

Securing Our e-City National Cybercrime Survey



10/14/2009

Prepared For ESET/Securing Our e-City

Field Dates: October 2nd – October 5th 2009

United States Residents

n=1003

Table of Contents

SUMMARY	1
SAMPLE CHARACTERISTICS	2
OVERVIEW	3
METHODOLOGY AND LIMITATIONS	4
FINDINGS	6
QUESTIONNAIRE WITH PERCENTAGES	16
NOTES TO THE CROSSTABULATIONS	22
CROSSTABULATIONS	23

Summary

Research Objective:	1) Assess American Cybercrime Awareness
Sample Size:	n=1003
Margin of Sampling Error:	± 3.1%
Confidence Level:	95%
Sample Methodology:	Simple Random Sampling from Listed Sample
Jurisdiction:	Continental United States
Eligibility:	Adults
Interview Method:	n= 952 via Landline Phones n=51 in Cell Phone-only Households
Average Duration:	Landlines: 8 Minutes, 1 Second Cell Phones: 9 Minutes, 8 Seconds
Field Dates:	October 2nd – October 5th 2009
Field Facility:	Competitive Edge Research, San Diego
Project Director:	John Nienstedt, Sr.

Sample Characteristics

GENDER	%
Male	46.5
Female	53.5

AGE	%
18 to 24	5.5
25 to 34	9.9
35 to 44	13.4
45 to 54	20.4
55 to 64	20.6
65 to 74	16.6
75 and Over	13.8

INCOME	%
Under \$20,000	15.9
\$20 to 40,000	24.6
\$40 to 60,000	20.3
\$60 to 80,000	13.3
\$80 to 100,000	10.3
\$100 to 150,000	15.6
Over \$150,000	15.9

TIME SPENT ONLINE	%
None at all	27.1
1 hour to less than 3 hours	18.5
3 hours to less than 8 hours	14.8
8 hours to less than 15 hours	13.1
15 hours to less than 20 hours	4.4
More than 20 hours	22.1

EDUCATION	%
Less than a high school diploma	5.9
High school	26.9
Some college	26.6
College degree	25.5
Advanced degree	15.1

REGION	%
Eastern	47.3
Central	29.3
Mountain	6.1
Pacific	17.3

LANGUAGE	%
English	98.1
Spanish	1.9

Overview

Competitive Edge Research & Communication, Inc. is very pleased to present the results of this study to ESET/Securing Our e-City. Competitive Edge was retained to conduct a telephone survey of voters residing in the continental United States. This survey was designed provide the client with information related to Americans views of cybercrime and computer security. This research also measured certain demographic characteristics and attitudes of the respondents.

All opinions expressed in this report are the professional judgments of Competitive Edge Research & Communication. The project director for this study was John Nienstedt. The questionnaire was principally designed by John Nienstedt. The data was analyzed by John Nienstedt and Research Analyst Liz Sheld.

This report contains the results of 51 cell phone surveys and 952 land-line telephone surveys. Qualified respondents were limited to adult residents of the continental United States. The random sample was provided by Political Data of Burbank, California.

Responses were gathered by professional telephone interviewers on October 2nd through October 5th, 2009. Landline interviews lasted an average of 8 minutes and 1 second, and cell phone interviews lasted an average of 9 minutes and 8 seconds. Verification procedures were followed and one survey was rejected in the process. Editing, coding, computer processing and tabulation of the data were done at Competitive Edge's office in San Diego. The computer tabulations were produced using SPSS PC+ version 15.0, a statistical package copyrighted by SPSS, Inc.

This survey is strictly the property of ESET.

Methodology and Limitations

SAMPLE METHODOLOGY

The sample is comprised of adult residents of the continental United States. Respondents were initially selected using a simple random sampling technique from a voter file maintained by a professional list vendor. The vendor appends phone numbers in order to enhance the Registrar's raw voter file. Based on post-hoc analysis, weighting the dataset on age and cell phone population was necessary to ensure an accurate representation of the overall population.

THE WEIGHTING PROCEDURE

The adjustment of a sample to match a population on specific sub-groups, sometimes called "post-stratification," is accomplished by multiplying the count in each sub-group by a number called a weight. This weight is defined as the ratio of its proportion of the total population to its proportion of the sample. In order to apply the adjustment to all measurements derived from a dataset, the weight value is attached to each individual case. The percentages for age were mathematically adjusted to bring them in line with the proportions found in the base sample of voters.

MARGIN OF SAMPLING ERROR

According to statistical theory, the confidence level associated with a sample of this type is such that, with a question where the respondents answer 50% "yes" and 50% "no," 95% of the time the results are within plus or minus $\pm 3.1\%$ of the *true value*, where true value refers to the results obtained if it were possible to interview every possible qualified respondent. The degree of error is reduced when responses have larger (e.g. 60%-40%, 70%-30%) percentage differences. Conversely, the margin of error increases when a subset of the entire 1003 responses is analyzed.

AVOIDING BIAS

In addition to error introduced by sampling variability, there are many other possible sources of bias such as how a question is worded, the question sequence, or individual interviewer techniques. Competitive Edge does everything in its power to minimize these potential sources of bias.

Another potential for systematic position bias exists when batteries of questions are not rotated. This would lead to respondents possibly being influenced by the most recent set of questions they heard. Therefore, the online banking and social network batteries were rotated to eliminate systematic position bias.

A “primacy” effect is when a respondent is biased toward the first choice they hear; whereas a “recency” effect is when a respondent is biased toward the most recent choice they hear. The order of response choices within questions was also randomized to avoid primacy and recency effects. The order of statements in Q13a and Q15a was alternated. The order of statements in Q13b and Q15b was randomized.

A SNAPSHOT IN TIME

A survey of this type is a good measure of current attitudes that may change over time.

Findings

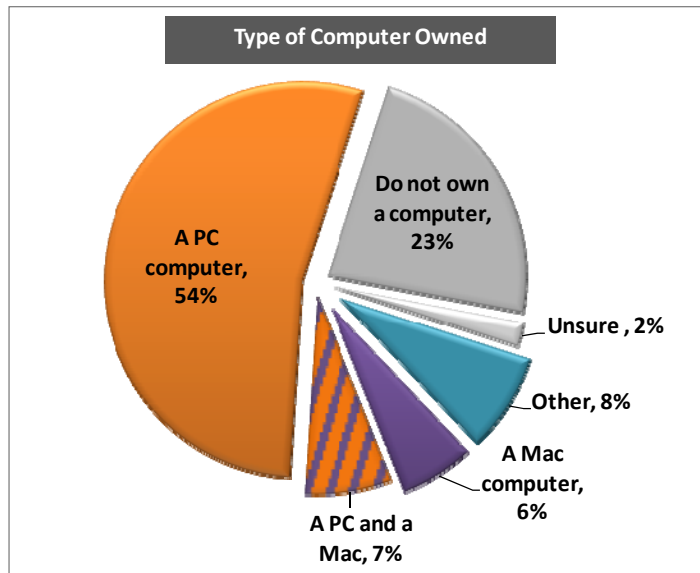
THE DIGITAL DIVIDE

Twenty-three percent of Americans do not own a computer. The digital divide now mainly separates the elderly from their younger counterparts, but also parses Americans based on income, education and language. Two-thirds of those over the age of 75 and 43% of those in the 65 to 74 year category do not own computers. As for income, only 5% of those earning more than \$80,000 annually are not computer owners. That increases to 12% among middle-income earners and eventually 42% of the poor (those in households earning less than \$40,000) are without a computer. Because we can control for income and filter out its effects, it is clear that the educated place a higher value on computing power. Only 13% of those with a college education do not own a computer, while the figure is 49% for those with less education. A whopping 84% of those who took the survey in Spanish are not computer owners. Again controlling for income, this suggests there is a huge language barrier to computer usage.

PC VERSUS MAC: MARKET SHARE

There is really no contest between PCs and Macs: the former enjoy a far larger share of the home computer market. More than 61% of adults own a PC computer whereas only 13% are Mac owners. That is a dominant ratio of 4.6:1. Of course, PCs are made by many different firms while Apple has a monopoly on Macs. Interestingly, there are as many people who own both types of computers as there are who only own a Mac.

Among computer owners, younger adults show a slight but significant preference for Macs. Nearly one in five of those under the age of 45 own a Mac. More importantly for Apple, Macs are most popular among upper income earners: 26% of those earning more than \$80,000 own Macs. However, that does not mean that upper income households shy away from PCs. On the contrary, 87% of them own a PC. This phenomenon is largely driven by the fact that those with incomes over \$80,000 are more likely to own both PCs and Macs. Twenty percent of those earning more than \$80,000 own both types of computers and that rises to one quarter among those with six-figure incomes!

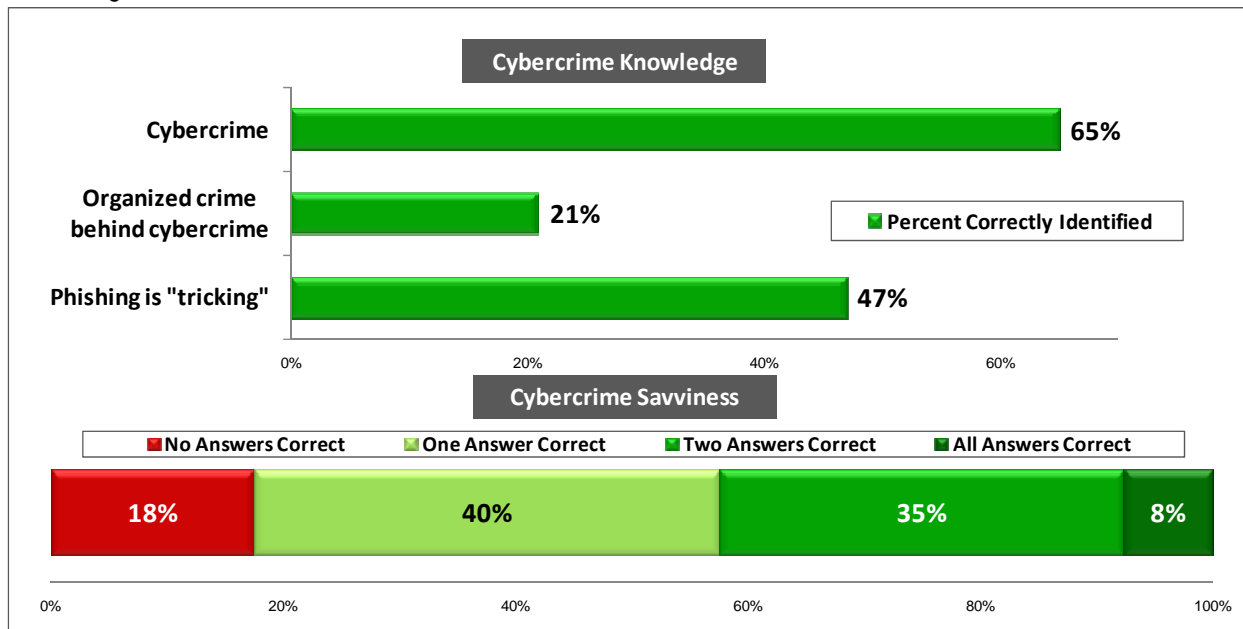


Among computer owners, younger adults show a slight but significant preference for Macs. Nearly one in five of those under the age of 45 own a Mac. More importantly for Apple, Macs are most popular among upper income earners: 26% of those earning more than \$80,000 own Macs. However, that does not mean that upper income households shy away from PCs. On the contrary, 87% of them own a PC. This phenomenon is largely driven by the fact that those with incomes over \$80,000 are more likely to own both PCs and Macs. Twenty percent of those earning more than \$80,000 own both types of computers and that rises to one quarter among those with six-figure incomes!

Computer Platforms (among computer owners, n=705)	Age						Income					
	18-24 (11%)	25-34 (18%)	35-44 (21%)	45-54 (23%)	55-64 (16%)	65-74 (7%)	<\$20K (8%)	\$20-40K (20%)	\$40-60K (22%)	\$60-80K (16%)	\$80-100K (14%)	>\$100K (20%)
PC Owner	77%	83%	80%	85%	82%	77%	81%	81%	78%	78%	90%	85%
Mac Owner	19	19	19	15	14	12	10	7	13	21	16	33
Own Both	8	12	9	8	9	4	2	4	4	7	12	25

KNOWLEDGE OF CYBERCRIME

Cybercrime is fairly well-known in America, as almost two-thirds of adults know that it refers to crime committed over the Internet. Twenty-nine percent are unsure about cybercrime and 6% confuse it with something else.



Knowledge of cybercrime is largely a function of whether someone uses the Internet, how much they use it as well as their level of schooling. Eighty percent of those who go online even a moderate amount (three or more hours per week) know what cybercrime is, and that gets up to 88% among moderate Internet users with a college education. On the other hand, slightly fewer than half of those who go online infrequently and who do not have a college degree know what cybercrime is. But those who avoid the Internet altogether are the least knowledgeable about cybercrime. A mere 32% of them know what it is.

WHO IS THE MODERN CYBERCRIME CRIMINAL?

The stereotypical "movie villain" computer hacker is a pervasive image among adults: 63% think that cyber criminals are mainly individual computer hackers, while only 21% see organized crime as primarily responsible for cybercrime. This finding of a "dark ages" mentality supports what other pros in the field have been saying: we are not winning the battle against cybercrime because our mindset is stuck in the 20th century.

Only urban-dwelling males in their late 20s and early 30s tend to get this question right. Sixty-five percent of this segment of the population knows that most cybercrime is perpetrated by organized crime. Knowing who is behind cybercrime is not so much about how much time you spend on the Internet as it is about who you associate with.

PHISHING

Fewer than half of adults (47%) correctly identify what the term "phishing" means. Twenty-one percent are unsure what the term means, but 32% identify phishing as something other than an attempt to mislead a person into giving up their personal information over the Internet, indicating a substantial amount of confusion.

The term is largely foreign for those who do not go on-line: only 28% of those who stay off the Internet know what phishing refers to. As with the term “cybercrime,” awareness of phishing is heavily related to Internet usage. A large majority of those who engage in heavy usage identify phishing’s correct definition. Among low to moderate users, knowledge of phishing tends to be limited to 25 to 34 year-olds who live outside the central time zone.

Cybercrime Savvy

Based on the responses to the three knowledge questions, we find that 8% of the population knows what phishing and cybercrime are and also knows that organized crime is the main cause of the problem. On the other end of the spectrum, 18% are unable to correctly answer any of the questions. In between are 75% of Americans who are moderately savvy about Internet-based crime.

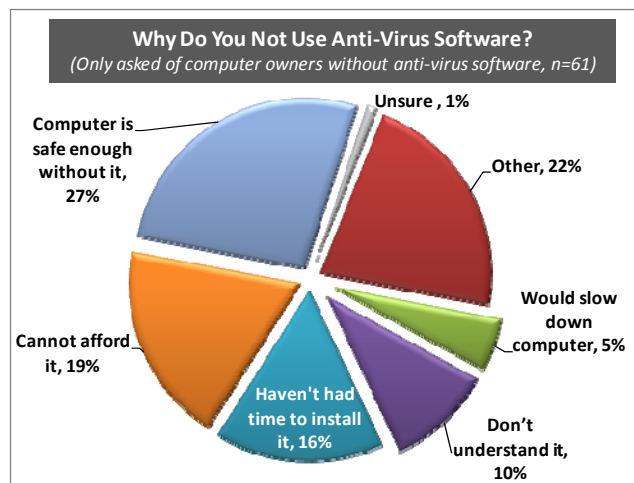
Those who spend three hours or more per week on the Internet are savvier, with college-educated male Internet users being the most knowledgeable of all. On the other hand, most of those who do not venture online and who do not have a high school education were wrong about all three questions.

USE OF ANTI-VIRUS SOFTWARE

The overwhelming majority of computer owners say they safeguard their machines: 89% say they use anti-virus software on their computer. The main issue here is whether the computer user goes online or not. Despite the ubiquity of the Internet, 5% of computer owners do not access it and, therefore, anti-virus software is far less of a concern for them. Only 36% of those who remain off-line report employing the software compared to 93% among those who go online during at least some portion of the week. So, virtually all Internet users are running an anti-virus program. Use of the software is also a matter of means. Although more than 96% of computer owners earning more than \$60,000 use anti-virus software, that slips to about 87% among those making between \$20,000 and \$60,000 and drops to 68% among the poorest computer owners. In addition to Internet usage and income contributing to the use of anti-virus packages, Mac ownership is also a significant factor driving down the use of the software. While 88% of non-Mac owners make use of anti-virus software, only 68% of Mac owners do so.

Anti-Virus Software Usage (among computer owners, n=705)	Internet User		Income						Computer Owned	
	Yes (95%)	No (5%)	< \$20K (8%)	\$20-40K (20%)	\$40-60K (22%)	\$60-80K (16%)	\$80-100K (14%)	> \$100K (20%)	Own Mac (17%)	Do Not Own Mac (83%)
Use Anti-Virus Software	93%	36%	68%	88%	86%	96%	96%	96%	68%	88%

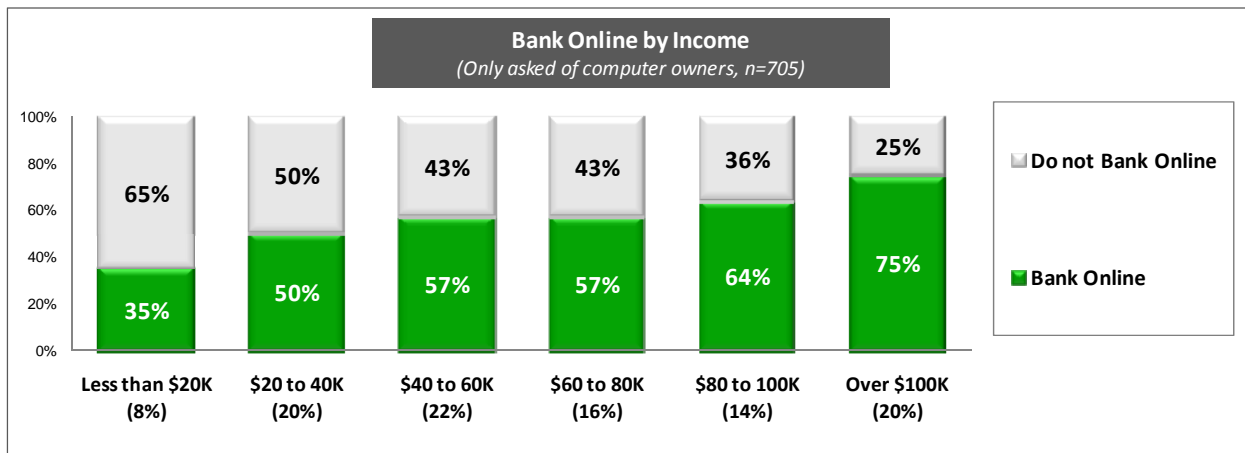
As for reasons why those who do not use anti-virus software avoid it, 27% say their computer is safe enough without it. However, this “safety rationale” is almost all driven by Mac owners. Fifty-seven percent of Mac owners not using anti-virus software say their main reason is that their computer is safe enough already. Only 8% of non-Mac owners claim the same thing. Lower income computer owners who do not use the software are more likely than those in middle and upper-income households to say they



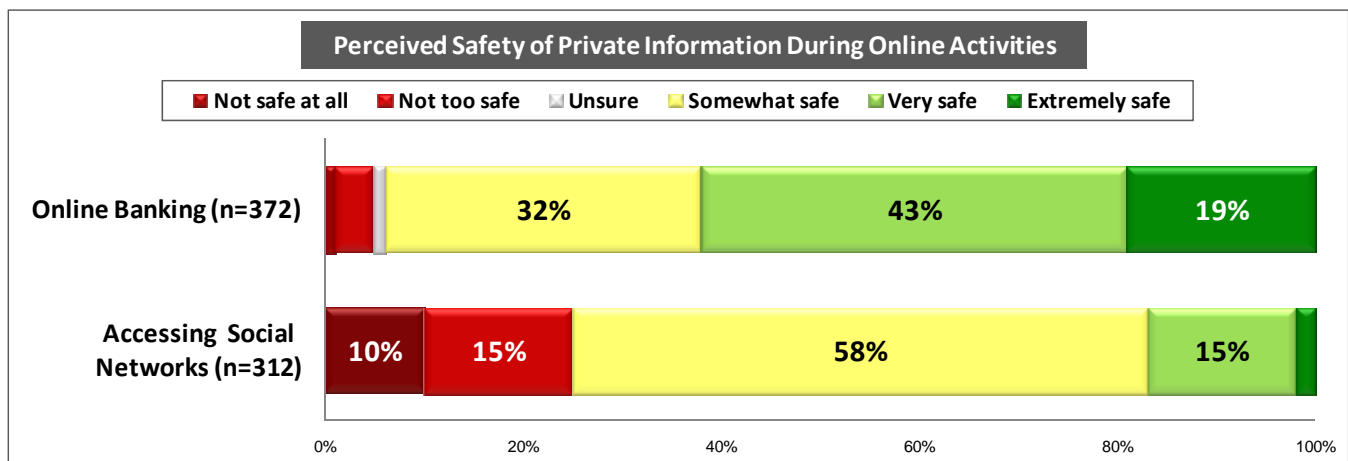
cannot afford it. Overall, 19% cannot afford virus protection, but this rises to 39% among those who earn less than \$20,000. One in six of those not using anti-virus software have yet to install it on their computers. The speed drain caused by anti-virus software is a minimal issue: only 5% say that is the main reason they do not use anti-virus software.

SAFETY OF ONLINE BANKING

More than half (57%) of computer owners now bank online. Using the Internet for banking is far more popular among affluent Americans. Two-thirds of computer owners who earn more than \$80,000 and three-quarters of those earning more than \$100,000 annually handle their banking online. The percentage conducting banking online slips to half among computer owners earning \$20,000 to \$40,000 and then to about one-third among the poorest segment. Internet banking also tends to be the province of the young. Well over 60% of computer owners under the age of 45 engage in it, while only 30% of those older than 65 do it. Interestingly, there is a geographic component to online banking. Those in the Pacific Time Zone are evidently more comfortable with the process because 71% of them bank online. Finally, computer owners with more education are more likely to bank online.

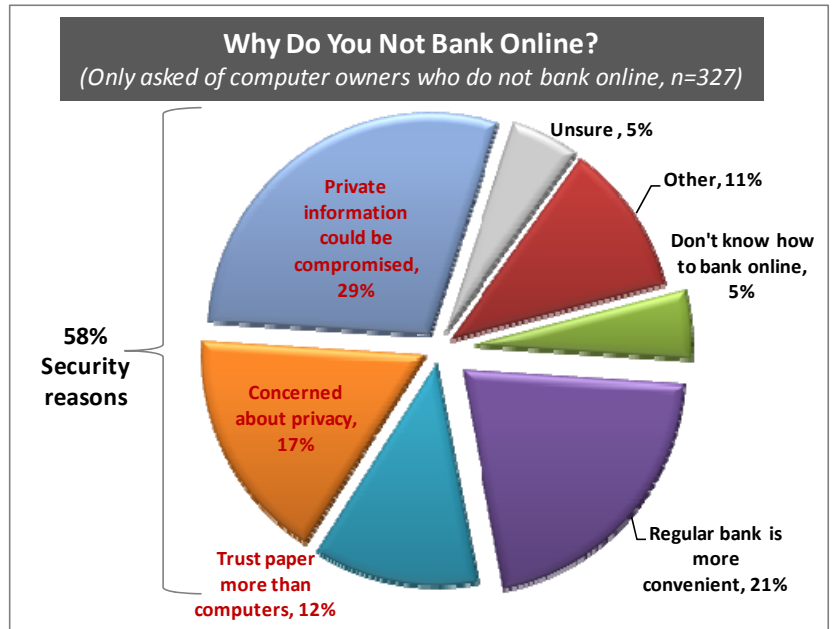


Most who handle their banking over the Internet (62%) believe their private information is *extremely* or *very* safe; a mere 5% say their private information is not too safe or not safe at all. It is notable, however, that those who have been bitten via a cybercrime attack are significantly more skeptical of online banking's



safety. Only 10% of those folks regard online banking as extremely safe. It makes sense that cybercrime victims would be more wary and perhaps banking scams have victimized them. The survey shows no difference between PC and Mac owners when it comes to how safe they perceive online banking to be.

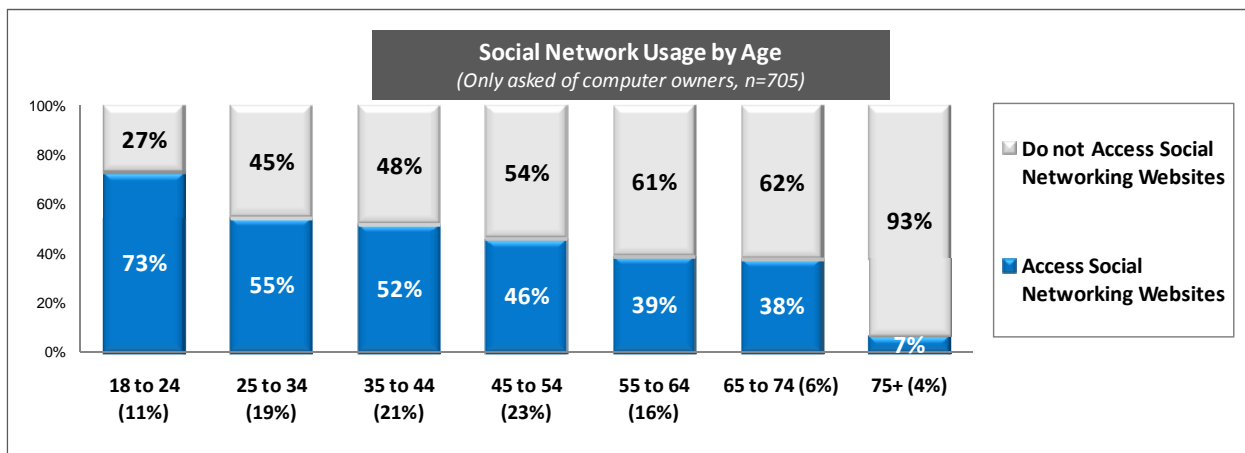
Of Americans who do not bank online, 58% cite some kind of security or trust issue as their reason: 29% say their information could be compromised, 17% have privacy concerns and 12% trust paper more than computers. One in five say their reason for not banking online is that their physical bank is more convenient and only 5% do not know how to bank on-line.



SAFETY OF SOCIAL NETWORKING

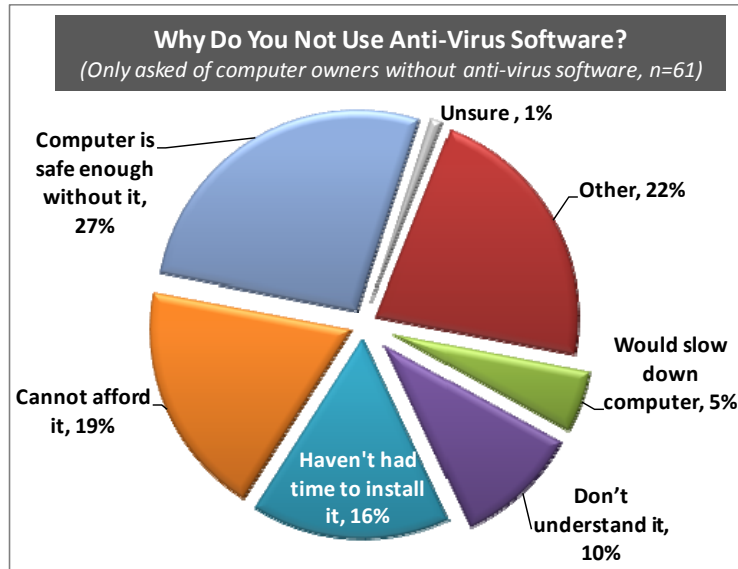
Social networkers clearly accept a lot less security than online bankers.

Forty-eight percent of computer owners access a social networking website, but this varies widely depending on a person's age. Social networks have clearly become a staple in the lives of younger Americans: 73% are social networkers. As the chart shows, that percentage drops precipitously from the 18 to 24 year cohort. It will be very interesting to see whether future surveys document a generational shift whereby people retain their social networking habit as they age. The alternative would be a situation where young social networkers give up their habit the older they get. The survey also shows that women tend to use social networks more than men do and lower income earners are a bit less likely than moderate income and affluent Americans to make use of social networks.



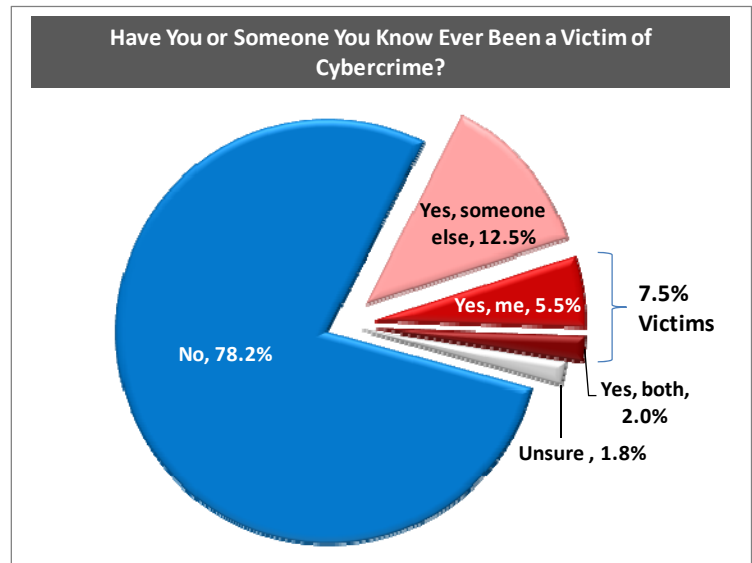
Despite the large percentage of online networkers, only 18% of them believe their private information is very or extremely safe. Even young networkers regard social networks as only somewhat safe. The survey shows no difference between PC and Mac owners when it comes to how safe they perceive social networking to be.

More than half of those who do not access a social networking site say they simply are not interested in them. Abstaining for security reasons is only a minor issue, as 17% name security as their reason for not participating.



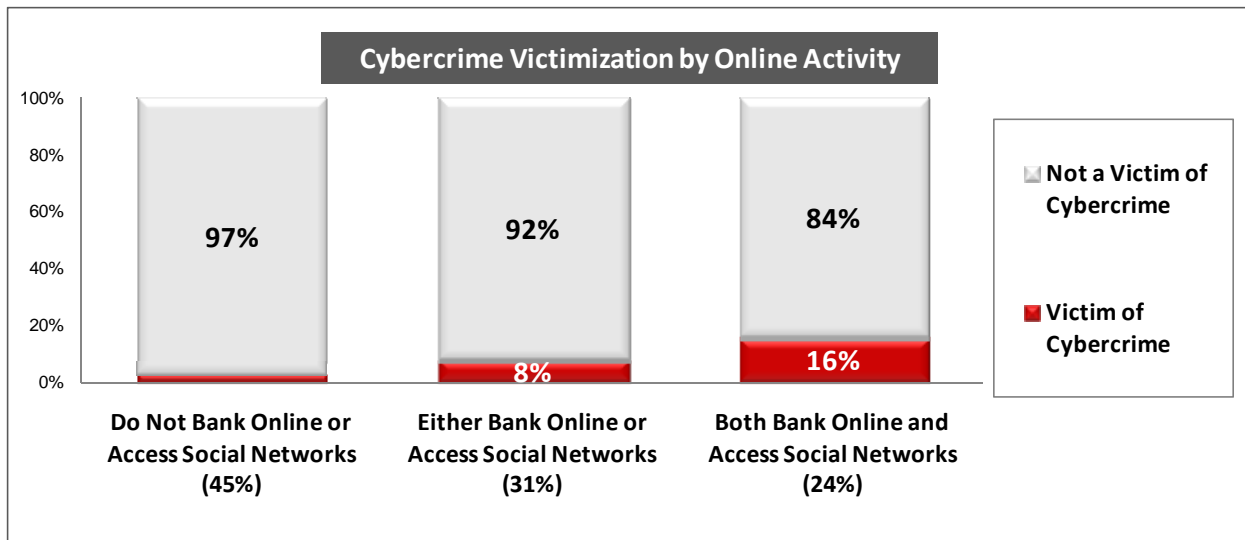
CYBERCRIME VICTIMIZATION

Seven and a half percent of the adult US population has been a victim of cybercrime at some point. Although 31% of those victims say that the crime did not result in any monetary loss, the average cybercrime victim has lost \$662. Roughly translated, cybercrime is an **\$11 billion problem** for US consumers. Fifteen percent know someone else who has been a victim. In February we found that 10% had been victims of “identity theft.” Cybercrime is therefore not quite as widespread as identity theft.

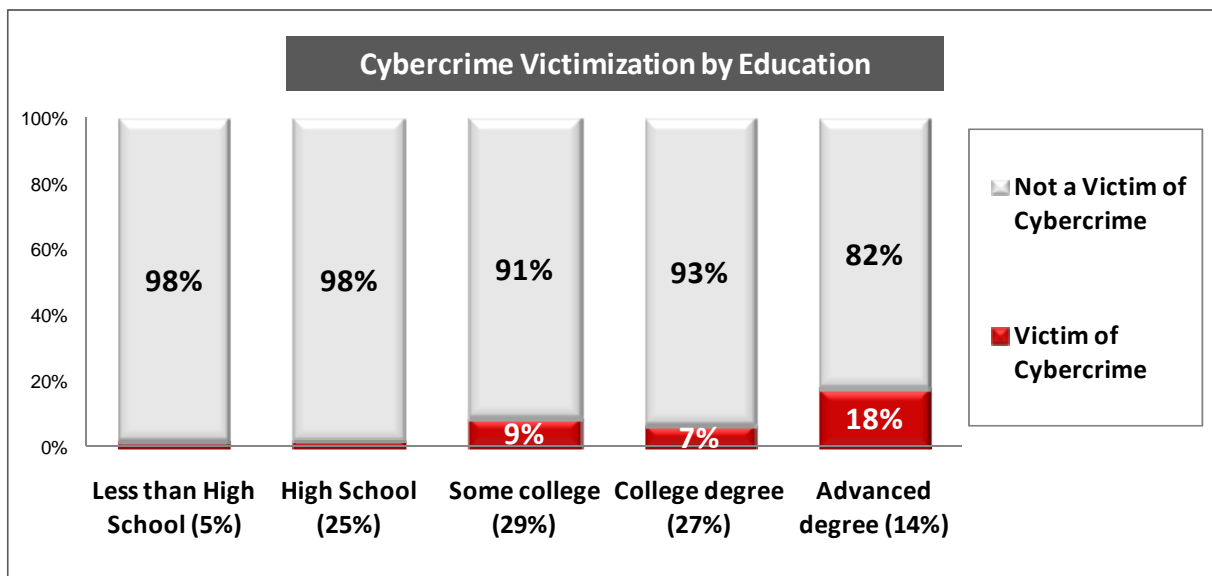


The data shows a very strong link between online activity and cybercrime victimization. Nearly one-quarter of Americans go online to bank and network socially. It is stunning to find that one out of every six of them has been victimized. In contrast, only 3% of those who do neither have fallen prey to cybercriminals. In between, are the folks who engage in one activity or the other: 8% of them have been victims. This clearly shows that the more activities one pursues online, the more likely one is to be hit by cybercrime. Although this finding is certainly statistically significant, it does not necessarily demonstrate that online banking or social networking leads to becoming a victim. It could be that

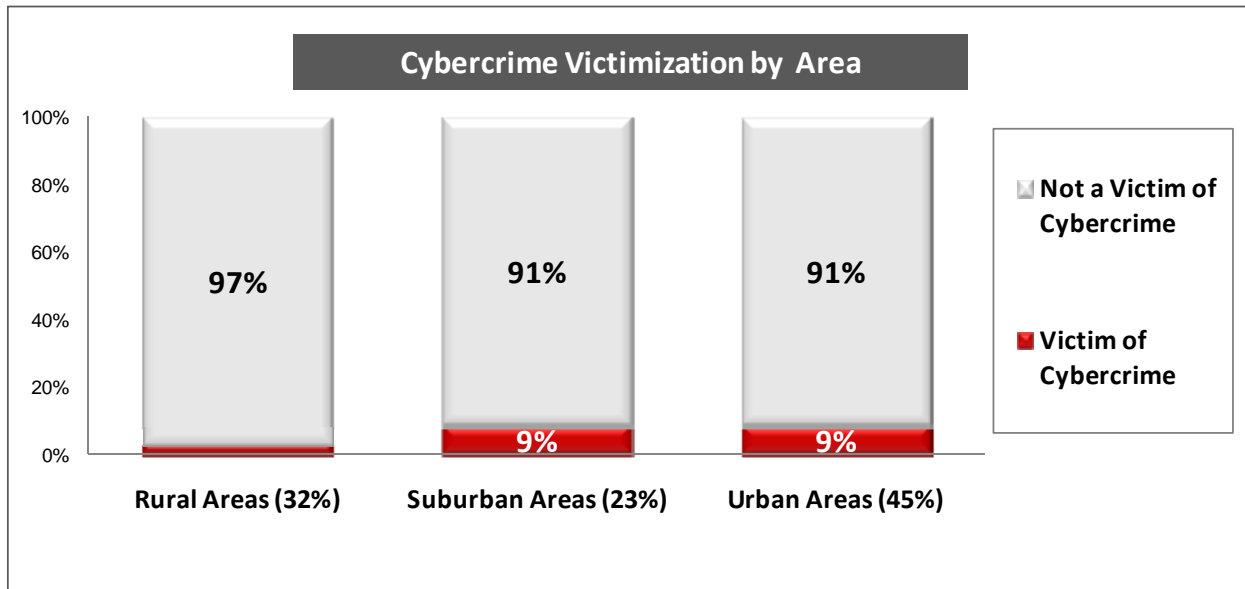
folks who engage in these activities are more likely to conduct other transactions over the Internet and it may be the concert tickets, the CD purchase or the download, rather than the banking activity or the social networking, which actually led to the crime. People who use the Internet in these ways may also be risk-takers who are more casual about conducting financial transactions over the Internet.



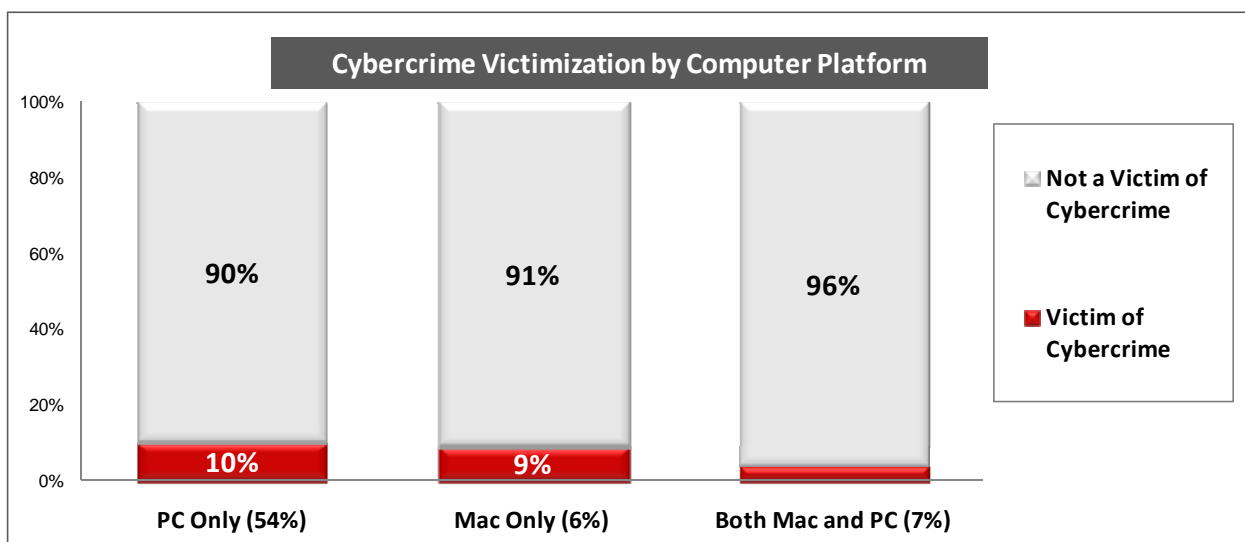
Surprisingly, cybercrime victimization is also strongly related to education levels, and the more educated are more likely to be victimized. As the chart shows, those who have not attended college are relatively immune to cybercrime. Among those with some college or a bachelors degree, victimization is at moderate levels. But those with advanced degrees have really been hard hit: 18% in this group have been victims of cybercrime. Although cybercrime tends to be even more prevalent among highly educated Americans who spend more time online, the victimization rate is high among those with advanced degrees even among those who are on the Internet less than three hours per week. This strong tie between education and victimization suggests that cybercriminals may more often target those who earn advanced degrees. Also, some hubris on the part of well-educated people along the lines of “this can’t happen to me” may occur and lead to riskier behavior.



Apparently one way to protect yourself from a cyber attack is by moving to rural areas or the central time zone. While folks in urban and suburban areas tend to be victimized at rates that are slightly above average, a mere 3% who live in rural zip codes are victims and that decreases to 3% if that rural zip code is in the central time zone. In fact, even suburban- and urban-dwellers in the central time zone are relatively immune to cyber attacks: the victimization rate in America’s heartland is only 4%.



Finally, although being a dedicated Mac owner does not provide greater safety, owning *both* a PC and a Mac does. One would think that having two computers affords twice the chance of getting hit by cybercrime, but that view is wrong. Those who own only a PC have a 10% chance of being a victim of cybercrime, while that figure is 9% for Mac owners – an insignificant difference. However, a mere 4% of those who own both a PC and a Mac have fallen victim to cybercrime. What we are seeing here is probably a measure of computer sophistication: owners of both computer types would tend to be more knowledgeable about computers in general and are therefore more likely to be aware of the threats that come with computer ownership. They probably take more steps than the “average” computer owner to protect themselves.



Interestingly, once the major factors associated with cybercrime – online banking being the most significant -- are accounted for, computer ownership, cybercrime savviness and Internet usage have almost nothing do with whether someone becomes a cybercrime victim. This suggests that what a person does on the Internet, rather than how much surfing they do, matters most when it comes to cybercrime.

Does Anti-Virus Software Lead to Cybercrime Victimization?

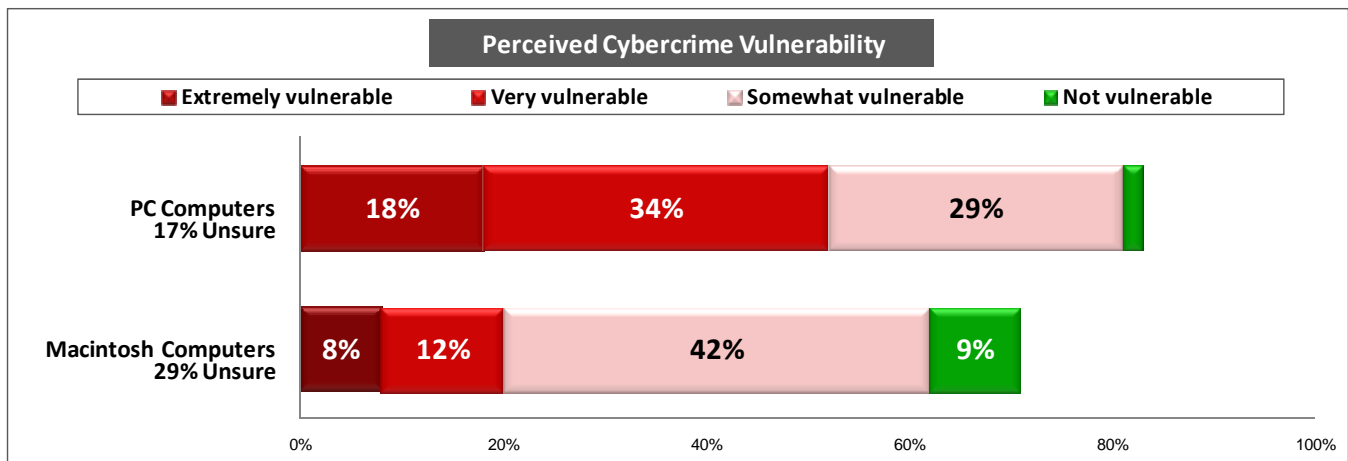
The data appear to say “yes.” Ten percent of computer owners who use anti-virus software have been victims of cybercrime, while only 4% of those who do not use anti-virus software are victims. However, there is no way to tell which came first: victimization or employing the software. It could very well be that some of those who use anti-virus software do so only after they have been hit by cybercrime. If, in reality, cybercrime victimization leads to more usage of anti-virus software, then expect software sales to grow as Internet-based crime spreads.

Who Stands to Lose More to Cybercrime?

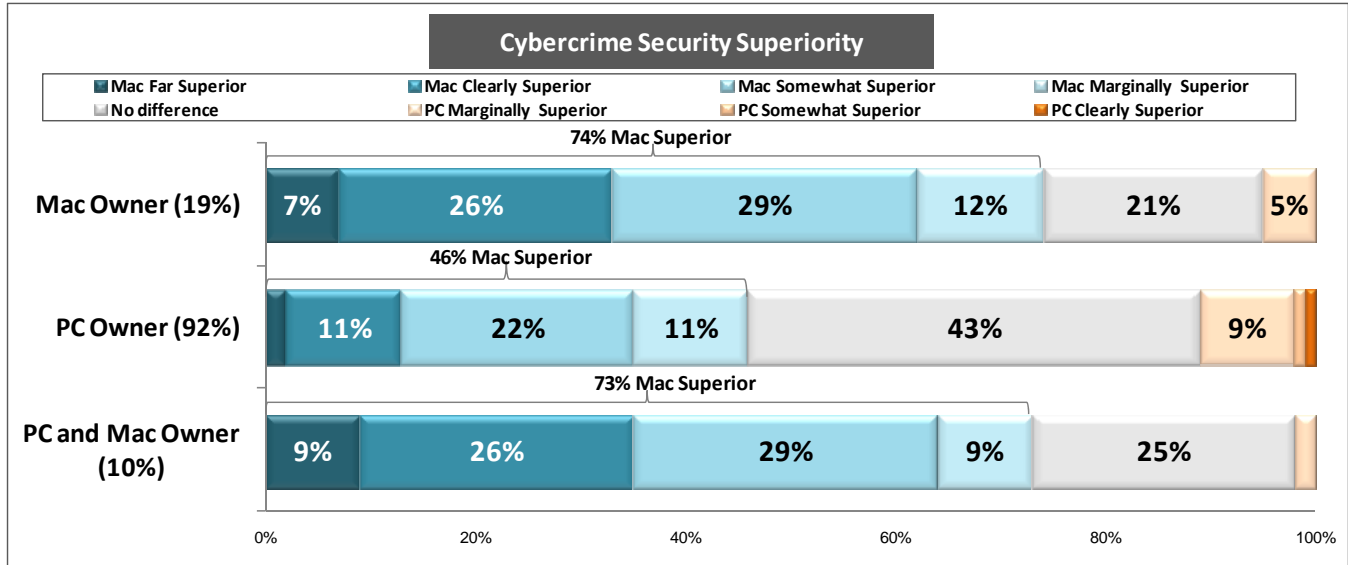
When we examine the amount of money lost to cybercrime the data clearly show that individual Mac owners have been victimized for a lot more than those who use PCs or other machines. The results suggest that the average Mac owner who has been a cybercrime victim has lost six times as much as a PC owner. A deep dive into the data shows that this is not due to Mac owners tending to be more affluent. Mac owners simply get taken for more money when they are stung. It is interesting that no other demographic shows signs of being victimized for significantly more money than Mac users.

PC VERSUS MAC: VULNERABILITY

Despite the reality that there is no significant difference between the two platforms, PC computers are clearly perceived to be less secure than Macs. More than half (52%) of Americans believe that PCs are very or extremely vulnerable to cybercrime attacks, while 17% are simply unsure about PC security. By contrast, only 20% say Macs are very or extremely vulnerable to attacks, although 29% are unsure about how safe a Mac is. The perception is that Macs are safer than PCs. Forty-one percent of Americans weigh in with that opinion; while a mere 10% believe PCs are safer than Macs. That said, most people believe that even Macs are at least somewhat susceptible to a cybercrime attack so neither type of computer is believed to be absolutely invulnerable.



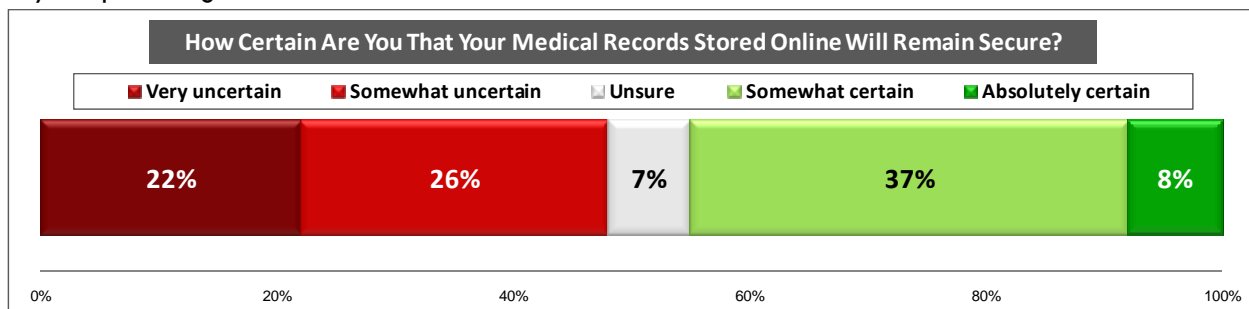
Mac users are known for their loyalty – some would label it as fanaticism – and the survey provides ample evidence for such a view. It is difficult to find a Mac user who sees their machine as inferior to a PC. Only 5% of Mac users register such views, while three-quarters of them claim Macs are less vulnerable than PCs (the balance believe Macs and PCs are equally vulnerable). The funny thing is, PC users tend to agree! Few of them see PCs as less vulnerable than Macs and 46% say PCs are more at-risk. In the fairest head-to-head test of all, we find that 73% of those who own both PCs and Macs agree that Macs are more secure. For PCs to dominate the marketplace in this environment, cyber security clearly must not be a priority for the computer-buying consumer.



The survey also shows that those who are less cybercrime savvy or who reside in lower income households or who have less education tend to perceive no difference between Macs and PCs when it comes to vulnerability to cybercrime attacks.

FAITH IN CONFIDENTIALITY OF ONLINE MEDICAL RECORDS

We find a lot of skepticism when it comes to the security of online medical records. Fifty-five percent of Americans are uncertain that their online medical records being truly confidential or simply do not know. Another 37% are only somewhat certain about the security of their medical records. Only 8% are absolutely convinced their online medical records will remain confidential. There is a big difference here between those who own computers and those who do not. The level of distrust registered by the non-owners is striking: 22% are very uncertain that their medical records will remain confidential. The extreme uncertainty drops somewhat among computer owners in general, but stands at 27% among unsavvy computer owners. This shows that concerns about medical record security tend to be a function of how comfortable Americans are with cyberspace in general.



ESET/Securing Our e-City National Cybercrime Survey

n=1003 US Adults

October 2-5, 2009

Margin of Sampling Error +/- 3.1%

Weighted to account for differences Cell Phone-only Population and Age

Hi this is _____ with Competitive Edge Research, a national polling firm and we're calling adults across the country that were selected at random to ask your opinion on a variety of interesting topics. We are absolutely not selling anything. People find it fun and all your answers will be kept strictly confidential. Please let me begin by asking . . .

Q1. What was your age on your last birthday?

	%
18 to 24	10.5
25 to 34	17.0
35 to 44	19.0
45 to 54	20.3
55 to 64	15.1
65 to 74	9.1
75 and over	8.9
Refused (<i>not read</i>)	0.1

Q2. Can you tell me what the term cybercrime refers to?

	%
A crime committed over the Internet	65.2
Something else	5.7
Unsure (<i>not read</i>)	29.1

Cybercrime refers to a crime committed over the Internet. (*Read to those who say "something else" or "unsure" in Q2*)

Q3. Of the following sources, do you think most cybercrime comes from . . .

	%
Individual computer hackers	63.4
Organized crime	20.8
Other (<i>not read</i>)	4.3
Unsure (<i>not read</i>)	11.6

Q4. I'm going to read you four definitions for the term phishing – that's phishing with a P-H. Please tell me which definition is the correct one.

	%
An attempt to mislead you into giving up your personal information over the Internet	46.7
Unsolicited e-mail that is sent to a large number of addresses	16.9
A computer program, usually hidden within another program, which copies itself and inserts those copies into other programs to perform malicious actions	10.4
A seemingly useful computer program which, when activated, performs a malicious action	4.6
Other (<i>not read</i>)	0.7
Unsure (<i>not read</i>)	20.7

Q5. Have you, or someone you know, been a victim of cybercrime?

	%
Yes, me	5.5
Yes, someone else	12.5
Yes, both	2.0
No	78.1
Unsure (<i>not read</i>)	1.8

Q6. What is your best estimate as to the amount of money or property you lost because of the cybercrime? (*Only asked of those who reported being a victim of cybercrime, n=71*)

	%
Nothing	31.0
\$1-100	6.1
\$101-200	11.9
\$201-500	6.8
\$501-1,000	17.1
More than \$1,000	5.3
Loss covered by third party (<i>not read</i>)	10.9
Unsure (<i>not read</i>)	8.8
Refused (<i>not read</i>)	2.1
Average amount	\$661.91

Please tell me how vulnerable you believe the following types of computers are to cybercrime attacks.

	Not Vulnerable	Some Vulnerable	Very Vulnerable	Extremely Vulnerable	Unsure
Q7. PC Computers	2.1	29.4	33.4	18.4	16.8
Q8. Macintosh Computers	9.2	41.8	11.7	7.7	29.7

Q9. Do you own . . .

	%
A PC computer	53.9
A Mac computer	5.6
Some other type of computer or	8.2
Do you not own a computer	23.2
Both (<i>not read</i>)	6.9
Unsure (<i>not read</i>)	2.1

Q10. Some people do not use anti-virus software. Do you currently use anti-virus software on your computer or not? (*Only asked of computer owners, n=705*)

	%
Yes	89.4
No	8.5
Unsure (<i>not read</i>)	2.1

Q11. Is that mainly because . . . (*Only asked of computer owners who do not use anti-virus software, n=61*)

	%
Your computer is safe enough without it	26.8
You cannot afford it	19.1
You haven't taken the time to install it	15.6
You don't understand it	10.2
It would slow down your computer	4.8
It interferes with other programs on your computer	0.0
Some other reason (<i>not read</i>)	22.5
Unsure (<i>not read</i>)	1.1

Q12- Q13 and Q14-Q15 were randomized

Q12. Do you use your computer to bank on-line? (*Only asked of computer owners, n=705*)

	%
Yes	56.8
No	42.6
Unsure (<i>not read</i>)	0.6

Q13a. When using your computer to bank on-line do you feel your private information is . . . (*Choices were alternated. Only asked of computer owners who bank on-line, n=372*)

	%
Extremely safe	18.6
Very safe	43.4
Somewhat safe	31.7
Not too safe or	4.0
Not safe at all	1.4
Unsure (<i>not read</i>)	0.9

Q13b. Do you not bank on-line because you feel. . . (Choices were randomized. Only asked of computer owners who do not bank on-line, n=327)

	%
Your private information could be compromised	29.4
Your regular bank is more convenient	21.2
You are concerned about your privacy	16.6
You trust paper more than computers	12.5
You don't know how to bank on-line	4.5
Other (not read)	11.1
Unsure (not read)	4.6

Q14. Do you use your computer to access a social network? (Only asked of computer owners, n=705)

	%
Yes	48.1
No	50.1
Unsure (not read)	1.8

Q15a. When using your computer to access social networks do you feel your private information is . . . (Choices were alternated. Only asked of computer owners who access social networks, n=312)

	%
Extremely safe	2.2
Very safe	15.4
Somewhat safe	57.4
Not too safe or	15.1
Not safe at all	9.6
Unsure (not read)	0.3

Q15b. Do you not access social networks because you feel. . . (Choices were randomized. Only asked of computer owners who do not access social networks, n=393)

	%
You are not interested	53.7
You don't have the time	15.5
You are concerned about your privacy	9.2
Your private information could be comprised	8.1
You might say something regrettable that will live forever on the Internet	3.1
Other (not read)	4.5
All of the above (not read)	2.6
Unsure (not read)	3.3

Q16. Most people's medical records are now stored on-line. Are you absolutely certain, somewhat certain, somewhat uncertain or very uncertain that your medical records will remain confidential?

	%
Absolutely certain	7.6
Somewhat certain	36.8
Somewhat uncertain	26.1
Very uncertain	22.2
Unsure (not read)	7.3

Thanks. Now I have some demographic questions to make sure we have a representative sample . . .

Q17. How many total hours per week, other than for sending and receiving emails, do you usually spend going online? Please think about time you may spend online at home, school, work or any other location.

	%
None	19.7
Less than one hour	3.8
1 hour to less than 3 hours	15.1
3 hours to less than 8 hours	16.1
8 hours to less than 15 hours	14.7
15 hours to less than 20 hours	4.7
20 hours or more	24.0
Varies too much to say (<i>not read</i>)	0.5
Unsure (<i>not read</i>)	0.3
Refused (<i>not read</i>)	1.2

Q18. What is the last level of education you have completed?

	%
Less than a high school diploma	5.3
High school	24.5
Some college	28.2
College degree	26.6
Advanced degree	14.3
Refused (<i>not read</i>)	1.0

Q19. And please stop me when I reach the category closest to your household's total annual income . . .

	%
Less than \$20,000	13.3
\$20 to 40,000	22.0
\$40 to 60,000	18.4
\$60 to 80,000	12.7
\$80 to 100,000	10.1
More than \$100,000	14.7
Refused (<i>Not read</i>)	8.9

20. GENDER (BY OBSERVATION)

	%
Male	46.5
Female	53.5

21. REGION (FROM SAMPLE)

	%
Eastern	47.3
Central	29.3
Mountain	6.1
Pacific	17.3

22. LANGUAGE (BY OBSERVATION)

	%
English	98.1
Spanish	1.9

Notes to Crosstabs

Crosstabulations of data are simply comparisons of how respondents to one question answered a separate question or rated in a different category. In statistical terms, crosstabulations attempt to determine whether responses to two different, but possibly related, questions are independent of, or dependent on, one another. The analyst's job is to determine which relationships are significant and then ascertain the underlying causes for those occurrences

Cells of data should always be compared first with the corresponding totals in the far right column and then compared among the other percentages in the original column. For instance, in the first table on page 1 of the crosstabulations, we compare the demographic variables age and gender with whether the respondents bank online, respondents' reasons for not banking online and the respondents' perceived safety of banking online.

Among other things, the table shows that 65% of the respondents who are 18 to 24 years old bank online. This is compared to the row total on the right which shows that 57% of all respondents bank online. One can conclude that the younger respondents have a higher likelihood of banking online than what would normally be expected for all respondents in this study. In other words, there may be some *cause* for the occurrence of a higher number of 18 to 24 year olds who bank online.

One should be careful to avoid making the mistake of inferring that the 65% pertains to *how many of the respondents who bank online are 18 to 24 years old*. The tables only show how the variable in the banner (top), or independent variable, relates to the variable in the stub (side), or dependent variable.

In addition to sampling error (see Limitations) relating to the size of the sample, sampling error also relates to the percentage breakdowns in each variable. Variables which have a 50% "yes," 50% "no" breakdown contain the maximum amount of sampling error. The table below shows the maximum sampling error at the different percentages of response for some segment sizes.

Response	Sub-Sample	Sub-Sample	Sub-Sample
Percentages	= 50	= 150	= 350
10 or 90%	8%	5%	3%
20 or 80%	11%	6%	4%
30 or 70%	13%	7%	4%
40 or 60%	14%	8%	5%
50%	14%	8%	5.2%