VA Engage Journal

Volume 6 Article 2

4-2018

Technology Literacy and Senior Citizens: Online Communication, Privacy and Phone Scams

Christine Hilbert
Virginia Commonwealth University

Technology Literacy and Senior Citizens: Online Communication, Privacy and Phone Scams

At Virginia Commonwealth University, while taking Inquiry and the Craft of Argument, I participated in 20 hours of community service. The class was a service-learning section focusing on technology integration in the community. The nature of this course was to allow our service work to guide our research with the goal that our participation would shed light on a community need. I gained a deeper understanding of how senior citizens, or persons over 65, became acquainted with new technology. The service work led me to the understanding that, although the residents were fluent in being able to access online websites and use phones, they were not fully aware of the privacy options available for their security. The research indicated that senior citizens using technology when they do not have an education on how to navigate the online services could encounter otherwise preventable situations. These include, but are not limited to, giving away money, posting private information to public platforms, and allowing a phone caller to coerce them into giving out private information.

My group partnered with Happy Days assisted living community in Richmond, Virginia, and the examples used in this analysis are stories the residents shared with me while engaging in routine technology tutoring. The name of the retirement community has been changed, and the quotations and italics attributed to the residents below are reenactments of the resident's stories and not their documented words. These are real-world instances that probably happen more than society would like to admit, and after my service work at Happy Days I realized that preventative measures can be taken for the senior citizen user to protect their privacy while answering phone calls or using online communication services. Technology education focusing on online privacy and how to handle an unwanted caller can help the senior citizen population protect themselves online as well as through the phone. This type of education creates foundational awareness for other social media sites and offers a universal script when handling an unwanted phone call. Raising awareness about privacy can be and perhaps should be integrated into all technology help given to seniors.

Senior Citizens' Interactions with Technology

In November 2016, in a small room at Happy Days, five senior citizens with eager expressions on their faces held devices such as laptops, tablets, and cell phones. The five seniors were there for technology tutoring and four college students, including myself, were there to help them in any way we could. A returning resident lit up when she saw me and we began a conversation that led to a shocking revelation. She commenced to tell me about a time that she had almost been scammed out of $3,500. Below is her account of the story:

I was needing a car and found a really good deal on Craigslist. He said he was in the Service, and it was a good car at a good price. He told me to send him money and he would ship the car to me. He told me to go to Wells Fargo and put the check into his cousin's account. Thinking about it now I feel so foolish. I always tell people to be careful and don't trust people online. Anyway, I go to Wells Fargo and try to send the check when the representative said, "let me check a few things." This was after they asked me if I knew the person personally to which I told them I did not. The man from Craigslist said I had to send the check within the hour, so there I was sitting in the bank when I started to get extremely anxious because it was getting to the hour mark. After a while, the manager and teller came out and told me that the account had several fraud flags on it so they were no longer honoring the account. After that happened, I called the Better Business Bureau to report the incident, and they said that it was one of the most common scams and that they couldn't believe I almost fell for it.

The scammer used a pressure tactic to persuade the victim to complete the transaction quickly so there would not have been time to reverse it, had the resident figured out she was not going to receive a car. Many victims can fall for this trap and the senior citizen population seems to be more vulnerable due to their trusting nature. Immediately trusting someone online or over the phone was a shortcoming I noticed both in my research and service work and I felt it necessary to look into further. I observed in my service that the residents desired to communicate and interact with others online and most of the time they were able to do this on a mostly fluent level. This is especially true of social media sites and email. As a society, further research and attention should address the reactions to reporting suspicious behavior as they have negative consequences if authorities do not receive the complaint with understanding and empathy. When the resident attempted to report the crime, the Better Business Bureau's response was unprofessional and off-putting. This type of situation can be detrimental to a senior citizen because they may no longer feel comfortable reaching out to a loved one or others they trust. The response could also have adverse effects when trying to be proactive about limiting the prevalence and influence of cyber criminals.

Living in a technological society, internet use is on the rise and this is true for the senior citizen population. According to Anderson and Perrin at the Pew Research Center (2017), 67% of adults over 65 go online (p. 8). Understanding privacy settings and the basic user foundations of social media sites like Facebook or email is pertinent to successful technology integration in the senior citizen population. Scam callers and automated calling is important to focus on during technology tutoring because the telephone is the technology that most senior citizens are commonly familiar with. Whether the senior citizen is using online services or phone communication, it is important to take into account how the population could be vulnerable to uncomfortable outcomes, should they be unaware of some of the risks. The remainder of this paper will explore the potential solutions to not only the situation mentioned above, but also many others like it such as unwanted calls or unintentional posting to social media sites by new internet users.

Senior Citizens' Understanding of Online Platforms and Privacy

During a visit to Happy Days, a resident asked me to teach her to delete emails. It quickly became apparent that she needed help understanding how her AOL email functioned. I worked through a step-by-step process that included showing the resident how to select all, delete, reply all, and how to compose emails. The resident was quick to log in and show me exactly what she needed help with. The interaction made me take a step back. I went in with the notion that the senior citizen population needed help using the technology in general, as if they did not understand anything. That was not the case, and it made me approach my service differently. I acknowledged after that moment that I had an unconscious bias towards the senior citizen population when they go online and that my bias was unfair to the population. I was able to understand better that they were fully capable of using the platforms, but they tended to need encouragement that they were capable as well as elevated tutoring to be confident users. When I asked the resident how she became so savvy with using the site she told me that most of it was on her own. Her daughter got frustrated with her when she asked how to use online platforms, so the resident did not ask for assistance until the service-learning students came. I began to reflect on how the rest of the population responds when a person over 65 asks for help using online services. The tendency to act dismissive when a senior citizen asks for help can lead to them not reaching out anymore which is unproductive.

As a service learning student, I went in with patience which lead to a lot of really good questions from the residents. After we worked through the email platform the resident asked me to help her message people privately on Facebook. She began to tell me of an uncomfortable instance when she sent an intimate letter to her pastor on Facebook. Rather than sending him a private message, she posted it to his main page without realizing that everyone could see the post. *"I was so humiliated*," recalls the resident. This instance is a prime example of knowing how to access the technology without understanding the functions of the platform. On Facebook, when posting to someone's wall, it can be misunderstood that it does not show that message to the public. The lack of familiarity comes from the senior citizen population not being properly educated on social media sites. An important concept to keep in mind is that the senior citizen population is completely capable and competent in understanding how to use the platforms even if they sometimes need help. Once they are able to navigate the software, things become much easier and they are further able to understand other platforms because they have gained a better foundation.

At Happy Days, the residents wanted to learn how to better use technology, so they could become more confident and independent in their usage. Technological education for senior citizens on social media sites and the potential cyber threats that come with its use is crucial to facilitate independence online. Having reaffirmation of information will help senior citizens protect themselves online and feel confident to report any suspicious behavior they encounter. In a study done by the Pew Research Center titled "Older Adults and Technology Use," Zickuhr and Madden (2012) found that 6 out of 10 seniors report using the Internet. On average, my peers and I helped 5 to 15 residents per two-hour visit to Happy Days. During these visits, I frequently received questions on how to use online platforms. Facebook was incredibly popular among the residents and most of their questions were centered around using the site. However, we realized that for the new users at Happy Days, we could not help the residents with discrete functions of the site without teaching them a foundational knowledge of the platform. This was evident when residents asked us how to search for people, how to add friends, how to delete requests, and how to log out, among other things. After we taught the residents about using the basics of the platform, they seemed to be much more confident in their own abilities.

Discussing privacy settings creates a new dimension of understanding that could not be taught until we gave the residents help with the platform's basic functioning. After establishing the foundations of navigating the site, we could better help them understand and use the privacy settings. For example, when posting something to your wall, Facebook has a small drop-down menu to the right of the text box that allows the post to be public or audience specific. There is a setting in the security features of the site that can allow for someone to change the public setting to friends only, but it is five clicks deep into the site. To understand how to access and use the security setting, the user will first have to understand where their post is going, how to see their post, and be cognizant of the audience of the post. After that, the explanation of where the default setting is located becomes much easier. If a senior citizen user does not choose to alter their security setting, and does not click on the friends only option before posting, their post becomes public to the world. Consequently, others could potentially use sensitive information the user posted to gain their trust and take advantage of them.

Once we had taught audience-specific security features, something my group wanted to elaborate on with the residents was the potential of unwanted posting to someone's page on social media sites. We thought this was important after discussing the privacy settings with the residents because it is a setting that can be changed in the security features of the site and can cause issues if not changed. This is troublesome because many times the residents had to really pay attention to the functions of the site to understand the parameters of the platform, let alone advanced security settings. In the article "Social Networking and Identity Theft in the Digital Society," Holm (2014) discusses the nature of how social media sites create a new vulnerability to internet criminals while online. An especially silent threat is “once information has been passed on, particularly to third parties, it is unclear as to what obligations will be adhered to and the responsibilities of these parties are not defined” (p. 161). We observed in the residents that default options of social media sites, such as allowing your profile to be public, are not changed to private because the new senior citizen user is unaware of privacy settings at all. This could impact their future privacy and personal security online. This led us to discussing the prevalence of phishing on social media sites after we found evidence of the frequency.

The older citizens of the United States who are new to using sites such as Facebook could possibly be unaware of security threats, and we found this to be true of the residential population at Happy Days who came out for technology tutoring. In the infographic report titled “International Internet Scam Hotspots,” backgroundcheck.org (2016) found that 65.9% of phishing scams, which are fraudulent messages sent out to obtain sensitive information such as passwords or credit card numbers, originated from the United States and target social media sites and email platforms. To prevent any vulnerability, we encouraged the residents to never give out their password and made them aware of what a safe URL looked like. However, a challenge we faced was that sometimes the residents did not want to hear the logistics behind security settings or what threats could be lurking online. For the most part, we worked with what they needed help with, but also learned to be broader in our explanations because we had a tendency to use implicit language which can be frustrating to a new user. We realized that when tutoring someone in social media platforms, it is really important to use unbiased and understandable language so that no one shuts down, including the tutor. When explaining how to directly message someone in the chat screen on Facebook, a resident kept saying that it was not working, and at that point, I was not really sure how to tell them in another way. However, I took a step back and realized that there was another way to do this that would be more straightforward and safe. Instead of trying to message the person from the chat screen, I had them go to their friends list, click on the person they wanted to talk to, and from there, click on the message screen located in the top right-hand corner of the persons page. This was a beneficial experience because it allowed me to see that the ways in which I explained other things may not have been so clear.

The accessibility of personal information online and the rise of technology use by the older population make it incredibly important to educate the new senior citizen user. There is an abundance of preventative measures that can be set in place such as changes in the privacy settings and teaching the basic foundations of the platform. Educational outreach programs for older persons could help make them aware of what settings to choose, and who to talk to or accept friend requests from, as well as enable them to guard themselves online. This would be a good step to increase self-protection for the senior citizen population.

Phone Usage and Automated Calling

In October 2016, I was called to the room of a couple who had been living at Happy Days for five years, and our interaction sparked a conversation about "robocalls." One of the residents told me her friends had been targeted by these phone calls and sucked in because it was hard for friends to say no or to "be rude." She said she was annoyed by these calls because she opted into a no-call list. She did not understand why they kept calling, yet she accepted it as an unavoidable annoyance. "*You know, I have a hard time hanging up with those people and the worst is the robot calls! I put us on the Do-Not-Call list and we still get them!*" she said with a sighing smile. Although the U.S. has enacted laws to protect individuals from cybercrime such as the "Do-Not-

Call Implementation Act," they may not always be helpful to the senior citizen population if a persistent caller catches them off guard.

Although there are laws to limit the number of automated callers, the laws are not well enforced because it is hard to keep up with the quickly progressing cellular usage among U.S citizens. A report released by the U.S Senate Special Committee on Aging titled "Fighting Fraud: U.S. Senate Aging Committee Identifies Top 10 Scams Targeting Our Nation's Seniors" (2016) discussed in depth the top 10 scams that seniors face in the United States and offered resources to help senior citizen victims. Robocalls were the third most frequent scam on the list. To combat this, Congress established a national Do-Not-Call registry "with the goal of putting an end to the plague of telemarketers who were interrupting Americans at all hours of the day with unwanted calls" (p. 7). The act was passed in 2003 to stop telemarketers from calling citizens, yet almost 15 years later it has not deterred criminals from contacting potential victims. The resident told me she placed them on the Do-Not-Call list but still received calls. This resonated with me because I have experienced similar situations. While the law may have worked in 2003, it is no longer effective because of how much the internet has evolved. Criminals can find numbers online easily and make thousands of calls instantly.

When I was working with the residents, I realized how frequently they used their phones, whether to call friends, family or even play games. The residents were fully capable of using this technology and were even aware that robocalls were a common issue. When I went back and discussed this with my group, we became more cognizant that, while we were doing technology tutoring, the residents of Happy Days were much more aware than we thought. It made us critically analyze the circumstances in which these situations play out. For us, when we see an unknown number, we let it go to voicemail or we ignore it all together if it is an "888" or "201" area code, because we learned growing up it was not a legitimate caller. However, many senior citizens have used landlines most of their lives. When landlines were first around, caller ID was not a common feature, and while the residents knew how to use the phones, they were in the habit of answering the phone without checking for the caller. We encouraged them to check the caller ID so they would have the ability to reject a call. Another reason they may be vulnerable after accepting a phone call is because they want someone to talk to. The residents loved to share their stories with us, and much of the time, it was unrelated to technology. Many are aware of what a robotic call sounds like or even a telemarketer, but sometimes it becomes hard to hang up because of the persistence of the caller.

For example, I helped a resident couple set up their voicemail. At the end of the call, the sales representative tried to sell them a product that was very expensive and unnecessary for the couple's phone use. I was swift to say "No thank you, goodbye," but after the interaction the residents thanked me for hanging up and acknowledged it would have been a nuisance for them to do so. Something I took away from this was that the residents are not unaware of the tactics of a sales person, telemarketer or robotic caller, but when it comes to hanging up, it can be hard to distinguish if what the caller is saying is important or not. Another vulnerability senior citizens have to these tactics is potentially the absence of facial cues which can make the differentiation between a helper or an upseller difficult. This made it clear that we could help them create preventative habits while engaging in cellular technology opposed to going over the rudimentary basics of using a phone. Another observation I made was that a lot of the time in the residents' cell phones, they had a series of numbers in their outgoing or incoming call log. When I asked who was who, they were able to tell me that it was their child or friend. Encouraging the add contact feature in the cell phone was a measure I took so that it would be easier for the residents to differentiate whether a caller was a familiar number or a random number that would be better left to voicemail.

Response to the Senior Citizen Victim

During a visit, I was having a conversation with a resident about the public service announcements around the assisted living campus, alerting the residents of IRS impersonators and lottery scam callers. This was an indication to me that someone in the region had potentially reported such behavior. I decided to inquire into the situation more to gain a better understanding of the frequency and nature of the occurrences. I asked the resident if she or anyone she knew had been scammed out of any money. She stated, "*I had a friend who told me someone called telling her she had won the lottery but had to give them money first. She didn't tell anyone about it because she felt uncomfortable sharing how much money she had given the caller.*" When discussing these occurrences, it is necessary to talk about how we can prevent these situations from happening. It is equally important to acknowledge what type of dialogue would be most appropriate so that the victim feels comfortable sharing.

There is evidence of senior citizens not wanting to report cybercrimes both through my service work as well as in the research my group and I conducted. In the article "Lies, Secrets, and Scams," *Consumer Reports* (2015) gathered eight case studies from those living along the East Coast and found that "among the factors that keep seniors from reporting scams are deep humiliation once they realize they've been had, and fear of reprisals from scammers who may have made threats to keep them silent" (p. 32). The article later states that in New York, only one in 44 people would report being caught in a scam. I observed this reluctance to report in my service work at Happy Days as well such as when the resident's friend did not want to tell anyone she had been caught in a lottery scam. The example at the beginning of this analysis is one of the more disconcerting cases. After I asked the resident caught in the Craigslist scam if she would feel comfortable reporting a cybercrime again, she said she would not because of how the Better Business Bureau responded to her complaint. The manipulation and ability of the scammer to create fear in a victim adds to the unwillingness to report cybercrime. This is a problem because when cybercrimes go unreported, inaccurate data on the frequency of the crime is released. This leads to less public awareness and therefore less urgency to investigate the perpetrator.

Some articles suggest that the older victim's trusting behavior of giving out information over the phone or online plays a key role in senior citizen identity theft. Holtfreter was the lead researcher in the 2015 study “Risky Remote Purchasing and Identity Theft Victimization Among Older Internet Users,” which analyzed and collected data on the behaviors of a randomly selected group of Arizona and Florida residents over age 60. Some of the characteristics described in the study were low self-control or risk-seeking behaviors of a victim. For instance, in a lottery scam, a victim may give out information to obtain a large amount of money like described above. The researchers concluded that “identity theft can be the end result of a complex process involving both personality characteristics and behavioral routines on the part of the victims” (p. 692). The study suggests that behavior plays an important role in being scammed, but it fails to take into account whether these victims received education on scams and identity theft or if they understood how to protect themselves from these crimes. The conclusions from this type of study can be misleading because of the way the data is analyzed. This type of study insinuates the victim’s behavior without taking into account what the scammer is saying to the victim or whether the victim was aware that there are malicious people out there who target senior citizens specifically for their trusting nature. This portrayal of the senior citizen victim can be harmful when we try to progressively eliminate these threats. To further help the senior citizen victim of a cybercrime, it is important to continue studies on technology use among the senior citizen community as well as include assessments on how officials respond to cybercrimes against the senior citizen.

Technology Education for Senior Citizens and Positive Outcomes

When I began my service-learning at Happy Days, I was enlightened to the role that technology has played in the senior citizen community. Prior to going into the service site, my reasoning for why the residents needed technology tutoring was that they did not understand the rudimentary functions of using technology. That assumption was proved wrong on day one. However, it was not until months later, after contemplation and reflection, that I realized I went into Happy Days with a bias about their ability to use technology. The relationships I forged with residents allowed me to gain insight into what the residents needed help with. Most of the time, they already understood how to use the technology; they just needed extra coaching on how to navigate the platforms they were becoming familiar with. Something notable about this population is how eager they all are to learn. Every session, there were residents who signed up for in home tutoring, or they were already waiting for us in our designated work-room. The readiness of senior citizens to further their technological education is exciting, and a sign that more should be done to teach new users how to protect themselves online and through the phone as well as offer workshops to brush up on the basics.

The senior citizen population has come to enjoy the benefits of internet and electronic services, which was especially observed at Happy Days assisted living facility. However, continued usage does not mean that they have emerged with a better understanding of how to protect their privacy, which is why technology tutoring is so important. Most of the residents have been engaging in cellular and landline phone communication for years, yet there were situations that led to unfortunate circumstances. Assessing why the senior citizen may become vulnerable to a robot caller or a scammer through the phone is important when trying to empathetically understand the population. Empathy is extremely important when educating because it allows for targeted insight that better helps the population.

This analysis has described why greater attention should be paid to helping senior citizens learn how to use and integrate new technology into their lives in a safe and positive way. This could change the discussion in helping the senior citizen population use technology and how we address protecting the population in general. Though the older generation sometimes requires extra attention, the concerns stated in this essay not only pertain to them, but to U.S citizens of all ages who use technology. They affect the family, the community and the future interactions the senior citizen may have towards technology use and personal interactions with others. These observations should not elicit a mistrust of technology or cause senior citizens to shy away from using it. Instead, it brings to light inconsistencies in how senior citizens are educated on technology use as well as how we respond to scams. It also brings to light how others may perceive an older user and how that can cause a deficit in communication.

At the conclusion of our service work, my group and I were asked to create a project which would help our community partner after our service work concluded. We designed and supplied brochures to be passed out at Happy Days illustrating common scams, typical language a scammer may use, tips for password security, and a list of resources available to victims of a cybercrime. As a group, we agreed a brochure would be the most accessible way for the residents to know about common scams and password securities and have information on who to contact if they suspect suspicious behavior online. A physical form of information was an ideal reference for the residents to have because they seemed more comfortable with printed or written out manuals on technology use. Many times, when explaining something to the resident, they would manually write down each step so that they would remember once we left. However, there is more to this than leaving a physical reminder behind. An important part of technology tutoring at Happy Days, especially in my work, was having the residents repeat back what we just walked through. I was confident in my ability to demonstrate what to do if they were able to explain it back to me, no matter how long that took. So while we gave the residents a physical reminder of things to watch out for, it was more important they knew how to use the online platforms and feel confident in reaching out to others should they feel uneasy about any virtual communication. While the residents did not outwardly say they had been scammed when I interacted with them and asked questions, they always had a story or an instance of being scammed, almost being scammed, or had known of someone that had been scammed. Throughout my research it became clear that there was a need for more studies and dissemination of the information on older adults and technology use.

If we begin to look at technology adoption issues with greater importance, we might reduce the rate of scams in the senior citizen community to save them from future heartache. One possibility for prevention could be outreach in communities in the form of workshops that focus on understanding online platforms. It is important to keep in mind that when engaging in technology tutoring with senior citizens, they usually have a solid understanding of how to use the technology. The goal then becomes achieving the next level of maneuvering through virtual communication. Another preventative measure could be simulations of a cybercriminal caller. In the moment, it can sometimes be hard to deduce if a caller has negative intentions and by having a simulation of the event, the senior citizen might become more aware and confident in themselves should that situation occur in real life. If we had an integrated community of technology education, it could enlighten those that are unaware of the senior citizens' need for technology education and could be a potential catalyst for larger involvement from the community. This is an issue that we have to take on as a nation. It will require cultural change, commitment to action, and empathetic understanding from everyone involved.

References

Anderson, M., & Perrin, A. (2017). *Tech Adoption Climbs Among Older Adults.* Washington, DC: Pew Internet. Retrieved from http://www.pewinternet.org/2017/05/17/older-americans-tech-methodology/

Holm, E. (2014). Social networking and identity theft in the digital society. *The International Journal on Advances in Life Sciences, 6*(3&4), 157-166.

Holtfreter K., Reisig, M.D, Pratt, T.C, & Holtfreter, R.E. (2015). Risky remote purchasing and identity theft victimization among older Internet users. *Psychology, Crime & Law*, *21*(7), 681-698, doi: 10.1080/1068316X.2015.1028545

International Internet Scam Hotspots. (2016). Backgroundcheck.org. Retrieved from https://www.backgroundcheck.org/international-internet-scam-hotspots/

Lies, Secrets, and Scams. (2015, November). *Consumer Reports*, *80*(11), 28-37.

Special Committee on Ageing. (2016). *Fighting Fraud: U.S. Senate Ageing Committee Identifies Top 10 Scams Targeting Our Nation's Seniors*. Washington, D.C.: U.S Government Publishing Office. Retrieved from https://www.aging.senate.gov/imo/media/doc/Fraud%20Book%202017.pdf

Zickuhr, K., & Madden, M. (2012). *Older adults and Internet use*. Washington, DC: Pew Internet and American Life Project. Retrieved from http://www.pewinternet.org/files/old-media/Files/Reports/2012/PIP_Older_adults_and_internet_use.pdf