Online Consumers' Reaction to Device Fingerprinting

Sponsored by

ThreatMetrix

Published by Ponemon Institute LLC

Publication Date: October 15, 2009

Ponemon Institute© Private & Confidential Document

Online Consumers' Reaction to Device Fingerprinting

By Dr. Larry Ponemon, October 15, 2009

The *Online Consumers' Reaction to Device Fingerprinting* study was sponsored by ThreatMetrix and conducted by Ponemon Institute. The purpose of the study is to learn what consumers who regularly use the Internet think about online fraud and what steps they believe should be taken to protect their personal information and identity.

We found that 80 percent of consumers surveyed have some level of concern about becoming a victim of online fraud. These consumers believe online merchants, banks and social networks should take steps to protect their personal information and identity.

IT security practitioners believe consumers' fears are well-founded and worry about the growing sophistication of cyber criminals. In Ponemon Institute's *2009 Security Mega Trends* study, 77 percent of practitioners surveyed said the risk of cyber crime will be high and very high in the next 24 months.

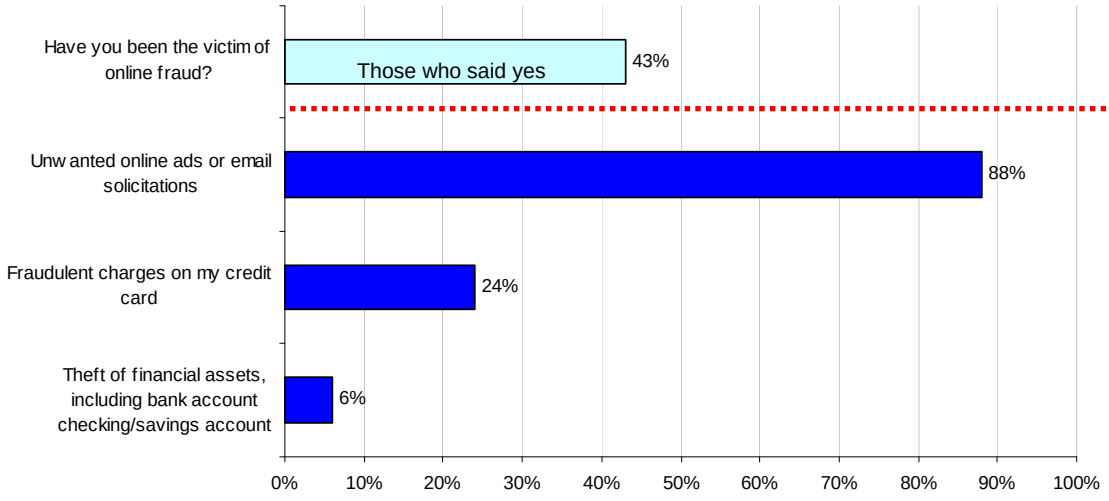
A total of 551 adult-aged U.S. consumers participated in the study. More than half of respondents spend between 10 and 40 hours per week on the Internet and 29 percent spend more than 40 hours. The most popular activities are: search and information gathering, shopping and emailing. The survey covered the following topics:

- Information consumers provide online to prove their identity.
- Whether they were victims of online fraud.
- Concerns about becoming a victim of online fraud.
- Solutions they believe would protect them from online fraud.
- Personal information they would be willing to share for authentication purposes.

Following are the most salient findings of this survey research. Please note that most of the results are displayed in bar chart format. The actual data utilized in each figure and referenced in the paper can be found in the percentage frequency tables attached in Appendix 1.

Finding 1: Many consumers have been victims of online fraud. Unwanted online ads or email are the biggest consequence.

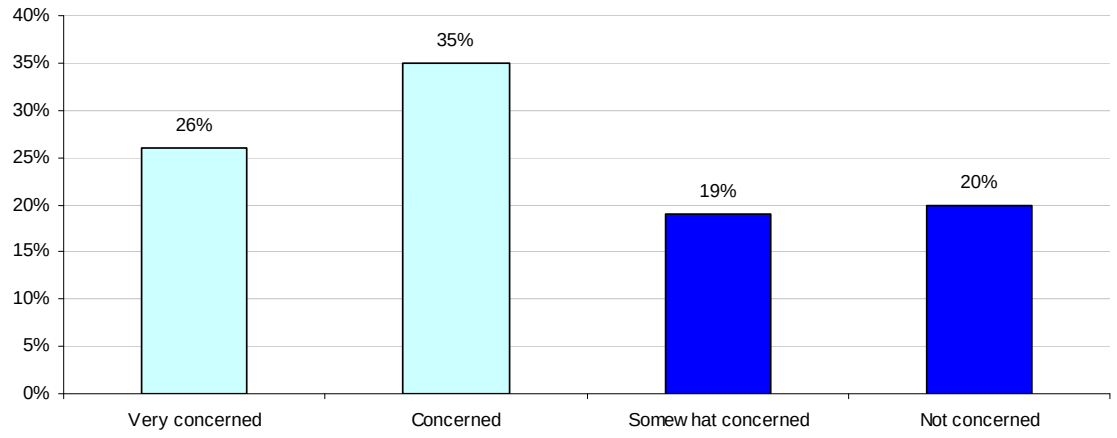
Bar Chart 1
Respondents' experience with online fraud



Forty-three percent have been a victim of online fraud. Most of these victims (88 percent) received online ads or email solicitations as a consequence followed by fraudulent charges on their credit card (24 percent).

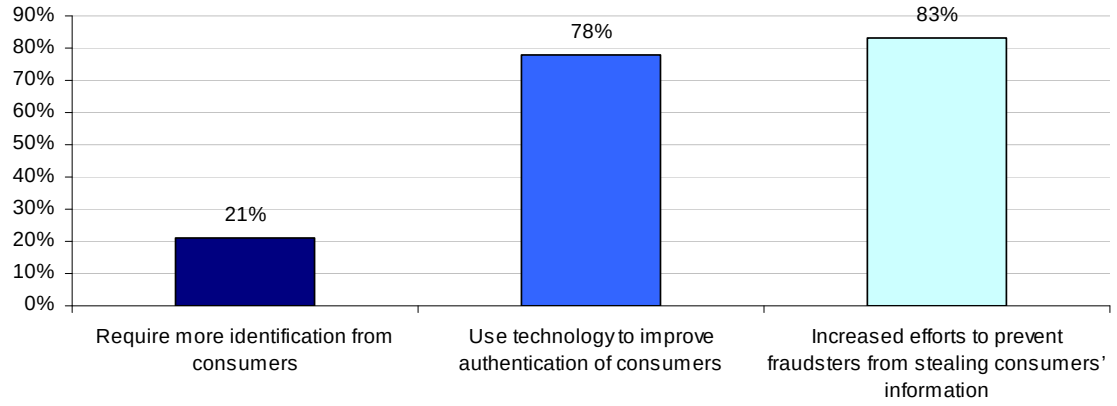
The vast majority, 80 percent of respondents, are very concerned or concerned about becoming a victim of online fraud.

Bar Chart 2
Respondents' level of concern about online fraud



The two steps consumers would like online merchants to take are: increased efforts to prevent fraudsters from stealing consumers' information (83 percent) and use of technology to improve authentication of consumers (78 percent). Only 21 percent want to provide more identification to prove their identity.

Bar Chart 3
What respondents want



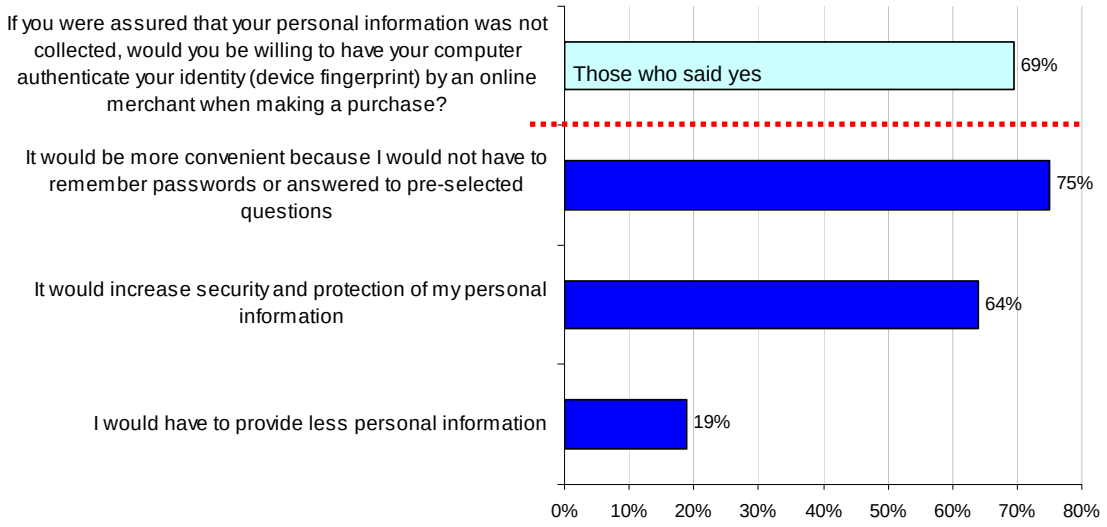
Finding 2: Consumers want both convenience and security in a technology solution.

A large number of consumers seem to like the idea of a technology solution that authenticates their computer. The primary reasons are that it would be more convenient than having to remember passwords or answers to pre-selected questions and it would increase security and protection of personal information.

Currently, most respondents provide passwords, personal history (i.e. mother's maiden name), answer to a pre-selected question and name to authenticate themselves.

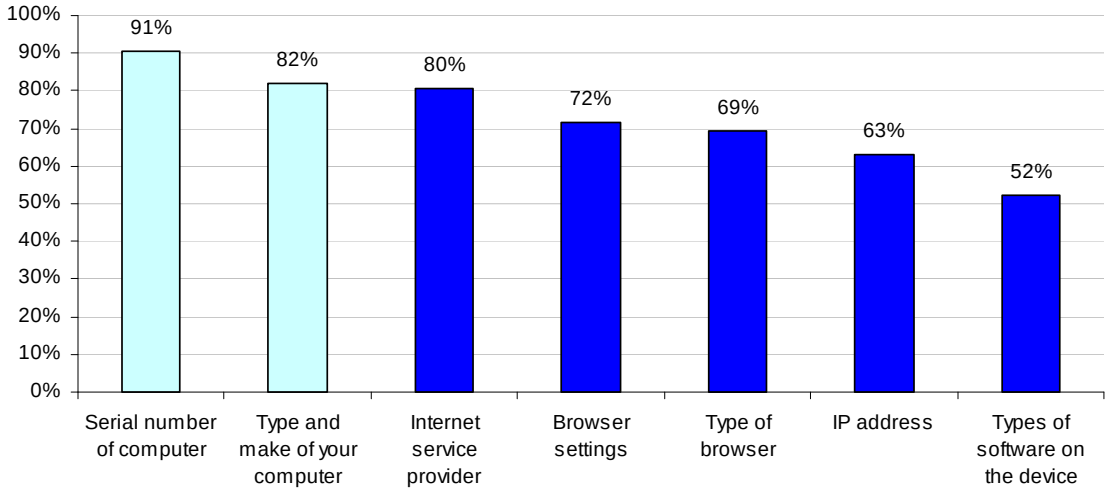
The few who do not want a technology solution say they would rather use passwords because they are concerned their identity would still be stolen, and they would worry their computer would be blacklisted even though they are a legitimate customer.

Bar Chart 4
Respondents hold a favorable impression about device fingerprinting



Respondents say they would be most willing to share the serial number of their computer (91 percent), type and make of the computer (82 percent) and Internet service provider (80 percent). Fewer respondents are willing to share zip code (7 percent), Social Security number (3 percent) and driver's license number (3 percent). Following are seven most highly rated data types.

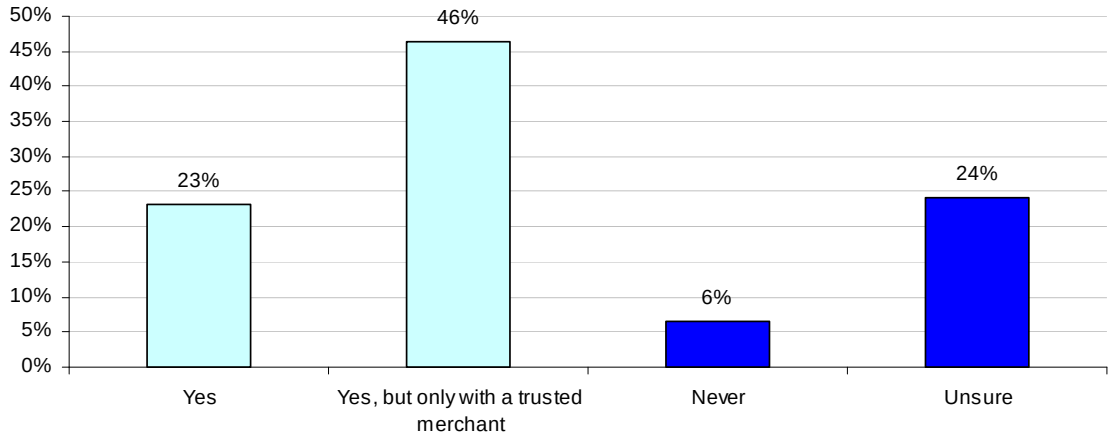
Bar Chart 5
Data types respondents are willing to share in order to authenticate their device



Finding 3: Consumers would consider having their computer authenticate their identity and most would allow a trusted online merchant to use cookies or software to prove their identity.

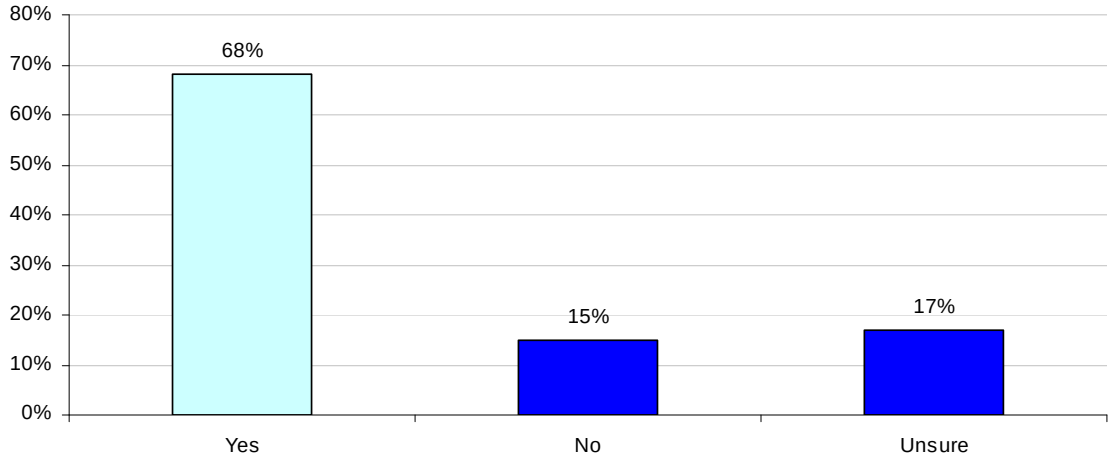
If they were assured that their personal information would not be collected, 69 percent of consumers in this study would consider having their computer authenticate their identity when making a purchase (23 percent say yes and 46 percent say it would depend upon whether they have a trusted relationship with the online merchant.) Only 6 percent say never and 24 percent are unsure.

Bar Chart 6
Respondents' willingness to participate in device fingerprinting



Further, 68 percent would allow a trusted online merchant to place a cookie or software on their computers to automatically authenticate their computer each time they visited the merchant's website. Only 15 percent say no and 17 percent are unsure.

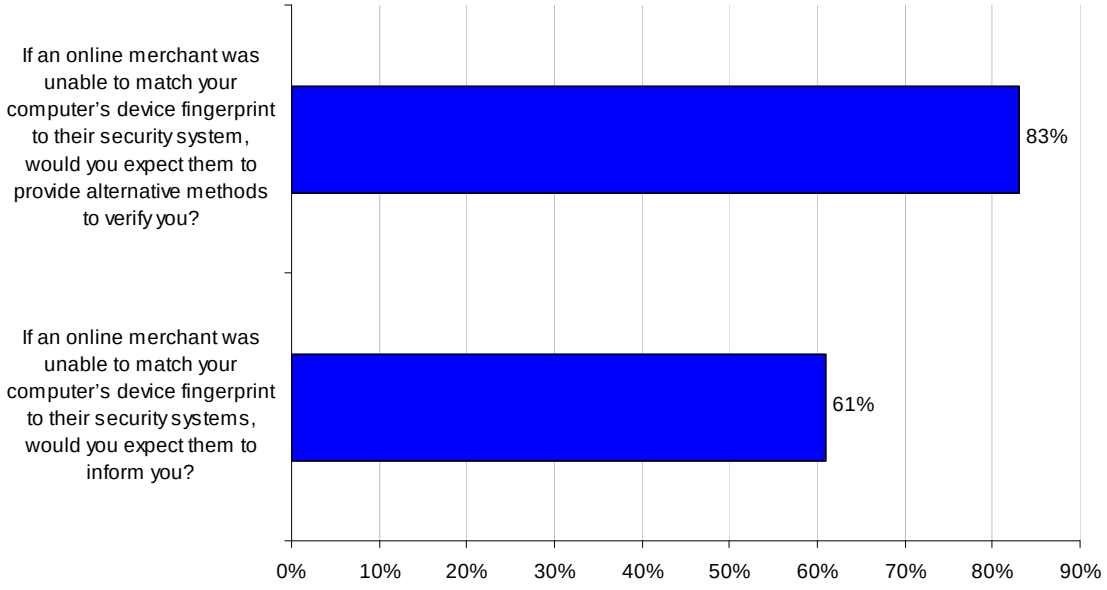
Bar Chart 7
Respondents' willingness to download cookie or software to authenticate their device



Finding 4: Consumers mostly agree on practices and procedures for authentication.

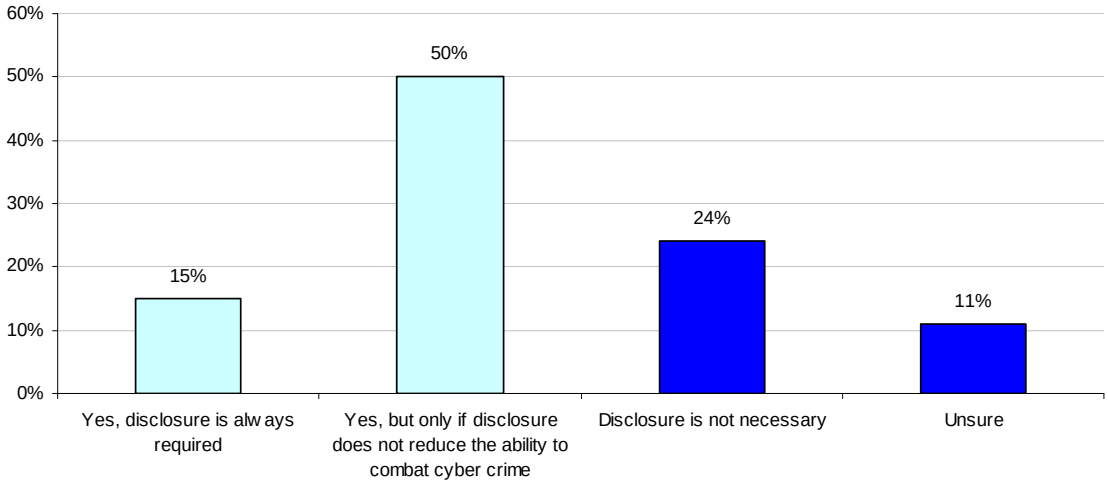
According to 61 percent of consumers in our study, if an online merchant was unable to match their computer's device fingerprint to their security systems they would expect to be informed. Further, if the online merchant was unable to match their computer's device fingerprint to their security system 83 percent would expect them to provide alternative methods to verify them.

Bar Chart 8
Respondents' expectations about alternative procedures if device fingerprint fails
Percentage Yes response to each question



More than half (52 percent) of consumers would not be concerned if an online merchant shared their device fingerprint with other online merchants. Only 15 percent believe an online merchant should disclose to consumers its use of device fingerprinting on its website and other notices.

Bar Chart 9
Respondents' expectations about disclosure before use



Method

A random sampling frame of 17,495 adult-aged individuals who reside within the United States was used to recruit participants to this survey. Our randomly selected sampling frame was selected from national lists of security practitioners. A bifurcated sampling plan was used to compare two sub-samples: respondents who have experienced data-stealing malware and those who have only experienced generic malware.

Table 1: Sampling statistics	Pct%
Sampling frame of adult-aged consumers	14,009
Bounce-back	2,453
Total sample (before reliability)	632
Response rate (before reliability)	4.5%
Total sample (final)	551
Response rate (final)	3.9%

In total, 632 respondents completed the survey. Of the returned instruments, 81 surveys failed reliability checks. A total of 551 surveys were used as our final sample, representing a 3.9 percent net response rate.

Ninety-two percent of respondents completed all survey items within 10 minutes. Table 2 reports the respondent's employment status. As can be seen, a majority of respondents are employed on a full-time or part-time basis. A total of 10 percent say they are unemployed, and 11 percent are students.

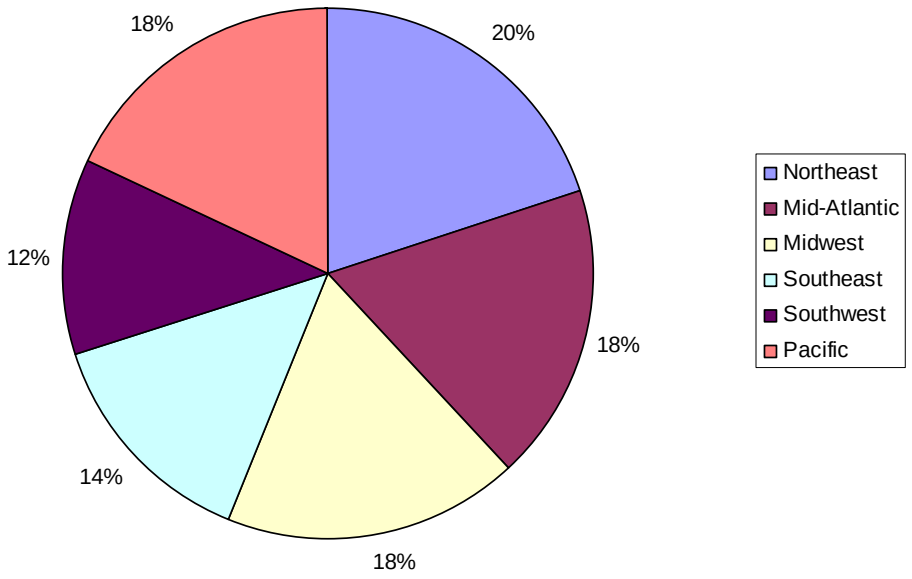
Table 2: Respondents' employment status	Pct%
Full time employee	51%
Part time employee	8%
Business owner	9%
Retired	5%
Student	11%
Active military	6%
Unemployed	10%
Total	100%

Table 3 reports the respondents' self-selected age range. As can be seen, a large number of respondents are at or below 45 years. In addition, 53 percent are female and 47 percent male. Sixty- four percent say they are head of household.

Table 3: Respondents' age range	Pct%
18 to 25	18%
26 to 35	26%
36 to 45	24%
46 to 55	14%
56 to 65	9%
66 to 75	5%
75+	3%
Total	100%

Pie Chart 1 reports the respondents' geographic location by region in the United States. As shown, the largest segment is in the northeast and the smallest segment is in the southwest.

Pie Chart 1
Respondents' location in the United States



Caveats to this study

There are inherent limitations to survey research that need to be carefully considered before drawing inferences from findings. The following items are specific limitations that are germane to most web-based surveys.

- Non-response bias: The current findings are based on a sample of survey returns. We sent surveys to a representative sample of American consumers, resulting in a large number of usable returned responses. Despite non-response tests, it is always possible that individuals who did not participate are substantially different in terms of underlying beliefs from those who completed the instrument.
- Sampling-frame bias: The accuracy is based on contact information and the degree to which the list is representative of individuals who use the Internet. We also acknowledge that the results may be biased by external events such as media coverage. We also acknowledge bias caused by compensating subjects to complete this research within a holdout period. Finally, because we used a web-based collection method, it is possible that non-web responses by mailed survey or telephone call would result in a different pattern of findings.
- Self-reported results: The quality of survey research is based on the integrity of confidential responses received from subjects. While certain checks and balances can be incorporated into the survey process, there is always the possibility that a subject did not provide a truthful response.

Conclusion

Instances of identify theft and online fraud are rising and the "bad guys" are getting smarter. Organizations must manage the risks associated with online transactions to protect their business and their customers. New technologies can help organizations mitigate online fraud and ID theft, reduce costs, and improve the customer's experience.

Consumers, according to our study, want both convenience and security when they are online. They also want online merchants to be proactive in protecting their information and identity. Consumers are weary of having to remember passwords or answers to pre-selected questions. Based on the findings of our consumer study, it seems as if it is the right time for organizations to forget password-based authentication methods and consider emerging technologies such as device fingerprinting to reduce online identity theft and fraud.

About Ponemon Institute LLC

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

As a member of the Council of American Survey Research Organizations (CASRO), we uphold strict data confidentiality, privacy, and ethical research standards. We do not collect any personally identifiable information from individuals (or company identifiable information in our business research). Furthermore, we have strict quality standards to ensure that subjects are not asked extraneous, irrelevant, or improper questions.

About ThreatMetrix, Inc

ThreatMetrix device identification (www.threatmetrix.com) helps companies control online fraud and abuse in real time so they can acquire more customers faster, reduce costs, and increase customer satisfaction. ThreatMetrix profiles the device used in an online transaction so companies can determine whether the users are fraudsters or customers. ThreatMetrix' simple and cost-effective approach to implementation – SaaS or on-premise – enables companies to get results in hours or days, rather than weeks or months. ThreatMetrix serves a rapidly growing customer base in the U.S. and around the world across a variety of industries including online retail, financial, social networks, and alternative payments.

Online Consumers' Reaction to Device Fingerprinting

Audited results presented by Dr. Larry Ponemon, September 2, 2009

The following tables summarize the percentage frequency results of all survey items. Please note that several tables sum to more than 100% because these questions permitted more than one choice. The total sample size for most questions is 551 adult-aged respondents. All individuals are located in the United States. The web-based survey window closed on August 28, 2009.

Sampling frame (U.S. IT & IT security)	14009
Bounce-back	2453
Total sample (before reliability)	632
Response rate (before reliability)	4.5%
Total sample (final)	551
Response rate (final)	3.9%

Screening questions

S1. In an average week, about how much time do you spend on the Internet?	Pct%
Less than 1 hour	4%
Between 1 to 5 hours	8%
Between 6 to 10 hours	6%
Between 10 to 20 hours	23%
Between 20 to 40 hours	30%
More than 40 hours	29%
Total	100%

S2.Which of the following online activities do you do in a typical week?	Pct%
Shopping	63%
Blogging	15%
Search & information gathering	68%
Online banking	19%
Entertainment such as music or gaming	30%
Emailing & communications	45%
Social networking (such as Facebook, MySpace)	39%
Work-related activities	15%
Uploading a video (such YouTube)	16%
Total	310%

S3. What is your primary source for local, national and world news?	Pct%
Print newspapers	29%
Television news	26%
Online news from news organizations	21%
Individual blogs	13%
No primary news source	11%
Other (specify)	0%
Total	100%

Survey questions

Q1. What information do you provide online about yourself to prove your identity? Please check all that apply.	Pct%
Name	47%
Home address	19%
Telephone number	36%
Passwords	96%
Social Security number	39%
Credit Card number	42%
Personal history (i.e. mother's maiden name)	62%
Special question (pre-selected by you)	62%
Total	401%

2a. Have you been the victim of online fraud?	Pct%
Yes	43%
No	57%
Total	100%

Q2b. If yes, what were the consequences?	Pct%
Fraudulent charges on my credit card	24%
Theft of financial assets, including bank account checking/savings account	6%
Unwanted online ads or email solicitations	88%
Other	2%
Total	120%

Q3a. How concerned are you about becoming a victim of online fraud?	Pct%
Very concerned	26%
Concerned	35%
Somewhat concerned	19%
Not concerned	20%
Total	100%

Q3b. If you are concerned or very concerned, what steps should be taken by online merchants, banks and social networks (any other?) to protect your personal information and identity?	Pct%
Require more identification from consumers	21%
Use technology to improve authentication of consumers	78%
Increased efforts to prevent fraudsters from stealing consumers' information	83%
Other	2%
Total	218%

Q4a. If you were assured that your personal information was not collected, would you be willing to have your computer authenticate your identity (device fingerprint) by an online merchant before when making a purchase?	Pct%
Yes	23%
Yes, but only if I have a trusted relationship with the vendor	46%
Never	6%
Unsure	24%
Total	100%

Q4b. If yes, why?	Pct%
It would increase security and protection of my personal information	64%
It would be more convenient because I would not have to remember passwords or answered to pre-selected questions	75%
I would have to provide less personal information	19%
Other	0%
Total	158%

Q4c. If no or unsure, why?	Pct%
I am concerned my personal information would be disclosed to online businesses and services	34%
I am concerned that fraudsters would still be able to steal my personal information or identity	35%
I would worry about merchants misuse or abuse the device fingerprint	12%
I would worry about my computer being blacklisted even though I'm not a fraudster	35%
I would rather use passwords to prove my identity	55%
Other	0%
Total	171%

Q5. Would your allow a trusted online merchant to place a cookie or software that is invisible to you onto your computer to automatically authenticate your computer each time you visited the merchant's website?	Pct%
Yes	68%
No	15%
Unsure	17%
Total	100%

Q6. If an online merchant was unable to match your computer's device fingerprint to their security systems, would you expect them to inform you?	Pct%
Yes	61%
No	39%
Total	100%

Q7. If an online merchant was unable to match your computer's device fingerprint to their security system, would you expect them to provide alternative methods to verify you?	Pct%
Yes	83%
No	17%
Total	100%

Q8. How concerned would you be if an online merchant shared your device fingerprint with other online merchants?	Pct%
Very concerned	16%
Concerned	13%
Somewhat concerned	19%
Not concerned	52%
Total	100%

Q9. Should an online merchant disclose its use of device fingerprinting on its website and other notices with consumers?	Pct%
Yes, disclosure is always required	15%
Yes, but only if disclosure does not reduce the merchant's ability to fight cyber crime.	50%
Disclosure is not necessary	24%
Unsure	11%
Total	100%

Q10. What information you willing to share with a trusted online merchant to fingerprint your computer device? Please check all that apply	Pct%
IP address	63%
Type and make of your computer	82%
Serial number of computer	91%
Internet service provider	80%
Types of software applications residing on your device	52%
Type of browser	69%
Browser settings	72%
Email address	41%
Telephone number	13%
Zip code	7%
Name	15%
Home address	14%
Social Security number	3%
Driver's license number	3%
Purchase history	41%
Date of birth	31%
Total	678%

Demographics

What is your present employment status?	Pct%
Full time employee	51%
Part time employee	8%
Business owner	9%
Retired	5%
Student	11%
Active military	6%
Unemployed	10%
Total	100%

Approximately, when did you start using the Internet or start doing email?	Pct%
Within the past 2 year	4%
Between 3 to 5 years	6%
Between 6 to 10 years	33%
More than 10 years	57%
Total	100%

What is your highest level of education attained?	Pct%
High School	31%
Vocational	24%
University or College	38%
Post Graduate	6%
Doctorate	1%
Total	100%

Please check your age range?	Pct%
18 to 25	18%
26 to 35	26%
36 to 45	24%
46 to 55	14%
56 to 65	9%
66 to 75	5%
75+	3%
Total	100%

Do you use social networking sites such as Facebook or MySpace?	Pct%
Yes	40%
No	60%
Total	100%

Are you the head of household?	Pct%
Yes	64%
No	36%
Total	100%

Please check gender:	Pct%
Female	53%
Male	47%
Total	100%

US regions:	Pct%
Northeast	20%
Mid-Atlantic	18%
Midwest	18%
Southeast	14%
Southwest	12%
Pacific	18%
Total	100%