FOR RELEASE APRIL 30, 2014

Heartbleed's Impact

39% of internet users have changed passwords or canceled accounts; 6% think their personal information was swiped

FOR FURTHER INFORMATION ON THIS REPORT:

Lee Rainie, Director, Internet Project
Maeve Duggan, Research Assistant, Internet Project

202.419.4372

www.pewresearch.org

RECOMMENDED CITATION: Pew Research Center, April 30, 2014, "Heartbleed's Impact" Available at:
http://www.pewinternet.org/2014/04/30/heartbleeds-impact/

About This Report

In early April, a major security flaw affecting perhaps 500,000 or more websites was announced and fixed. But the patch to the "secure socket" program that is supposed to encrypt and protect user information on secure websites was only made after more than two years of vulnerability on some of the most heavily trafficked sites, including Facebook, Google, YouTube, Yahoo and Wikipedia. Analysts warned that untold numbers of internet users might have had key personal information compromised either in their use of those websites, or their use of email, instant messaging, and even supposedly secure virtual personal networks.

This report covers public response to the revelation of the security code flaw. It was conducted among 1,501 adults between April 23-27 on landline and cell phones and in English and Spanish. It has a margin of error of plus or minus 2.9 percentage points in the overall sample and 3.1 points among the internet users in the sample (N=1,303).

The software bug was named "Heartbleed" and it was accidentally introduced to the OpenSSL encryption program on New Year's Eve 2011. OpenSSL is an open-source program that is used by many of the sites and email programs that have the "https" prefix and "green lock" icon in their URLs. Some security commentators called Heartbleed "catastrophic" and said it one of the worst vulnerabilities ever discovered on the web.

The flaw basically allowed people to "break the lock" on sophisticated encryption software, get into the memory of security systems and gather up whatever personal information was there, including usernames, passwords, and the actual content of accounts such as credit card data or other sensitive personal information.

This report is a collaborative effort based on the input and analysis of the following individuals.

Lee Rainie, *Director, Internet Project*
Maeve Duggan, *Research Assistant, Internet Project*
Alec Tyson, *Research Associate, U.S. Politics Project*

Find related reports about privacy, safety, and security at
http://www.people-press.org/topics/privacy-and-safety/
http://www.pewinternet.org/topics/privacy-and-safety/

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. It conducts public opinion polling, demographic research, media content analysis and other empirical social science research. The center studies U.S. politics and policy views; media and journalism; internet and technology; religion and public life; Hispanic trends; global attitudes 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.

Main findings

The Heartbleed security flaw on one of the most widely used "secure socket" encryption programs on the internet had an impact on a notable share of internet users[1], according to a new survey by the Pew Research Center:

- 39% of internet users say that after they learned of the online security problems they took steps to protect their online accounts by doing such things as changing passwords or canceling accounts.
- 29% of internet users believe their personal information was put at risk because of the Heartbleed bug.
- 6% of internet users say they believe their personal information was stolen.

Responses to Heartbleed

*% of internet users who took the following steps in response to the widely reported security bug…**

* These questions were asked of the 64% of internet users who say they had heard of the Heartbleed bug

Pew Research Center survey, April 2014.

PEW RESEARCH CENTER

As a news story, the revelations about Heartbleed drew the attention of a notable segment of adults. Some 60% of adults (and 64% of internet users) said they had heard about the bug. Some 19% of adults said they had heard "a lot" about it and 41% said they had heard "a little" about it.

By comparison, though, the Heartbleed story drew much less intensity and scope of attention than other big news stories. In this same survey, 46% of respondents said they had heard "a lot" about tensions between Russia and Ukraine and 34% said they had heard "a little."

And last June, when Edward Snowden leaked details of the National Security Agency surveillance programs collecting phone and email records of Americans, 51% of adults said they had heard "a lot" about the story and another 35% said they had heard "a little."

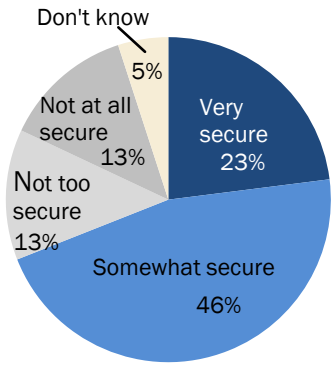
Overall, internet users generally have mixed and middling views about the security of their personal information online: About half (46%) say they think their information is "somewhat

[1] 87% of American adults said they were internet users in this survey.

secure." Some 23% believe their information is "very secure," and 26% say it is "not too secure" or "not at all secure."

How secure are your online accounts?

Among internet users



Pew Research Center survey, April 2014.

PEW RESEARCH CENTER

About this survey

These findings come from a survey of 1,501 American adults (ages 18+) conducted between April 23-27 on landline and cell phones. The survey was administered in English and Spanish. It has a margin of error of plus or minus 2.9 percentage points for the overall sample and 3.1 percentage points for the 1,303 internet users in the sample. The questions about Heartbleed's impact were asked of the 897 respondents who were internet users and who had heard about the security flaw. The margin of error for those results is plus or minus 3.8 percentage points.

Heartbleed arises

The revelations about the Heartbleed bug in the OpenSSL program were a major story in early April because of the nature of the flaw (it allowed bad actors to discover supposedly secure encrypted information) and the potential size of the affected population. Perhaps 500,000 or more websites use OpenSSL to allow their visitors to have supposedly secure interactions. Such internet behemoths as Facebook, Yahoo, Google, YouTube, and Wikipedia were affected.

Moreover, the flaw went undetected for more than two years. The open-source nature of the OpenSSL program meant that it was available for free to the companies that wanted an easy–and respected—way to allow users of their sites to have encrypted interactions with the sites.

It also meant that unpaid, volunteer coders were the primary designers of the software. Few of the firms actually using the code on their websites provided financial support for its development. Ironically, the open-source nature of OpenSSL meant that few people had financial incentive to look for flaws and fix problems.

There was consensus in the internet security community that the safest user response after announcement of the problem was to first check whether a particular website was employing repaired versions of OpenSSL. Several testing sites were created so that people could stick in a Web address to see if a site still used the problem software. Experts also suggested that people change their passwords or even cancel accounts if they felt the accounts were vulnerable.

Who was aware of Heartbleed

This survey finds that a sizable share of the public was aware of the problem: 60% of the public had heard at least a little about Heartbleed, including 64% of internet users had. Some 19% of adults said they had heard “a lot” about Heartbleed and another 41% said they had heard “a little.”

The most noteworthy traits of those who had heard about the security problem on the internet was that they were likely to be relatively well educated and higher income Americans: 77% of those with college educations were aware of Heartbleed, along with 75% of those living in households earning $75,000 or more.

As a news story, Heartbleed was not nearly as prominent in public awareness as some other recent stories. In this survey, we also asked if people had heard of the tensions between Russia and Ukraine and 46% of respondents said they had heard “a lot” and another 34% said they had heard “a little.”

In previous surveys about people's awareness of news stories, Pew Research has found a number of news events that have gained much more public attention than Heartbleed. For instance:

- 88% of Americans said they had heard "a lot" about the Newtown, Connecticut shootings in December 2012.
- 60% of Americans said they had heard "a lot" about Pope Benedict's announcement he would step down from the papacy in February 2013.
- 42% of Americans said they had heard "a lot" about Republican presidential nominee Mitt Romney's of Rep. Paul Ryan to be his running mate in August 2012.

The Heartbleed story registered roughly the same level of public awareness as the U.S.-Iran negotiations and agreement to allow monitoring of Iran's nuclear program (in November and December 2013) and Catholic Bishops in the U.S. protesting Obama Administration policies they believe restricted religious liberty (July 2012).

Who felt vulnerable

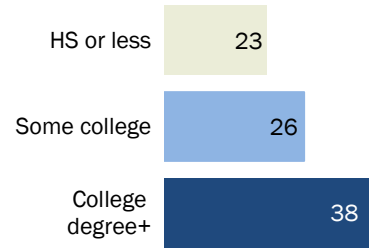
After establishing in our survey who was aware of Heartbleed, we then asked the 64% of internet users those who had heard of the bug a series questions about how vulnerable they felt. In other words, the 36% of internet users[2] who had not heard of Heartbleed *were not asked the follow-up questions* about the security bug's impact on users.

Some 29% of all internet users said they believed their online information was put at risk by Heartbleed. That amounts to 45% of the internet users who had heard of Heartbleed who said they felt vulnerable.

Those who are relatively upscale were more likely to feel their information was put at risk: 38% of online Americans with college or graduate degrees said they thought their information was put at risk, compared with 23% of internet users with a high school diploma or less. Among other reasons, this likely happened because those

Those with higher levels of education felt the most risk from Heartbleed

% of internet users who say their personal info was put at risk by Heartbleed



Pew Research Center survey, April 2014.

PEW RESEARCH CENTER

[2] N=406

with higher education were also more likely to have heard a lot about Heartbleed.

Similarly, internet users in higher income households were more likely than those in lower-income households to fear that Heartbleed put their information at risk: 34% of the internet users living in households earning $75,000 or more said the bug put their information at risk, compared with 25% of the internet users living in households earning less than $30,000.

Some 6% of internet users said they felt their information had actually been stolen because of Heartbleed. There was no notable variance in this figure when it came to different demographic groups.

Who took precautionary steps in response to Heartbleed

Some 39% of internet users say they changed their password or closed an account in response to the revelations about Heartbleed. This amounts to 61% of the internet users who had heard of Heartbleed.

Again, those with higher levels of education were the most likely to have taken such steps: 48% of the internet users with college educations changed their password or deleted an account, compared with 31% of the internet users with high school educations or less and 40% of those who attended at least some college.

And 46% of the internet users in households earning $75,000 or more had changed their passwords or deleted an account, compared with 33% of the online Americans living in households earning less than $30,000.

Who feels secure or insecure

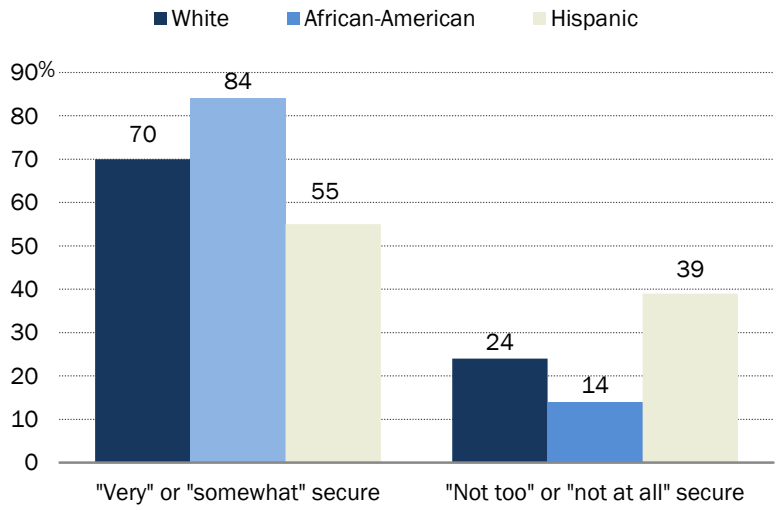
Despite the latest security issues involving the internet, almost seven-in-ten internet users (69%) think that their online accounts and private information are generally secure. Some 23% believe that their accounts are “very secure,” while another 46% say their accounts are “somewhat” secure.

Others are less confident. One-in-four internet users (26%) think their online accounts are not secure, including 13% who say that they are “not too secure” and another 13% that think they are “not at all secure.”

African-Americans who use the internet are more likely than others to feel confident about the security of their accounts and online Hispanics are the most likely not to feel confident. Whites who use the internet fall in the middle:

Online security by race

Among internet users, the % of each racial/ethnic group who feel secure vs. insecure about their online accounts and private information



Pew Research Center survey, April 2014.

PEW RESEARCH CENTER

Some 84% of African-American internet users say their online accounts and private information are “very” or “somewhat” secure, the highest percentage of any racial group.

On the opposite end, Hispanics are the most likely to say their online interests are “not too” or “not at all” secure, with 39% saying so.

White users are more likely than Hispanics to feel secure, but also more likely than African-Americans to feel insecure.

Methods

The analysis in this report is based on telephone interviews conducted April 23-27, 2014 among a national sample of 1,501 adults, 18 years of age or older, living in all 50 U.S. states and the District of Columbia (600 respondents were interviewed on a landline telephone, and 901 were interviewed on a cell phone, including 449 who had no landline telephone). The survey was conducted by interviewers at Princeton Data Source under the direction of Princeton Survey Research Associates International. A combination of landline and cell phone random digit dial samples were used; both samples were provided by Survey Sampling International. Interviews were conducted in English and Spanish. Respondents in the landline sample were selected by randomly asking for the youngest adult male or female who is now at home. Interviews in the cell sample were conducted with the person who answered the phone, if that person was an adult 18 years of age or older. For detailed information about our survey methodology, see http://people-press.org/methodology/ .

The combined landline and cell phone sample are weighted using an iterative technique that matches gender, age, education, race, Hispanic origin and nativity and region to parameters from the 2012 Census Bureau's American Community Survey and population density to parameters from the Decennial Census. The sample also is weighted to match current patterns of telephone status and relative usage of landline and cell phones (for those with both), based on extrapolations from the 2013 National Health Interview Survey. The weighting procedure also accounts for the fact that respondents with both landline and cell phones have a greater probability of being included in the combined sample and adjusts for household size among respondents with a landline phone. Sampling errors and statistical tests of significance take into account the effect of weighting.

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 ...
Total sample	1,501	2.9 percentage points
internet users	1,303	3.1 percentage points
internet users aware of Heartbleed	897	3.8 percentage points

Sample sizes and sampling errors for other subgroups are available upon request.

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.

Survey questions

PEW RESEARCH CENTER FOR THE PEOPLE & THE PRESS
APRIL 2014 POLITICS AND NEWS SURVEY
FINAL TOPLINE
April 23-27, 2014
N=1,501, margin of error +/- 2.9 percentage points
N=1,303 for internet users, margin of error +/- 3.1 percentage points
N=897 for respondents who were internet users who had heard of Heartbleed, margin of error +/- 3.8 percentage points

ASK ALL:
Next,
INT1 Do you use the internet, at least occasionally?
ASK IF DOES NOT USE THE INTERNET (INT1=2,9):
INT2 Do you send or receive email, at least occasionally?
ASK IF DOES NOT USE THE INTERNET OR EMAIL (INT2=2,9):
INT3M Do you access the internet on a cell phone, tablet or other mobile handheld device, at least occasionally?

Apr 23-27 2014	
87	Yes to any
13	No/Don't know/Refused to all

ASK INTERNET USERS (INT1=1 OR INT2=1 OR INT3=1) [N=1,303]:
Q.12 Would you say your own online accounts and private information are generally **[READ]**?

Apr 23-27 2014	
23	Very secure
46	Somewhat secure
13	Not too secure [OR]
13	Not at all secure
5	Don't know/Refused **(VOL.)**

ASK ALL:
Q.HB1 How much, if anything, have you read or heard about the Heartbleed bug, an internet security problem that affected many websites. Have you heard … **[READ]**

Apr 23-27 2014		Internet users
19	A lot	20
41	A little	44
38	Nothing at all	35
1	Don't know/Refused **(VOL.)**	**1**

ASK IF HEARD A LOT OR A LITTLE AND INTERNET USER ((INT1=1 OR INT2=1 OR INT3=1) AND (Q.HB1=1,2)) [N=897]:

Q.HB2 Do you think your own online personal information was put at risk by the Heartbleed bug, or do you think your information was not put at risk?

Apr 23-27 2014		All internet users
45	Own information put at risk	29
47	Own information not put at risk	30
8	Don't know/Refused **(VOL.)**	**5**

Not asked=36%

ASK IF OWN INFORMATION PUT AT RISK (Q.HB2=1):

Q.HB3 And do you think your own online personal information was actually stolen because of the Heartbleed bug, or don't you think this happened to you?

BASED ON INTERNET USERS WHO HAVE HEARD A LOT OR A LITTLE [N=897]:

Apr 23-27 2014		All internet users
9	Own information was actually stolen	6
29	Don't think this happened	19
7	Don't know/Refused **(VOL.)**	**4**
55	*Thinks own information not put at risk/Don't know (Q.HB2=2,9)*	

ASK IF HEARD A LOT OR A LITTLE AND INTERNET USER ((INT1=1 OR INT2=1 OR INT3=1) AND (Q.HB1=1,2)) [N=897]:

Q.HB4 As a result of the Heartbleed bug, have you taken any steps to help protect your online accounts and information, such as changing your passwords or cancelling an account?

Apr 23-27 2014		All internet users
61	Yes	39
37	No	24
2	Don't know/Refused **(VOL.)**	**1**

Not asked=36%