



Cybersecurity Awareness to Bridge the Digital Valley

**Created by the Digital Valley Group:
Jonathan Berck, Katelyn Lansang, Jenn
Marron, Eugenia Schatoff, and Julin
Sharp**

Introduction

The Pattern Plan Forward report showed that technology was expanding quickly, even before COVID-19. The pandemic forced everyone to adapt to technology or face being left out, which highlighted the digital valley. As connectivity grew through the pandemic, so did the risk of being a victim of cybercriminals.



The report also indicated that all people should have access to training that helps them be digitally literate. We found through our research that many groups were receiving education in cybersecurity awareness, but that we were missing one key demographic. That demographic is senior citizens.

According to the U.S. Department of State, Ensuring the security of cyberspace is fundamental to protecting America's national security and promoting the prosperity of American people. Cyberspace is an integral component of all facets of American life, including the country's economy and defense. Yet private and public entities still struggle to secure their systems, and adversaries have increased the frequency and sophistication of their malicious cyber activities.

It is time to protect our seniors from cybercrimes as they are becoming the top target for such activity reported worldwide. They are vulnerable to internet scams and malware attacks. This can include many aspects of a senior's life, including physical health, mental well-being, and personal finances. Elderly individuals are more likely to be targeted by online financial fraud, and when they lose money, it is a higher amount than average, according to researchers. Protecting them from cyber-criminals is an area of growing concern.

What is Cyber-crime, Cyber-criminals & Cyber-security?

- **Cyber-Crimes:** criminal activities carried out by means of computers or the internet
- **Cyber-Criminals:** a person who engages in criminal activity by means of computers or the internet
- **Cyber-Security:** measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack

In the US Census latest estimates, the population aged 65 and older is over 50 million, which represents 16.5 % of the total population. In New York State, the population aged 65 and older makes up 16.1% of the population.

The technology habits and attitudes of a typical senior citizen makes them attractive to cyber criminals. Adults aged 65 and older have embraced technology, 73% of seniors are internet users, 46% use a smartphone. Unfortunately, most are not tech-savvy, only 26% of senior internet users feel “very confident” when using computers and surfing the internet. As more core services are shifted online by providers, many seniors who have yet to embrace the internet will be forced to in order to access such services.

The lack of tech savviness, believing that they will never become a cyber victim, underestimating the havoc a cyber-attack can create, make seniors incredibly attractive to cyber criminals. Some of the most popular scams are phishing/vishing, social engineering, social media scams, relative/grandchild/romance scam, Health care-insurance/Medicare fraud, just to name few. The FBI Internet Crime Complaint Center (IC3) released its 2020 Elder Fraud Report. According to the report, victims over 60 reported nearly \$1billion in fraud related losses in 2020, which represents 28% of all losses reported to the IC3. Unfortunately, year over year this number increases.

Background Statistical Significance

“Internet literacy” can be many things, from learning how to navigate to topics and sites of interest, to discerning good sources of information from “fake news,” to rules of the road for social media, and so forth.

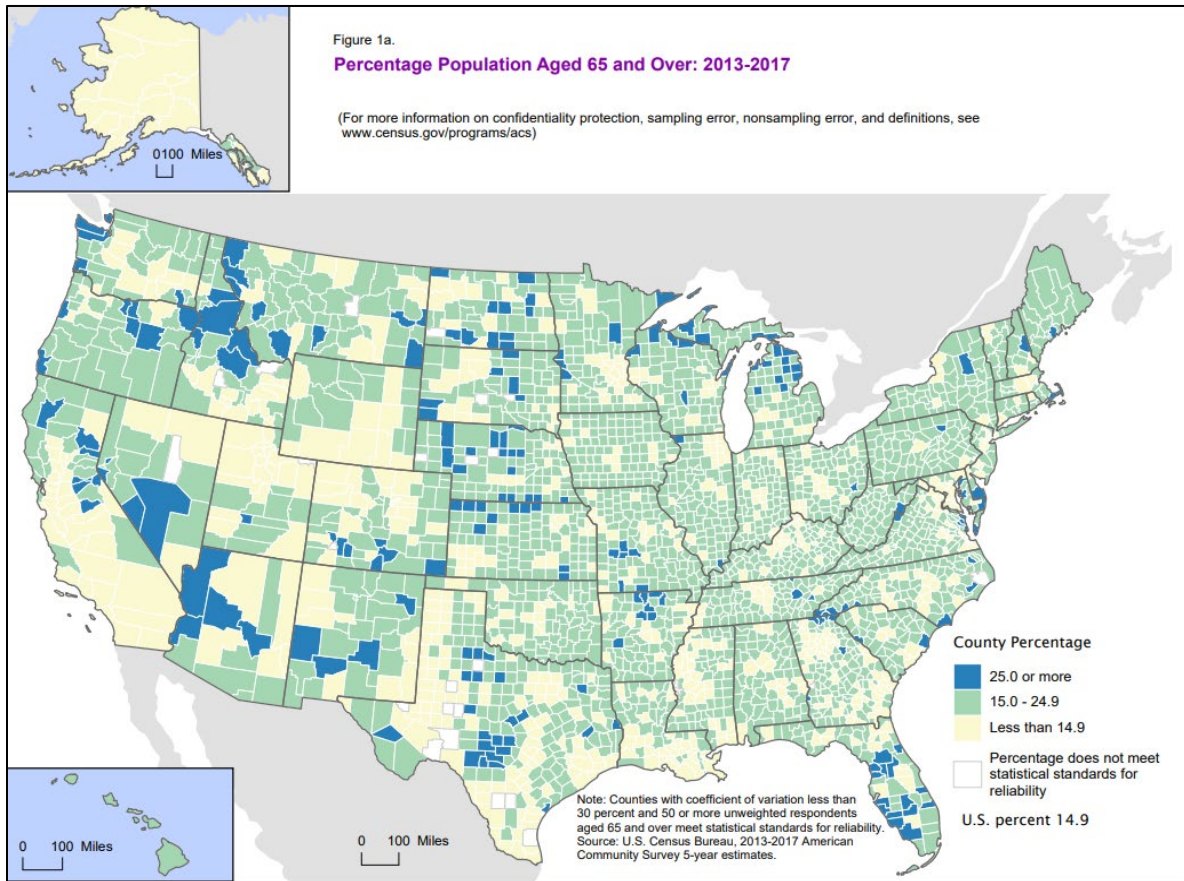
In addition, the need for “internet literacy” varies by demographic:

- By age, with younger people more internet savvy than oldsters;
- By accessibility, which correlates in part to age and in part to economic status;
- By economic means, with those lower on the income scale having limited access to broadband (and thus content that can only be reached through broadband, such as videos) and to time for surfing;
- By gender, which, though not a natural barrier, reflects social norms that put males in charge of technology.

Across all of these strata, some people prove susceptible to bad actors: phishers, who look to infiltrate systems or engage in ID theft; scammers who peddle snake oil or engage in confidence ploys to fleece the unwary; catfishers, who perpetuate false identities in order to influence thought or separate fools from their money; etc.

Anecdotally, the elderly seem to be the target of many scams, given their relative lack of familiarity with the medium.

We researched the statistical significance of senior citizens (65+) as a population demographic on the national, state, and Hudson Valley level. We also looked into the economic impact of cybersecurity.



Older adults in the United States were scammed out of \$1.7 billion through fraud schemes in 2021, a 74% increase from 2020, according to a report from the FBI’s Internet Crime Complaint Center.

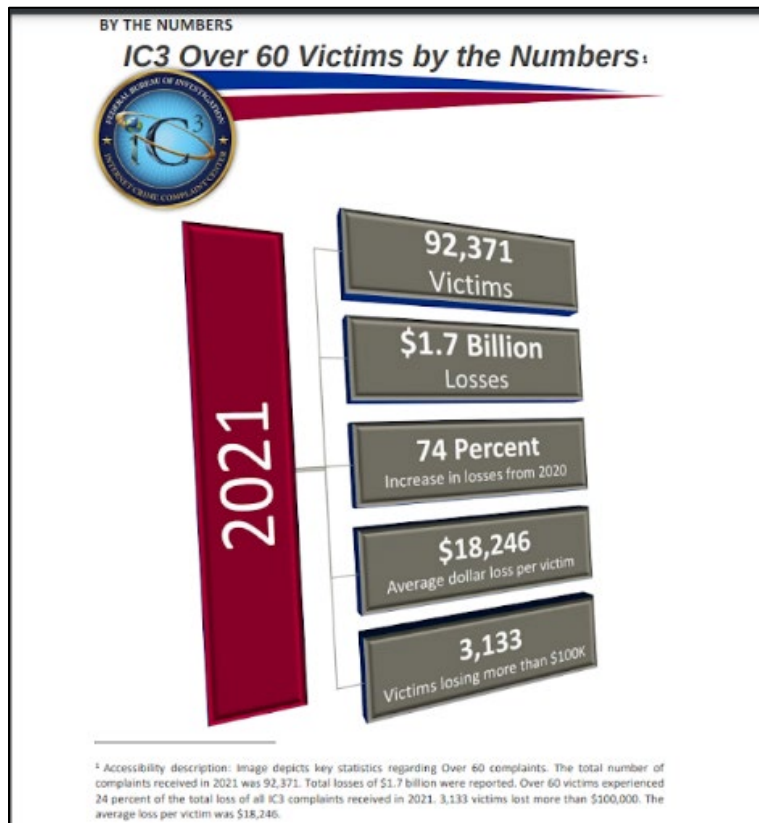
Last year, more than 92,000 victims aged 60 or more years reported losses to fraud schemes. The average dollar loss per victim was \$18,246, with 3,133 victims losing more than \$100,000, according to the 2021 IC3 Elder Fraud Report.

In New York State, according to the Center for Urban Future, from 2010-2020, the number of New Yorkers aged 65 and over increased by 26%, representing over 3.2 million residents.

According to the US Census Bureau, 14.9% of the US population is over the age of 65 over, representing over 54 million residents.

Existing Programs/Best Practices

Our team researched existing senior cybersecurity programs including a review of National, State, and Regional models. Established programs focus on senior citizens and cybersecurity using a variety of approaches.



National

Government: Resources available that include teaching materials, flyers, promotional materials and videos, all focused on reaching the individual senior and providing information, best practice, tips, tricks, and advice about cybersecurity and safety online. They provide examples of the most well known or typical scams, resources for victim support, and all work towards more public awareness. Some government resources provide data and track the reported cases of fraud against older Americans, supporting the large-scale economic impact of elder fraud in the US (the ICC for example).

Others provide action plans for next steps once you are the victim of a scam or crime, and they assist with reporting, documentation, and notification (the FTC for example).

- [Cybersecurity and Infrastructure Security Agency](#)- Older American Resources
- [The Federal Bureau of Investigation](#)- Elder Fraud Schemes
- [US Department of Justice](#) - Older Adult Financial Exploitation
- [US Department of Justice](#) - Elder Fraud Report 2021
- [Internet Crime Complaint Center](#) - File Elder Fraud Complaints
- [Federal Trade Commission](#) - Consumer advice regarding identity theft, helps with recovery plan of action and next steps.
- [Office for Victims of Crimes](#) - National Elder Fraud hotline with information about common scams, FAQ, awareness materials and resources.

Private:

Banking: Many banks provide resources to customers that include websites, videos, continuing education, and flyers about elder scams, cybersecurity, and fraud. They also provide victim support and ways of reporting fraud.

- [Morgan Stanley](#)
- [Huntington](#)
- [Seacoast](#)
- [Middlefield](#)
- [American Bankers Association](#)
- [Wells Fargo](#)

Nonprofit:

- [National Council on Aging](#) - First hand accounts of fraud, and tips for finance, money.

A poster for a "CYBER SECURITY FOR ADULTS" course. The title is in large blue letters at the top. Below it, a paragraph describes the course for beginners and intermediate users, covering information security, mobile devices, and wireless networks. It includes the date "Thursday, June 24th at 6:30PM" and the contact info "pearlriverlibrary.org - 845.735.4084". On the right side of the poster is a large blue padlock icon with a white 'T' inside. At the bottom left is the Pearl River Public Library logo, and at the bottom right is the "learning@PRPL LAB" logo.

CYBER SECURITY FOR ADULTS

This course is intended for beginners and intermediate users who want to increase their understanding of information security issues and practices with computers at home or in the office. All the up-to-date, need-to-know info: protecting mobile devices and wireless local area networks. Register for the Zoom link.

**Thursday, June 24th
at 6:30PM**

pearlriverlibrary.org - 845.735.4084

 Pearl River Public Library



Government: The State of NY provides resources New York State Office of Information Technology Services “Keeping Seniors Safe”

<https://its.ny.gov/newsletter/keeping-senior-citizens-safe-online>

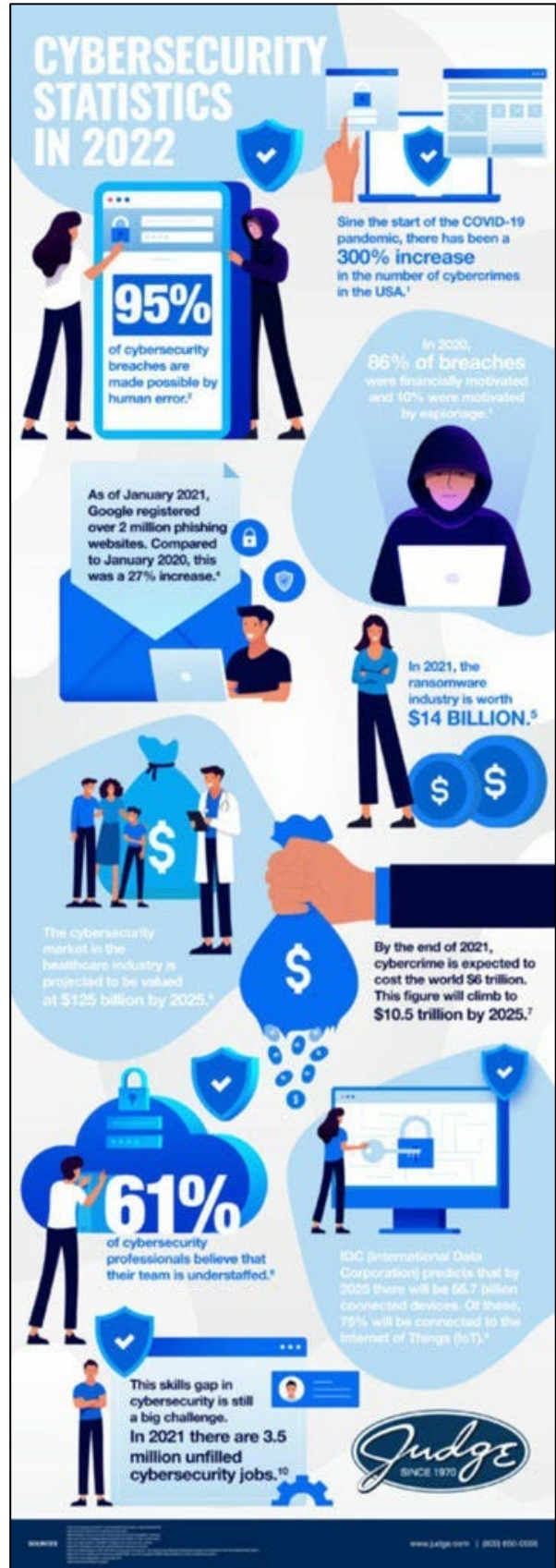
Hudson Valley

- Individual Counties provide resources for seniors on cybersecurity and elder fraud.
- [Rockland County Office For the Aging](#)
- Public libraries offer classes and one on one technology training to assist seniors.

Course Discussion

Strong skills in cybersecurity are important for everyone, yet the cybercrimes are constantly evolving. Students as young as kindergarteners are learning how to detect cyber scams in school, and industries are adding cybersecurity training as part of their traditional practices. However, we fail to train those who are no longer in school or the workforce. These people are targeted more frequently due to their lack of training.

To effectively reach senior citizens, a basic training course is recommended since most breaches happen due to human error. Senior citizens may not know the correct places to go to ensure that they remain safe online. In fact, based on discussions with people in our target demographic, all feel that courses in cybersecurity would be beneficial. We felt as though the course should be basic, with links to sites that would be routinely updated. The course should contain the following components.





Device Security

Password protection is very important when securing a device. People need to learn about how to properly create and store passwords so that they aren't at risk. Many times, people gravitate toward passwords that they can remember. Those passwords are easier to hack.

- Passwords should not include personal information
- Passwords should use numbers, symbols, and letters
- Passwords should be at least 16 characters long
- Passwords shouldn't be used more than once
- Passwords shouldn't use real words

Many people need to rethink the way they use passwords because 68% of people reuse the same password for multiple things. This creates risk of identity theft, data breaches, and more.



Protect from Phishing

Protecting yourself from phishing attempts is very important as well. Phishing attacks attempt to steal your money, identity, or passwords. Cybercriminals are very good at looking like legitimate companies or legitimate emails and sometimes even family or friends. It's important to identify potential phishing attempts.

- They typically use urgent calls to action
- Many times there are spelling or grammar mistakes
- They use generic greetings
- They may include links to click
- Email domains may be incorrect – like gmail instead of gmail

People should always report phishing emails using the “report message” feature in the email program that is used.



Internet Safety

Senior citizens are on the internet more often in 2022 than pre-COVID. They go online to do a multitude of things such as seeing pictures of their loved ones, making and having doctor’s appointments, banking, participating in social events, and more. To stay safe, there are many things that people can do.

- Get a quality antivirus software
- Only visit secure websites (HTTPS)
- Keep your operating system updated
- Always go to the source website, not a secondary website
- Ask for help if you’re unsure

We’ll end the course with a list of resources that people can visit to ensure that they are up to date with the current trends.

Ongoing Adoption

An awareness to cybersecurity is a critical foundation to digital literacy. Two factors must be considered for the basic training course to be effective: adoption and ongoing maintenance.

Once the basic training course is developed and published, the Patterns team will partner with local resources to ensure the training can be socialized to reach the target audience. It is recommended that the course be made available through the public library system and senior centers throughout the Hudson Valley. Further, Patterns could leverage the robust alumni and partner network to provide training access for an extended outreach. Example partners could include, but are not limited to local colleges, financial institutions, government agencies, and small

businesses. Through their employee and customer base, the training course could be shared to reach the greatest number of senior citizens within our region.

As previously stated, the digital world is ever-evolving, and the nature of technology and cybersecurity is rapidly changing. Staff or volunteers affiliated with Patterns for Progress will own the basic training course and perform a regular review to ensure the course remains current and effective. Ongoing maintenance is necessary to ensure the target audience is receiving the most up-to-date information as it relates to cybersecurity.

References

AARP - <https://www.aarp.org/home-family/personal-technology/info-2019/privacy-for-seniors.html>

Connect Safely - <https://www.connectsafely.org/seniors-guide-to-online-safety/>

County Percentage Population Age 65 and Over 2013-2017, US Census Bureau

Microsoft - <https://support.microsoft.com/en-us/windows/protect-yourself-from-phishing-0c7ea947-ba98-3bd9-7184-430e1f860a44>

Norton - <https://us.norton.com/internetsecurity-privacy-password-security.html>

Pattern For Progress report - <https://www.pattern-for-progress.org/reports/>

Safety Detectives - <https://www.safetydetectives.com/blog/the-ultimate-internet-safety-guide-for-seniors/>