Paul B. Batten. Keeping Up With the Times: A Comparison of Generational Internet Safety Education. A Master's Paper for the M.S. in I.S degree. May, 2009. 32 pages. Advisor: Jose-Marie Griffiths.

Internet safety has been an issue since the Internet's introduction into mainstream society. Although there was little suspected about the dangers posed by the Internet originally, many issues have come to light as the development of this resource advanced. This study describes results of an online survey of public computer users at Eva Perry Library in Apex, NC and Cameron Village Library in Raleigh, NC. The survey was conducted to assess the changes in Internet safety education of the generation that was still enrolled in school during the initial wide-spread acknowledgment of the Internet.

Headings:

Internet Safety

Use Studies/Internet

KEEPING UP WITH THE TIMES: A COMPARISON OF GENERATIONAL
INTERNET SAFETY EDUCATION

by
Paul B. Batten

A Master's paper submitted to the faculty
of the School of Information and Library Science
of the University of North Carolina at Chapel Hill
in partial fulfillment of the requirements
for the degree of Master of Science in
Information Science.

Chapel Hill, North Carolina

May 2009

Approved by

Jose-Marie Griffiths

Table of Contents

Introduction

Over the past two decades, the Internet has become a major component in everyday life. Regardless of how beneficial the technology is, people are finding malevolent ways to use this same luxury against the common user. While most would say that protecting one's identity online is as simple as using common sense, those same people do not realize that common sense is something that is learned through either education or experience. When dealing with Internet safety, five concepts have been identified, by FBI founded organization i-SAFE, as topics discussed in modern curricula: Cyber-community, Cyber-bullying, Cyber-security, Intellectual Property, and Predators (Tanneta, 2006). While most common users know little about these topics, it is imperative that a greater number of common users become educated in the field. The goal of this study is to determine whether there is a discrepancy in knowledge about Internet safety over a broad age population.

Cyber-community is akin to the previously mentioned idea of common sense, where the rules of the real world apply similarly to the rules of the online world. In the real world, one would not give their credit card numbers to someone they just met for the promise of ten thousand dollars, so why do it in the online world? An example of this would be what is known as a "419" scam (Smith), an instance of which is displayed below:

> *"ATTN: Dear Sir/M,*
> *I am Mr. David Mark, an Auditor of a BANK OF THE NORTH INTERNATIONAL, ABUJA (FCT). I have the courage to Crave indulgence for this important business believing that you will never let me*

down either now or in the future. Some years ago, an American Mining consultant/ contractor with the Nigeria National Petroleum Corporation, made a numbered time (fixed)deposit for twelve calendar months, valued $12M.USD (TWELVE MILLION US DOLLARS) in an account. On maturity, the bank sent a routine notification to his forwarding address but got no reply. After a month, The bank sent another reminder and finally his contract employers, the Nigerian National Petroleum Corporation wrote to inform the bank that he died without MAKING A WILL, and all attempts by the American Embassy to trace his next of kin was fruitless. I therefore, made further investigation and discovered that the beneficiary was an immigrant from Jamaica and only recently obtained American citizenship. He did not declare any kin or relations in all his official documents, including his Bank deposit paper work. This money total amount $12M.USD (TWELVE MILLION US DOLLARS) is still sitting in my bank as dormant Account. No one will ever come forward to claim it, and according to Nigerian banking policy, after some years, the money will revert to the ownership of the Nigerian Government if the account owner is certified dead. This is the situation, and my proposal is that I am looking for a foreigner who will stand in as the next of kin to beneficiary, and OPEN a Bank Account abroad to facilitate the transfer of this money. This is simple, all you have to do is to OPEN an account anywhere in the world and send me its detail for me to arrange the proper money transfer paperwork, and facilitate the transfer. The money will then be paid into this Account for us to share in the ratio of 60% for me, 35 % for you and 5% for expenses that might come up during transfer process. There is no risk at all, and all the paper work for this transaction will be done by me using my position and connections in the banks in Nigeria. This business transaction is guaranteed. And the first phase of the transfer will be ($4M.USD) FOUR MILLION DOLLARS as advised by our insider in the bank. If you are interested, please reply immediately through my personal email sending the following details:
(1) Your Full Name/Address
(2) Your Private Telephone/fax Number.
Please observe the utmost confidentiality, and be rest assured that this transaction would be most profitable for both of us because I shall require your assistance to invest some of my share in your country. I look forward to your earliest reply.
Yours,
Mr. David Mark." (Kestenbaum)

While these scams seem obvious to some, they defrauded individuals and businesses of as much as $3 billion dollars in 2005(Smith).

The concept of cyber-bullying is one more commonly seen in younger age groups, but has emerged in older users quite often as well. Cyber-bullying is the simple act of insulting and harassing people over the Internet. Many times, this is done using

fake instant messenger screen names, websites, email addresses, and social networking profiles. In extreme cases, the person being bullied has been pushed far enough to commit suicide (Current Events, 2008).

Cyber-security is seen as protecting the physical integrity of the user's computer from threats such as viruses and malware. By not protecting their computer, the user is keeping it open to attacks that will allow hackers to steal their information, or use their computer to commit acts against others.

The problem of intellectual property appears when someone is stealing works that are not their own, either without paying for them when it is required or re-posting the work as their own. This issue has become much larger in the past decade due to the court cases involving peer-to-peer sharing programs such as Napster, and lawsuits filed by the RIAA against people illegally downloading music.

What is probably considered the most dangerous threat on the Internet is the predator. Once again, this threat is most commonly placed against younger age groups, but even older computer users are not immune to these cyber-stalkers. Predators are those who prey on people typically for the purpose of perverse sexual fantasies, though not always. They often find their victims on online chat sites and attempt to befriend them under false pretenses; then attempt to use the friendship for their own reprehensible desires.

2 Literature

As technology becomes more complex, the means of educating people in order to keep up with the changes must become equally complex. Wolinsky illustrated the gap between the implementation of new technology and new technology education as showing continued growth, but had no research to support this hypothesis (Wolinsky, 2008). That is the purpose of this article: to assess the education of Internet safety in the past, how it has evolved to its present state, and where it may be headed.

While there have been articles in the past that judged the safety skills of younger generations on the Internet, there has been very little effort put into examining the skills of those who grew up with the Internet from its wide-spread introduction in the early nineties. In the beginning, there was little suspicion of how large the Internet would grow, or the dangers it would pose to adults and children alike. As the Internet generation of children developed, they had little chance for formal education of Internet safety, meaning they learned by experience or from other people's mistakes.

A similar article to Wolinsky's was published in April 2004 by Carolyn Walpole, Randy Jacobs, and Erik Jorgensen to assess the difference between parents' assumptions of their child's Internet usage and how their child actually uses the Internet (Walpole, 2004). While the article describes the differences between generations, it focused on how well the "i-SAFE" website educated parents and children about safety on the Internet. It did not necessarily discern how that dissimilarity between the cyber-education of the parents and children was made.

Walpole's study greatly influenced the questions that I decided upon for the survey I used to collect data, but their sample showed a much wider age gap than I am looking for. In the Walpole article, the statistics showed a gap between parents and their children, which would likely be a gap of 18 years or more. This will show an obvious learning gap, due to the larger expanse of time that the parent has had to acquire their safety skills. By selecting groups with a smaller gap in age, I hope to show during what years an individual is most likely to develop Internet safety skills.

In Brendesha Tyne's "Internet Safety Gone Wild" article, she explores the necessity of allowing children to explore social networking sites so that they may interact with their friends. However, many of these children are incapable of accessing these websites, due to parental restrictions. In most of these cases, the media has displayed distorted versions of statistics to the public in order to make news. Parents with little knowledge of Internet safety become paranoid that their children are the direct focus of a phantom imperilment on the Internet, causing the parents to restrict the access that their children have to the Internet (Tyne, 2007). If proper Internet safety techniques are taught to adults, they may pass their knowledge on to their children, allowing them to feel more at ease with fewer Internet restrictions.

The goal of this study is to determine whether there is a discrepancy in knowledge about cyber-security and where that discrepancy is over a broad age population, rather than two widely differing ages. These articles have suggested a distinct need for cyber-education; a clear focus should be made on determining whether specific age groups should be targeted. This will also lead to better means of determining methodologies for educating the population.

3 Methodology

3.1 Approach

In order to determine how aware people are about the risks involved with maintaining security on the Internet, a survey-research format was used. The primary reason for using this method was for ease of data collection. This method allowed for fundamental data to quickly be gathered and then analyzed. The disadvantage to using this method was the lack of ability to ask custom follow up questions. Questions of accuracy can also arise in a survey-research format. While this sort of formatting introduces some disadvantages, it was the best solution in this situation as it provided the most comprehensive amount of information in the shortest amount of time, and yielded the strongest population distribution.

In an attempt to reduce the problems with this method the chosen questions were very direct and specific. For example, "Where did you receive the most Internet safety education? Please select one of the following: School, Home, Personal Experience". In order to survey the widest range of people, subjects of various levels of education, different races, and genders were surveyed. This helped in gaining an overall distribution of various people, when attempting to relate cyber-education to age.

3.2 Recruitment

In order to quickly and efficiently retrieve survey results, subjects were selected from individuals who were in the process of using a computer at the Eva Perry Regional Library in Apex, NC and the Cameron Village Regional Library in Raleigh, NC. Cards

with a few details about the study and the web address for the survey were distributed among the computer users. They were then asked to take a few minutes to fill it out. By selecting people who are already at computers to fill out survey, it was hypothesized that the subjects would be more likely to fill the survey out. If these same cards were to be handed out at random locations with no access to a computer, it was thought that there would be a much higher chance of the cards ending up in the nearest trash receptacle. Unfortunately, this hypothesis proved to be wrong, and surveys arrived as slowly as if they had been handed out on a street corner. Given the time constraints and the speed with which the survey results were being reported, this study ended with a sample size of 200 subjects, split unevenly into the four age groups.

3.3 Survey

While summarizing the survey findings, I feel that the easiest form of analysis is quantitative. By using a survey, I will be more likely to gain relevant numerical data from the respondent than relevant open-ended responses. Some of the questions will be open-ended to allow for non-uniform answers across respondents. These non-uniform responses will be used to back up the numeric data that I will be analyzing.

The survey was divided into six separate sections; one section for each of the five curricula topics, and one for general information. First is the general information section that would be used to weed out people who attempt to take the survey while outside of the specified age range. This section also allows us to determine how this specific user gained Internet safety experience, and what level of user they consider themselves to be.

Cyber-community is the next section to be explored in the survey. In this section, the subject is asked questions about their confidence in their privacy as a part of the

cyber-community. The subject is asked about how they format their passwords and who they allow access to those passwords. As a member of the cyber-community, the subject is bound to any Terms of Service (ToS) that they might agree to. As such, it is pertinent to this survey as to whether the subject actually reads these terms and conditions before agreeing.

The next section of the survey requests details about the security of the subject's computer, and the actions they take to supplement these security measures. Security measures that the subject may have implemented include firewalls and virus protection software. While these measures might help to protect the subject's computer locally, their actions on the Internet may still endanger their data. That is the purpose of survey questions about the subject's knowledge of http vs. https, and their knowledge of procedures to follow relating to email attachments and other downloads.

Cyber-bullying has become the topic of much discussion due to the actions of a teenager and her mother leading to the death of another teen (Current Events, 2008). In this section of the survey, the subject is questioned about their use of social applications on the Internet. Focusing mainly on instant messaging clients, the survey determines if the subject has ever been harassed or heard of anyone being harassed over an instant messaging client. The subject is then asked what the proper course of action to take would be if they were being harassed.

The next section of the survey deals with intellectual property. This section is filled with open-ended questions about the subject's views of copyrighted materials. The subject is also asked for their opinion about downloading music without paying for it and using artwork without the knowledge of the owner.

Questions regarding predator safety make up the last section of the survey. This section, though arguably the most important, is made up of the fewest number of questions. The questions in this section are designed to gather information about how the subject meets people through the Internet, and whether they take precautions to keep themselves safe.

4 Data Analysis

4.1 General Subject Information

Given the purpose of this study, the most obvious question to be asked is where these subjects received the most Internet safety training. Ideally, the subjects would have received the most training at an institution of some sort. This however was not the case. Only 16% of the subjects who took the survey reported learning about Internet safety at school. It seems that the majority of the subjects received their Internet safety education through personal experience, an overwhelming 71%. Below is a breakdown of at what point those that did learn Internet safety in school.

Institution of Internet Safety Education by Age Group

	1972-1976	1977-1981	1982-1986	1987-1991
Elementary School	0	0	1	0
Middle School	0	1	2	5
High School	1	2	5	4
College/University	2	3	6	0
Graduate School	0	0	0	0

This table shows at what institutional level the subjects learned about Internet safety.

From this table, we can see that the number of subjects learning about Internet safety in school increases as the age groups get lower. Not only that, but the subjects seem to be taught at a younger and younger age. The older age groups learned most of their skills in college, while the younger age groups have begun learning in high school, middle school, and even elementary school. While this is a decent start, it is still a problem that most of the subjects learned how to keep themselves safe online outside of the classroom. It could be inferred from this data that the subjects have had to learn from either their own

mistakes, or the mistakes of others. If this should be true, then it is possible that the lack of Internet safety education caused harm to the subject.

4.2 Cyber-Community

In the second section of the survey, we examine the community behaviors of the subjects. As individual members of the cyber-community, we must have a way of differentiating ourselves. The most common way of doing this is through usernames and passwords. However, if someone's passwords were known by another person, they could impersonate the first person easily. When asked who should have access to their passwords, most of the subjects understood that only they should have access to their passwords. One differentiation in the data however, was that the older groups were more likely to include the System Administrator as one who should have access to their passwords. This is a common misconception that seems to be clearing up as time goes on. The system administrator should have the ability to change your password to a random password that they still will not have access to. This helps to minimize the chance for abuse of power.

In order to further keep passwords from being compromised, a measure of care should be taken when choosing a password. What is considered to be a secure password is one that combines upper-case and lower-case letters with numbers and symbols. The majority of the subjects knew this to be the case, with about 65% of the subjects using this format. A meager 5.5% use a simple date or name, and the remaining percentage used a password that was simple for them to remember. From these results, we can determine that the subjects within these age groups understand the necessary safety measures involved in keeping their passwords safe.

Individualism online in recent years has begun to connect more and more with the physical world through social networking sites. These sites take any personal information provided by the user and make it publicly available. Results from the survey show that 88% of each age group would make their real first name available online and between 78.5% of the subjects would make their last name available. Given that first and last names are easily available to anyone in the United States due to the Freedom of Information Act; this is not a wholly surprising discovery. However, an average of 76% of the subjects admitted to posting their email address somewhere online. This practice one of the greatest causes of spam, and gives information to people who would attempt 419 scams.

As in the physical world, contracts exist to protect the providers and users of services on the Internet. These are known as Terms of Service (ToS). When asked if they have ever read the ToS for a web service, 65% of the two older groups admit to not having read the ToS, while only 48% of the younger groups have not. When asked why, the most common responses were that the ToS was too long, they were too lazy, or that they assumed that they wouldn't understand what it said. One user in the 1977-1981 age group suggested a summary of the terms be placed in the agreement.

From the results of this survey, it could be said that most of the subjects did not see themselves as members of a cyber-community. Though a majority of the subjects knew how to protect their individuality through secure passwords, there was less stress place upon keeping their other personal information secure. This along with the lack of seriousness placed in the Terms of Service implies that the subjects still consider themselves to be anonymous individuals when they are on the Internet. However, given

the fact that the ToS is starting to be read by the younger age groups, it seems that the importance of these terms is starting to seem more serious.

4.3 Cyber-Security

The threat of computer viruses is not new to the Internet. With 52.5% of the subjects having been infected by at least one computer virus, it's not new to them either. It is likely that because of this fact that 83.5% of the subjects had some type of virus protection in place, with little significant variation across the age groups. The remaining percentage either didn't know if they had ever received a virus, or were confident that they would not be the victim of a computer virus. The majority of those who felt confident were either Mac users, or claimed not to take part in any risky Internet behavior.

As further protection for computers, some people will use firewalls to give permission for data transmissions to and from their computer. When questioned about their use of a firewall, 74.5% of the responses verified that they did indeed use a firewall. Even some of the negative responses used a firewall, but not on their computer. A number of those who did not use firewall software on their computer used a router that implemented some sort of firewall.

A major problem when dealing with viruses and malicious software is the human component. Email viruses work under the assumption that people will open anything that gets sent to their email box. Based on survey results, the reality of the situation is that people will only open the file if it is from someone they know. The problem with this is that the email address that sent the file could be a fake address (or spoof address), or it could had been sent by a virus that propagated itself through a victims address book to

send emails with the virus to friends of the original victim. The only way to avoid one of these situations is to request information about the file directly from the sender.

When sending and receiving sensitive data over the Internet, it is necessary to ensure that the data is not being captured by an outside entity. In order to prevent this, websites will encrypt their data using a Secure Socket Layer (SSL). Evidence of this protocol being used is visible in the address bar of web browsers when "http" is replaced with "https." With 41.5% of the subjects not understanding what this meant, it is possible that any of these individuals could have had personal information stolen from them, including credit card numbers or social security numbers. When comparing this data against where the subjects learned about Internet safety, it should be noted that a much larger percentage of the subjects who know about https learned about Internet safety outside of school. The number of people lacking knowledge of the difference between http and https is especially unnerving because 82% of the individuals lacking this knowledge perform some kind of sensitive activity online.

Keeping the computer free of viruses and malicious software is the first line of defense when considering cyber-security, but understanding how data transmissions can be secured is another way to keep data protected. We can see from the data collected, that the majority of the subjects kept virus and firewall software on their computers in order to prevent viruses from implanting themselves unnoticed on computers. This seems like a necessity when a great deal of the subjects would also open an email attachment on the basis that they know who sent it. While this keeps the computer relatively safe, the number of people sending sensitive data, without understanding whether it is encrypted or not, is overwhelming. This lack of knowledge could lead to

much larger problems, meaning that the public should be educated about this feature that is available to them.

4.4 Cyber-Bullying

Cyber-bullying is a problem that extends across multiple platforms including instant messenger clients, websites, social networking sites, and chat rooms. At the beginning of this section of the study, the subjects were asked to take harassment to mean being subjected to some form of verbal abuse (racial slurs, threats, cause to feel unsafe). This study focused on bullying through instant messenger clients. 69.5% of the subjects in this study admitted to using some form of instant messaging client. When those who used the clients were asked if they had ever been harassed through those means, 22.3% admitted to being harassed in some way.

Though the majority of instant messenger users have not been harassed over the Internet, they are aware of others being harassed. 72% of the subjects have heard about people being harassed through an instant messenger client, and 86% have heard about harassment over the Internet in general. Because of the danger involved in cyber-bullying, it is important for the victim to understand what course of action to take in such a situation. The subjects chose the logical steps of ignoring the user, as well as contacting the site administrator. The two age groups from 1977-1981 and from 1982-1986 also strongly emphasized writing down all information about the incident. This could be helpful advice if the harassment goes too far. In such cases, contacting the police may become necessary, which 29% or the subjects selected as an option.

Cyber-bullying has become a major nuisance on the Internet, and has even affected some of the test subjects. But judging by their survey answers, the subjects

seemed to understand the proper steps to follow when they are being harassed. Ignoring the user is a good idea, but it may just cause him to focus on another user. Notifying the system administrator is the next step, causing the harassing party to lose privileges associated with their account. Although there is no sure-fire way to avoid being bullied on the Internet, by following these step the possible victim can defend themselves.

4.5 Intellectual Property

Intellectual property has been a hot topic of discussion since Napster came on the scene in 1999, bringing with it massive copyright violations. When asked what copyrights meant to them, subjects came up with a myriad of answers but most had one thing in common: copyrighted work is owned by someone. Other variations on this included issues on distribution, attribution to the creator or owner, and consent. When asked specifically, what works could be copied without repercussions, a surprising number did not choose the "none of the above" option. Members of the age groups between 1972 and 1986 seemed to have less of a problem copying audio and video files than subjects in the 1987-1991 age group. However, many subjects chose to allow the use of images, documents, and ideas taken from the Internet across all age groups.

When discussing music in general, the majority of the subjects seemed to have no problem with downloading music illegally. Some offered legal alternatives, such as subscription services, or services that allow the customer to purchase individual songs cheaper. But even more felt that by downloading the music without paying for it, they were attacking the RIAA and musicians who have more than enough income already. Another group was apathetic to the laws surrounding the music, because they just wanted

something to listen to. Of those that expressed an opinion, 41% of the subjects approved of illegal downloading of music, while 59% disapproved.

Napster caused quite a stir when it first appeared, allowing users to copy whatever songs they wanted from other users. When courts finally became involved, the issue became front page news and alerted many, who knew nothing about intellectual property, to the possibility of legal actions for taking copyrighted materials. Judging by the lower acceptance of using copyrighted audio and video files among the youngest age group in the study, it seems that media attention has brought enough attention to this issue that people are learning about the legal repercussions for their actions. However, there are still a large percentage of the subjects who are willing to use these materials, regardless of the laws surrounding this matter.

4.6 Predators

In the past, chat rooms were the largest hang out for Internet predators. Over the past decade, predators have begun to move towards social networking sites to meet potential victims. When asked if they had a profile on any social networking site, 79.5% of subjects said yes. Of those that have a profile on a social networking site, 37% were connected to an individual that they did not personally know. Connecting to individuals that they do not know, puts the subject at risk of leaking personal information that could include addresses and phone numbers. If this data reaches a predator on the Internet that wishes to harm the subject in any way, it could evolve into a dangerous situation.

Predators become a more immediate threat when they are able to come in contact with their victim in the physical world. A little more than half of the 89% of subjects who use social networking sites at some point or another have met someone that they first

met online. Without further insight into the circumstances behind the subjects meeting people online, this seems to be a dangerous trend that should quickly be remedied.

This study has indicated that there is a lack of emphasis on the dangers posed by predators to those who are not children. The subjects of this study entered into risky behavior by giving their personal information to strangers, not to mention those that would go on to meet those same strangers offline. Due to inconsistent data over the age groups, it is uncertain as to whether or not education plays a role in preventing the subject from putting themselves in harms way.

5 Conclusion and Future Implications

The significance of this study can be measured through its ability to aid in the development of more advanced Internet safety education courses. This study's outline came from the i-SAFE curriculum involving five core topics. In cyber-community, individuals learn that the Internet's social rules are similar to those in the physical world. Cyber-security attempts to protect the identity and assets of the individual. Protecting the mental and emotional state of the individual is covered by cyber-bullying. Intellectual property teaches the individual respect for the property of others. Lastly, the topic of predators is meant to keep the individual physically safe from harm.

Based on the findings of this study, Internet safety education has begun to reach lower age groups. But it seems that this specific curriculum may have been too late to reach the age groups in this study. This study may be used as a bench mark in the future to see how well this curriculum aids in the teaching of Internet safety to future generations.

6 Works Cited

"Cyberbullied." *Current Events* v108 n4. 29 Sep 2008 4-5. Web.3 Dec 2008.

    <http://search.ebscohost.com/login.aspx?direct=true&

    db=aph&AN=35001248&site=ehost-live >.

Kestenbaum, Lawrence. "Fraud Email from July 7, 2006." *Fraud Gallery*. 4 Apr 2009

    <http://fraudgallery.com/2006-07-07.html>.

Smith, Andrew. "Nigerian Scam E-Mails and the Charms of Capital." *Cultural Studies*

    v23 n1. 2009 27-47. Web.4 Apr 2009.

Tannetta, Maureen. "Internet Safety Night Brought to You by the Library Media

    Specialist." *School Library Media Activities Monthly* v23 n2: 31-32. Print.

Tynes, Brendesha M. "Internet Safety Gone Wild? Sacrificing the Educational and

    Psychological Benefits of Online Social Environments." *Journal of Adolescent*

    Research v22 n6. 2007 575-584. Web.1 Dec 2008.

    <http://jar.sagepub.com/cgi/reprint/22/6/575>.

Walpole, Carolyn, Randy Jacobs, Erik Jorgensen. "Internet Generation Gap: An Analysis

    of Student Assessments and Parent Surveys from an Active Learning Internet

    Safety Environment." *iSAFE.org*. Apr 2004. FBI. 1 Dec 2008

    <http://www.isafe.org/imgs/pdf/internet_generation_gapef.pdf>.

Wolinsky, Art. "We Can Get There From Here." *MultiMedia & Internet@School 15*

    2008: 26-30. Print.

Appendix A – Survey Results

		During which of the following year ranges were you born?					
		1972-1976	1977-1981	1982-1986	1987-1991	None of the above	Total
Where did you receive the most Internet safety education?	School	3 7.32%	6 10.71%	14 22.58%	9 21.95%	0 0%	32 16.16%
	Home	1 2.44%	6 10.71%	9 14.52%	8 19.51%	0 0%	24 12.12%
	Personal Experience	37 90.24%	44 78.57%	38 61.29%	23 56.1%	0 0%	142 71.72%
If school, what stage?	Elementary School	0 0%	0 0%	1 1.61%	0 0%	0 0%	1 3.13%
	Middle School	0 0%	1 1.79%	2 3.23%	5 12.2%	0 0%	8 25%
	High School	1 2.44%	2 3.57%	5 8.06%	4 9.76%	0 0%	12 37.5%
	College/University	2 4.88%	3 5.36%	6 9.68%	0 0%	0 0%	11 34.38%
	Graduate/Professional School	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%
How much time do you typically spend on the Internet each week?	0 hours	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%
	1-5 Hours	5 12.2%	6 10.71%	6 9.68%	0 0%	0 0%	17 8.63%
	6-10 Hours	9 21.95%	10 17.86%	9 14.52%	8 19.51%	0 0%	36 18.27%
	11-15 Hours	6 14.63%	7 12.5%	4 6.45%	10 24.39%	0 0%	27 13.71%
	16-20 Hours	7 17.07%	15 26.79%	14 22.58%	7 17.07%	0 0%	43 21.83%
	21+ Hours	13 31.71%	18 32.14%	28 45.16%	15 36.59%	0 0%	74 37.56%
How would you describe your knowledge of the Internet and Internet Technology?	Novice	0 0%	0 0%	0 0%	0 0%	0 0%	0 0%
	Beginner	2 4.88%	3 5.36%	0 0%	0 0%	0 0%	5 2.65%
	Intermediate	17 41.46%	26 46.43%	29 46.77%	17 41.46%	0 0%	89 47.09%
	Advanced	18 43.9%	24 42.86%	17 27.42%	18 43.9%	0 0%	77 40.74%
	Expert	3 7.32%	2 3.57%	11 17.74%	2 4.88%	0 0%	18 9.52%
Total		41 100%	56 100%	62 100%	41 100%	0 100%	100%

		During which of the following year ranges were you born?					
		1972-1976	1977-1981	1982-1986	1987-1991	None of the above	Total
Who should be allowed know or have access to your passwords? (Select all that apply)	You	40 97.56%	55 98.21%	59 95.16%	39 95.12%	0 0%	193 80.08%
	Parents	5 12.2%	2 3.57%	4 6.45%	3 7.32%	0 0%	14 5.81%
	Siblings	1 2.44%	0 0%	2 3.23%	3 7.32%	0 0%	6 2.49%
	Teachers	1 2.44%	0 0%	0 0%	1 2.44%	0 0%	2 0.83%
	System Administrators	5 12.2%	14 25%	4 6.45%	1 2.44%	0 0%	24 9.96%
	Friends	0 0%	1 1.79%	0 0%	1 2.44%	0 0%	2 0.83%
How secure are your passwords? Do you use:	Usually, a date of birth or a name	5 12.2%	3 5.36%	2 3.23%	1 2.44%	0 0%	11 5.7%
	A simple password, so you do not forget it	7 17.07%	18 32.14%	11 17.74%	16 39.02%	0 0%	52 26.94%
	Numbers, uppercase and lowercase letters	28 68.29%	34 60.71%	46 74.19%	22 53.66%	0 0%	130 67.36%
Do you ever read the Terms of Service (TOS) or End-User License Agreement (EULA) for a program of we...	Yes	13 31.71%	20 35.71%	29 46.77%	20 48.78%	0 0%	82 42.27%
	No	27 65.85%	36 64.29%	30 48.39%	19 46.34%	0 0%	112 57.73%
Do you use your computer for sensitive transactions, such as online banking?	Yes	36 87.8%	51 91.07%	53 85.48%	24 58.54%	0 0%	164 85.42%
	No	3 7.32%	5 8.93%	6 9.68%	14 34.15%	0 0%	28 14.58%
What personal information have you made publicly available on the Internet? (Select all that apply)	Nothing	1 2.44%	4 7.14%	2 3.23%	0 0%	0 0%	7 0.68%
	First Name	36 87.8%	49 87.5%	54 87.1%	37 90.24%	0 0%	176 17.04%
	Last Name	33 80.49%	44 78.57%	50 80.65%	30 73.17%	0 0%	157 15.2%
	Address	15 36.59%	16 28.57%	8 12.9%	3 7.32%	0 0%	42 4.07%
	E-mail Address	33 80.49%	41 73.21%	43 69.35%	35 85.37%	0 0%	152 14.71%
	Home Phone	6 14.63%	11 19.64%	5 8.06%	2 4.88%	0 0%	24 2.32%
	Cell Phone	15 36.59%	14 25%	12 19.35%	12 29.27%	0 0%	53 5.13%
	School	16 39.02%	30 53.57%	34 54.84%	28 68.29%	0 0%	108 10.45%
	Instant Messenger ID	7 17.07%	18 32.14%	19 30.65%	24 58.54%	0 0%	68 6.58%
	Birthdate	13 31.71%	34 60.71%	33 53.23%	32 78.05%	0 0%	112 10.84%
	Photo	21 51.22%	43 76.79%	43 69.35%	27 65.85%	0 0%	134 12.97%
Total		41 100%	56 100%	62 100%	41 100%	0 100%	100%

		During which of the following year ranges were you born?					
		1972-1976	1977-1981	1982-1986	1987-1991	None of the above	Total
Do you use virus protection software on your home computer?	Yes	32 78.05%	52 92.86%	49 79.03%	34 82.93%	0 0%	167 86.98%
	No	5 12.2%	4 7.14%	9 14.52%	4 9.76%	0 0%	22 11.46%
	Don't know	2 4.88%	0 0%	0 0%	1 2.44%	0 0%	3 1.56%
Do you use firewall software on your home computer?	Yes	26 63.41%	43 76.79%	44 70.97%	36 87.8%	0 0%	149 77.6%
	No	9 21.95%	12 21.43%	11 17.74%	2 4.88%	0 0%	34 17.71%
	Don't know	4 9.76%	1 1.79%	3 4.84%	1 2.44%	0 0%	9 4.69%
Has your computer ever been infected with a virus?	Yes	22 53.66%	27 48.21%	34 54.84%	22 53.66%	0 0%	105 54.4%
	No	16 39.02%	24 42.86%	23 37.1%	13 31.71%	0 0%	76 39.38%
	Don't know	1 2.44%	5 8.93%	2 3.23%	4 9.76%	0 0%	12 6.22%
Have you ever purchased something through the Internet using a credit card?	Yes	39 95.12%	55 98.21%	57 91.94%	35 85.37%	0 0%	186 96.37%
	No	0 0%	1 1.79%	2 3.23%	4 9.76%	0 0%	7 3.63%
If yes, did you feel safe doing so?	Yes	38 92.68%	53 94.64%	57 91.94%	35 85.37%	0 0%	183 98.39%
	No	1 2.44%	2 3.57%	0 0%	0 0%	0 0%	3 1.61%
Do you understand the difference between "http://" and "https://"?	Yes	21 51.22%	32 57.14%	34 54.84%	23 56.1%	0 0%	110 56.99%
	No	18 43.9%	24 42.86%	25 40.32%	16 39.02%	0 0%	83 43.01%
You receive an email with a file attachment. What do you do?	Open it to see what it is about	2 4.88%	2 3.57%	1 1.61%	1 2.44%	0 0%	6 3.14%
	Ask the sender about the file	3 7.32%	2 3.57%	6 9.68%	2 4.88%	0 0%	13 6.81%
	Delete the e-mail	0 0%	1 1.79%	2 3.23%	2 4.88%	0 0%	5 2.62%
	Only open attachment if I know the person who sent it	34 82.93%	49 87.5%	50 80.65%	34 82.93%	0 0%	167 87.43%
Total		41 100%	56 100%	62 100%	41 100%	0 100%	100%

		During which of the following year ranges were you born?					
		1972-1976	1977-1981	1982-1986	1987-1991	None of the above	Total
Do you use an Instant Messaging client (AOL Instant Messenger, ICQ, GChat, IRC, etc.)?	Yes	21 51.22%	38 67.86%	49 79.03%	31 75.61%	0 0%	139 72.4%
	No	18 43.9%	18 32.14%	10 16.13%	7 17.07%	0 0%	53 27.6%
If yes, have you ever been harassed by this means?	Yes	3 7.32%	7 12.5%	10 16.13%	11 26.83%	0 0%	31 22.3%
	No	18 43.9%	31 55.36%	39 62.9%	20 48.78%	0 0%	108 77.7%
Have you ever heard of someone being harassed through an Instant Messaging client?	Yes	24 58.54%	38 67.86%	51 82.26%	31 75.61%	0 0%	144 74.61%
	No	15 36.59%	18 32.14%	8 12.9%	8 19.51%	0 0%	49 25.39%
Have you ever heard of someone being harassed over the Internet?	Yes	30 73.17%	50 89.29%	54 87.1%	38 92.68%	0 0%	172 89.12%
	No	9 21.95%	6 10.71%	5 8.06%	1 2.44%	0 0%	21 10.88%
Which of the following should you do if you are harassed through an Instant Messenger? (Select all t...	Contact the police	12 29.27%	21 37.5%	16 25.81%	9 21.95%	0 0%	58 13%
	Ignore the user	26 63.41%	34 60.71%	43 69.35%	32 78.05%	0 0%	135 30.27%
	Trace the user's IP address and contact them in person	0 0%	3 5.36%	2 3.23%	2 4.88%	0 0%	7 1.57%
	Contact the site/program administrator	24 58.54%	38 67.86%	41 66.13%	25 60.98%	0 0%	128 28.7%
	Harass the person harassing you	1 2.44%	2 3.57%	3 4.84%	3 7.32%	0 0%	9 2.02%
	Write down information about the harassment	20 48.78%	32 57.14%	36 58.06%	21 51.22%	0 0%	109 24.44%
Have you ever observed materials online that would suggest or threaten violence?	Yes	14 34.15%	22 39.29%	30 48.39%	24 58.54%	0 0%	90 46.63%
	No	25 60.98%	34 60.71%	29 46.77%	15 36.59%	0 0%	103 53.37%
Total		41 100%	56 100%	62 100%	41 100%	0 100%	100%

		During which of the following year ranges were you born?					
		1972-1976	1977-1981	1982-1986	1987-1991	None of the above	Total
Which of the following can be copied without legal repercussions? (Select All That Apply)	Images	8 19.51%	12 21.43%	9 14.52%	5 12.2%	0 0%	34 12.06%
	Audio Files	6 14.63%	7 12.5%	6 9.68%	2 4.88%	0 0%	21 7.45%
	Video Files	6 14.63%	7 12.5%	6 9.68%	2 4.88%	0 0%	21 7.45%
	Documents	7 17.07%	14 25%	8 12.9%	4 9.76%	0 0%	33 11.7%
	Ideas	10 24.39%	11 19.64%	9 14.52%	7 17.07%	0 0%	37 13.12%
	None of the above	27 65.85%	37 66.07%	46 74.19%	26 63.41%	0 0%	136 48.23%
	Total	41 100%	56 100%	62 100%	41 100%	0 100%	100%

		During which of the following year ranges were you born?					
		1972-1976	1977-1981	1982-1986	1987-1991	None of the Above	Total
Have you ever met someone in real life that you met through a website?	Yes	17 41.46%	26 46.43%	33 53.23%	15 36.59%	0 0%	91 48.4%
	No	21 51.22%	29 51.79%	25 40.32%	22 53.66%	0 0%	97 51.6%
Do you have a profile on a social networking site (MySpace, Facebook, etc.)?	Yes	28 68.29%	45 80.36%	52 83.87%	34 82.93%	0 0%	159 84.57%
	No	10 24.39%	10 17.86%	6 9.68%	3 7.32%	0 0%	29 15.43%
If yes, are you connected to people you do not personally know though the site?	Yes	14 34.15%	15 26.79%	21 33.87%	24 58.54%	0 0%	74 46.84%
	No	14 34.15%	30 53.57%	30 48.39%	10 24.39%	0 0%	84 53.16%
If you have joined a social networking site, did you customize the privacy settings?	Yes	25 60.98%	44 78.57%	50 80.65%	29 70.73%	0 0%	148 83.62%
	No	9 21.95%	8 14.29%	5 8.06%	7 17.07%	0 0%	29 16.38%
	Total	41 100%	56 100%	62 100%	41 100%	0 100%	100%

Appendix B

IRB Study #__09-0424_

Consent Form Version Date: _2/16/2009_

Study title: Keeping Up With the Times: A Comparison of Generational Internet Safety Education

Primary Investigator: Paul Batten (pbatten@email.unc.edu, (336) 416-1399

Research Advisor: Jose-Marie Griffiths (jmgriff@unc.edu, (919) 962-8363

UNC School of Information and Library Science

I am writing to request your participation in a research study, the purpose of which is to learn about the evolution of Internet safety education over the past two decades. This study is focused on people born between 1972 and 1991 who have received some form of education about safety on the Internet. The results of this study will form the basis of my master's paper.

Full details of the study can be found below together with answers to specific questions you might have, and your consent to participate. **At the bottom of this email is a link to the survey**. I appreciate your participation in this.

Thank you in advance for your time!

_____

_____

What are some general things you should know about research studies?

You are being asked to take part in a research study. To join the study is voluntary. You may refuse to join, or you may withdraw your consent to be in the study at any time, for any reason, without penalty.

 Research studies are designed to obtain new knowledge. This new information may help people in the future.   You may not receive any direct benefit from being in the research study. There also may be risks to being in research studies.

 Details about this study are discussed below. It is important that you understand this information so that you can make an informed choice about being in this research study. You should ask the researcher named above, or staff members who may assist them, any questions you have about this study at any time.

What is the purpose of this study?

The purpose of this research study is to learn about the evolution of Internet safety education since the Internet's wide spread introduction in the early 1990's.

Are there any reasons you should not be in this study?

You should not participate in this study if you are not between the ages of 18 and 37.

How many people will take part in this study?

If you decide to participate, you will be one of 200 people requested to participate in this research study.

How long will your part in this study last?

The survey will take approximately 10 minutes to complete.

What will happen if you take part in the study?

You are asked to fill out an online survey gathering basic demographic information and information regarding your opinions and experiences as they relate to the study. All questions are voluntary and you do not have to answer any questions if you so choose.

What are the possible benefits from being in this study?

Research is designed to benefit society by gaining new knowledge. While you may not benefit personally from being in this research study your participation is important to help us understand how education has evolved to combat new threats posed by our increasingly technology based society..

What are the possible risks or discomforts involved from being in this study?

There are no known risks or cause for discomfort in taking part in this study.

How will your privacy be protected?

Your name or other identifying information is not required for participation in this study. All IP (Internet Protocol) addresses will be removed from the data prior to its analysis. Participants *will not* be identified in any report or publication about this study. Although every effort will be made to keep research records private, there may be times when federal or state law requires the disclosure of such records, including personal information. This is very unlikely, but if disclosure is ever required, UNC-Chapel Hill will take steps allowable by law to protect the privacy of personal information. In some cases, your information in this research study could be reviewed by representatives of the

University, research sponsors, or government agencies for purposes such as quality control or safety.

The survey will be administered using the Qualtrics software system, which maintains data behind a firewall. All data are accessed only by the owner of the survey, who must provide password and user id. All pieces of data are keyed to that owner identification and cannot be accessed by anyone other than the owner or, by the owner's request, technical assistance staff. Technical assistance staff include server administrators at Qualtrics who will respond to hardware or software failures, or Teresa Edwards, the UNC administrator for the Qualtrics Software Agreement. Ms. Edwards has completed Human Subjects Research certification at UNC-CH, and will only access survey data at the account owner's request.

Will you receive anything for being in this study?

You will not receive anything for taking part in this study.

Will it cost you anything to be in this study?

There will be no costs for being in the study

What if you are a UNC student?

You may choose not to be in the study or to stop being in the study before it is over at any time. This will not affect your class standing or grades at UNC-Chapel Hill. You will not be offered or receive any special consideration if you take part in this research.

What if you have questions about this study?

You have the right to ask, and have answered, any questions you may have about this research. If you have questions, or concerns, you should contact the primary researcher listed above.

What if you have questions about your rights as a research participant?

All research on human volunteers is reviewed by a committee that works to protect your rights and welfare. If you have questions or concerns about your rights as a research subject you may contact, anonymously if you wish, the Institutional Review Board at 919-966-3113 or by email to IRB_subjects@unc.edu.

Thank you for helping me with this study.

<u>Participant's Agreement:</u>

I have read the information provided above. I have asked all the questions I have at this time. By continuing with the following web survey, I voluntarily agree to participate in this research study.

[Click here to signify your consent to participate and take the survey](#)