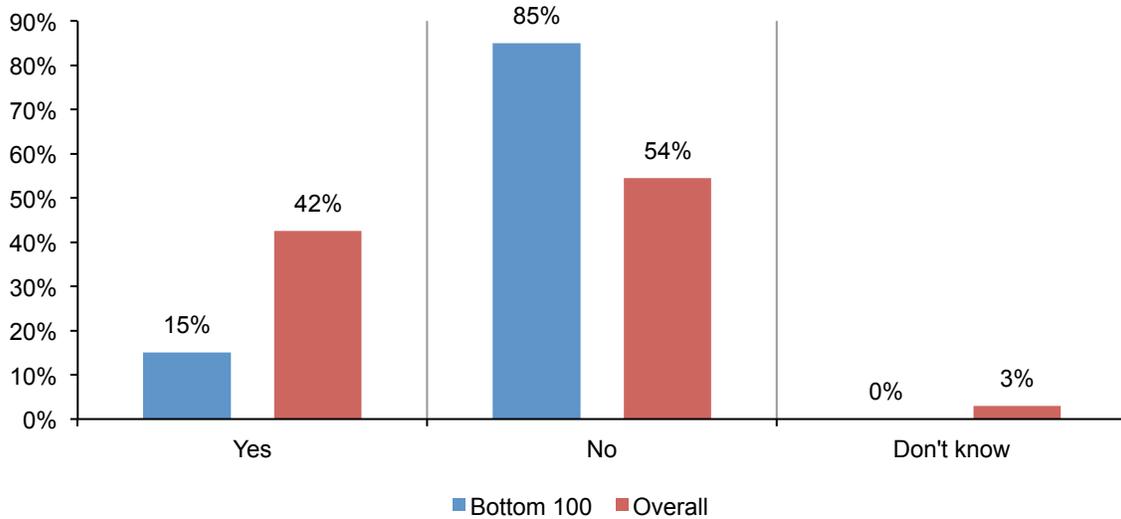
Figure 5. Did you make any changes to your online behavior?

More than one response permitted



Consistent with the previous charts, Figure 6 shows that 42 percent of the overall Overall sample, as compared to only 15 percent of the Bottom 100 subsample, say they use credit monitoring of another identity protection service.

Figure 6. Do you use a credit monitoring or identity protection service?



The Impact of malware or phishing attacks on cyber hygiene

Figure 7 shows the percentage of respondents who said they experienced one or more malware attacks over the past 12 months. Our hypothesis is that consumers whose data-bearing devices were negatively impacted as the result of malware were less likely to have strong cyber hygiene at the time of the attack.

As can be seen, over 46 percent of the Bottom 100 subsample experienced more than 10 attacks over the past year. Twenty-one percent of the Overall sample experienced more than 10 malware attacks. In contrast, 35 percent of the Overall sample, and none of the Bottom 100 subsample, said they did not experience a malware attack on any data-bearing device.

Figure 7. Over the past year, how many times was your PC, tablet and/or smart phone negatively impacted as a result of malware?

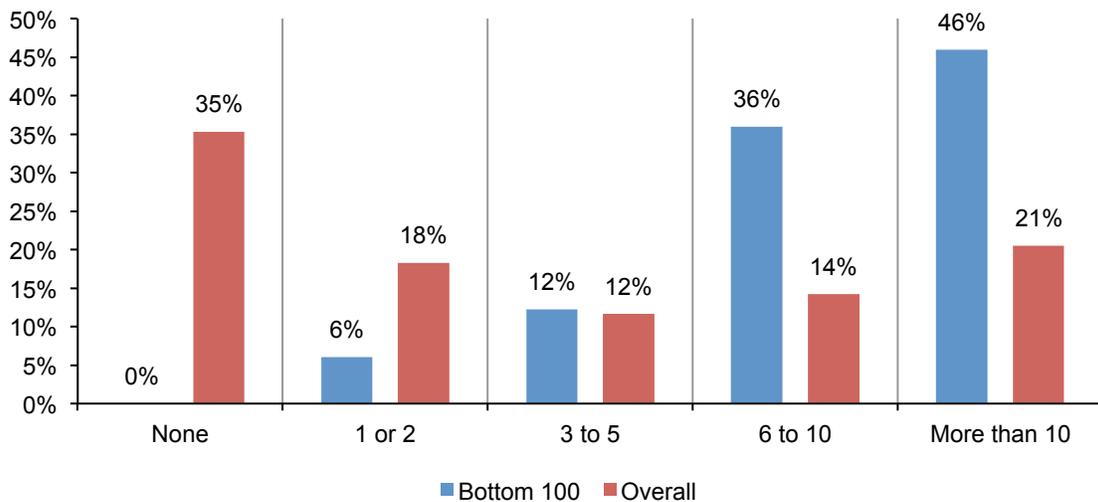
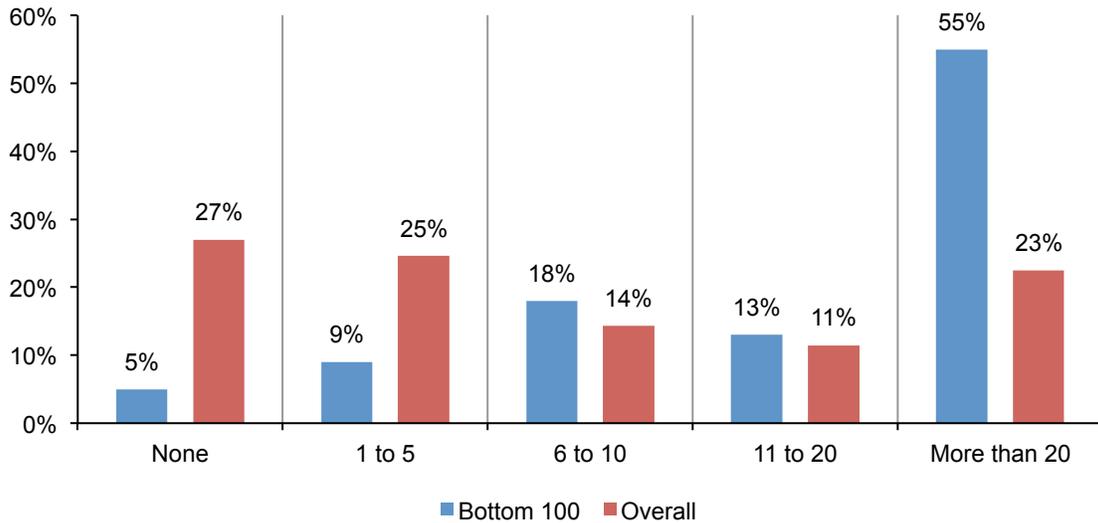


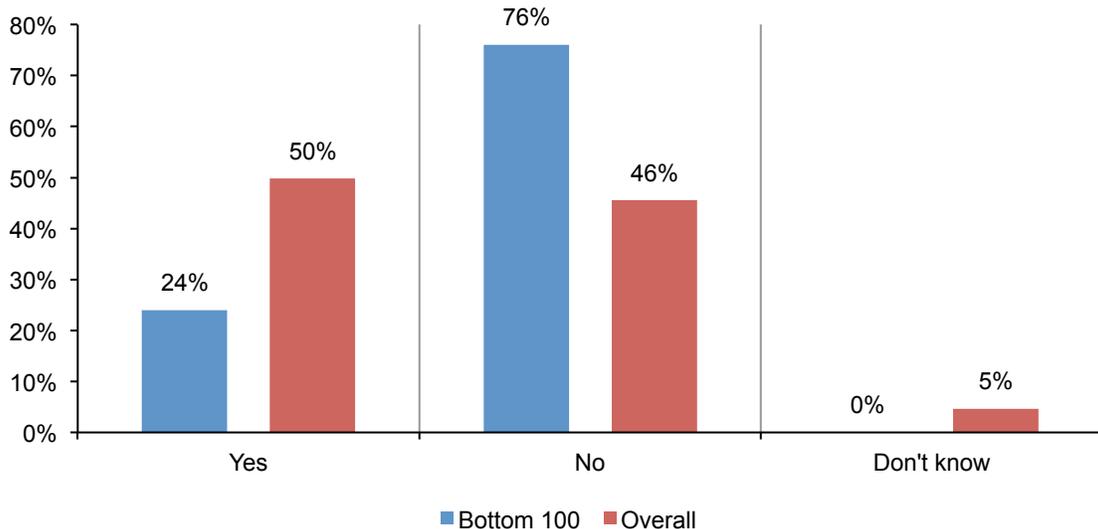
Figure 8 shows the percentage of respondents who said they experienced one or more phishing attempts over the past 12 months. Fifty-five percent of the Bottom 100 subsample experienced more than 20 phishing attempts over the past year. Twenty-three percent of the Overall sample experienced more than 20 attempts. In contrast, 27 percent of the Overall sample, and only 5 percent of the Bottom 100 subsample, said they did not experience any phishing attempt.

Figure 8. Over the past year, how many times do you suspect that you received a phishing email?



The percentage of respondents who use anti-virus software on their laptop, desktop and/or smart phone is shown in Figure 9. Half of all respondents and 24 percent of the Bottom 100 subsample said they use one or more AV solution on their data-bearing devices.

Figure 9. Do you use anti-virus software (AV) on your laptop, desktop or smart phone?



According to Figure 10, 65 percent of all Windows-based PCs have AV. Another 33 percent of Mac PCs have AV. With respect to the Bottom 100 subsample, 38 percent of Windows-based PCs and 29 percent of Mac PCs have AV.

Figure 10. Which of your data-bearing devices have AV software?

More than one response permitted

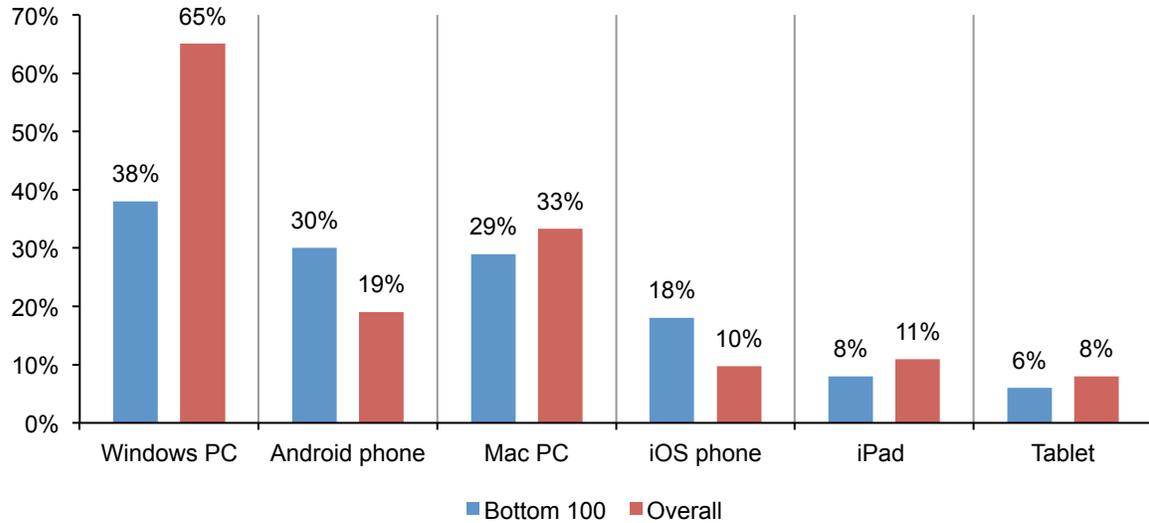


Figure 11 shows the frequency of AV software updates. Forty-three percent of respondents in the Bottom 100 subsample, versus 20 percent in the sample have no set schedule for updates. In contrast, 24 percent of respondents in the Bottom 100 subsample and 41 percent in the overall sample update automatically in real time.

Figure 11. How frequently do you update your AV software?

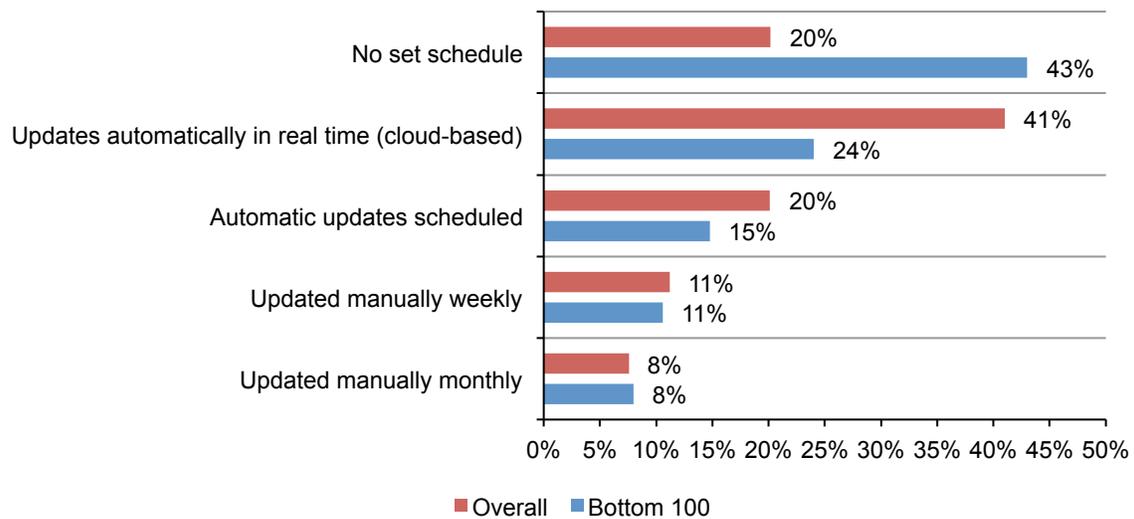
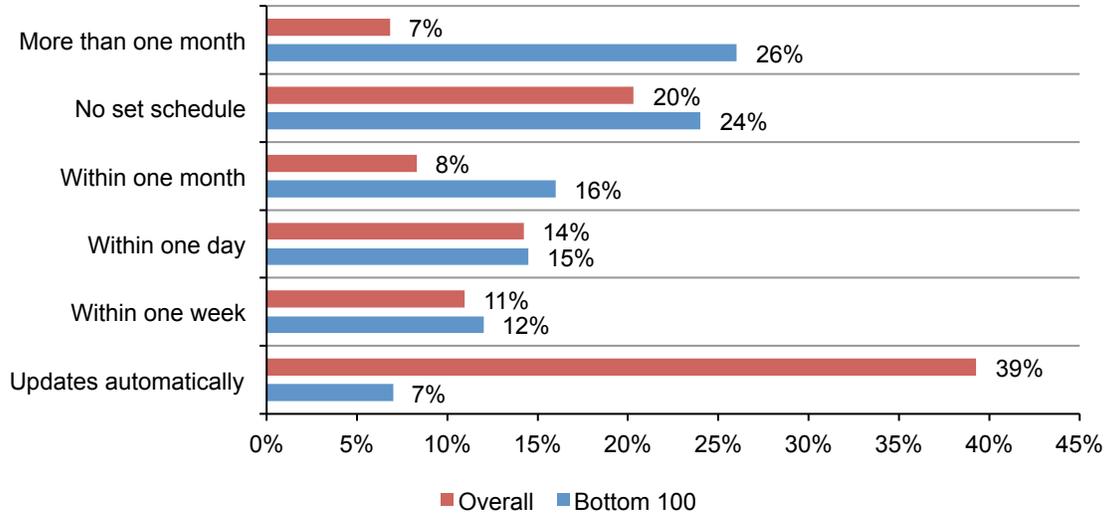


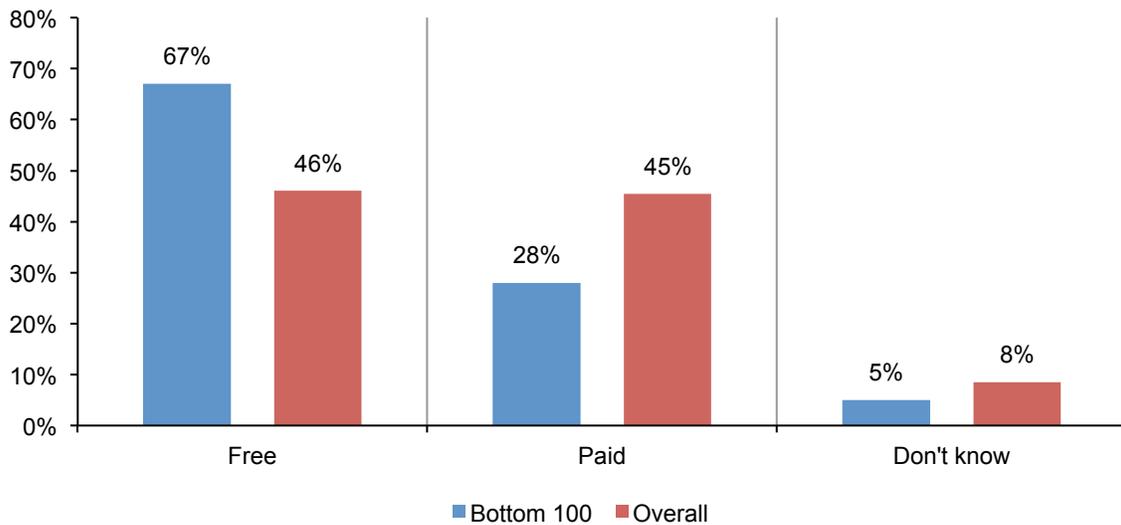
Figure 12 shows the frequency of computer operating system updates. Twenty-six percent of respondents in the Bottom 100 subsample but only 7 percent in the overall sample update on more than a monthly cycle. In contrast, 7 percent of respondents in the Bottom 100 subsample, and 39 percent in the overall sample, update automatically.

Figure 12. How frequently do you update your computer operating system?



According to respondents that use AV software, 46 percent deploy free software and 45 percent deploy paid software. With respect to the Bottom 100 subsample, 67 percent use free AV software and 28 percent use paid software, as shown in Figure 13.

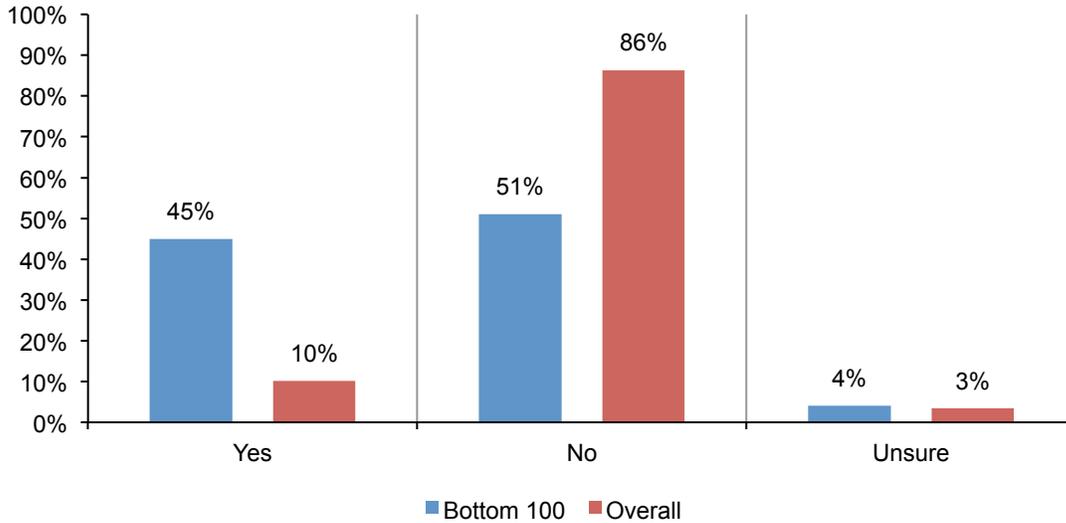
Figure 13. Do you use paid or free AV software?



The impact of a lost device on cyber hygiene

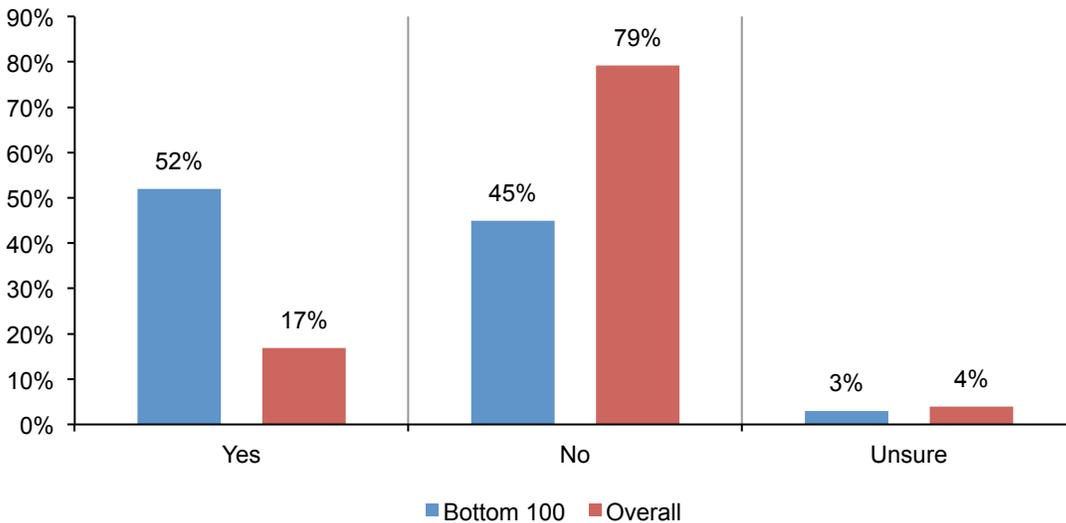
According to the Overall sample, only 10 percent said they lost a PC, tablet, smart phone and/or USB memory stick over the past 12 months. With respect to the Bottom 100 subsample, 45 percent said they lost one or more data-bearing devices over the past 12 months, as shown in Figure 14.

Figure 14. Over the past year, did you lose a PC, tablet, smart phone or USB memory stick?



According to Figure 15, 7 percent of respondents in the Overall sample said they retired, traded-in, sold or gave away a PC, tablet, smart phone and/or USB memory stick over the past 12 months. With respect to the Bottom 100 subsample, 52 percent said they retired, traded-in or gave away one or more data-bearing devices over the past 12 months.

Figure 15. Over the past year, did you retire, trade-in, sell, giveaway or recycle a PC, tablet, smart phone or USB memory without first resetting to factory settings?



The impact of password practices on cyber hygiene

As shown in Figure 16, 19 percent of respondents in the Overall sample frequently share passwords with others. Another 45 percent share passwords but said it rarely happens. With respect to respondents in the Bottom 100 subsample, nearly half (49 percent) said they frequently share passwords or other access credentials with others. In addition, only 36 percent in the Overall sample and 15 percent in the Bottom 100 subsample said they never share passwords.

Figure 16. Do you ever share passwords or other access credentials with others?

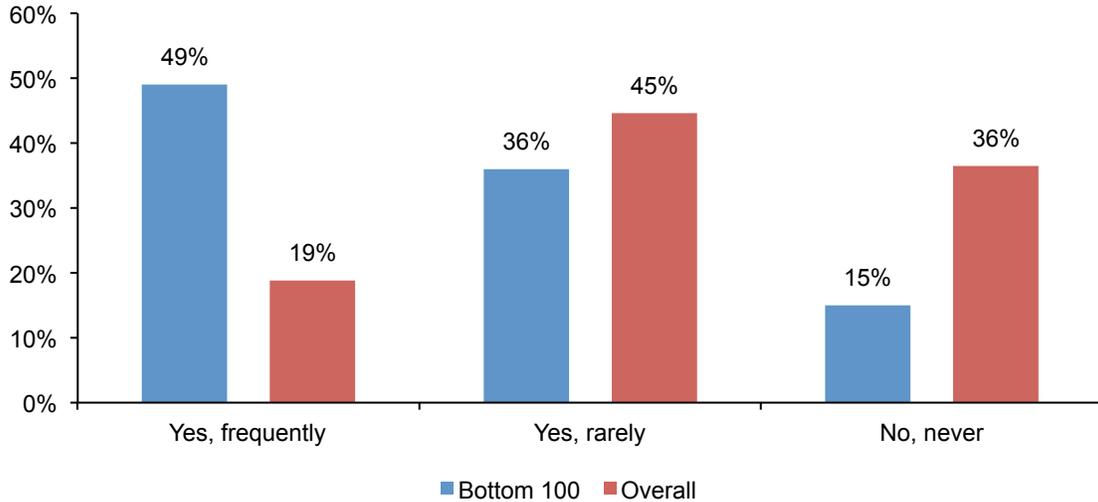


Figure 17 shows the percentage frequency of passwords or passphrases maintained by the Overall sample. According to the Overall sample, 15 percent said they maintain one or two separate passwords. In contrast, 41 percent of the Bottom 100 subsample maintain one or two separate passwords. Twenty-three percent of the overall sample and 5 percent of the Bottom 100 subsample maintain more than 20 separate passwords.

Figure 17. How many separate passwords or passphrases do you maintain on a regular basis?

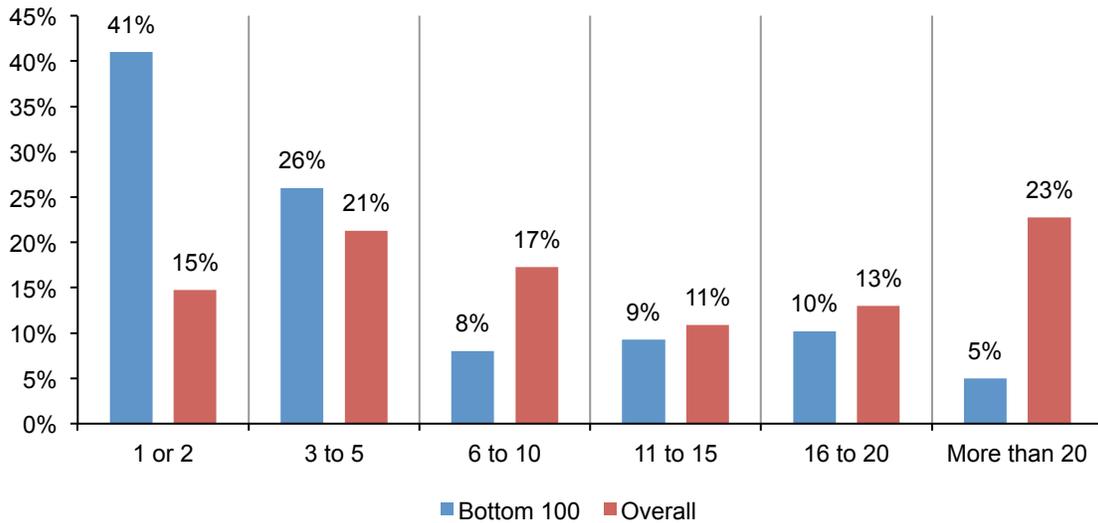
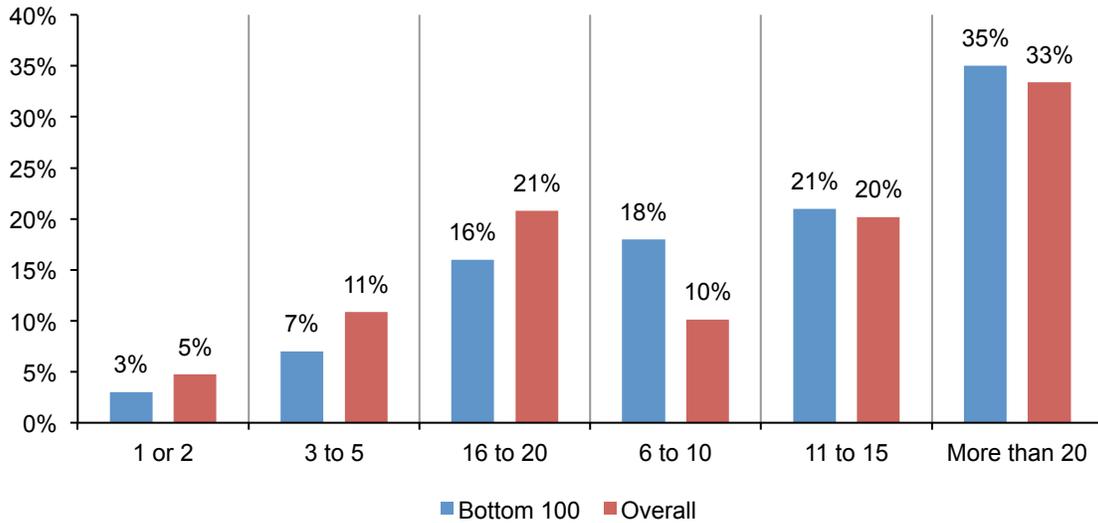


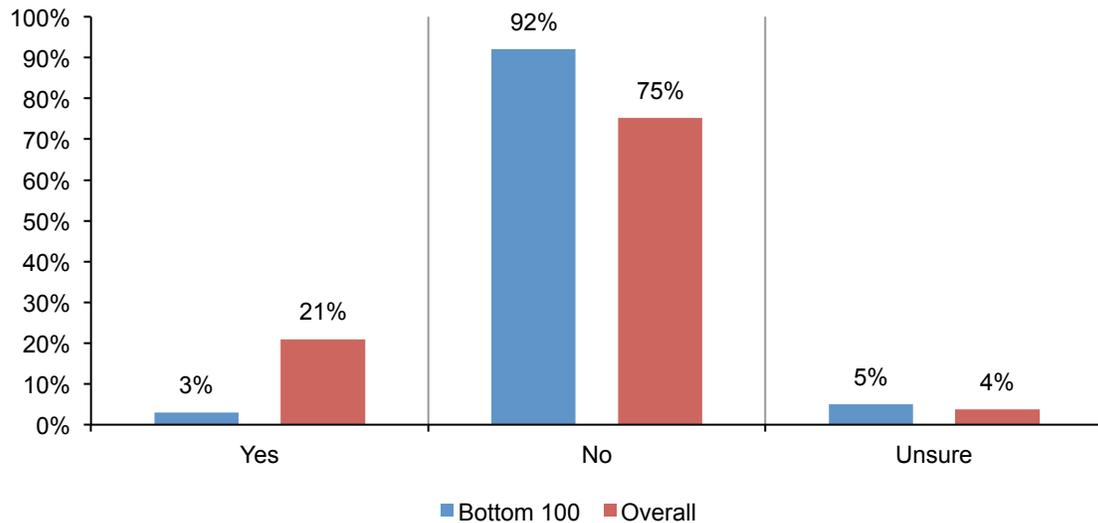
Figure 18 shows the percentage frequency of online accounts that require a username and password. According to the overall sample, one-third said they maintain more than 20 online accounts. Similarly, 35 percent of the Bottom 100 subsample maintain more than 20 online accounts. Only 5 percent of the Overall sample, and 3 percent of the Bottom 100 subsample, maintain more one or two separate online accounts.

Figure 18. How many online accounts do you have that require a username and password?



According to the Overall sample, 21 percent said they use a password manager. With respect to the Bottom 100 subsample, only 3 percent said they use a password manager.

Figure 19. Do you use a password manager, a software tool that assists in generating and retrieving complex passwords?



The impact of online behavior on cyber hygiene

Figure 20 shows that only 9 percent of respondents in the Overall sample, and none of the respondents in the Bottom 100 subsample said they use a privacy filter when working or traveling in tight spaces to prevent others from seeing content on their laptop or tablet.

Figure 20. Do you use a “privacy filter” (screen) when working or traveling in tight spaces?

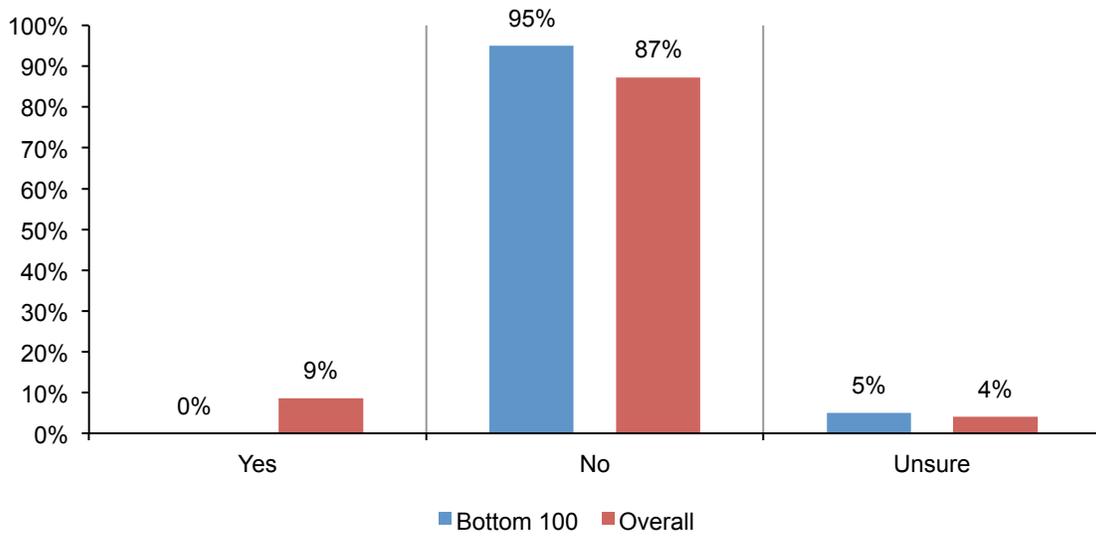
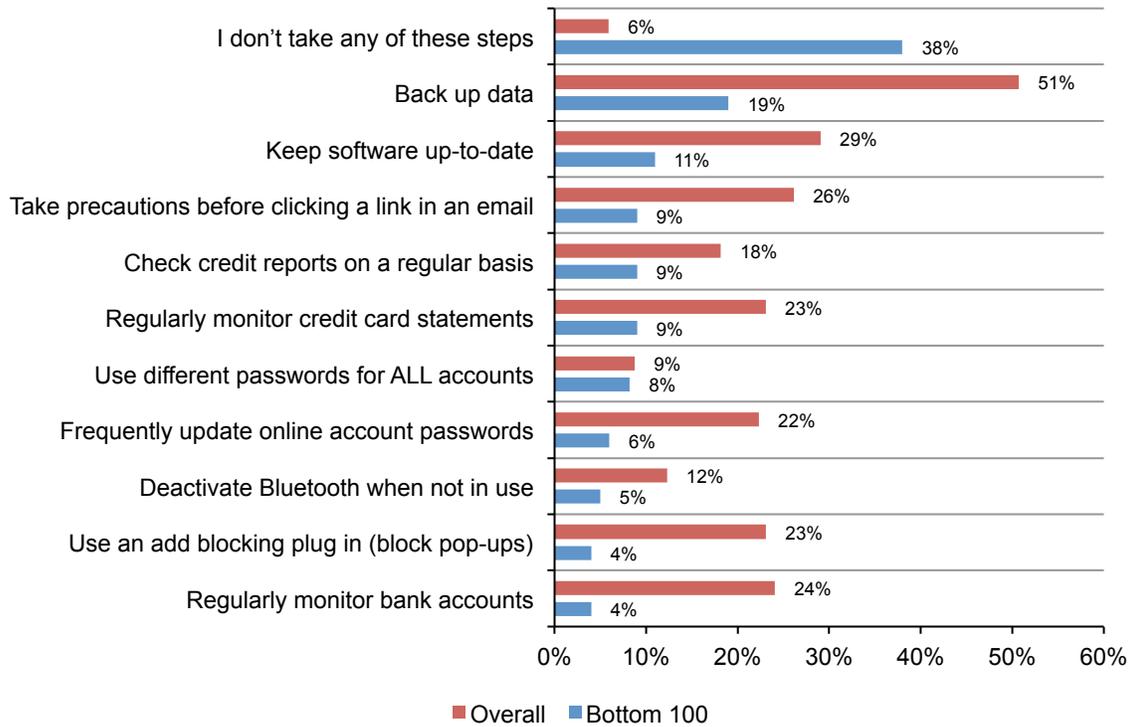


Figure 21 lists the good cyber hygiene practices or “online habits” exercised by respondents. As can be seen, the Bottom 100 subsample falls below the overall sample in every case. For example, 51 percent of the Overall sample backup data as compared to only 19 percent in the Bottom 100 subsample. In addition, only 6 percent of the overall sample said they don’t exercise any of these online habits versus 38 percent of respondents in the Bottom 100 subsample.

Figure 21. Which of the following online habits do you currently practice on a regular basis?



Part 3. Demographics

The following tables summarize 12 demographics for respondents in the overall sample and a group of respondents representing the riskiest individuals called the Bottom 100. Please use the margin of error when comparing the difference between the overall and Bottom 100 subsample. The margin of error was calculated for each question contained in our survey instrument. The grand Overall margin of error is simply the weighted Overall rate of 4.3 percent, which is specified at the 95 percent level of significance (two-tailed tests).

With respect to gender, female respondents represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than male respondents.

Gender:	Bottom 100	Overall	Diff
Female	60%	53%	7%
Male	40%	47%	-7%
Total	100%	100%	0%

Younger-aged respondents represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than older-aged respondents. The extrapolated age of respondents in the overall sample is 37 years, and 27.5 years in the Bottom 100 subsample.

Age:	Bottom 100	Overall	Diff
Under 18	5%	9%	-4%
18 to 21	30%	12%	18%
22 to 24	27%	14%	13%
25 to 30	13%	12%	1%
31 to 40	15%	12%	3%
41 to 45	5%	10%	-5%
46 to 50	0%	9%	-9%
51 to 55	0%	7%	-7%
56 to 60	3%	6%	-3%
61 to 65	2%	5%	-3%
66 to 70	0%	3%	-3%
Over 70	0%	1%	-1%
Total	100%	100%	0%
Extrapolated value	27.5	37.0	-9.4

With respect to marital status, single respondents represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than married respondents.

Marital status:	Bottom 100	Overall	Diff
Married	30%	40%	-10%
Single	70%	60%	10%
Total	100%	100%	0%

With respect to ethnic status, Caucasian respondents represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than respondents with other ethnicities.

Ethnic status:	Bottom 100	Overall	Diff
African American	10%	14%	-4%
Asian	10%	12%	-2%
Caucasian	66%	55%	11%
Hispanic	14%	15%	-1%
Other	0%	4%	-4%
Total	100%	100%	0%

With respect to education, respondents who earned a college degree represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than respondents with other educational backgrounds.

Highest level of education:	Bottom 100	Overall	Diff
High School	15%	22%	-7%
Vocational	14%	19%	-5%
Some college (attended, no degree)	25%	26%	-1%
College (4 year degree)	36%	23%	13%
Graduate School	10%	9%	1%
Post Graduate / Doctorate	0%	1%	-1%
Total	100%	100%	0%

Respondents with a higher household income represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than respondents with a lower household income. The extrapolated income of respondents in the overall sample is \$70.48 thousand, and \$88.58 thousand in the Bottom 100 subsample.

Household Income:	Bottom 100	Overall	Diff
Less than \$25,000	9%	6%	3%
\$25,000 to \$40,000	11%	17%	-6%
\$40,001 to \$60,000	24%	27%	-3%
\$60,001 to \$80,000	19%	25%	-6%
\$80,001 to \$100,000	16%	14%	2%
\$100,001 to \$150,000	11%	8%	3%
\$150,001 to \$250,000	6%	2%	4%
\$250,001 to \$500,000	3%	1%	2%
More than \$500,000	1%	0%	1%
Total	100%	100%	0%
Extrapolated value (\$000 omitted)	\$88.58	\$70.48	\$18.09

Respondents without children living in the household represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than respondents with children living in the household.

Children living in household:	Bottom 100	Overall	Diff
None	85%	55%	30%
One	15%	29%	-14%
Two or three	0%	13%	-13%
Four or five	0%	2%	-2%
More than five	0%	1%	-1%
Total	100%	100%	0%

With respect to employment status, respondents who are employed on a full or part-time basis represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than respondents who are not employed on a full or part-time basis.

Employment status:	Bottom 100	Overall	Diff
Business owner	0%	3%	-3%
Full time employee	59%	46%	13%
Part time employee	35%	26%	9%
Student	6%	12%	-6%
Retired	0%	8%	-8%
Military	0%	1%	-1%
Unemployed	0%	5%	-5%
Total	100%	100%	0%

With respect to the number of desktops or laptops in the household, respondents who have 3 to 5 desktops or laptops have a higher level of cyber riskiness (or a lower level of cyber hygiene) than respondents with 6 or more desktop or laptop computers.

How many desktops or laptops do you have in your household?	Bottom 100	Overall	Diff
None	0%	1%	-1%
1 or 2	41%	41%	0%
3 to 5	33%	43%	-10%
6 to 10	14%	10%	4%
More than 10	12%	6%	6%
Total	100%	100%	0%

With respect to desktop or laptop operating systems, Windows-based operating systems represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than computers with Mac-based operating systems.

What percent of desktops or laptops are Windows (vs. Mac)	Bottom 100	Overall	Diff
Windows is less than 50%	29%	46%	-17%
Windows is more than 50%	71%	54%	17%
Total	100%	100%	0%

With respect to the number of tablets or smart phones in the household, respondents who have 3 to 5 tablets or smart phones have a lower level of cyber riskiness (or a higher level of cyber hygiene) than respondents with 1 or 2 devices.

How many tablets or smart phones do you have in your household?	Bottom 100	Overall	Diff
None	0%	1%	-1%
1 or 2	30%	38%	-8%
3 to 5	45%	38%	7%
6 to 10	15%	17%	-2%
More than 10	10%	6%	4%
Total	100%	100%	0%

With respect to tablet or smart phone operating systems, Android operating systems represent a higher level of cyber riskiness (or a lower level of cyber hygiene) than devices with an iOS operating systems.

What percent of tablets or smart phones are Android (vs. IOS)	Bottom 100	Overall	Diff
Android less than 50%	36%	50%	-14%
Android is more than half (50%)	64%	50%	14%
Total	100%	100%	0%

Appendix 1: Cyber Hygiene Index and riskiest state ranking

U.S. State	Abbreviation	Sample size	Index value	Rank 1	Rank 2
Florida	FL	142	-6.29	1	51
Wyoming	WY	40	-5.55	2	50
Montana	MT	47	-4.28	3	49
New Mexico	NM	51	-3.78	4	48
Illinois	IL	138	-3.07	5	47
California	CA	195	-3.05	6	46
Arkansas	AR	56	-2.94	7	45
Louisiana	LA	71	-2.91	8	44
Idaho	ID	47	-2.86	9	43
Arizona	AZ	75	-2.82	10	42
Washington DC	DC	85	-2.75	11	41
Hawaii	HI	47	-2.73	12	40
Alabama	AL	56	-2.72	13	39
Oklahoma	OK	59	-2.62	14	38
Georgia	GA	107	-2.61	15	37
Connecticut	CT	88	-2.56	16	36
Mississippi	MS	52	-2.47	17	35
Missouri	MO	115	-2.42	18	34
Delaware	DE	72	-2.38	19	33
Colorado	CO	100	-2.37	20	32
Virginia	VA	127	-2.36	21	31
Maryland	MD	89	-2.27	22	30
North Carolina	NC	102	-2.23	23	29
Nevada	NV	87	-2.13	24	28
Alaska	AK	49	-2.11	25	27
South Carolina	SC	79	-2.10	26	26
Tennessee	TN	80	-2.06	27	25
West Virginia	WV	65	-2.05	28	24
South Dakota	SD	47	-1.99	29	23
Kentucky	KY	80	-1.93	30	22
New York	NY	179	-1.90	31	21
Pennsylvania	PA	119	-1.62	32	20
New Jersey	NJ	116	-1.56	33	19
Texas	TX	159	-1.44	34	18
Indiana	IN	92	-1.15	35	17
North Dakota	ND	48	-0.92	36	16
Iowa	IA	94	0.13	37	15
Washington	WA	84	0.17	38	14
Oregon	OR	96	0.25	39	13
Vermont	VT	55	0.35	40	12
Kansas	KS	81	0.48	41	11
Wisconsin	WI	80	0.74	42	10
Ohio	OH	89	0.82	43	9
Michigan	MI	93	0.89	44	8
Maine	ME	56	0.96	45	7
Nebraska	NE	53	1.14	46	6
Minnesota	MN	80	1.90	47	5
Rhode Island	RI	49	2.30	48	4
Utah	UT	56	2.44	49	3
Massachusetts	MA	91	4.20	50	2
New Hampshire	NH	72	4.29	51	1

Appendix 2: Survey questions plus index weighting

Background and cyber hygiene

Q1a. Over the past year, did you have your identity stolen?	Score	Bottom 100	Overall
Yes	-4	15%	11%
No (skip to Q4)	0	75%	81%
Don't know (skip to Q4)	-2	10%	8%
Total		100%	100%

Q1b. If yes, how many times in the past years were you a victim of identity theft?	Score	Bottom 100	Overall
1 time	NA	55%	50%
2 times	NA	19%	23%
3 times	NA	9%	9%
4 times	NA	4%	5%
5 times	NA	2%	2%
More than 5 times	NA	6%	6%
Don't know	NA	5%	5%
Total		100%	100%

Q2. What were the main consequences of the identity theft incident? Please select all that apply.	Score	Bottom 100	Overall
Misuse of my credit or debit card/ATM card	NA	41%	43%
Criminal took control of my bank accounts	NA	9%	7%
Creation of new debt such a loan or mortgage	NA	9%	9%
My tax return was stolen	NA	11%	10%
My credit (FICO) score declined	NA	46%	50%
My private information was stolen	NA	35%	34%
My medical records were stolen	NA	8%	10%
My social media accounts were misused	NA	9%	8%
Other (please specify)	NA	1%	1%
None of the above	NA	6%	5%
Don't know	NA	3%	4%
Total		178%	182%

Q3a. Did the identity theft incident impact your level of cautiousness when connected to the Internet or when sharing your personal information?	Score	Bottom 100	Overall
Yes, significant impact	4	5%	42%
Yes, some impact	2	35%	33%
Yes, minimal impact	0	0%	11%
No impact	-4	60%	14%
Total		100%	100%

Q3b. If yes, did you make any changes to your online behavior?	Score	Bottom 100	Overall
Changed passwords	1	11%	54%
Limited online purchases	1	13%	14%
Limited making online purchases only to websites I believe are reputable	1	15%	26%
Stopped online banking and other financial transactions	1	11%	10%
Started credit monitoring or identity protection service	0	15%	37%
Monitor financial accounts more closely	1	9%	39%
No changes made	-4	62%	14%
Total		136%	196%

Q4. Do you use a credit monitoring or identity protection service such as LifeLock, EZ Shield, ID Watch Dog or others?	Score	Bottom 100	Overall
Yes	2	15%	42%
No	-2	85%	54%
Unsure	0	0%	3%
Total		100%	100%

Q5. Over the past year, how many times was your PC, tablet and/or smart phone negatively impacted as a result of malware (including ransomware)?	Score	Bottom 100	Overall
None	4	0%	35%
1 or 2	0	6%	18%
3 to 5	-2	12%	12%
6 to 10	-4	36%	14%
More than 10	-4	46%	21%
Total		100%	100%

Q6. Over the past year, how many times do you suspect that you received a phishing email (malicious email based on the definition above)?	Score	Bottom 100	Overall
None	0	5%	27%
1 to 5	0	9%	25%
6 to 10	-1	18%	14%
11 to 20	-1	13%	11%
More than 20	-2	55%	23%
Total		100%	100%

Q7. Do you use anti-virus software (AV) on your laptop, desktop or smart phone (Norton, McAfee, Webroot etc.)	Score	Bottom 100	Overall
Yes	2	24%	50%
No (skip to Q12)	-2	76%	46%
Unsure (skip to Q12)	0	0%	5%
Total		100%	100%

Q8. Which of your devices has AV software?	Score	Bottom 100	Overall
Windows PC	NA	38%	65%
Mac PC	NA	29%	33%
iOS phone	NA	18%	10%
Android phone	NA	30%	19%
iPad	NA	8%	11%
Tablet	NA	6%	8%
Total		129%	146%

Q9. In general, how frequently do you update your AV software?	Score	Bottom 100	Overall
Updates automatically in real time (cloud-based)	1	24%	41%
Automatic updates scheduled	1	15%	20%
Updated manually weekly	0	11%	11%
Updated manually monthly	0	8%	8%
No set schedule	0	43%	20%
Total		100%	100%

Q10. In general, how frequently do you update your computer operating system?	Score	Bottom 100	Overall
Updates automatically	1	7%	39%
Within one day	1	15%	14%
Within one week	0	12%	11%
Within one month	0	16%	8%
More than one month	0	26%	7%
No set schedule	0	24%	20%
Total		100%	100%

Q11a. Do you use paid or free AV software?	Score	Bottom 100	Overall
Free	-1	67%	46%
Paid	1	28%	45%
Unsure (skip to Q12)	0	5%	8%
Total		100%	100%

Q11b. If free, which of the following AV software solutions to you use?	Score	Bottom 100	Overall
Avast	NA	20%	16%
AVG	NA	16%	21%
Bitdefender	NA	20%	20%
Kaspersky	NA	22%	23%
Adaware	NA	6%	7%
Comodo	NA	10%	8%
Other (please specify)	NA	7%	5%
Total		100%	100%

Q11c. If paid, which of the following AV software solutions to you use?	Score	Bottom 100	Overall
Webroot	NA	15%	20%
Norton	NA	20%	21%
McAfee	NA	16%	14%
Trend Micro	NA	17%	17%
Kaspersky	NA	15%	15%
Avast	NA	10%	9%
Other (please specify)	NA	6%	5%
Total		100%	100%

Q12. Over the past year, did you lose a PC, tablet, smart phone or USB memory stick?	Score	Bottom 100	Overall
Yes	-1	45%	10%
No	0	51%	86%
Unsure	0	4%	3%
Total		100%	100%

Q13. Over the past year, did you retire, trade-in, sell, giveaway or recycle a PC, tablet, smart phone or USB memory without first resetting to factory settings?	Score	Bottom 100	Overall
Yes	-3	52%	17%
No	0	45%	79%
Unsure	-2	3%	4%
Total		100%	100%

Q14. Do you ever share passwords or other access credentials with others?	Score	Bottom 100	Overall
Yes, frequently	-4	49%	19%
Yes, rarely	-2	36%	45%
No, never	2	15%	36%
Total		100%	100%

Q15. How many separate passwords or passphrases do you maintain on a regular basis?	Score	Bottom 100	Overall
1 or 2	-3	41%	15%
3 to 5	-2	26%	21%
6 to 10	-1	8%	17%
11 to 15	0	9%	11%
16 to 20	1	10%	13%
More than 20	2	5%	23%
Total		100%	100%

Q16. How many online accounts do you have that require a username and password?	Score	Bottom 100	Overall
1 or 2	NA	3%	5%
3 to 5	NA	7%	11%
6 to 10	NA	18%	10%
11 to 15	NA	21%	20%
16 to 20	NA	16%	21%
More than 20	NA	35%	33%
Total	NA	100%	100%

Q17. Do you use a password manager, a software tool that assists in generating and retrieving complex passwords?	Score	Bottom 100	Overall
Yes	2	3%	21%
No	-1	92%	75%
Unsure	0	5%	4%
Total		100%	100%

Q18. Do you use public WiFi when traveling for business or leisure? For example in an airport, library or coffee shop?	Score	Bottom 100	Overall
Yes, frequently	-2	50%	45%
Yes, rarely	-1	39%	29%
No, never	2	11%	25%
Total		100%	100%

Q19. Do you use a secure gateway such as a virtual private network (VPN) when connecting to the Internet?	Score	Bottom 100	Overall
Yes	2	1%	20%
No	-1	94%	76%
Unsure	0	5%	4%
Total		100%	100%

Q20a. How often do you backup data and applications contained on your PC, tablet, smart phone or other data-bearing devices?	Score	Bottom 100	Overall
Updates automatically	3	6%	23%
Daily	2	0%	3%
Weekly	1	2%	2%
Monthly	0	0%	3%
A few times each year	-1	14%	7%
No set schedule	-2	18%	15%
I never backup my data and applications (skip to Q21)	-3	60%	46%
Total		100%	100%

Q20b. How do you backup your data? Please select all that apply.	Score	Bottom 100	Overall
Cloud	NA	38%	38%
Locally on my computer	NA	29%	28%
External hard drive	NA	21%	21%
Burned CD/DVD	NA	12%	13%
Total		100%	100%

Q21. Do you use a "privacy filter" (screen) when working or traveling in tight spaces (e.g., to prevent others from seeing content on your laptop or tablet).	Score	Bottom 100	Overall
Yes	1	0%	9%
No	-1	95%	87%
Unsure	0	5%	4%
Total		100%	100%

Q22. Which of the following online habits do you currently practice on a regular basis? Please check all that apply.	Score	Bottom 100	Overall
Frequently update online account passwords	1	6%	22%
Regularly monitor bank accounts	1	4%	24%
Regularly monitor credit card statements	1	9%	23%
Check credit reports on a regular basis	1	9%	18%
Use an add blocking plug in (block pop-ups)	1	4%	23%
Use reliable antivirus software	0	3%	50%
Use different passwords for ALL accounts	0	8%	9%
Keep software up-to-date	0	11%	29%
Take precautions before clicking a link in an email	1	9%	26%
Use a VPN	0	6%	18%
Deactivate Bluetooth when not in use	1	5%	12%
Back up data	0	19%	51%
Use privacy screen when traveling or in open spaces	0	0%	8%
Use a password manager	0	5%	21%
I don't take any of these steps	-4	38%	6%
Total		136%	339%

Thank you for your participation. All responses are completely confidential.
Please contact research@ponemon.org or call us at 800.887.3118 if you have any questions.

Ponemon Institute

Advancing Responsible Information Management

Ponemon Institute is dedicated to independent research and education that advances responsible information and privacy management practices within business and government. Our mission is to conduct high quality, empirical studies on critical issues affecting the management and security of sensitive information about people and organizations.

We uphold strict data confidentiality, privacy and ethical research standards. We do not collect any personally identifiable information from individuals (or organization identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant or improper questions.