



NASSAU
RE/IMAGINE



REIMAGINING RETIREMENT IN A POST-COVID WORLD

Creating Online Security for Seniors

And Their Hard-Earned Savings

Context

For years, the industry debated the relevance of the internet for seniors engaged in planning for, and actively managing, their retirement savings. Gradual adoption of technology by this age group gave way in 2020 to broad scale use of mobile devices, webcams, online chats, and social media. Seniors have learned how to connect with

family, church, and community via web calls. This includes higher online engagement with their financial services providers, which unfortunately opens the door for bad actors on the web to target a new set of individuals.


Our discussion forum

In a virtual forum on December 16, 2020, we discussed the rapid

adoption of digital technologies by seniors and the security risks it now presents for institutions charged with protecting the safety of their savings. We will summarize our discussion and provide a series of steps the retirement industry should consider pursuing in the next year.

Current industry landscape

Prior to the pandemic, our industry widely understood that the senior market represented one of the fastest growing segments for social media platforms. However, we have been slow to prepare for a rapid surge of adoption. One year ago, 70% of users over the age of 55+ visited us via a desktop device over a 7-day period. Taken



“What do we need to present on our websites to give confidence to the older prospect that their purchase will be secure?”

- Craig Simms, Forest Lake Consulting

broadly, the data foreshadowed an impending sea of change in behavior. Fast forward to the same week in 2020, we see that number drop to 53%. Users coming to us through smartphones has jumped from 29% to 47%. They use online chat with no hesitation. They will join us on Zoom calls, with their camera on, to discuss planning needs and policy information.

They do not typically ask if we have encrypted our chat conversations. They volunteer their policy numbers and other personal information that could easily be used for nefarious purposes by the wrong individuals. How we engineer and build our systems in the next few years will prove critical for the continued growth of our industry that is poised to invest considerable resources in this sector.

Ken Goldstein, our moderator and Clinical Instructor of Risk Management and Insurance, University of Hartford drove home this point. “If you fast forward 10 years, there’s going to be upwards of over \$84 billion being spent on technology products by folks that are in the 50 and up age group,” he observed.

Possible steps to provide more online security for seniors

DON'T MAKE BROAD ASSUMPTIONS BASED ON CHRONOLOGICAL AGE

In a recent episode of That Annuity Show with Moshe Milevsky, he discussed the difference between chronological and biological age of seniors. Biological age is a person’s age by date of birth. Chronological age is the relative age of the person and how they behave, particularly in the online environment.

Our speakers reinforced the point that we can’t address senior security issues with a single broad stroke. Timothy Zeilman, VP, Global Product Owner – Cyber, Hartford Steam Boiler, said, “The reality is that we don’t see that much difference in the usage of technology by seniors...Seniors use technology in the same way and for most of the same purposes that we see in other demographic groups, with some slight differences.”

IDENTIFY THE DIFFERENCES AND UNIQUE VULNERABILITIES


Sheryl O’Connor, CEO and Founder of Income Conductor

addressed this nuance. “The issue is not so much adoption, but proficiency and knowledge about the security threats that are out there,” she added.

“It sounds like we have identified at least some disconnect. I wonder how much the last nine months have contributed to that or if it’s been true for years,” observed Tom Buckingham, Head of Product & Operations at Nassau Financial Group. What segmentation of seniors should we use when we build a security strategy?

FOLLOW FAMILIAR SECURITY SOLUTIONS

We need to remember that our environment will be but one of many that seniors come to use and trust. The more we can build security tools that resemble platforms like Facebook, Zoom, and Amazon, we will find higher adoption rates among seniors.



“If you fast forward 10 years, there’s going to be upwards of over \$84 billion being spent on technology products by folks that are in the 50 and up age group.”

- Ken Goldstein,
University of Hartford

We should leverage good habits created by other influential parties. Sometimes those will be social media and shopping sites.

In other instances, they will be experiences created by other trusted authority sources like the doctor's office. "With the COVID pandemic, we're starting to see seniors getting concerned about things like, 'Hey, I'm not able to go into my physician's office, how can I meet with my physician to do things?'," said Paresh Nana from Google. The way hospitals and health insurance companies work with seniors will set their expectations for how we should work with them as well. What behaviors should we adopt to verify seniors and what should we realistically expect of them?

LOOK FOR TECHNOLOGY THAT WILL REDUCE THE PROBLEM

More advanced technology on the front of the user experience, as well as the back end, promises to make it harder for bad actors to attack seniors. "Distributed ledger technology could be a way to actually implement end-to-end security in terms of making sure that every transaction flow, every website, every URL that gets clicked, and every packet that flows through a network is digitally signed by some party or authority," Paresh Nana suggested.

BUILD A CX THAT INCREASES SECURITY FOR SENIORS

Yes, technology promises to help raise the bar for bad actors

hoping to find flaws in the system. However, a better design of our communication and engagement makes it difficult for criminals to impersonate us.

Craig Simms, Principal at Forest Lake Consulting would start with websites. "On the marketing side, what do we need to present on our websites to give confidence to the older prospect that their purchase will be secure?" he asked. Careful creation and implementation of brand voice guidelines offers a strong frontline defense for senior clients. Just as people have learned to identify phishing attempts or social media hacks by tone of voice, so too can seniors separate malicious communications if a corporation meticulously presents a coherent, broadly defined branded experience from acquisition to issue of service. Branding of a service experience grows even more important than it has in the past.

"As we focus on the insurance market, we've also seen that a lot of traditional insurance related processes like being able to submit a claim, getting underwritten for a new policy, for example, are also becoming virtualized, and seniors are starting to embrace more and more of that," observed Paresh Nana. What subtle branding, tone of voice, and/or engagement strategy will make it harder for the typical online criminal to copy?

"These can be scary events, and we want to give policyholders somebody to hold their hand a little bit, and provide them some emotional support."

- Timothy Zeilman, HSB

ENCOURAGE THE USE OF THE LATEST DEVICES

Historically, our industry has focused on building backward-compatible technology. We have traditionally supported browsers on our websites that may be 10 years old because our senior population used older machines. We proved slower than other industries to adopt security standards like MFA, in large part because of the demand it put on older consumers. Much of our approach has changed due to the ease of implementing higher levels of security, regulatory demands, and changing consumer behavior.

Our next step may be to aggressively push our clients to use much newer devices with automatic software updates to access our systems. "The nice thing about a lot of these Internet

connected devices is that they are able to download security patches over the air, and you can, in most cases, configure them to do it automatically,” said Paresh Nana. Do we require consumers to purchase devices or do we give them away as a small cost that potentially avoids massive security breaches and ensuing costs later?

INCREASE ORGANIZATIONAL IQ OF LATEST CRIMINAL THREATS

Given the rapidly changing angles of attacks, any area of institutions with customer engagement should be aware of the most recent strategies. Authorities increasingly report the use of unsuspecting individuals as key actors in criminal activity. “More and more, we’re seeing individual victims being used as part of criminal activity,” noted Edward Chang, Assistant United States Attorney. How can security teams generate

“Distributed ledger technology could be a way to actually implement end-to-end security in terms of making sure that every transaction that flows through a network is digitally signed by some party or authority.”

- Paresh Nana, Google

even higher awareness among employees of potential threats and effectively create a network of thoughtful observers?

TEST REVERSE SOCIAL ENGINEERING FOR SECURITY

Through many news stories and personal experiences, we have all grown aware of the fundamental security weakness of humans. All too often, the best security systems prove vulnerable to exploits enabled through relatively simple social engineering efforts. In the senior space, catfishing repeatedly proves to be one of the most common schemes to gain access to money, and has grown more sophisticated.

Paul Mackay, Chief Technology Officer for Nassau Financial Group added, “Folks are setting up fake IDs, posing as friends and family members and spamming people that way. I think there’s a lot of different angles now. It’s not just the email that we all know and love.” New devices and services like the Ring Doorbell, however, have shown the promise of engaging a community to detect criminal activity. Is there a strategy that better involves the senior community as a whole to detect attacks and alert others?

USE THE KIDS TO MAKE THE ADULTS SMARTER

Education of users remains one of the most important, but elusive solutions. Paul Mackay focused on this issue. “I think one of the biggest problems we have with

this age group is that there’s a woeful lack of knowledge, understanding, and trending for them. They’re really buying the most complicated device they’ve ever purchased. They think either Windows or Apple iOS is nice and easy to “use,” but they’re not really trained on it at all, and they are just exploited. How do you teach your 80-year-old mother-in-law to hover over the email address, check for spelling, and be certain domain name is right?” he asked. As a company, we have observed that seniors have grown more comfortable using services like Zoom thanks to the training efforts of their children.

During the forum, we discussed the possibility of using the children to train them to be more sophisticated in detecting threats. Children’s book author Ellen Sabin suggested that we teach the adults through interactions with even very young children. “Kids often are the Trojan horses that change adult behavior. Getting smart habits into homes, often through kids’ conversations can prove incredibly important,” she said. What organization or what set of individuals will prove most effective for increasing the cyber-risk awareness of seniors?

TRIAGE RISK FOR SENIORS

With online threats coming from multiple directions, we should help seniors focus on protecting their most critical assets first. “For individuals, that’s almost always going to be your bank accounts, your retirement accounts, and your assets,” advised Edward Chang.

MAKE IT EASY FOR INDIVIDUALS TO INSURE THEMSELVES

We should make it easier for seniors to obtain cyber insurance that will reduce the costs of recovery and repair due to an attack. It can also reduce an enormous amount of stress if this happens. Cyber insurance initially focused on protecting institutions,

not individual customers. However, in the last five years, the personal lines cyber insurance market has matured substantially. “There’s a very important service component to it. However, part of this, frankly, is emotional and psychological. These can be scary events, and we want to give policyholders somebody to hold their hand a little bit, provide them some emotional

support, walk them through what’s happened to them and help them understand it, so that they can better understand and deal with the situation,” offered Tim Zeilman.

Appreciation

We want to thank our distinguished panel for framing the discussion:

- Edward Chang, Assistant United States Attorney
- Paul Mackay, Chief Technology Officer, Nassau Financial Group
- Paresh Nana, Google
- Timothy Zeilman, VP, Global Product Owner – Cyber, Hartford Steam Boiler
- Ken Goldstein, Clinical Instructor of Risk Management and Insurance, University of Hartford (Moderator)

We also want to thank all the retirement industry leaders who joined us for this event and shared their unique insight on problems to solve and their investment opportunities. Also, this event could not have occurred without the leadership of Laura Dinan Haber, Program Manager of Nassau Re/Imagine, Ramsey Smith, Founder and CEO of ALEX.fyi, and the marketing team of Nassau Financial Group. Support and funding comes from Nassau Financial Group, Launc[H] and Symetra.

About the Author

Paul Tyler serves as the Chief Marketing Officer for Nassau Financial Group. He leads the branding, marketing, and digital engagement for the company. He founded the incubator Nassau Re/Imagine in 2019 as a place to help companies create the future of insurance today.

About Re/Imagine

Nassau Re/Imagine serves as incubator for companies intending to build a presence in Hartford. We actively support individuals and teams committed to building a vibrant insurtech ecosystem in the heart of our insurance community.



PODCAST



WEBSITE



VIDEO

Opinions expressed in this document reflect only those of participants and do not necessarily express the views or opinions of their employers or our sponsors.

SPONSORS



NASSAU

LAUNC[H]ARTFORD



ALEX.fyi