SECURE YOUR SPACE

Search

Cybersecurity jobs

Preparing Millennials to Lead in Cyberspace
October 2014

Results from the Raytheon-NCSA Millennial Survey
of career aspirations, attitudes and behaviors of
young American adults online

NATIONAL CYBERSECURITY ALLIANCE

Raytheon

Overview

In this digital age, news reports detail increasing numbers of identity thefts and other online security breaches. To prevent and combat these incidents, our nation needs to strengthen its cybersecurity workforce. The demand for cybersecurity professionals is growing 3.5 times faster than the overall IT job market, and 12 times faster than the total labor market. In 2013, there were 209,749 national postings for open cybersecurity positions, and these postings took recruiters 36 percent longer to fill than all other job postings combined.[1] These imbalances have created a talent gap at a time when cyber activity has become both an economic engine and a national security concern.

Young adults, also known as millennials (ages 18 to 26), hold the key to close the cyber talent gap. Having grown up in a digital environment, millennials are well positioned for these cybersecurity careers, since they are at the stage when they need to choose a profession and will be in the workforce for several decades.

In support of National Cyber Security Awareness Month (October), Raytheon and the National Cyber Security Alliance (NCSA) commissioned a survey to understand U.S. millennials' career interests, level of career preparedness and their online attitudes and behaviors. This study was fielded by Zogby Analytics, which also conducted the first Raytheon-NCSA Millennial Survey in 2013.

As the study showed, many young adults raised on social networking are concerned about their online safety, including identity theft, personal collection of data, and devices being infected by malware. However, despite their concerns, they continue to exhibit risky behavior when it comes to their online lives.

Millennials say they want careers in which they can make the Internet safer, but they don't know what working in "cybersecurity" means. The study also revealed inadequate technology education, which inhibits young adults from getting interested in and pursuing careers in computer science, including cybersecurity. Despite students' general interest in pursuing related careers, they often lack the needed skills and encouragement educators and business leaders should provide to grow the talent pipeline. In addition, more information about what cybersecurity jobs entail would increase their interest in this career path.

After so many high profile cybersecurity breaches over the past year, it should come as no surprise that so many students are curious about what cybersecurity jobs entail. This represents both a challenge and an opportunity for the private sector and the government to team with educators to help inspire our next generation of innovators and cyber defenders. High schools and current cyber professionals need to play a stronger role in education and awareness to sharpen young people's cyber hygiene habits and attract them to cyber careers.

[1] Burning Glass Technologies (2014). The Growth of Cybersecurity Jobs. Retrieved from http://www.burning-glass.com/research/cybersecurity/

Methodology and Sample Characteristics

The 2014 Raytheon-NCSA Millennial Cyber Survey was fielded by Zogby Analytics from Aug. 27 to Aug. 28, 2014. The responses were generated from a survey of 1,000 adults in the U.S. aged 18 to 26. Using trusted interactive partner resources, thousands of adults were invited to participate in this interactive survey. Each invitation was password coded and secured, so that one respondent could only access the survey one time. Using information based on census data, voter registration figures, CIA fact books and exit polls, Zogby used complex weighting techniques to best represent the demographics of the population being surveyed. Weighted variables may have included race and gender. Results have a margin of error of plus or minus 3.2 percentage points at a 95-percent confidence interval. Note: The 2013 and 2014 surveys did not poll the same individuals but culled responses from the same population.
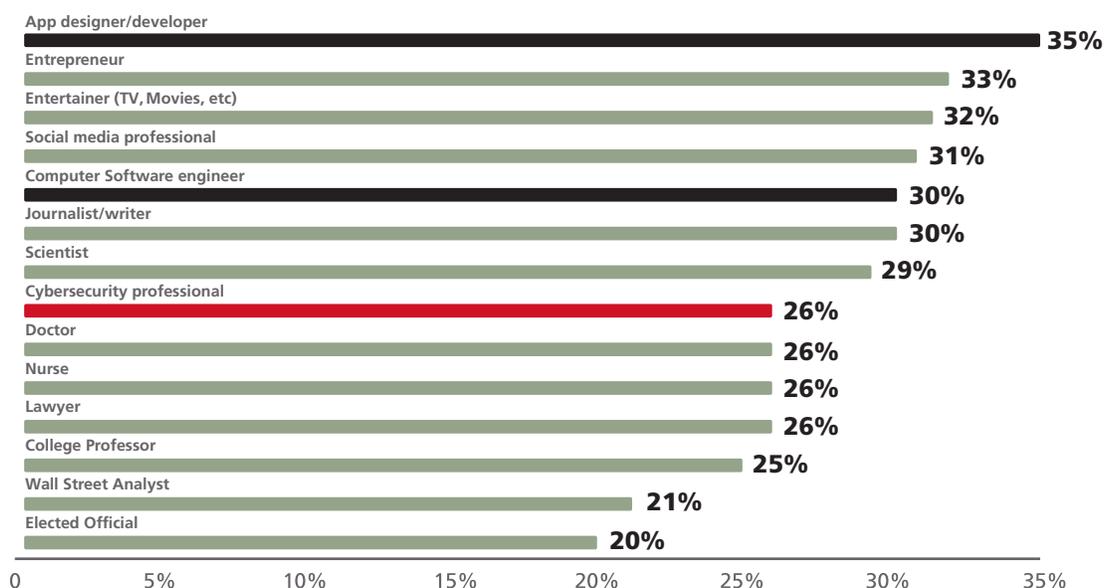
Building Tomorrow's Cybersecurity Workforce

Millennials are interested but unprepared to enter the cybersecurity profession, uncertain about the responsibilities of someone in this job, and lack mentors to help bridge the gap.

Millennials were more likely to express an interest in pursuing a career as a computer scientist than as a doctor, politician or Wall Street analyst. Digging deeper into computer-related careers, young adults are slightly more interested in becoming app developers (35 percent) than cybersecurity professionals (25 percent). While it's encouraging that one in four young adults indicated interest in a career as a cybersecurity professional, why isn't that number higher?

Which careers do Millennials say they want?

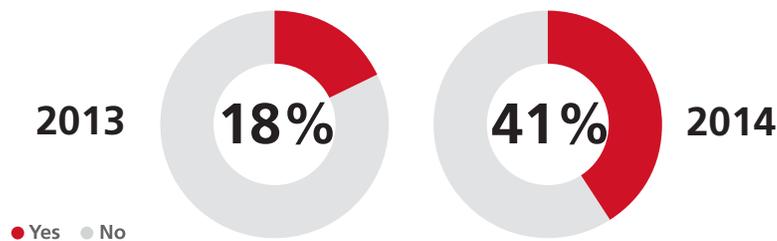| Career	Percent
App designer/developer	35%
Entrepreneur	33%
Entertainer (TV, Movies, etc)	32%
Social media professional	31%
Computer Software engineer	30%
Journalist/writer	30%
Scientist	29%
Cybersecurity professional	26%
Doctor	26%
Nurse	26%
Lawyer	26%
College Professor	25%
Wall Street Analyst	21%
Elected Official	20%

Building Tomorrow's Cybersecurity Workforce

Almost two-thirds of millennial respondents don't know or aren't sure what the "cybersecurity" profession is. However, nearly 40 percent said they are more likely now than 12 months ago to choose a career in which they can make the Internet safer and more secure. Young adults need to be informed that working to make the Internet safer is what cybersecurity professionals do.

Compared to 12 months ago, are you now more or less likely to consider a career where you could make the Internet safer and more secure?
- More likely
- Less likely
- No change

38%
43%
19%

Are you aware of the typical range of responsibilities and job tasks involved in the cyber profession?
- Yes
- No/Not sure

63%
37%
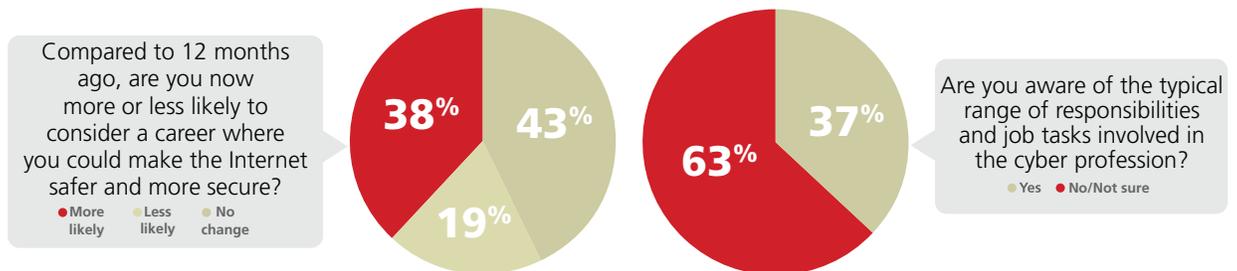
In this year's survey, 41 percent said that during high school, at least one teacher, guidance or career counselor or other adult in an after-school program or extra-curricular activity discussed or mentioned the idea of a career in cybersecurity. Educators have made a significant improvement over last year, when only 18 percent of millennials reported this type of conversation.

During high school did any teacher, guidance or career counselor or other adult in an after-school program or extra-curricular activity ever mention or discuss the idea of a career in cybersecurity?

2013   18%   41%   2014

- Yes
- No

Unfortunately, a large majority — 64 percent — did not have access to computer classes in high school to build the skills necessary for cyber careers, including computer science.

Did/do your high school computer classes offer the skills necessary or prepare you to pursue a career in cybersecurity and/or a related degree like computer science in college?
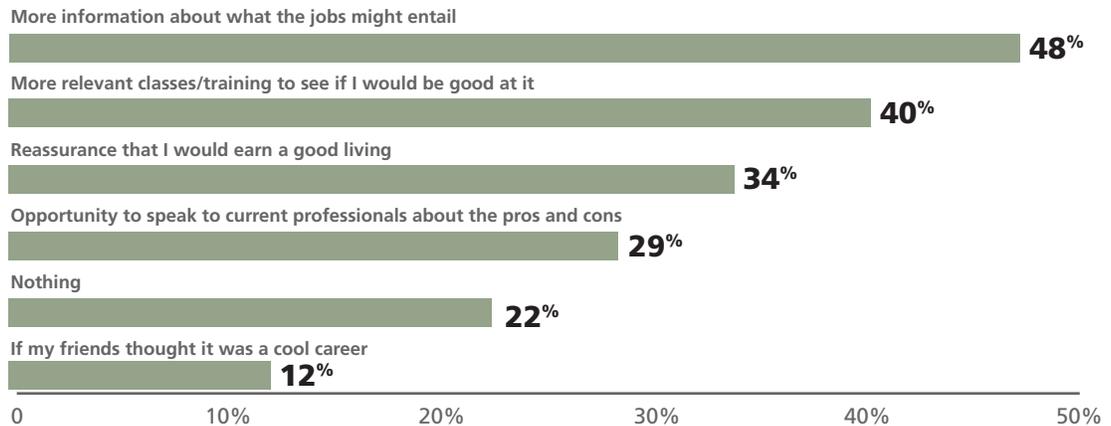
48% No

Yes 36%

16% Not sure
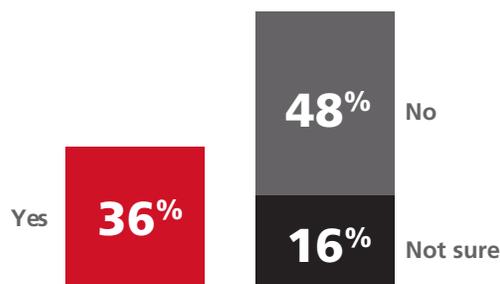
Building Tomorrow's Cybersecurity Workforce

Millennials have specific needs to help them determine if a cyber career is right for them.

What would increase your interest in a career in cybersecurity?

More information about what the jobs might entail
48%

More relevant classes/training to see if I would be good at it
40%

Reassurance that I would earn a good living
34%

Opportunity to speak to current professionals about the pros and cons
29%

Nothing
22%

If my friends thought it was a cool career
12%

0   10%   20%   30%   40%   50%

These results reveal at least some of the sources of the U.S. cyber talent gap. Armed with this new understanding of the motivations and needs of tomorrow's leaders, our nation can build a stronger cyber workforce.

Millennials' Risky Online Behavior

Millennials are aware of computer safety concerns, but they are still taking actions — such as connecting to public Wi-Fi without a password or using a USB device given to them by someone else — that are security risks. They are concerned about devices being infected by malware, credit or debit card theft, someone hacking into financial information or falling victim to online scams or fraud.
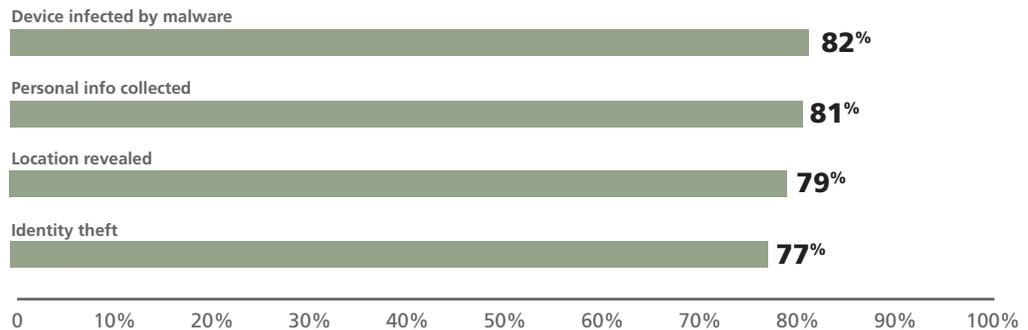
72% have connected to public — no-password-required — Wi-Fi at coffee shops, airports, etc., in the last month

52% have plugged in a USB device such as a memory stick or accessory of some kind that was given to them by another person in the last three months
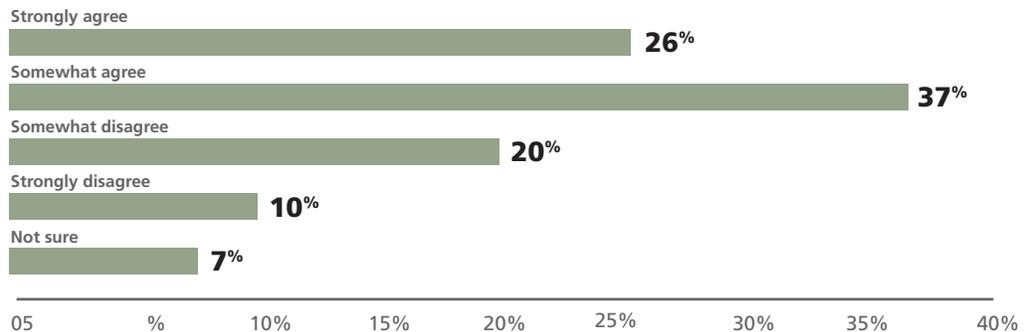
Millennials' Risky Online Behavior

How concerned are you that each of the following can happen when using the Internet?

Device infected by malware — **82%**

Personal info collected — **81%**

Location revealed — **79%**

Identity theft — **77%**

| 0 | 10% | 20% | 30% | 40% | 50% | 60% | 70% | 80% | 90% | 100% |

Only 26 percent of respondents strongly agreed that their high school education prepared them to use technology safely, securely, ethically and productively in the workplace.

Would you agree that your high school education prepared you to use technology safely, securely, ethically and productively in the workplace?

Strongly agree — **26%**

Somewhat agree — **37%**

Somewhat disagree — **20%**

Strongly disagree — **10%**

Not sure — **7%**

| 05 | % | 10% | 15% | 20% | 25% | 30% | 35% | 40% |

Millennials Take Steps for Online Protection

Most millennials received their first "cyber talk" about computer security from their parents, who provided guidance about being safe online.

Who gave you your first 'talk' about staying safer online?

● Parent   ● Teacher
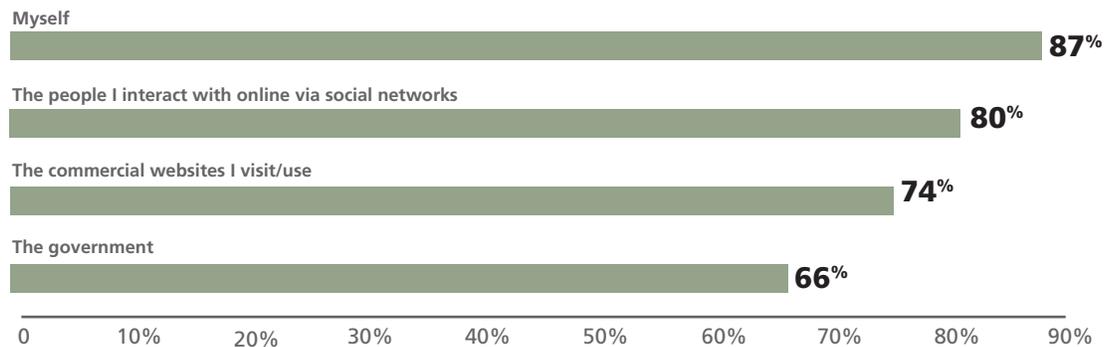● Friend   ● Other adult

17%
18%
20%
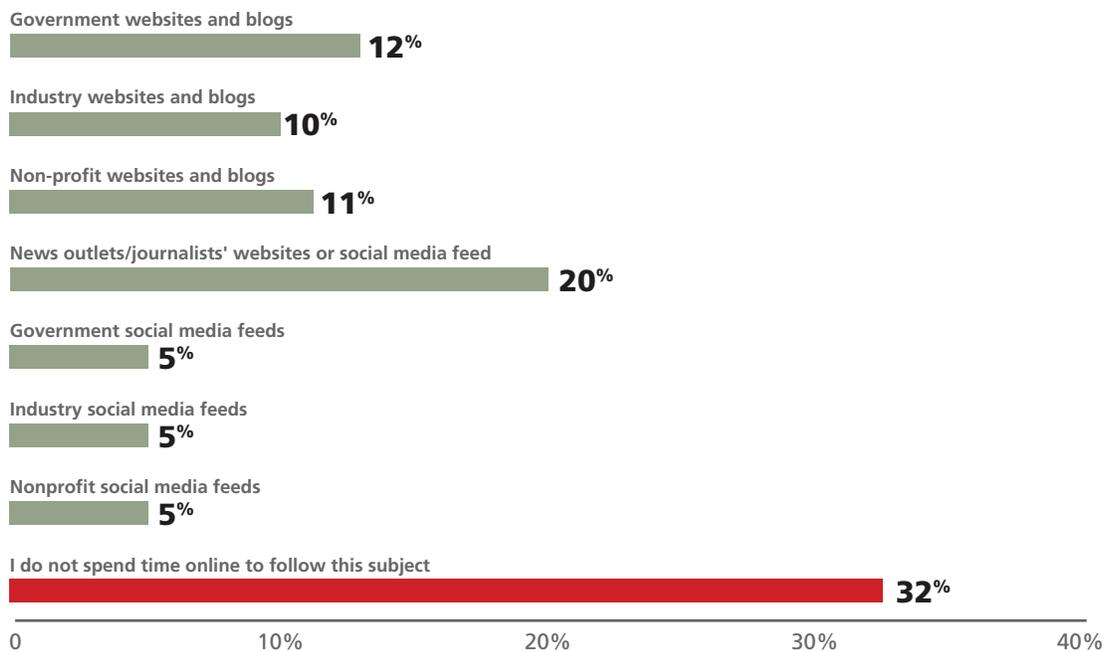**45%**

Millennials Take Steps for Online Protection

This early informal education prompted millennials to take personal responsibility for their safety in cyberspace.

How involved should the following entities be to keep you safe and secure online?

Myself
87%

The people I interact with online via social networks
80%

The commercial websites I visit/use
74%

The government
66%

0   10%   20%   30%   40%   50%   60%   70%   80%   90%

More than two thirds follow the latest developments on cybersecurity topics on a regular basis.

Where do you look for information on current cybersecurity concerns?

Government websites and blogs
12%

Industry websites and blogs
10%

Non-profit websites and blogs
11%

News outlets/journalists' websites or social media feed
20%

Government social media feeds
5%

Industry social media feeds
5%

Nonprofit social media feeds
5%

I do not spend time online to follow this subject
32%

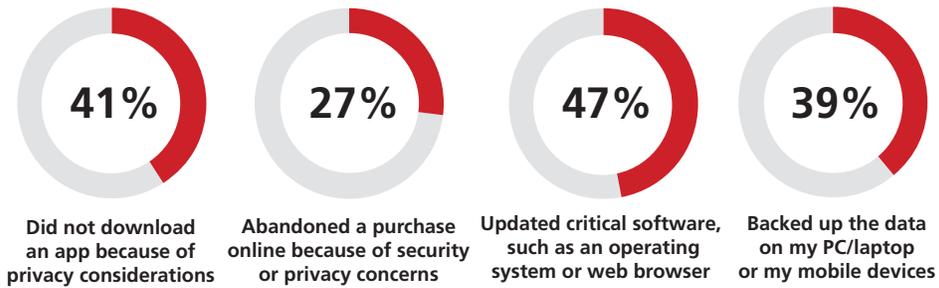0   10%   20%   30%   40%

Millennials Take Steps for Online Protection

Millennials are taking action to protect themselves and they are more cautious in some areas. For example, in the 2014 survey, 40 percent said they did not download an app in the last month because of privacy concerns, compared to 31 percent who answered the question in 2013.

Which of the following have you done in the last month?

41%
Did not download an app because of privacy considerations

27%
Abandoned a purchase online because of security or privacy concerns

47%
Updated critical software, such as an operating system or web browser

39%
Backed up the data on my PC/laptop or my mobile devices

For the 2014 survey, remarkably 60 percent reported an online violation in the last 12 months. In response to this violation, 70 percent changed their online behavior; 62 percent changed passwords on retail or other sites where they stored financial information, and 39 percent changed the privacy or security settings on a social media account.

Has any of the following happened to you in the last 12 months?

12%
Credit card number stolen or other identity theft

33%
Device infected by virus or other malware

28%
You were embarrassed by a photo or comment someone posted about you on the Internet

12%
Other personal online violation

40%
None

70% changed an online behavior as a response to the violation

What behavior(s) or habit(s) have you changed as a response to the violation?

62%
I change my password on retail or other site(s) where I store my financial information more often

66%
I no longer store my financial information on retail sites

29%
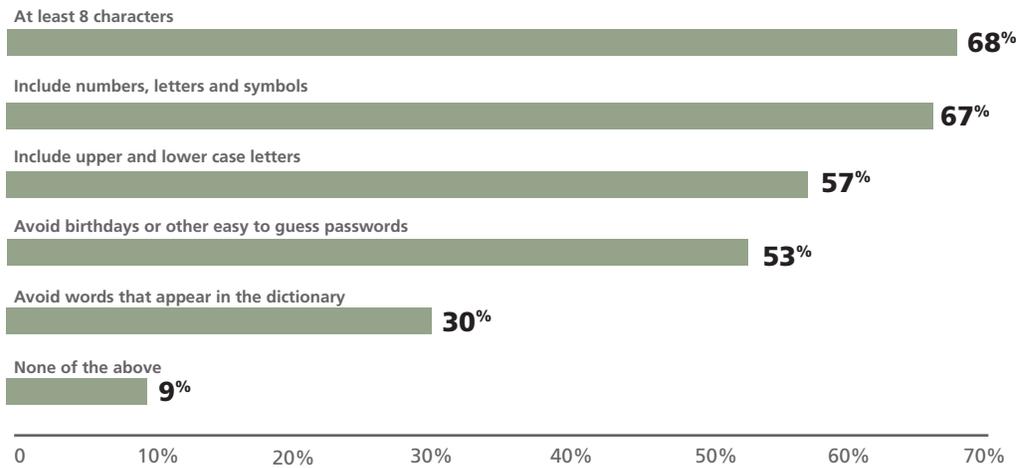I am more careful about what I click on or download to my device

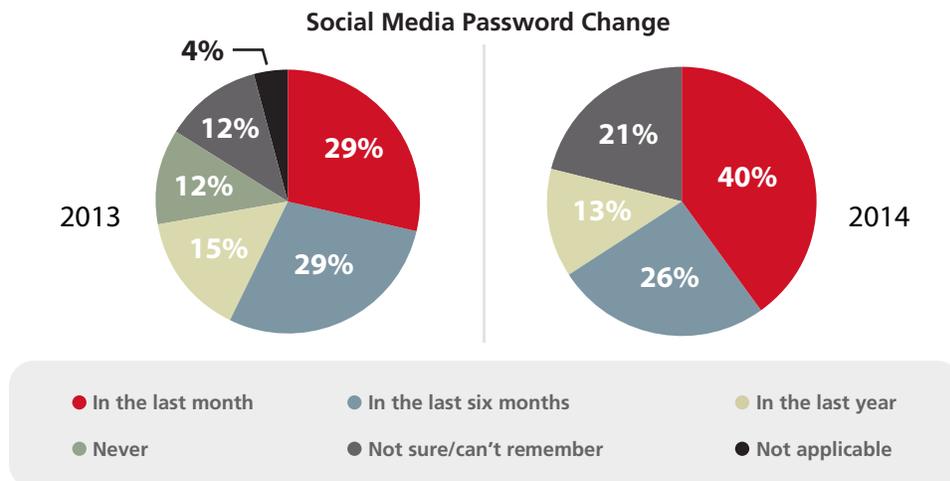# Millennials Take Steps for Online Protection

In general, young adults are following online best practices such as password protecting their devices (75 percent) and following password strength principles.

75%

● Yes

Is your mobile device (smartphone or tablet) password or PIN protected?
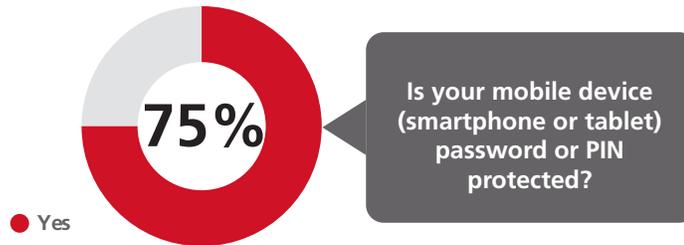
Which of the following password strength principles do you use when choosing passwords?

At least 8 characters
68%

Include numbers, letters and symbols
67%

Include upper and lower case letters
57%

Avoid birthdays or other easy to guess passwords
53%

Avoid words that appear in the dictionary
30%

None of the above
9%

0   10%   20%   30%   40%   50%   60%   70%

The 2014 survey also showed 40 percent of respondents changed their password on a social media account in the last month, compared to only 29 percent who did so in 2013.

Social Media Password Change

2013

4%
12%
12%
15%
29%
29%

2014

21%
13%
40%
26%

● In the last month   ● In the last six months   ● In the last year

● Never   ● Not sure/can't remember   ● Not applicable

Conclusion

According to the U.S. Department of Homeland Security, "Our daily life, economic vitality, and national security depend on a stable, safe, and resilient cyberspace. We rely on this vast array of networks to communicate and travel, power our homes, run our economy and provide government services."

It is critical that the United States focus on developing a cyber workforce to secure the nation's economic interests.

With online breaches and attacks trending in today's headlines, there is a golden opportunity for parents and educators to bring up cybersecurity careers and generate more interest with millennials and younger generations. Educators and current cyber professionals need to collaborate to develop courses, provide information about cybersecurity job responsibilities and salary ranges, and offer mentoring and job shadowing. Millennials would be more interested in cyber professions if they had information about the career path and the required training.

The private sector, government and educational institutions need to work together to help inspire our next generation of innovators and cyber defenders. We'll need millennials' talent to protect data and devices as the world becomes increasingly connected.

About Raytheon

Raytheon Company, with 2013 sales of $24 billion and 63,000 employees worldwide, is a technology and innovation leader specializing in defense, security and civil markets throughout the world. With a history of innovation spanning 92 years, Raytheon provides state-of-the-art electronics, mission systems integration and other capabilities in the areas of sensing; effects; and command, control, communications and intelligence systems, as well as cybersecurity and a broad range of mission support services. Raytheon is headquartered in Waltham, Mass. For more about Raytheon, visit us at www.raytheon.com and follow us on Twitter @Raytheon.

About Zogby Analytics

For three decades, the Zogby companies have produced polls with an unparalleled record of accuracy and reliability. Zogby telephone and interactive surveys have generally been the most accurate in U.S. Presidential elections since 1997.

Zogby Analytics is composed entirely of senior level executives from Zogby International. Zogby Analytics, along with renowned pollster John Zogby, have continued in the tradition of conducting telephone and interactive surveys, while keeping an eye on the future by incorporating social media tracking and analysis into our work.

Zogby Analytics conducts a wide variety of surveys internationally and nationally in industries, including banking, IT, medical devices, government agencies, colleges and universities, non-profits, automotive, insurance and NGOs.

About The National Cyber Security Alliance

The National Cyber Security Alliance (NCSA) is the nation's leading nonprofit public private partnership promoting the safe and secure use of the Internet. Working with the Department of Homeland Security (DHS), private sector sponsors and non-profit collaborators to promote cybersecurity awareness, NCSA board members include ADP, AT&T, Bank of America, Comcast Corporation, EMC Corporation, ESET, Facebook, Google, Intel, Leidos, McAfee, Microsoft, PayPal, Symantec, Trend Micro, Verizon and Visa. Through collaboration with the government, corporate, non-profit and academic sectors, NCSA's mission is to educate and empower a digital citizenry to use the Internet securely and safely protect themselves and the technology they use and the digital assets we all share. For more information on NCSA please visit: http://www.staysafeonline.org/about-us/overview/

Raytheon

Customer Success Is Our Mission