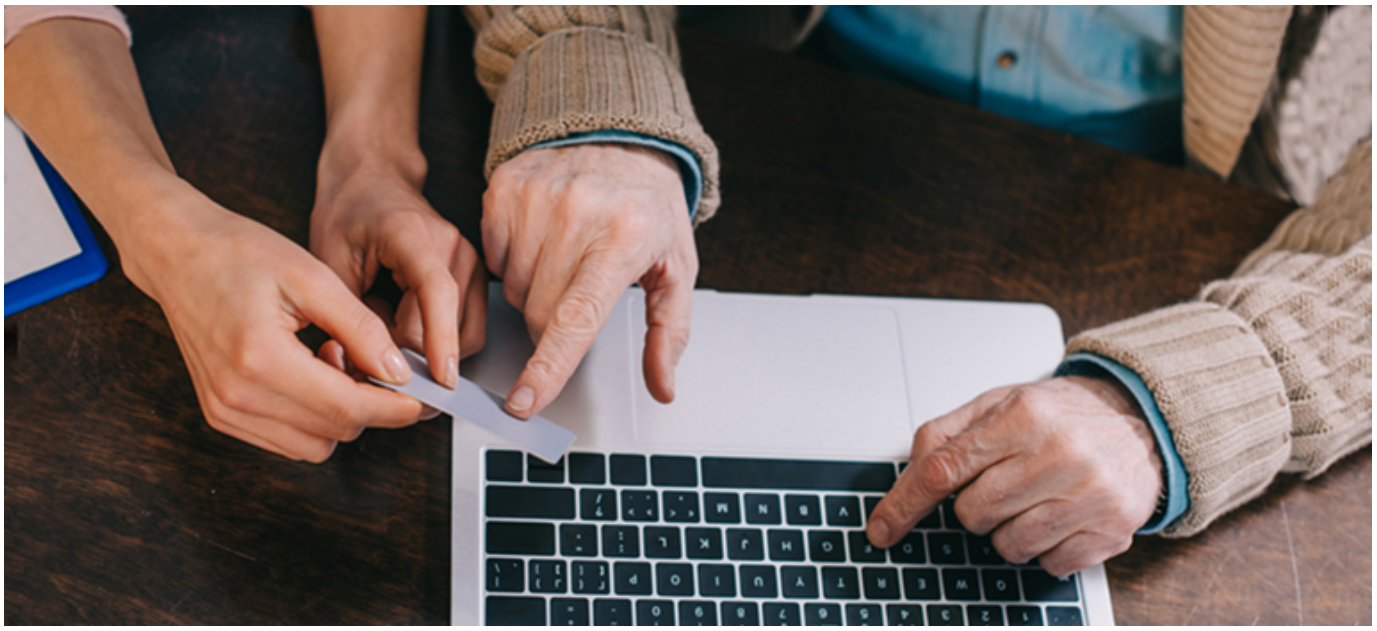
{CYBERSECURITY} Magazine
A MULTI PLATFORM PUBLISHING PORTAL

From the Winter 2020 Issue

The Threat and Threat Intelligence

Doing More to Support Those Residing in Assisted-Living or Eldercare Facilities with Cybersecurity and Cybercrime Prevention

Stan Mierzwa
Managing Assistant Director, Center for Cybersecurity | Kean University



INTRODUCTION

As the U.S. population continues to age, those entering senior living arrangements will continue to grow and with that potential this population is more likely to be the regular users of computers, laptops, smartphone/tablets and Internet. The U.S. Census reports that as of 2016, 86.9% of older Americans aged 65 to 74 have computer ownership with 83.2% using the Internet (See Table 1). Compare that with the age group 75-84, and the number drops to 74.2% for computer ownership and 70% Internet usage. Finally, for those aged 85 and older, the number drops even further to 57.5% with computer ownership and 55.1% Internet access.[1] Couple that reality with the potential that those in the age group 65 to 74-year-old may ultimately enter the older adult living communities and are more likely to be using technology routinely; therefore, there is a potential for an increase in Cybercrime.

Age Group	% Computer Ownership	% Using the Internet
65 to 74	86.9%	83.2%
75 to 84	74.2%	70%
85 or older	57.5%	55.1%

Table one: US Census American Community Survey (ACS) Report

According to the U.S. Census Bureau's 2018 population estimates, 52 million Americans are age 65 or older and 25% of them live in California, Florida, or Texas. If one includes the U.S. states of Georgia, Illinois, Michigan, New York, North Carolina, Ohio, and Pennsylvania, they account for the next 25% of Americans over age 65. Seniors live in all areas of the United States, are surrounded by families and friends, and so bringing attention to this issue of cybercrime targeting seniors is beneficial to everyone.

BACKGROUND ON ELDER CYBERCRIME

Overall it is estimated that cybercriminals steal $37 billion from vulnerable older adults in the United States.[2] As in the case of humans globally, seniors and the elderly are going online more and more and are considered enticing targets for cybercriminals. **The FBI maintains that fraud against senior citizens is a target for cybercriminals because they are more likely to have savings, possess excellent credit, and were born in a time (1930s – 1950s) when they were raised to be polite and trusting.**[3]

> Several known strategies are utilized to scam the elderly via online services. Indeed, these strategies employ trickery with the ultimate goal of financial advances to the benefit of the scammers.

One prominent example is the now common "tech support" scam that was uncovered and ultimately criminally charged in 2017. In this scam, criminals purchased pop-up browser advertisements which appeared on victims' screens and locked their browsers.[4] [5] The pop-ups noted text suggested the systems were compromised and that the victim needed technical support to correct the problem. In this case, the reports indicated that over 80,000 people from around the world were victimized and that criminals gained $25 million USD. [5]
Although one can analyze or deep-dive into statistics on any state, as an example specific to New Jersey, the current population reported by the United States Census is just over 9 million with 15.7% age 65 years and older.[6] The FBI reported that New Jersey stands at 15th among the 50 states in percentage of residents getting scammed via cyber or Internet related qualities and ninth in the losses per person. The middle-aged and elderly are the top victims in New Jersey. [3]

The top six reported types of Internet crime reported by the FBI are:[8]

1. Non-payment/non-delivery
2. Extortion
3. Personal Data Breach
4. No Lead Value
5. Phishing/Vishing/Smishing/Pharming
6. Business Email Compromise(BEC)/E-Mail Account Compromise(EAC)

Scams can include different technology platforms. For example, robocalls, which include technology in the back-end with automated mechanisms to make phone calls, have continued to explode. A U.S. Senate Special Committee on Aging reports that nearly half of all mobile calls are spam. In the past year, robocalls were the second-most reported complaint to the Senate Aging Committee's Fraud Hotline.

SEVERAL SIMPLE STEPS TO HELP THE ELDER COMMUNITY WITH CYBERSECURITY

The Kean University Center for Cybersecurity has made available on their website many useful links to information that the general public can refer to with help on cybersecurity awareness. In particular, the site provides specific links dedicated to seniors from the FBI, FCC, and U.S. Senate. Some advice that can be provided to seniors as an initial step in cybersecurity education includes:

1. Notify them that Cybercrimes happen to everyone, not just the elderly, and they are not to be blamed because of their age. However, let them know they are targeted by cybercriminals for reasons outside their disposition. Perhaps they may have savings, excellent credit, or are considered to have trusting nature.
2. If a senior is believed to be a victim of a cybercrime, they should speak up and not keep quiet about it. The FBI maintains a website (ic3.gov) that allows a complaint to be filed.
3. Educate the senior regarding the common practice of false promises made via Internet offers.
4. Regarding Telemarketing Fraud, the FBI reports these warning signs for you to be aware of these techniques used by cybercriminals:
   a. Mentioning any of these actions the senior must take are red flags: “You must act now, or the offer will not remain”; “You’ve won a free gift, but you have to pay charges to receive”; “Asking the senior to provide a credit card or bank account number before they have a chance to truly consider the offer”.
5. With computer use, follow these basic tips:
   a. Choose strong passwords. The longer the better, and use a mix of numbers, letters, and symbols. If possible, use a long “passphrase” or sentence that means something to only you.
   b. To the fullest extent possible, do not use the same email address or a user account for all your web-based services.
   c. Keep your mobile devices, smartphones, tablets, and laptops with you at all times and be aware of your surroundings.
   d. Do not provide personal information over email if a business or organization contacts you unsuspectedly.
   e. With social networking sites, limit the amount of personal information posted and use privacy settings to avoid sharing information unnecessarily.
   f. Keep your computing device’s operating system updated with security patches, as well as your anti-virus software. If assistance is required, the senior should seek it.
   g. Bring greater attention to privacy settings in the applications the seniors’ use.

COMMON SENIOR FRAUD

There exist many strategies employed by cybercriminals to defraud seniors. The United Sates Senate Special Committee on Aging has performed an analysis ranking the top scams targeting our nation’s seniors.[7] With the Senate report, one can review the top scams in each state. Specific to New Jersey, the Senate Special Committee ranked the below top 5 scams in the state:

1. Consumer Complaints
2. Robocalls and Unsolicited Phone Calls
3. Computer Tech Support Scams
4. IRS Impersonation Scams
5. Social Security Impersonation Scams

As an example, we detail several well-known scams related to seniors below. However, for additional information regarding each of these scams with examples and tips for preventing and securing seniors from these scams, visit: https://www.aging.senate.gov/fraudbook/index.html

COMPUTER TECH SUPPORT SCAM

In general this scam involves cybercriminals representing themselves falsely from well-known large computer companies, such as Microsoft or Apple, and notifying the senior they have a virus or problem on their computer.[7] The criminal then convinces the senior to give them remote access to their computers, perhaps even their private personal information. If access is provided, any number of bad things can happen. For example, the criminal can install software to monitor all the seniors' activity on the computer, gaining user IDs and passwords. Or, the criminal may falsely claim to have corrected the issue after receiving payment.

GRANDPARENT SCAMS

The grandparent scam targets older Americans. In this scam, the cybercriminal pretends to be a grandchild of the victim or pretends to be holding the grandchild. The criminal then claims the grandchild is in trouble and that money needs to be sent urgently in order to help with this emergency. Examples of these problems could a relative or grandchild in jail, trouble paying a hospital bill, or an inability to leave a country without payment.

CONCLUSION

Generally, cybercriminals that are interested in benefiting financially will present themselves where there is the greatest opportunity for success. Given the data presented in this article, the seniors in the U.S. are certainly targeted. Plenty of information from many sources is available to assist seniors with their cyber hygiene; however, it would be beneficial to give the effort much greater awareness.

Consider a campaign, one could reference the Stop-Think-Connect campaign as a launch pad, and target it for seniors. Bringing the family of seniors into the fold will both aid the seniors, and also themselves in gaining greater knowledge of the issue. It's very likely and possible that if a family senior member was targeted for a cybercrime, they may not necessarily say anything. Therefore, extended family must be able to talk about it with seniors and knowing the warning signs will be a good starting place.

Focusing on this article's topic at assisted-living and healthcare conferences would be beneficial in bringing greater light and attention to the problem of cybercrime and seniors. Finally, as a further step, investigating the issue of cybercrime and seniors internationally can be approached to determine if this problem persists, or is greater. This deep-dive could be useful for those seniors traveling or deciding to reside outside the United States.

References

1. [1] Roberts, Andrew; Ogunwole, Stella; Blakeslee, Laura; Rabe, Megan; Most Older Adults Lived in Households with Computer and Internet Access, https://www.census.gov/library/stories/2018/10/snapshot-fast-growing-us-older-population.html, 2018
2. [2] Leiber, N., How criminals steal $37 billion a year from America's elderly, http://www.bloomberg.com/news/features/2018-05-03/america-s-elderly-are-losing-37-billion-a-year-to-fraud, 2018
3. [3] FBI.GOV, Scams and Safety: Fraud Against Seniors – https://www.fbi.gov/scams-and-safety/common-fraud-schemes/seniors, 2018
4. [4] Nurse, Jason; Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit, arXiv.org, 2017
5. [5] US Department of Justice (DoJ): Seven charged in international tech support scam. https://www.justice.gov/usao-sdil/pr/seven-charged-international-tech-support-scam (2017) 81.
6. [6] CENSUS.GOV, 2017 American Community Survey 1-Year Estimates – https://data.census.gov/cedsci/profile?q=New%20Jersey&g=0400000US34&table=DP05&tid=ACSDP1Y2018.DP05, 2017
7. [7] SENATE.GOV, Special Committee on Aging – https://www.aging.senate.gov/press-releases/senators-collins-casey-continuing-to-lead-fight-against-illegal-robocalls, 2019.
8. FBI Internet Crime Complaint Center (ICE), Internet Crime Report – https://pdf.ic3.gov/2018_IC3Report.pdf, 2018

LEAVE A COMMENT

0 Comments Sort by **Oldest**

Add a comment...

Facebook Comments Plugin

TABLE OF CONTENTS

ISSUE INDEX