What does it mean to be "safe" online? An exploration of under-recognized digital privacy concerns and online protective practices in a rural community

Elizabeth Taylor[1], Sherry Hamby[1], Lisa Jones[2], Alli Smith[1], & Kimberly Mitchell[2]

[1]Appalachian Center for Resilience Research & Life Paths Appalachian Research Center, [2]University of New Hampshire

Exploring, Understanding, Overcoming.

Abstract

Purpose: From social media, to email, and online shopping, there is more information about who we are and what we like in the digital world than ever before. Prior research shows 85% of adults and 95% of teens are online, 74% of adults and 90% of teens use social media. With an extensive online presence, what does it mean to be "safe" digitally? Remarkably, little attention has been directed toward how persons themselves report protecting themselves online. Our study explored digital privacy concerns in a rural community, known to have high poverty rates.

Method: Our sample included a general community sample of 65 adults and adolescents who participated in semi-structured focus groups and 24 adults and adolescents who participated in in-depth cognitive interviews that explored digital privacy concerns. All sessions were audiotaped, transcribed, and analyzed with grounded theory analysis.

Results: Several themes emerged: challenges distinguishing legitimate from malicious intents given large, diffuse social networks; concerns about aggressive commercial solicitations; and concrete digital protective strategies in six distinct categories: restricting information sharing, restricting use of certain devices or programs, refusing contact, posting fake information, overall security vigilance, and skilled security behaviors.

Conclusions: Most previous research centers on cyberbullying and stalking. Yet, our findings suggest that digital concerns is more complex because of the range of online relations common today.

Introduction

- Digital technology has become increasingly more prevalent with the rise of smart phones and tablets that ensure almost instant access to the Internet (Palfrey & Gasser, 2008; Lee & Page, 2016).
- With expanding access to the Internet and social media, concerns about online privacy and privacy violations have increased as well, including those involving sharing and tracking of personal information online (Smith & Agarwal, 2010).
- In 2014, there were 269,422 Internet scam complaints, roughly 22,000 online scam complaint each month (Internet Crime Complaint Center, 2014). Scams are becoming increasingly sophisticated as individuals share more information online.
- However, little attention has been directed toward personal strategies for online protection privacy. Most previous research focuses on personal attributes of victims and has focused much less on characteristics of scams or perpetrators of internet fraud (Fischer, Lea, & Evans, 2013; Modic & Lea, 2012).
- Our study analyzed qualitative interviews of individuals from a rural community for challenges they have identifying the legitimacy of a scam, and what range of online protective strategies are employed to protect their digital privacy.
- Research Questions:
  - What types of privacy violations do people who live in rural areas experience?
  - What are the range of online protective strategies that people living in a rural community employ to protect them online?

Method

Participants

Focus Groups. 65 participants from rural Appalachia who participated in 9 focus groups (average 7 people per group). Three focus groups were conducted with adolescents ages 12 to 16, one group with undergraduate college students, and 5 groups were conducted with adults. Participants were 58% female. The majority of the sample identified as White/European American (non-Latino) (92.3%), followed by Latino/a (3.3%), reports of being more than one race (3.3%) and African American/Black (non-Latino) (1.5%).

In-depth narrative interviews. 24 participants from rural Appalachia completed in-depth semi-structured interviews in which they were asked to review and comment on draft questionnaire items generated from the focus groups. Participants ages ranged from 12 to 70+ ; 25% were ages 12-17, 16.7% were ages 18-24, 8.3% were ages 25-29, 16.7% were ages 30-39, 12.5% were ages 40-59, 12.5% were ages 60-69, and 8.3% were 70 years of age or older. The sample was 62.5% female and 37.5% male. The majority of the sample (87.5%) was White/European American (non-Latino), 8.3% were Latino/a, and 4.2% of the sample were African American/Black (non-Latino).

Procedure

Focus groups. In semi-structured focus groups, participants answered questions regarding technology use, problems faced when using technology (scams) and strategies that protect their privacy. Sample items include, "Do you think that some technologies are safer than others?" "We live in a very rural area. How do you think living in a rural area affects your use of technology?" Each focus group participant received a $20 gift card for participation.

In-depth cognitive interviews. The in-depth interviews were structured like the focus groups, except that participants received a $50 gift card for participation. The interview participants were shown a list of items on digital privacy concerns, that were developed from the focus groups by the research team and reviewed by 6 external researchers.

Data Analysis

We utilized grounded theory analyses (Corbin & Strauss, 1990; Walker & Myrick, 2006) to formulate codes, categories, subcategories, and themes from participants' own words.

Results

Challenges Determining Legitimacy of Contact

"I had this one that keeps recurring that's like, 'There's a problem with your PayPal account.' It's just, you don't want there to be a problem with your PayPal account and they use the PayPal logo which also makes it...look pretty good. So you look at this email, and then of course you know better, and then you independently log in like you're supposed to, and you find that there's nothing, there's no problem." – Adult male

"I thought in the picture, [the scammer] looked friendly and kind of old, and I'm like, 'Maybe one of her kids knows me or something?'"- Adult female

So, when [an email] says, 'Network Administrator needs your account,' 'There's been an account breach,' or something like that, 'There's been a problem with your account.' All of those things seem to make it more challenging because you're motivated to resolve it." – Adult male

Concerns about Aggressive Commercial Solicitations

"Lately we've been getting these advertisements from these loan companies, and they know more about our account than we do …. They'll send us an offer every few months and they'll tell us what our payment is now and how much we still owe and how much we can save if we will go to them and I'm offended by it. I don't understand how they know that much." – Adult female

"Lately it's been a robo-call from Bridgette and Bridgette will say, 'Hold if you want to talk to a customer who's bought your credit cards,' or whatever, they'll come across like there's something wrong with your credit cards or, they'll say they have a better offer for you and punch one to talk to somebody. But like the other day I got [a call], I said, 'Listen, I want my name off your list, do not call me again, I'm on the Do Not Call list. If you continue calling me I'm going to turn you over to the authorities.'" – Adult Male

"I mean, it's kind of annoying, but I've also just accepted that that's the internet now and so it's just like if I want to use Google, Google's going to track my various searches and then pull ads from that too." – Adult female

Concrete Online Protective Strategies

Restricting Information Sharing

"I never put what state I'm in unless I feel comfortable telling the person. I never tell my age." – Adolescent female

"I don't share as much personal information on Tumblr, like no birthday or I don't even know if my full name is on there." – College-aged female

Restricting Use of Certain Devices or Programs

"If we leave, we don't post...checking in somewhere is the biggest paranoia because if you check in, then you're automatically saying, 'I've left all of these things unattended.'" – College-aged female

Refusing Contact

"The rule in our house is to let it go to voicemail if you don't recognize it. My parents are like, 'If we are not home, do not answer the phone unless it's us or some relative and then you just say, 'Hey, they're not home.'"" – Adolescent female

Posting Fake Information

"[I] just [use] a lot of fake names and if it says, 'You have to tell us where you live,' I just put in a random state, like, 'I live in New York.'" – Adolescent male

Overall Security Vigilance

"When I heard about [GPS tracking], I went right to it and it showed exactly where I was for the last, you know, 6 months; every address, every time, everything and I just went, 'Well we'll just turn that little thing off.'" – Adult male

"We've all been there...like, 'I'm going to search something,' and be like, 'No, not on this Wi-Fi. I'm going to switch to a more secure connection or maybe like a personal connection.'" – College-aged male

Skilled Security Behaviors

"You can also get a steel mesh wallet. [There is a scanner] you can hold up to someone's back pocket through their wallet and read their credit card information and so they make these little steel mesh wallets. It's sort of like a barcode scanner but for your credit card." – College-aged male

Discussion

- Several interconnected themes arose through our content analysis of the focus groups and cognitive interviews.
  - Several participants noted that it was challenging to determine if an email or a Facebook account was legitimate because the scam appealed to their emotions, eliciting fear, trust, or hope.
  - Additionally, participants noted that aggressive commercial solicitations, though not illegal, were more "annoying," inconvenient, and at times, frightening because of the amount of personal information these companies had accessed.
  - Lastly, participants endorsed such online protective strategies as ignoring emails or phone calls from people they do not know, restricting the amount of personal information shared online, and being wary of public Wi-Fi as a route to stealing private information.
- Much of previous research on digital privacy strategies tend to centralize around cyberbullying violations for adolescents (Moreno, Egan, Bare, Young, & Cox, 2013), whereas we are still learning about privacy harms and how serious the resulting harm is.
- These results suggest that digital concerns expands beyond merely avoiding cyberbullying, but that online vigilance while navigating diffuse social networks is imperative as well.

Limitations and Future Directions

- Though our sample was taken from an often underrepresented rural population in psychology, the lack of diversity in our sample is apparent and may impact the generalizability of these findings.
- Our qualitative analyses provide a unique framework for studying online privacy protection and future research would benefit from delving further into how individuals perceive their online presence through mixed methodology.

References

- Corbin, J., & Strauss, A. (1990). Grounded theory research: Procedures, canons, and evaluative criteria. *Qualitative Sociology, 13*(1), 3–21.
- Fischer, P., Lea, S., & Evans, K. (2013). Why do individuals respond to fraudulent scam communications and lose money? The psychological determinants of scam compliance. *Journal of Applied Social Psychology, 43*, 2060–2072.
- Internet Crime Complaint Center. (2014). 2014 Internet Crime Report. Federal Bureau of Investigation. Retrieved from https://www.fbi.gov/news/news_blog/2014-ic3-annual-report.
- Lee, R., & Page, D. (2016). Privacy and information sharing. *Pew Research Center.* Retrieved from http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/
- Palfrey, J., & Gasser, U. (2008). *Born digital: Understanding the first generation of Digital Natives.* New York: Basic Books.
- Modic, D., & Lea, S. E. G. (2012). How Neurotic are Scam Victims, Really? The Big Five and Internet Scams. *SSRN Electronic Journal.* http://doi.org/10.2139/ssrn.2448130
- Moreno, M.A., Egan, K.G., Bare, K., Young, H.N., & Cox, E.D. (2013). Internet safety education for youth: Stakeholder perspectives. *BMC Public Health, 13*(1), 543.
- Smith, C., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral patterns. *MIS Quarterly, 34*(3), 613–643.
- Walker, D., & Myrick, F. (2006). Grounded theory: An exploration of process and procedure. *Qualitative Health Research, 16*(4), 547–559.

This project was made possible through the support of a grant from the Digital Trust Foundation. The opinions expressed in this project are those of the authors and do not necessarily reflect the views of the Digital Trust Foundation.