PewResearchCenter

NUMBERS, FACTS AND TRENDS SHAPING THE WORLD

FOR RELEASE MARCH 22, 2017

What the Public Knows About Cybersecurity

A majority of internet users can answer fewer than half the questions correctly on a difficult knowledge quiz about cybersecurity issues and concepts

BY *Kenneth Olmstead and Aaron Smith*

FOR MEDIA OR OTHER INQUIRIES:

Lee Rainie, Director, Internet, Science and Technology Research
Aaron Smith, Associate Director, Research
Dana Page, Senior Communications Manager
202.419.4372

www.pewresearch.org

RECOMMENDED CITATION: Pew Research Center, March, 2017, "What the Public Knows About Cybersecurity"

About Pew Research Center

Pew Research Center is a nonpartisan fact tank that informs the public about the issues, attitudes and trends shaping America and the world. It does not take policy positions. The Center conducts public opinion polling, demographic research, content analysis and other data-driven social science research. It studies U.S. politics and policy; journalism and media; internet, science and technology; religion and public life; Hispanic trends; global attitudes and trends; and U.S. social and demographic trends. All of the Center's reports are available at www.pewresearch.org. Pew Research Center is a subsidiary of The Pew Charitable Trusts, its primary funder.

What the Public Knows About Cybersecurity

A majority of internet users can answer fewer than half the questions correctly on a difficult knowledge quiz about cybersecurity issues and concepts

In an increasingly digital world, an individual's personal data can be as valuable – and as vulnerable – to potential wrongdoers as any other possession. Despite the risk-reducing impact of good cybersecurity habits and the prevalence of cyberattacks on institutions and individuals alike, a Pew Research Center survey finds that many Americans are unclear about some key cybersecurity topics, terms and concepts. A majority of online adults can identify a strong password when they see one and recognize the dangers of using public Wi-Fi. However, many struggle with more technical cybersecurity concepts, such as how to identify true two-factor authentication or determine if a webpage they are using is encrypted.

This survey consisted of 13 questions designed to test Americans' knowledge of a number of cybersecurity issues and terms. Cybersecurity is a complicated and diverse subject, but these questions cover many of the general concepts and basic building blocks that cybersecurity experts stress are important for users to protect themselves online. However, the typical (median) respondent answered only five of these 13 knowledge questions correctly (with a mean of 5.5 correct answers). One-in-five (20%) answered more than eight questions accurately, and just 1% received a "perfect score" by correctly answering all 13 questions.

These are the key findings from an online survey of 1,055 adult internet users living in the United States conducted June 17-27, 2016.

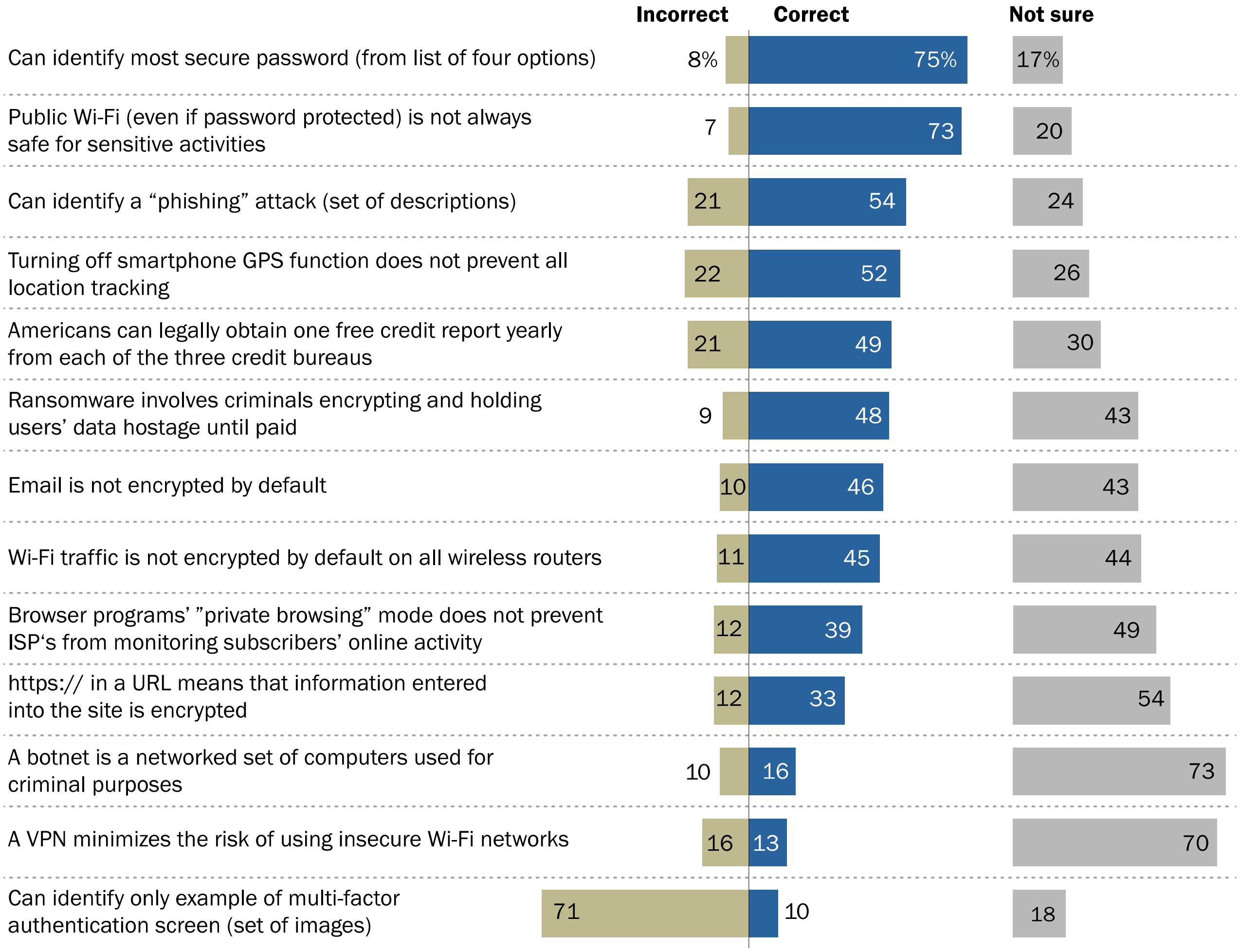
Cybersecurity knowledge varies widely by topic and level of technical detail

Of the 13 questions in the survey, a substantial majority of online adults were able to correctly answer just two of them. First, 75% of online adults can correctly identify the strongest password from a list of four options. The correct password in this case is the password that does not contain words in the dictionary; does contain letters, numbers and symbols; and has a combination of both upper and lower case letters. A similar share (73%) is aware that if a public Wi-Fi network is password protected, it *does not* necessarily mean that it is safe to perform sensitive tasks, such as online banking, using that network.

Meanwhile, around half of internet users are able to correctly answer several other questions in the survey. Some 54% of internet users are able to identify examples of phishing attacks. Similarly, 52% correctly say that turning off the GPS function of a smartphone *does not* prevent all tracking of that device (mobile phones can also be tracked via the cellular towers or Wi-Fi networks to which they are connected).

Many Americans are unsure on a range of cybersecurity topics

% of internet users answering each question …



Source: Survey conducted June 17-27, 2016.
"What the Public Knows About Cybersecurity"

PEW RESEARCH CENTER

Additionally, 49% of internet users know that Americans are legally entitled to get one free copy of their credit report annually from each of the three major credit bureaus. This issue is not specifically related to any technical aspects of cybersecurity, but cybersecurity experts recommend that anyone who uses the internet for financial or other sensitive transactions regularly check their credit reports to discover evidence of identity theft or other kinds of fraud. A similar share (48%) can correctly define the term "ransomware." This refers to criminals accessing someone's computer, encrypting their personal files and data, and holding that data hostage unless they are paid to decrypt the files.

Americans' practical understanding of email and Wi-Fi encryption is also relatively mixed: 46% of internet users are able to correctly identify that the statement "all email is encrypted by default" is false. Some email services do encrypt users' messages, but this is not a standard feature of all email services. At the same time, 45% correctly identify the statement "all Wi-Fi traffic is encrypted by default on all wireless routers" is also false.

Public knowledge of cybersecurity is lower on some relatively technical issues

Internet users' understanding of the remaining cybersecurity issues measured in the survey is lower – in some cases dramatically so. For instance, 39% of internet users are aware that internet service providers (ISPs) are able to see the sites their customers are visiting while utilizing the "private browsing" mode on their internet browsers. Private browsing mode only prevents the browser itself, and in some cases the user's computer or smartphone, from saving this information – it is still visible to the ISP. And one-third (33%) are aware that the letter "s" in a URL beginning with "https://" indicates that the traffic on that site is encrypted.

Meanwhile, just 16% of online adults are aware that a group of computers that is networked together and used by hackers to steal data is referred to as a "botnet." A similar share (13%) is aware that the risks of using insecure Wi-Fi networks can be minimized by using a virtual private network, or VPN.

Lastly, cybersecurity experts commonly recommend that internet users employ "two-factor" or "multi-factor" authentication on any account where it is available. Two-factor authentication generally requires users to log in to a site using something the user *knows* (such as a traditional password) along with something the user *possesses* (such as a mobile phone or security token), thus providing an additional layer of security in the event that someone's password is hacked or stolen. But when presented with four images of different types of online login screens, just 10% of online adults are able to correctly identify the one – and only one – example in the list of a true multi-factor authentication process. In this case, the correct answer was a picture of a login screen featuring a temporary code sent to a user's phone that will only help them login for a limited period of time. Several of the other answer options illustrated situations in which users were required to perform a secondary action before accessing a page – such as entering a captcha, or answering a security question. However, none of these other options are examples of two-factor authentication.

A significant share of online adults are simply not sure of the correct answer on a number of cybersecurity knowledge questions

Although the share of online adults who can correctly answer questions about cybersecurity issues varies from topic to topic, in most cases the share providing an actual incorrect answer is relatively small. Rather, many users indicate that they simply are not sure of the correct answer to a large number of the questions in this survey.

At the low end, around one-in-five online adults indicate they are not sure how to identify the most secure password from a list (17%), how to identify multi-factor identification (18%) or whether public Wi-Fi is safe for sensitive activities (20%). At the high end, a substantial majority of internet users are not sure what purpose a VPN serves (70%) or what a botnet does (73%). There are also a number of other questions in this survey where "not sure" responses are markedly more common than incorrect answers. These include the definition of ransomware, whether or not email and Wi-Fi traffic are encrypted by default, whether private browsing mode prevents ISPs from monitoring customer activity and how to identify whether or not a webpage is encrypted. In fact, there is only one question on the survey – how to identify a multi-factor authentication screen – for which a larger share of respondents answer incorrectly than indicate they are not able to answer the question at all.

Those with higher levels of education and younger internet users are more likely to answer cybersecurity questions correctly

Broad differences in cybersecurity knowledge by educational attainment

% of internet users answering each question correctly

	HS or less	Some college	College+	College+ – HS or less diff
Wi-Fi traffic is not encrypted by default on all wireless routers.	30%	46%	64%	+34
https:// in a URL means that information entered into the site is encrypted	22	29	54	+32
Email is not encrypted by default	33	44	65	+32
Ransomware involves criminals encrypting and holding users' data hostage until paid	35	47	66	+31
Turning off smartphone GPS function does not prevent all location tracking	38	58	65	+27
Can identify most secure password (from list of four options)	63	77	88	+25
Americans can legally obtain one free credit report yearly from each of the three credit bureaus	38	52	61	+23
Can identify a "phishing" attack (set of descriptions)	45	54	65	+20
Browser programs' "private browsing" mode does not prevent ISPs from monitoring subscribers' online activity	32	37	51	+19
Public Wi-Fi (even if password protected) is not always safe for sensitive activities	65	75	83	+18
A botnet is a networked set of computers used for criminal purposes	11	14	25	+14
Can identify only example of multi-factor authentication screen (set of images)	5	9	19	+14
A VPN minimizes the risk of using insecure Wi-Fi networks	10	11	21	+11
AVERAGE NUMBER CORRECT OVERALL	4.0	5.5	7.0	+3.0

Note: Some college includes those who attended but did not graduate with four-year degrees as well as those with two-year degrees.
Source: Survey conducted June 17-27, 2016.
"What the Public Knows About Cybersecurity "

PEW RESEARCH CENTER

Internet users' knowledge of cybersecurity varies by several demographic factors. The most consistent differences are related to educational attainment.

Those with college degrees or higher answered an average of 7.0 of the 13 questions in the survey correctly, compared with an average of 5.5 among those who have attended but not graduated from college and an average of just 4.0 for those with high school diplomas or less.

Roughly one-quarter (27%) of those with college degrees answered 10 or more questions correctly, compared with 9% of those who have attended but not graduated from college and just 4% of those with high school diplomas or less.

On all 13 questions in the survey, there is at least an 11 percentage point difference in correct answers between the highest- and lowest-educated groups. And there are four questions with a difference of 30 percentage points or more between the highest- and lowest-educated groups. These include whether or not Wi-Fi traffic is encrypted by default on all wireless routers (a difference of 34 points); what "https://" in a URL refers to (32 points); whether or not all email is encrypted by default (32 points); and the definition of ransomware (31 points).

Modest differences in cybersecurity knowledge by age

% of internet users answering each question correctly

	18-29	30-49	50-64	65+	Youngest – oldest diff
Browser programs' "private browsing" mode does not prevent ISPs from monitoring subscribers' online activity	52%	46%	31%	25%	+27
Turning off smartphone GPS function does not prevent all location tracking	63	54	49	40	+23
Can identify only example of multi-factor authentication screen (set of images)	17	14	6	3	+14
A botnet is a networked set of computers used for criminal purposes	24	19	11	10	+14
Public Wi-Fi (even if password protected) is not always safe for sensitive activities	78	72	75	68	+10
https:// in a URL means that information entered into the site is encrypted	33	43	28	26	+7
Wi-Fi traffic is not encrypted by default on all wireless routers.	45	50	44	39	+6
Can identify most secure password (from list of four options)	78	78	69	73	+5
Email is not encrypted by default	46	49	45	42	+4
Ransomware involves criminals encrypting and holding users' data hostage until paid	49	51	46	46	+3
A VPN minimizes the risk of using insecure Wi-Fi networks	13	18	11	10	+3
Americans can legally obtain one free credit report year from each of the three credit bureaus	48	55	45	46	+2
Can identify a "phishing" attack (set of descriptions)	52	55	54	54	-2
AVERAGE NUMBER CORRECT OVERALL	6.0	6.0	5.0	5.0	+1.0

Source: Survey conducted June 17-27, 2016.
" What the Public Knows About Cybersecurity "

PEW RESEARCH CENTER

Cybersecurity knowledge also varies by respondent age, although these differences are much less dramatic than the differences pertaining to educational attainment. Indeed, on a number of these questions internet users age 65 and older are just as knowledgeable as those ages 18 to 29. For instance, older and younger users are equally likely to be able to identify a phishing attack, identify the most secure password from a list and know how many free credit reports Americans are entitled to by law. However, younger users score higher on certain questions – such as whether “private browsing” mode prevents ISPs from tracking users’ online activities (a 27 point difference) or whether turning off the GPS feature on a smartphone disables all tracking of that device (a 23 point difference).

Overall, 18- to 29-year-olds correctly answered a mean of 6.0 out of 13 questions, compared with a mean of 5.0 among those 65 and older.

Acknowledgments

This report was made possible by The Pew Charitable Trusts. It is a collaborative effort based on the input and analysis of the following individuals:

Primary researchers

Kenneth Olmstead, *Research Associate*
Aaron Smith, *Associate Director, Research*

Research team

Lee Rainie, *Director, Internet, Science and Technology Research*
Maeve Duggan, *Research Associate*
Monica Anderson, *Research Associate*
Andrew Perrin, *Research Assistant*

Editorial and graphic design

Margaret Porteus, *Information Graphics Designer*
Shannon Greenwood, *Copy editor*

Communications and web publishing

Dana Page, *Senior Communications Manager*
Shannon Greenwood, *Associate Digital Producer*

Methodology

The analysis in this report is based on a survey conducted June 17-27, 2016, among a sample of 1,055 adult internet users 18 years of age or older. The survey was conducted in English and Spanish by the GfK Group using KnowledgePanel, its nationally representative online research panel. KnowledgePanel members are recruited through probability sampling methods and include both those with internet access and those without (KnowledgePanel provides internet access for those who do not have it and, if needed, a device to access the internet when they join the panel). A combination of random-digit dialing (RDD) and address-based sampling (ABS) methodologies have been used to recruit panel members (in 2009 KnowledgePanel switched its sampling methodology for recruiting panel members from RDD to ABS). The panel includes households with landlines and cellular phones, including those only with cellphones and those without phones. KnowledgePanel continually recruits new panel members throughout the year to offset panel attrition as people leave the panel.

To qualify for the survey, a panel member must have been 18 years of age or older and a current internet user. In all, 1,804 panelists were invited to take part in the survey. Of 1,088 cases completing the main survey, 1,055 were determined to be valid cases to be included in the final analyses. The remaining 33 cases were excluded due to refusing to answer more than one-quarter of the substantive survey questions or completing outside of three standard deviations of the duration time. All sampled members received an initial email to notify them of the survey and provide a link to the survey questionnaire. Additional follow-up reminders were sent to those who had not yet responded as needed.

The final sample of 1,055 adults was weighted using an iterative technique that matches gender and, within gender, age, race/ethnicity, education, region, household income, household internet access and primary language to parameters from the March 2015 Census Bureau's Current Population Survey (CPS). This weight is multiplied by an initial sampling or base weight that corrects for differences in the probability of selection of various segments of GfK's sample and by a panel weight that adjusts for any biases due to nonresponse and noncoverage at the panel recruitment stage (using all of the parameters described above). Details about the GfK panel-level weights can be found at:

http://www.knowledgenetworks.com/knpanel/docs/KnowledgePanel(R)-Design-Summary-Description.pdf

Sampling errors and statistical tests of significance take into account the effect of weighting at each of these stages. The margin of sampling error at the 95% confidence level is plus or minus 3.2

percentage points for results based on the full sample (n=1,055). The following table shows the unweighted sample sizes and the error attributable to sampling that would be expected at the 95% level of confidence for different groups in the survey:

Group	Unweighted sample size	Plus or minus ...
All internet users 18+	1,055	3.2
Ages 18-29	175	7.8
30-49	310	5.8
50-64	327	5.7
65+	243	6.6
High school or less	380	5.3
Some college	306	5.9
College+	369	5.4

In addition to sampling error, one should bear in mind that question wording and practical difficulties in conducting surveys can introduce error or bias into the findings of opinion polls.

Pew Research Center is a nonprofit, tax-exempt 501(c)(3) organization and a subsidiary of The Pew Charitable Trusts, its primary funder.

Topline questionnaire

PEW RESEARCH CENTER
JUNE 17 – JUNE 27, 2016
TOTAL N=1,055 INTERNET USERS AGE 18+

RANDOMIZE ORDER OF RESPONSE OPTIONS

Q1 What does the "https://" at the beginning of a URL denote, as opposed to http:// (without the "s")?

33	That information entered into the site is encrypted (C*orrect*)	
67	Net incorrect/not sure	
	2	That the site has special high definition
	1	That the site is the newest version available
	1	That the site is not accessible to certain computers
	8	None of the above
	54	Not sure

RANDOMIZE ORDER OF RESPONSE OPTIONS

Q2 Which of the following is an example of a "phishing" attack? [SELECT ALL THAT APPLY]

54	All of the above (*Correct*)	
46	Net incorrect/not sure*	
	9	Sending someone an email that contains a malicious link that is disguised to look like an email from someone the person knows
	11	Creating a fake website that looks nearly identical to a real website, in order to trick users into entering their login information
	4	Sending someone a text message that contains a malicious link that is disguised to look like a notification that the person has won a contest
	24	Not sure

**Note: Because respondents were allowed to select multiple options, totals may sum to more than 100%. "Correct answer" totals include respondents who selected "all of the above" answer option in survey, as well as those who selected all three individual answer choices. "Incorrect answer" totals include only respondents who did not select all items in list.*

RANDOMIZE ORDER OF RESPONSE OPTIONS

Q3 A group of computers that is networked together and used by hackers to steal information is called a….

16		Botnet (*Correct*)
84		Net incorrect/not sure
	3	Rootkit
	3	DDoS
	4	Operating system
	73	Not sure

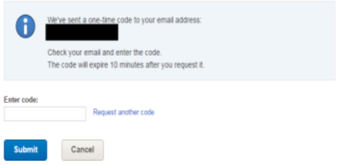
Q4 All Wi-Fi traffic is encrypted by default on all wireless routers.

45		False (*Correct*)
55		Net Incorrect/not sure
	11	True
	44	Not sure

RANDOMIZE ORDER OF RESPONSE OPTIONS

Q5 Some websites and online services use a security process called two-step authentication. Which of the following images is an example of two-step authentication?

10 *Correct*

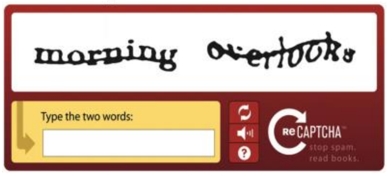


We've sent a one-time code to your email address:
[redacted]
Check your email and enter the code.
The code will expire 10 minutes after you request it.

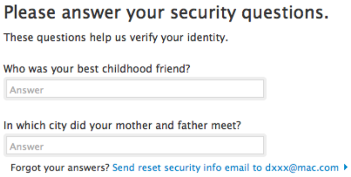
Enter code:

90 Net Incorrect/not sure*

29



39



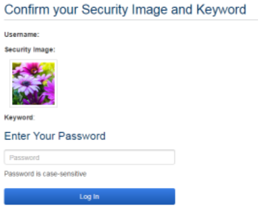
Please answer your security questions.
These questions help us verify your identity.

Who was your best childhood friend?

In which city did your mother and father meet?

Forgot your answers? Send reset security info email to dxxx@mac.com

43



Confirm your Security Image and Keyword

Username:
Security Image:
Keyword:

Enter Your Password

Password is case-sensitive

2 None of these

18 Not sure

Note: Because respondents were allowed to select multiple options, totals may sum to more than 100%. In total, 38% of respondents accurately described the correct picture as an example of two-step authentication. However, the "correct answer" totals shown here include <u>only</u> those respondents who selected the correct example of two-step authentication, and <u>no other items</u> in the list.

RANDOMIZE ORDER OF RESPONSE OPTIONS

Q6 Which of the following four passwords is the most secure?

75	WTh!5Z (*Correct*)	
25	Net incorrect/Not sure	
	6	into*48
	1	Boat123
	1	123456
	17	Not sure
	1	Refused

RANDOMIZE ORDER OF RESPONSE OPTIONS

Q7 Criminals access someone's computer and encrypt the user's personal files and data. The user is unable to access this data unless they pay the criminals to decrypt the files. This practice is called….

48	Ransomware (*Correct*)	
52	Net incorrect/Not sure	
	3	Spam
	3	None of the above
	2	A botnet
	1	Driving
	43	Not sure

[NO Q8]

Q9 "Private Browsing" is a feature in many internet browsers that lets users access web pages without any information (like browsing history) being stored by the browser. Can internet service providers see the online activities of their subscribers when those subscribers are using private browsing?

39	Yes (*Correct*)	
61	Net incorrect/Not sure	
	12	No
	49	Not sure

Q10 Turning off the GPS function of your smartphone prevents any tracking of your phone's location.

52	False (*Correct*)		
48	Net incorrect/Not sure		
		22	True
		26	Not sure

Q11 All email is encrypted by default.

46	False (*Correct*)		
54	Net incorrect/Not sure		
		10	True
		43	Not sure

Q12 By law, how many free credit reports can Americans obtain in a calendar year from each of the three major credit bureaus?

49	One (*Correct*)		
51	Net incorrect/Not sure		
		19	Three
		1	Five
		1	Zero
		30	Not sure

Q13 If a public Wi-Fi network (such as in an airport or café) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?

73	No, it is not safe (*Correct*)		
27	Net incorrect/Not sure		
		7	Yes, it is safe
		20	Not sure

RANDOMIZE ORDER OF RESPONSE OPTIONS

Q14 What kind of cybersecurity risks can be minimized by using a Virtual Private Network (VPN)?

13	Use of insecure wi-fi networks (*Correct*)	
87	Net incorrect/Not sure	
	6	Phishing attacks
	5	Tracking by website operators
	3	De-anonymization by network operators
	2	Key-logging
	70	Not sure

TOTAL NUMBER CORRECT (13 questions in total)

1%	13 of 13 correct
2%	12 of 13
4%	11 of 13
5%	10 of 13
8%	9 of 13
8%	8 of 13
10%	7 of 13
10%	6 of 13
11%	5 of 13
11%	4 of 13
12%	3 of 13
7%	2 of 13
5%	1 of 13
5%	0 of 13