Multiple sources for security: The influence of source networks on coping self-efficacy and protection behavior habits in online safety

Ruth Shillair
Michigan State University
Shillai7@msu.edu

Jingbo Meng
Michigan State University
jingbome@msu.edu

Abstract

Internet users face threats of increasing complexity and severity. To protect themselves they rely on sources for online safety information. These sources may either build up, or undermine, the coping self-efficacy and motivation needed to protect oneself. A survey of 800 subjects asked about which sources they relied on for information about online safety: media, work, school, friends and family, and specialized web sites. Individuals who said they had no comprehensive source for information reported the lowest levels of both coping self-efficacy ($b= -0.609$, $p< 0.001$) and protection habit strength ($b= -0.900$, $p< 0.001$). On the other hand, those who had an affiliation of school, work and specialized web sites had a positive relationship with both coping self-efficacy ($b= 0.517$, $p< 0.05$) and protection habit strength ($b= 0.692$, $p< 0.05$). Results suggest that some information affiliation networks are correlated with higher coping self-efficacy and stronger protection habits.

1. Introduction

Computer safety threats and online dangers are in the news on almost a daily basis. Since information and communication technologies (ICTs) are the backbone of industry, commerce, and interpersonal communications, these issues cannot be ignored. Our mobile devices and computers often hold extensive personal information and are used for banking transactions, shopping, work and recreation. Devices that are infected with viruses or malware can work as keys to unlock information that can lead to compromising larger systems. What was once limited to computer has now expanded into devices all around us [1]. The complexity of this growing infrastructure and the constantly increasing risk surfaces frequently leave all but the most highly trained professionals at a loss.

Exacerbating this problem is that even the basics of online safety are widely misunderstood and poorly applied [2][3]. Individuals who want to learn how to protect themselves face an array of sources [4]. Media, government, businesses, educational institutions, and non-profit organizations offer everything from breaking news to advanced technical training. Friends and family who may know more about technology offer advice or stories about experiences with security violations [5]. Even though all these groups have the same general goal of helping individuals improve their online safety habits, little is known how different sources affect security beliefs and behaviors. This research aims to (1) examine which sources of online safety information people rely on, and (2) better understand how various combinations of sources are correlated with individuals coping self-efficacy and their protection behavior habits.

1.2. Protection Motivation Theory

Online safety refers to a set of behaviors to protect private personal information and computing devices[6], [7]. These can include a wide range of behaviors, for this research we include: being careful about information shared on social media; having strong and unique passwords; keeping software and operating systems patched, not responding to phishing emails, not entering financial or personal information to sites that are not encrypted (https). Some technology users are very careful and intentional about their use while others are very apathetic about security precautions. Researchers have sought to understand why some users undertake certain online safety behaviors [8], what messages can motivate them to better safety practices [7] [8], and how mental

URI: http://hdl.handle.net/10125/41766
ISBN: 978-0-9981331-0-2

models influence security behaviors [11]. Protection motivation theory (PMT) is often used to understand the coping and threat appraisal process individuals go through when facing a potential security threat [2][10][11]. According to PMT, a trigger, such as news of a major database hack, causes individuals to mentally do a threat appraisal (i.e., threat susceptibility and threat severity) and a coping appraisal (i.e., coping self-efficacy, response efficacy, and response cost) and then decide what they will do in response to the threat [12][13]. The stronger coping appraisal process will produce adaptive, or protective behaviors, while a stronger threat appraisal process tends to produce maladaptive behavior [2][14]. Recent research has also included the importance of protective habit strength as predicting adaptive behavior [7][10]. Previous research looked at the nature of the sources of information for the trigger mechanism in health communication [17]. Environmental triggers, such as those that came through communication, learning or observation made a difference on the response as well as intrapersonal factors such as prior experience and personality variables [17]. In the online safety realm it is not known how the nature of information sources may affect the coping and threat appraisal process. Better understanding of this process may give insight into why user behaviors are often frequently poor despite years of mass media reports that illustrate the effects of poor online safety behavior [2][16].

This study will look at five categorical sources of online safety information: media, school, work, specialized web sources, and friends and family. By treating each individual source as an affiliation node. This method sees multiple affiliations networks of information flows to individuals, as suggested by Borgatti and Halgin (2011). This research is unique in that it examines the most used combinations of sources and their relationships to higher self-efficacy in coping and higher protective habit strength.

1.3. Strength and weakness of individual sources

Different sources have varying agendas and therefore they may not all be equally effective in helping promote the online safety practices of individuals. It is understandable that a source providing information will construct their message to accomplish their specific goals or reflect their beliefs. This may lead to gaps of information or a cognitive bias. However, rather than just having one individual source of information, people may rely on multiple sources. These sources may complement each other by filling in details that the other missed. Or, they could provide conflicting messages leaving the individual overwhelmed, and ultimately making no changes in their personal protection.

Media outlets are able to widely broadcast information about breaking threats, but analysis of media reports shows that most of the stories cover larger, more sensational issues such as major data breaches and criminal hacking [20]. This provides important awareness of the dangers in cyber space, but this could lead to a negative user response, in that massive hacks may lead to a sense of helplessness and lowered personal diligence [9]. Since media outlets rely on keeping the attention of a wide audience, more mundane, detailed, or repetitive reports (e.g., how to make a strong password) are not appealing to station managers.

The workplace has motivation to instruct their employees on the best safety practices. Poor safety choices by employees can endanger a company's databases, proprietary information, customer trust, and ultimately the bottom line. Many researchers have looked at ways to improve employee cyber safety practices. Ifinedo (2012) found that self-efficacy, response efficacy and a sense of social norms were some of the important elements for following cyber safety policies. Explicit policies were found to be helpful [21] while punishments for violating safety policies were not [22]. Message strategies that encouraged high levels of coping self-efficacy, protective habits, beliefs in response efficacy and lower response cost were effective in encouraging employees to following safer behaviors [2]. Knowledge of what to do, belief that the response is effective, and if employees had a habit of usually following company policies could predict future employee compliance with online safety practices [23], [24]. Despite the deeper training and insight offered in the workplace, these opportunities are often limited to individuals who already have high levels of technical efficacy. Entrepreneurs and individuals who don't work in positions that offer online safety training do not have the opportunity to learn from this type of information.

Schools theoretically offer an optimal position to educate young people about how to protect themselves online. Professional educators

could incorporate online safety practices with other basic health and safety information. Schools could also see a range of benefits if online safety were widely taught, a study of 25,000 European children and teens showed a strong correlation with improved online safety skills and other informational processing skills [25]. However, it is challenging to build consensus on what aspects should be taught and how this information is age appropriate [26], [27]. Also, the need to train teacher themselves about these issues is a major concern given tight budgets and multiple agendas [28], [29]. Despite the potential benefits of promoting online safety, many educators express the belief that primary responsibility should be that of parents or family members [30].

Some individuals may be fortunate enough to have a close friend or family member who works in the IT field or is knowledgeable about online safety to help them. However, given the worldwide shortage in cyber security and IT professionals, it is likely that personal connections are not an expert [31]. However, they may easily know enough to give sufficient advice about how users should protect themselves. The advantages of a personal expert as a resource include immediacy and the lower levels of personal effort needed to get help. Rather than trying to keep up with the latest threats, an individual can simply ask the friend or family member for advice. However, this makes security issues seem like something for the realm of "experts" and doesn't scaffold the steps of learning so that the individual knows what to independently [32].

Since specialized web sites are always available and can be dynamically updated to reflect the latest threats and findings, they are a comprehensive source of online safety. However, individuals may not be aware of these resources, or know where to look for information about an emergent threat, leaving many individuals to rely on hearsay [5]. Using search engines to find help is often challenging. It is difficult for the novice user to differentiate between legitimate services and scams. There are many web sites that appear to be technical support, when in fact they may be a source for scams and malware. A search for "top online safety web sites" in the fall of 2015 found that the top ten results were two spam sites, a self-promotion speaker site, four sites geared for protecting children from bullying and only three that actually dealt with actionable information about online safety. There are reliable sites sponsored by industry and governmental alliances, such as OnGuardOnline.gov or StaySafeOnline.org that provide comprehensive and detailed information for the home computer user. However, these are not widely known, only reaching a small fraction of the online population.

Since each source has specific strengths as well as weaknesses, combined sources may be able to overcome the inherent weakness in a single source. There are a myriad of possible two, three, four, or even five alliance sources that individuals may rely on for online safety information. This research sees these sources as more than distinct bodies, not acting statically but have a role in intensifying beliefs through an incubator effect [33]. This ideological incubator effect may be similar to social networks, where affiliations can often predict similarity in attitudes or behaviors [34]. Ideas and information shared within or between nodes are perceived as more salient as they are reinforced by supportive and iterative environments [35].

Therefore, we hypothesize that –

H1: Individuals who view more than one information outlet as a major source of information will have higher levels of both a) coping self-efficacy and b) protection habit strength than those who have only one or none.

As mentioned before, since specialized web sites are able to give more detailed information about online threats and what users should do to protect themselves. Also, media is able to quickly alert people to emerging threats; therefore, we hypothesize that-

H2: Individuals who relied on the combination of media and specialized web sources will have higher levels of a) coping self-efficacy and b) protection habit strength than those with other alliance combinations examined.

Since people may have family members that are professionals in IT or be highly trained in online safety, these sources of information may be valuable. The workplace may also offer individuals well trained in online safety to act as expert resources for individuals. However, family and friends may be giving advice that is not as timely or accurate as specialized web sources and media reports. Therefore, we hypothesize that

H3: Individuals who rely on the combination of family and friends and the workplace will have higher levels of a) coping self-efficacy and b) protection habit strength than those who have no specific source for information, but lower

than those who have an alliance that includes media and specialized web sources.

Many individuals may not be aware of resources for information about online safety, or they may have constructed their own mental models for online safety and not pursued keeping updated on emerging threats or how to protect themselves. These are individuals that would indicate they have no alliance network as an information source. Therefore, we hypothesize that:

H4: Individuals who do not have a single comprehensive source of information nor a combination of sources they rely on will have lower levels of a) coping self-efficacy and b) protection habit strength than individuals who have an alliance network.

2. Methods

To minimize the potential confound of infrequent computer use on coping self-efficacy we wanted to sample Internet users that were active online. This could be demonstrated if individuals were using the Internet not just for entertainment, but also for sensitive transactions such as banking or work. Therefore, we sought out Amazon M-Turk workers. They enroll with Amazon to do small tasks that computers are not good at doing, such as tasks that are helping train algorithms for machine learning, these tasks are usually small in nature and can be done during workers' free time [36]. We surveyed a sample of 800 individuals; we pre-screened them to assure they all had unique U.S. IP addresses and they had each satisfactorily completed more than 100 previous tasks. The survey instrument included questions about experiences with online safety breaches, their perceptions about the efficacy of responses to online safety threat and their sources of information. Attention and quality checks were included in the survey instrument. Only completed surveys that passed quality controls were used in the research. These controls included taking too little time to complete the survey, having the same answer across multiple questions, not completing the entire survey, or not answering the attention check questions correctly. There were 20 surveys that did not pass the quality checks and were deleted from the results, leaving a final total of 780 participants.

2.1. Measures

To assess sources for online safety, participants were asked using a seven point Likert type scale if they strongly disagreed (1) to strongly agreed (7) with the following statements: I've learned comprehensive information about computer safety from media reports; I have received comprehensive computer safety training at work; I have received comprehensive computer safety training at school; I have friends or family members to help me with online safety issues; I go to specialized sources (e.g., online safety web sites) to learn more about online safety issues.

To measure coping self-efficacy (CSE) questions were used from previous PMT study in online safety practices [2]. Answers were on a 7-point Likert type scale if participants strongly disagreed (1) to strongly agreed (7) with the following statements: I feel comfortable taking measures to secure my primary home computer; taking necessary security measures is entirely under my control; I have the resources and the knowledge to take necessary security measures; Taking necessary security measures is easy. To measure protection habit strength (PHS), we asked the participants to respond on a 7-point Likert type scale if they strongly disagreed (1) to strongly agree (7) with the following statement: the use of security protections has become a habit for me, using security protection has become natural to me, online security is something I do automatically, online protection is something I do without thinking, and online safety protection is a part of my regular routine.

3. Results

3.1. Descriptive Statistics/ Results

A little over half (51.2%) were female and 78.3% were white, 9.6% were Asian and 7.6% were African American. Most participants grew up with computers as 84.1% born between 1970-1996. The ages ranged from 19-74 with the mean age being 35. Our sample was well educated with 85.1% having at least some college. The mean education level was 15 years of formal education beyond kindergarten. For employment: 51.7% were employed full time, 19.6% employed part time, 9.6% were homemakers (not employed outside the home), 7.1% were students (not working for wages), 8.6% were unemployed, 1.8% were disabled (not working outside the home), 1.8% were retired and 3.0% are unknown. The zero order correlations of the constructs used in this study:

coping self-efficacy and protection habit strength, as well as sources for information are presented in Table 1. We used Cronbach's alpha to test for internal validity. Values of greater than .70 are usually considered acceptable [35][36]. Coping self-efficacy in online security was α= 0.879 and protection habit strength was α= 0.846, passing the standard for internal consistency.

Table 1: Pearson's Correlations

		1	2	3	4	5	6	7
1	Media	1						
2	Work	0.34**	1					
3	School	0.29**	0.54**	1				
4	Family & Friends	0.11**	0.08*	0.09*	1			
5	Web	0.27**	0.29**	0.22**	0.07*	1		
6	Protection Habit Strength	0.21**	0.20**	0.21**	-0.07*	0.25**	1	
7	Coping Self-Efficacy	0.13**	0.15**	0.15**	-0.14**	0.21**	0.67**	1
	Means	3.84	3.08	2.99	3.42	4.03	5.35	5.70
	(SD)	(1.62)	(1.93)	(1.85)	(1.96)	(1.83)	(1.26)	(1.27)

*Correlation is significant at the 0.01 level (2-tailed).
**Correlation is significant at the 0.05 level (2-tailed).

3.2. Hypothesis measures

Two multiple regression models were run with the five information sources as independent variables and CSE and PHS as dependent variables respectively. The factors of gender, age, educational level, and work (e.g., part time or full time) were controlled for in the regression. As shown in Table 2 friends & family were significant but had a negative related to coping self-efficacy and protection behavior habits. Web sites as a source of information had a positive relationship with both constructs. Those who somewhat agreed, agreed or strongly agreed with the statements about a source were coded into "1" others were coded "0." Thus, a two-mode network was created with individual participants and the five information sources as nodes, and use of sources as edges. NodeXL was used to visualize the source affiliation network, as presented in Figure 1.

To test H1-4, a network analysis was first used to construct affiliations to information sources for individual participants. The sources were dummy coded to indicate the presence of a tie between a participant and an information source. Individuals who strongly agreed (7), agreed (6), and somewhat agreed (5) with the statements about a source were coded into "1," those who neither agreed nor disagreed,

Next, we did correspondence analysis to produce a matrix that put those who had similar sources in alignment with each other [19] . These alliances were sorted using Excel and coded. The correspondence analysis produced a number of groupings for sources. These were further analyzed using Excel so that individuals were counted for their particular alliance network only once.

Table 2: Information Sources Regression

Predicting coping self-efficacy (R^2= .108)	
	Beta
Media	0.101
Work	0.179*
School	0.231*
Friends & Family	-0.328**
Web Sites	0.195*
Predicting protection behavior habits (R^2= .135)	
Media	0.258**
Work	0.269**
School	0.354**
Friends & Family	-0.333**
Web Sites	0.377**

*Coefficient is significant at the 0.05 level
**Coefficient is significant at the 0.01 level (2-tailed).

There were more than 20 different combinations reported, some with only a handful of individuals reporting a particular alliance combination.

The top 16 alliances were analyzed using regression analysis again, only now each

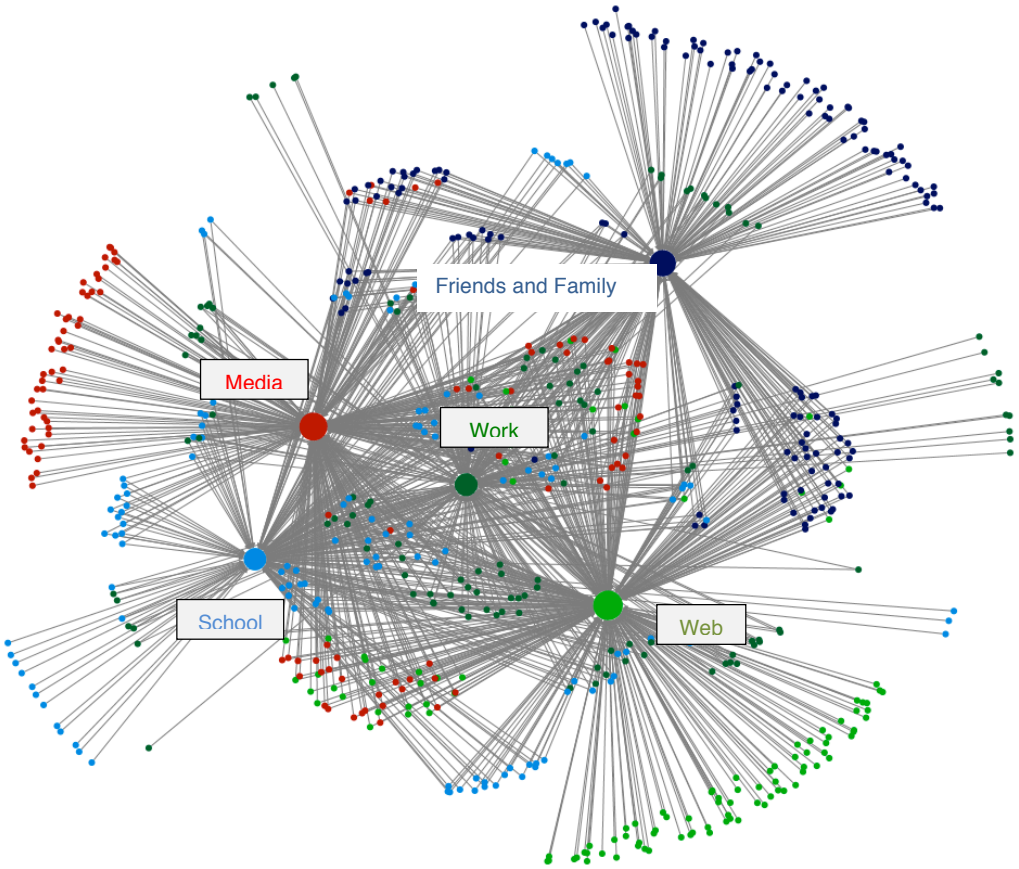

Figure 1: Network Visualization
*light blue= school; red=media; light green=web; dark blue= friends &family; dark green=work
Points are individuals, lines show the connections between sources

grouping had only the individuals who had reported the same alliances of information sources. The data was controlled for age, education, employment and gender. The results of all analyses for both coping self-efficacy and protection habit strength are in Table 3.

Table 3: Regressions of Source Networks

		CSE	PHS
	N	Beta	Beta
No Sources	121	-0.615**	-0.972**
Family Only	69	-0.045	0.077
Web Only	75	0.268	0.494**
Media/ Web	50	0.378*	0.607**
Media Only	47	-0.489**	-0.692**
Family/ Web	46	0.279	0.127
School/ Web/ Work	16	-0.291	-0.196
All Sources	33	0.616*	0.683*
School/ Media/ Web/ Work	28	0.583**	0.726**
School/ Web	16	0.550*	0.811**
Work Only	16	0.249	0.469
School Only	15	0.246	0.014
Family/ Media	12	-0.111	0.081
Family/ Work	12	-0.225	0.152
Web/ Work	11	0.316	0.197
Media/ Work	9	-0.157	0.148

*p<.05, **p<.001

There were 222 people who reported as only having one source and an additional 121 who reported having no comprehensive source for information about online safety for a total of 343 without multiple sources. Those who had no source had the lowest levels of both CSE (β= -0.615, p< .001) and PHS (β= -0.972, p< .001).

Those who relied on web only had CSE (β =0.268, n.s.) and PHB (β =0.494, p<.001). Those who relied on media only also had lower CSE (β =-0.498, p<.001) and PHS (β =-0.692, p<.001). However, those who had web as their source did have significantly higher PHS (β= 0.494, p<.001). Those who used all sources had CHB (β=0.616, p<.05) and PHS (β=683, p<.05). Those who had school and web had CSE (β =0.550, p<.05) and PHS or school, media, web, and work all had higher CSE (β=0.583, p<.001) and PHS (β= 0.726, p<.001). These results partially support Hypothesis 1.

In looking at those who had a network of: family and web; school, web and work; family and media; family and work; web and work and even media and work all showed no significant differences in either coping self-efficacy or protection habit strength. Only those who relied on the combination of media and specialized web sites and the network of school, media, web and work had a significantly positive impact on both coping self-efficacy and protection habit strength.

To test if the means of the alliance of media and web, and school, media, websites, and work were significantly different than the other alliances a linear regression to test the highest, lowest and a mean of the sources that were significant using a bias corrected bootstrap with a 1000 re-samples of the standardized beta of the coefficient using a confidence level of 95%. If the confidence intervals do not overall by less than half, then the p is still statistically significant [39]. Several of the networks were tested. The influence of no sources was significant for CSE, but not PHS; the bootstrapping process showed a CI that no longer was significant. The network of school, media, work and websites was significant for CSE but not PHS. The comparison of the confidence intervals for CSE and PHS are in Table 4. Figure 2 helps illustrate how the confidence intervals do not overlap by more than 50 percent. Only the groups of sources that were significantly influencing the CSE and PHS were analyzed using this method. Media was a significant factor in CSE in combination with web sources but not PHS. Therefore, Hypothesis 2 was partially supported.

Table 4: Comparison of Confidence Intervals

Coping Self-Efficacy			
Source	CI Low	Beta	CI High
No Sources	-0.778	-0.545	-0.307
Family/ Media	-0.936	-0.184	0.470
School/ Media/ Web/ Work	0.141	0.500	0.819
Protection Habit Strength			
No Sources	-0.512	-0.193	0.127
Family/ Media	-0.822	0.144	1.111
School/ Media/ Web/ Work	-0.383	0.232	0.846

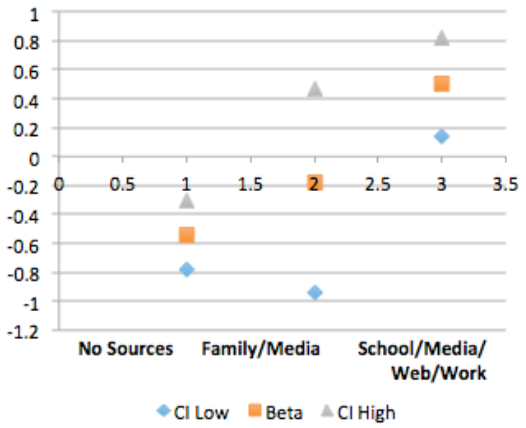

Figure 2: CI of Source Influence on Coping Self-Efficacy

As mentioned before, those who relied on family and friends for information had a statistically significant negative effect to both CSE and PHS. Compared to other information sources this was lower and stronger in influence. Therefore, Hypothesis 3 was not supported.

The individuals who had no comprehensive source for information about online safety had the lowest CSE and PHS. The confidence intervals and beta means are in Table 4. Therefore, Hypothesis 4 was supported.

4. Discussion

Having the knowledge and confidence to be able to correctly enact protection measures, as well as seeing oneself as routinely following safe practices, is important for people to better protect themselves [40]. The results of the analysis suggest that certain combinations of sources of information influence coping self-efficacy and self-protection habit strength. Those having organized, systematic training from school or work also having higher CSE would indicate that the construct of CSE is based on actually knowing what to do rather than a blind confidence. On the other hand, there were strong correlations between not having any source for

information and lower CSE and PHS; this was also true of those who relied on family and friends to help them.

The combination of sources that produced highest levels of self-efficacy and protection habits was school, work and web. These sources complement each other in proving a multi-pronged outlook when used together as a whole. School, as a source, has the potential to systematically introduce information about important digital safety practices, however it was not widely seen as a comprehensive source. The workplace can provide practical guidelines and policies that help develop good habits in employees. The addition of specialized web sites allowed for individuals to find out more details about emerging threats and how users can protect themselves. These three sources have the benefit of trained educators, professionals from the workplace and the opportunity to have step-by-step instructions when needed. However, despite the potential for this alliance, only 5% (n=37) individuals reported having this as their network.

There were quite a few surprises, especially number of the individuals not having any comprehensive source for information about online safety (15%, n=121). This condition had a tremendous impact on their comfort with protecting themselves online, leaving individuals with the lowest coping self-efficacy and lowest protective habits among the sample. It is not hard to imagine the situations that would lead to this condition. Perhaps the individuals didn't know where to go for help, couldn't understand how to utilize sources they had, or they didn't see the sources as valid enough to utilize. This is especially concerning since our population sample is computer proficient and had done over 100 M-Turk tasks before participating in this project. In thinking about the larger population of Internet users who are not so experienced, there is a strong likelihood that this problem could be endemic. Relying on media alone also led to lower coping self-efficacy. This may be a result of media reports that tend to emphasize larger database hacks and system-wide security failures that may leave the average user feeling helpless. People make decisions based on the information that they have and if they believe the actions they take are going to be effective. If a significant percentage of computer users do not have any understanding of online safety issues, or feel that whatever they do is useless, this could cause systematic weaknesses. Lower personal protective behaviors can lead to more computers being hijacked by malware or viruses unbeknownst to the owners of these devices [41].

The other major surprise was the strong correlation of friends and family as a source that was associated with lower coping self-efficacy and lower protection habits. This could be due to one of several different reasons; it could be that family and friends provide guidance in a way that leaves the information seeker feeling inadequate, giving advice in such a way that it feels intimidating. Or, it could be that the personal presence of an expert allows the individual to not bother to learn details about online safety for themselves. In other words, if a person can quickly call a family member into the room to "fix" the computer and work as their tech support, it is easy for them to just ask for help rather than spend time in learning how to do it. Having friends and family as a source was associated with lower levels of self-efficacy and lower protection habits even when they had other sources of information. Since support from family and friends was an element in many of the combinations reported, this is something that should be further investigated.

Educational solutions seem to offer hope. Despite only a few individuals reporting having online safety training at as part of their education, this was tied to higher levels of CSE, which is a key component to attitudinal and behavioral change according to PMT. Many of the reported combinations did not appear to make a significant difference, yet those who had almost any combination of sources, except for family only, were better off than those with nothing. This research shows the potential for more purposeful alliances across the boundaries of educational institutions, businesses and web site hosting organizations. By working collaboratively, stakeholders can each add their area of expertise and help provide users meaningful and timely information.

Having good online safety practices, sometimes referred to as digital hygiene, is much like learning to wash our hands or brush our teeth. Simple practices can help reduce the spread of disease and improve not only individual health, but community health as well. In the same way digital hygiene, such as resisting phishing attempts or having strong passwords, can protect not only individuals but networks as well. This research shows that we have a long way to go to communicate about online safety, informing and motivating people to follow online safety practices.

5. Limitations

There are many limitations to this research. Since the survey is based on self-reported attitudes and beliefs they are always subject to error, as individuals may over or under report their actual beliefs. The population sample is actively engaged in online tasks and might have higher levels of self-efficacy in using computers than the general population. The demographics of the participants indicate a fairly high social economic status, with most having at least some college level training. This research did not assess those who are marginalized and may not have had an educational background that included online safety training. Also, those with jobs that entail more work with computers will probably have better and more frequent training through the workplace about online safety issues. The participants in this research are probably one of the better-informed populations that use the Internet.

A limitation on the types of social network analysis that can be done with this data is that users were allowed to rate each source freely, but they were not asked to rank the sources. The ranking process would provide additional insight and allow further methods of analysis. Also, due to space limitations, further analysis that gave deeper insight into this population was not included. The findings of this research and the limitations indicate that further research should be done in this realm. This would be especially beneficial to include more diverse populations. The results would help us to better understand how networks of information could be constructed that would enable people to know how to protect themselves.

6. Suggestions for Future Research

Finding ways to improve the cyber safety habits of individuals is an area of extreme importance. This research suggests that looking more carefully at how information is disseminated has potential to better help individuals. Future research could look more closely at how to supporting users in ways that not only inform them, but also help motivate and support them. Most informational material is in response to a specific threat and basically patches for an emerging threat. Research could explore the effects of more systematic and holistic security training that is accurate yet simple enough for all users to benefit.

7. References

[1] V. G. Cerf, P. S. Ryan, M. Senges, and R. S. Whitt, "IoT Safety and Security as Shared Responsibility," *J. Bus. Informatics*, pp. 1–18, 2016.

[2] C. L. Anderson and R. Agarwal, "Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions," *MIS Q.*, vol. 34, no. 3, pp. 613–643, 2010.

[3] M. Bada and A. Sasse, "Cyber Security Awareness Campaigns Why do they fail to change behaviour?," *Global Cyber Security Capacity Centre.* 2014.

[4] S. Furnell, V. Tsaganidi, and A. Phippen, "Security beliefs and barriers for novice Internet users," *Comput. Secur.*, vol. 27, no. 7–8, pp. 235–240, 2008.

[5] E. Rader, R. Wash, and B. Brooks, "Stories as informal lessons about security," *Proc. Eighth Symp. Usable Priv. Secur. - SOUPS '12*, p. 1, 2012.

[6] H. S. Tsai, M. Jiang, S. Alhabash, R. LaRose, N. J. Rifon, and S. R. Cotten, "Understanding online safety behaviors: A protection motivation theory perspective," *Comput. Secur.*, vol. 59, no. 1318885, pp. 138–150, 2016.

[7] R. Shillair, R. LaRose, M. Jiang, N. J. Rifon, S. Alhabash, and S. R. Cotten, "Understanding Online Safety Behavior: The Influence of Prior Experience on Online Safety Motivation," in *AEJMC 2015*, 2015.

[8] P. Ifinedo, "Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory," *Comput. Secur.*, vol. 31, no. 1, pp. 83–95, Feb. 2012.

[9] R. Shillair, S. R. Cotten, H. S. Tsai, S. Alhabash, R. Larose, and N. J. Rifon, "Online safety begins with you and me : Convincing Internet users to protect themselves," *Comput. Human Behav.*, vol. 48, pp. 199–207, 2015.

[10] H. Liang and Y. Xue, "Understanding security behaviors in personal computer usage: A threat avoidance perspective," *J. Assoc. Inf. Syst.*, vol. 11, no. 7, pp. 394–413, 2010.

[11] R. Wash and E. Rader, "Influencing mental models of security: a research agenda," *Proc. 2011 NPSPW.*, pp. 57–66, 2011.

[12] A. Vance, M. Siponen, and S. Pahnila, "Motivating IS security compliance: Insights from Habit and Protection Motivation Theory," *Inf. Manag.*, vol. 49, no. 3–4, pp. 190–198, May 2012.

[13] D. L. Floyd, S. Prentice-Dunn, and R. W. Rogers, "A Meta-Analysis of Research on Protection Motivation Theory," *J. Appl. Soc. Psychol.*, vol. 30, no. 2, pp. 407–429, Feb. 2000.

[14] R. W. Rogers, "A protection motivation theory of fear appeals and attitude change," *J. Psychol.*, vol. 91, no. 1, pp. 93–114, 1975.

[15] J. E. Maddux and R. W. Rogers, "Protection

motivation and self-efficacy: A revised theory of fear appeals and attitude change," *J. Exp. Soc. Psychol.*, vol. 19, no. 5, pp. 469–479, Sep. 1983.

[16] P. A. Rippetoe and R. W. Rogers, "Effects of components of protection-motivation theory on adaptive and maladaptive coping with a health threat.," *J. Pers. Soc. Psychol.*, vol. 52, no. 3, pp. 596–604, 1987.

[17] S. Milne, P. Sheeran, and S. Orbell, "Prediction and Intervention in Health Related Behavior: A Meta Analytic Review of Protection Motivation Theory," *J. Appl. Soc. Psychol.*, vol. 30, no. 1, pp. 106–143, 2006.

[18] J. Cox, "Information systems user security: A structured model of the knowing–doing gap," *Comput. Human Behav.*, vol. 28, no. 5, pp. 1849–1858, Sep. 2012.

[19] S. P. Borgatti and D. S. Halgin, "Analyzing Affiliation Networks," in *Sage Handbook of Social Network Analysis.*, J. Scott and P. J. Carrington, Eds. Thosand Oaks, CA: SAGE Publications, 2011, pp. 417–434.

[20] E. Rader and R. Wash, "Identifying Patterns in Informal Sources of Security Information," vol. 0, no. 0, pp. 1–46, 2015.

[21] L. Li, W. He, L. Xu, A. Ivan, M. Anwar, and X. Yuan, "Does Explicit Information Security Policy Affect Employees' Cyber Security Behavior? A Pilot Study," *2014 Enterp. Syst. Conf.*, pp. 169–173, 2014.

[22] J.-Y. Son, "Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies," *Inf. Manag.*, vol. 48, no. 7, pp. 296–302, Oct. 2011.

[23] B. A. C. Johnston and M. Warkentin, "Fear appeals and information security behaviors: An empirical study," *MIS Q.*, vol. 34, no. 3, pp. 549–566, 2010.

[24] A. Vance and M. Siponen, "IS Security Policy Violations: A rational choice perspective," *J. Organ. End User Comput.*, vol. 24, no. 1, pp. 21–41, 2012.

[25] N. Sonck, S. Livingstone, E. Kuiper, and J. de Haan, "Digital literacy and safety skills," *EU Kids Online*. 2011.

[26] P. Pusey and W. Sadera, "Preservice Teacher Concerns about Teaching Cyberethics, Cybersafety, and Cybersecurity: A Focus Group Study," in *Society for Information Technology & Teacher Education International Conference*, 2012, vol. 2012, no. 1, pp. 3415–3419.

[27] M. A. Moreno, K. G. Egan, K. Bare, H. N. Young, and E. D. Cox, "Internet safety education for youth: stakeholder perspectives.," *BMC Public Health*, vol. 13, no. 1, p. 543, Jan. 2013.

[28] C. Chou and H. Peng, "Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience," *Internet High. Educ.*, vol. 14, no. 1, pp. 44–53, Jan. 2011.

[29] R. Hanewald, "Confronting the pedagogical challenge of cyber safety," *Aust. J. Teach. Educ.*, vol. 33, no. 3, pp. 1–16, Jun. 2008.

[30] S. Livingstone, L. Haddon, A. Görzig, and K. Ólafsson, "Risks and safety on the internet: the perspective of European children: full findings and policy implications from the EU Kids Online survey of 9-16 year olds and their parents in 25 countries," *EU Kids Online*. 2011.

[31] L. Fourie, S. Pang, T. Kingston, H. Hettema, P. Watters, and H. Sarrafzadeh, "The global cyber security workforce : an ongoing human capital crisis." Global Business and Technology Association, 01-Jul-2014.

[32] J. Radford, P. Bosanquet, R. Webster, P. Blatchford, and C. Rubie-Davies, "Fostering learner independence through heuristic scaffolding: A valuable role for teaching assistants," *Int. J. Educ. Res.*, vol. 63, pp. 116–126, 2014.

[33] J. Scott, "Relational Sociology, Culture, and Agency," in *The Sage Handbook of Social Network Analysis*, J. Scott and P. J. Carrington, Eds. Thousand Oaks CA: SAGE Publications, 2011, pp. 80–99.

[34] M. McPherson, L. Smith-Lovin, and J. M. Cook, "Birds of a Feather: Homophily in Social Networks," *Annu. Rev. Sociol.*, vol. 27, no. 1, pp. 415–444, 2001.

[35] R. S. Burt, "Social Contagion and Innovation: Cohesion versus Structural Equivalence," *Am. J. Sociol.*, vol. 92, no. 6, p. 1287, 1987.

[36] K. Casler, L. Bickel, and E. Hackett, "Separate but equal? A comparison of participants and data gathered via Amazon's MTurk, social media, and face-to-face behavioral testing," *Comput. Human Behav.*, vol. 29, no. 6, pp. 2156–2160, Nov. 2013.

[37] L. J. Cronbach, "Coefficient alpha and the internal structure of tests," *Psychometrika*, vol. 16, no. 3, pp. 297–334, Sep. 1951.

[38] M. Tavakol and R. Dennick, "Making sense of Cronbach's alpha," *Int. J. Med. Educ.*, vol. 2, pp. 53–55, Jun. 2011.

[39] G. Cumming, "Inference by eye: Reading the overlap of independent confidence intervals," *Stat. Med.*, vol. 28, no. 2, pp. 205–220, Jan. 2009.

[40] R. LaRose, N. J. Rifon, and R. Enbody, "Promoting personal responsibility for internet safety," *Commun. ACM*, vol. 51, no. 3, pp. 71–76, Mar. 2008.

[41] K. Vaniea, E. Rader, and R. Wash, "Betrayed By Updates : How Negative Experiences Affect Future Security," in *CHI 2014, One of a CHInd*, 2014, pp. 2671–2674.