TESTIMONY

Ahmad Sultan
Affiliated Researcher, Center for Long-Term Cybersecurity

Before the 116th United States Congress, House of Representatives
Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Innovation
"Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help."
Cannon House Office Building, Room 310
Tuesday, June 25, 2019

Chairman Richmond, Ranking Member Katko and members of the Subcommittee. Thank you for inviting me here today to testify on the topic of cybersecurity challenges for state and local governments.

My name is Ahmad Sultan and I am testifying in my personal capacity as the author of a white paper published by the Center for Long-Term Cybersecurity. This paper was adapted from my Master's thesis at UC Berkeley's Goldman School of Public Policy, titled "Cybersecurity Awareness for the Underserved Population of San Francisco". The research was funded by the Center for Long-Term Cybersecurity, and it was commissioned by the City and County of San Francisco's Committee on Information Technology. The scope of my testimony is based on my expertise in cybersecurity before joining ADL. Any views presented here are not on behalf of or necessarily reflective of ADL positions or beliefs.

The topic of today's hearing should be of interest to government policy makers, researchers, and to individual targets of cyber-attacks. Thanks to the rise of mobile devices, the "digital divide" which is the gap between those who have access to online services and those who do not—has been shrinking, yet there exists a stark contrast in the online experience of low-income and high-income individuals[1]. As the adoption of digital services becomes more widespread, a new divide has emerged between those who can manage and mitigate potential cybersecurity threats and those who cannot.

While the increasing frequency of cyberattacks, which caused catastrophic data breaches[2] have led to organizations and governments investing billions of dollars to defend themselves, a critical part of society is falling through the cybersecurity cracks: underserved populations, defined as low-income earners, seniors, or immigrants.

This comes at a time when an increasing number of Americans' daily activities are facilitated and governed by internet services. Low levels of cyber-hygiene, which refers

[1] Digital gap between rural and nonrural America persists. (n.d.). Retrieved from https://www.pewresearch.org/fact-tank/2019/05/31/digital-gap-between-rural-and-nonrural-america-persists/

[2] Includes the 2015 Office of Personnel Management breach in which an estimated 21.5 million records of personally identifiable information were stolen, and the 2014 Sony Pictures Hack, which included 47,000 unique Social Security numbers.

to the best-practices and steps that internet users take to maintain system health and improve online security, pose serious challenges to the economic, social, and emotional wellbeing of underserved populations. weaken the security of systems in businesses and government, and pose existential threats to the democratic values of liberty, equality, and justice for all.

The findings of my own research into the topic of cybersecurity awareness, detailed later in this testimony, are alarming but not surprising. Underserved respondents in San Francisco have poor cybersecurity outcomes and do not follow best-practices. A large number of respondents do not know about the existence of common threats like viruses and online scams.

Yet, the interconnected nature of online networks means that poor cybersecurity outcomes for underserved populations can affect countless others. It not only deepens inequalities for those already most vulnerable to existing economic and social forces, but reduces trust in online services for all. With 5G networks and Artificial Intelligence systems promising smarter cities where key government services are powered by strong mobile connections and trained machine learning algorithms, the risk of ignoring poor cybersecurity outcomes are at an all-time high[3]. It is imperative that we work diligently towards raising awareness and educating underserved populations about cybersecurity.

Solutions exist but they require close coordination between Federal, state, and local governments.

WHY SHOULD GOVERNMENT CARE?

A large number of Americans from low-income households have low digital literacy and cybersecurity skills, and many do not own internet connected devices or have broadband internet at home. While internet adoption has been sporadic over the last few years[4], improved internet access in cities across the country means millions of Americans are expected to become active internet users, many of whom will have little knowledge on cybersecurity. Even as connectivity increases, the cybersecurity divide threatens to exacerbate existing inequalities.

According to recent estimates by Pew[5], roughly three-in-ten American adults with household incomes below $30,000 a year (29%) do not own a smartphone. More than

[3] Toward AI Security: Global Aspirations for a More Resilient Future - CLTC UC Berkeley Center for Long-Term Cybersecurity. (n.d.). Retrieved from https://cltc.berkeley.edu/towardaisecurity/

[4] Demographics of Internet and Home Broadband Usage in the United States. (2019, June 12). Retrieved from https://www.pewinternet.org/fact-sheet/internet-broadband/

[5] Digital divide persists even as lower-income Americans make gains in tech adoption. (n.d.). Retrieved from https://www.pewresearch.org/fact-tank/2019/05/07/digital-divide-persists-even-as-lower-income-americans-make-gains-in-tech-adoption/

four-in-ten do not have home broadband services (44%) or a traditional computer (46%). And a majority of lower-income Americans are not tablet owners. By comparison, each of these technologies is nearly ubiquitous among adults in households earning $100,000 or more a year, coupled with higher levels of educational attainment and cybersecurity outcomes.

The lack of cybersecurity preparedness for large swathes of underserved populations is concerning for a variety of reasons. These include:

- Cybersecurity inequality: Underserved populations who tend to be the most vulnerable to real world social and economic forces are also the most vulnerable to cyber threats like scams, viruses, harassment, and disinformation. Like a mirror to the physical world, low levels of cyber-hygiene and cybersecurity knowledge are associated with low income-households and low education attainment. Most figures on poor cyber outcomes are also underreported. This is because many underserved users are unaware of cyber threats and do not know if their devices have been hacked or if they have been victim to a cyber scam. This inequality in cybersecurity outcomes is a form of market failure that governments need to correct through trainings and strategic public-private partnerships.

- Digital Inequality: Internet users exist on a cybersecurity spectrum that includes users who can defend against cyber threats and those who cannot. Low levels of cyber-hygiene create a distinct online experience filled with fear, low confidence, and distrust that I have seen lead to a complete withdrawal from internet use. Without addressing the underlying causes for the distinct differences in the online experience, underserved populations are being denied a wide range of opportunities and conveniences.

- Diminished Economic Opportunities: Fearing cyber threats, large numbers of underserved users are not taking advantage of economic opportunities on the internet. These include job search services like LinkedIn, listing platforms like Craigslist, social networking, email, or online banking. All these services are crucial to remaining competitive in today's job market. They are also excluded from obtaining lower prices through online shopping, online health services, and digital financial inclusion services.

- First Amendment Protections: The internet, and social media platforms in particular, are viewed as the new public squares. Cyber threats can be used to silence speech, create fear, and disrupt key Democratic processes.

Yet, poor cybersecurity outcomes are not exclusive to underserved populations as the lack of awareness of best-practices and capacity for negligence exists at all levels of society. A holistic approach is required where cybersecurity outcomes are addressed at a societal level, much like public health issues. This is because poor cybersecurity practices can cause viruses, scams, and data breaches to spread and impact countless

people, devices, infrastructure and entire organizations in unpredictable ways. The increasing frequency of attacks on local government systems are a product of poor cyber-hygiene, even in populations that have higher digital literacy. In just the last three years, the state and local governments of Colorado, Baltimore, Atlanta, San Francisco, Jackson County, Riviera Beach, Imperial County, Sammamish have had to deal with ransomware attacks[6][7].

The reason cybersecurity researchers and experts adapt lessons and concepts, like cyber-hygiene, from public health literature is because of the unique interconnectedness of society and networks. Human error is the weakest link in both fields and has the potential to inadvertently cause unimaginable damage. While the underprivileged in society are disproportionately affected and most likely to be targeted by attackers and scammers, awareness of cybersecurity threats and best-practices needs to seep into public discourse at a societal level. Digital literacy is not enough, it needs to be paired with cybersecurity awareness.

This is not just a state and local government problem. Cyber vulnerabilities exist across the country, and cyber-attacks can flow seamlessly between state and city lines. It is incumbent upon Federal, state and local governments to provide programs and engage in strategic partnerships that aim to improve cybersecurity outcomes.

HOW CAN THE FEDERAL GOVERNMENT HELP?

State and local governments face many constraints to improving cybersecurity awareness. These include fiscal and budgetary challenges, lack of social and technical expertise, low organizational capacity, and geographically bound networks. While I provide a detailed list of recommendations in a later section of this document, some ways that the Federal government can assist state and local governments include:

- Direct funds towards local cybersecurity awareness trainings: Local governments can partner with nonprofits to roll out trainings aimed at improving the cybersecurity knowledge and outcomes for underserved residents. These trainings can be expensive as they require devices and equipment, qualified trainers, monetary or other incentives for participants, and fixed locations scattered throughout the city. Local government budget might not be able to justify prioritizing these expenses.

- Design baseline training programs: Not all state and local governments have the capacity or expertise to design a cybersecurity training program. The Federal government should work with local governments to design a baseline training

[6] Calvert, S., & Kamp, J. (2019, June 07). Hackers Won't Let Up in Their Attack on U.S. Cities. Retrieved from https://www.wsj.com/articles/u-s-cities-strain-to-fight-hackers-11559899800

[7] As More Governments Get Hacked, Concerns Grow Over Mounting Costs. Retrieved from https://www.governing.com/topics/finance/gov-government-costs-hacked.html

program which details the core topics that all training programs should address. While the Federal government should design the baseline topics and curriculum, the programs should be informed by and tailored to the ground realities of each city and should not limit any government from going further than its selected baseline topics.

- Develop and rollout public awareness campaigns: Public awareness campaigns are more cost-effective and can scale better to reach larger audiences when developed centrally. This streamlines the process of disseminating content to schools, broadcast TV, online and physical publications, social media platforms, and radio.

- Coordinate public-private partnerships: The Federal government is uniquely positioned to work with private technology companies to create advice resources, cross-company collaborations in areas like phishing scams and coordinated disinformation campaigns, and technological solutions like cybersecurity chat bots and apps for smart-phones that no longer receive security updates. As I will explain later in this testimony, underserved populations tend to place a high level of trust on advice resources provided by private technology companies. It would be highly inefficient for every state and local government to individually approach technology companies for their own respective solutions.

STUDY: CYBERSECURITY AWARENESS FOR UNDERSERVED POPULATIONS

A growing number of cities across the United States have invested in digital literacy training programs that aim to educate underserved populations in the basics of computer usage and commonly used software[8]. Such programs often combine the provision of digital services, such as free public wi-fi, with digital literacy training to help groups who are at risk of digital and social exclusion. These initiatives are often led by nonprofits and local governments and aim to improve citizens' skills and confidence, as well as increase their motivation to engage in online activity.

San Francisco has a digital literacy initiative under its Office of Digital Equity[9], where the City government works with local partners in the nonprofit space to provide digital literacy training to its residents, the vast majority of whom come from low-income households, are immigrants, and seniors. Early discussions with City residents were revealing: They expressed frustration at their inability to prevent and resolve cyber-attacks such as phishing scams, viruses, and harassment. They were afraid of using important online services like banking apps and social media platforms.

[8] https://www.digitalinclusion.org/digital-inclusion-trailblazers/
[9] https://sfcoit.org/digitalequity

The theory of change in digital literacy programs normally involve encouraging internet use to increase employment, education, creativity and entrepreneurship. But vulnerable populations are easily discouraged from using important internet services when faced with complex threat vectors.

We widen digital inequities and reduce the efficacy of digital literacy trainings when we do not actively teach cybersecurity. Moreover, by neglecting the duty to educate and inform, we leave a large portion of the population at the mercy of bad actors who can exploit digital vulnerabilities for their own gain.

RESEARCH FINDINGS

I conducted a survey of underserved residents in the City and County of San Francisco to understand the scope and nature of the underserved communities' cybersecurity outcomes, and to create evidence-based solutions. These residents were either low-income earners ($25,000 household income or less), senior citizens (65 years of age or older), or foreign language speakers (whose primary spoken language is not English). The 48-question survey was designed to gauge the scope and nature of residents' cybersecurity outcomes, and to understand their cybersecurity knowledge and abilities.

A total of 295 respondents were surveyed. This included 153 respondents from the underserved population. While this is not technically a representative sample, these were the maximum number of respondents I could survey who were enrolled in digital literacy programs across San Francisco. Their experiences revealed through surveys, semi-structured interviews and roundtable discussions reflect social and structural inequities that have persisted for too long. In addition to the 153 underserved respondents, 142 respondents from the comparison group were also surveyed.

POOR CYBERSECURITY KNOWLEDGE AND SKILL LEVEL

Underserved respondents generally have a poor understanding of basic cybersecurity concepts such as online scams and viruses. They also have low skill level and motivation to follow best practices as gauged by cyber-hygiene relevant questions. These include setting a complex password for online accounts and employing preventative methods when reading and interacting with the contents of an email.

I designed a Knowledge and Skill index to make meaningful comparisons between the underserved and comparison group respondents. The maximum combined score for the Knowledge and Skill index is 18.0.

- Average cybersecurity Knowledge and Skill index score for the underserved respondents = 9.0/18
- Average (and Median) cybersecurity Knowledge and Skill index score comparison group respondents = 15.0/18

Underserved respondents struggle with fundamental cybersecurity knowledge questions. When asked about their knowledge of core cybersecurity concepts, 20

percent indicated they did not know about online crime, 21 percent were not familiar with email spam, 26 percent did not know about computer or phone “viruses,” and 31 percent did not know about anti-virus software. Respondents indicated they did not understand the risks associated with sharing their private account passwords or writing down their passwords on paper.

VICTIMS OF CYBERCRIME

A large number of respondents from the underserved group reported being targets of cyber scams and internet viruses. Respondents provided information about the types of personal information that has either been stolen from them online, or that they have divulged to a complete stranger online. Together, these results paint a picture of an underserved population in San Francisco that is highly vulnerable to internet fraud.

- Nearly 26 percent of the underserved respondents reported that they have been a target of a cyber scam, compared with 15 percent for the comparison group.
- Nearly a third (31%) of those scammed have been scammed three times or more.
- Forty percent of underserved respondents reported that their computer and/or phone has been infected by a virus at least once.

AWARENESS OF CYBERCRIME VICTIMHOOD

Although many underserved respondents reported being a victim of cybercrime, an equally large number of respondents are not aware whether they have been a victim to a cyber scam, if their devices have ever had a virus, or if they ever provided personal information to a complete stranger online.

- Nineteen percent of underserved respondents do not know if they have ever been a victim to a cyber scam.
- Forty-one percent do not know if their device has ever had a virus.
- Forty-four percent think they have provided personal information to complete strangers online but cannot remember the exact details.

INTERNET WITHDRAWAL IS RELATED TO LOW-CONFIDENCE

A significant portion of the underserved sample self-assess as having either “high confidence” (36 percent) or “low confidence” (38 percent) in their ability to protect themselves from online crime. High-confidence respondents can be described as being “over-confident” in their cybersecurity skills while demonstrating poor levels of precaution and possessing low levels of cybersecurity knowledge, while “low-confidence” respondents can be described as being “overly-concerned” about existing risks online while possessing and demonstrating above-average cybersecurity knowledge and precaution.

- Self-assessed “low-confidence” underserved respondents are more concerned about the existence of cybercrime than underserved and comparison group respondents.
- For example, 47 percent of low-confidence underserved respondents do not use online banking due to cybercrime, compared to eight percent in the comparison group. These services also include social media use, downloading software, and email.
- This suggests that trust and security play a larger role in determining online service usage for the underserved as compared to the comparison group.

CYBERSECURITY ADVICE RESOURCES DETERMINE CYBERSECURITY OUTCOMES

Underserved respondents tend to rely on informal resources for advice about cybersecurity which leads to worse cybersecurity outcomes. In fact using online resources for advice on cybersecurity is expected to increase a respondent’s cybersecurity index score by roughly 0.23 points. The only other predictor with a statistically significant coefficient is Educational Attainment—the higher the level of schooling achieved, the higher will be the cybersecurity index score.

- 39 percent of underserved respondents rely on friends/relatives for cyber advice
- Only 21 percent of underserved respondents refer to websites, and seven percent refer to government websites.
- More than a third of respondents (34 percent) do not seek cybersecurity advice from any resource. Comparison group respondents are more likely to seek help (82 percent) and are more than twice as likely to rely on websites for cybersecurity advice (48 percent).

RECOMMENDATIONS

Federal, state and local governments have a variety of options and approaches available to improve cybersecurity awareness of underserved populations.

GAIN AN UNDERSTANDING OF THE SITUATION IN YOUR COMMUNITY

The Federal government should work with cities seeking to improve cybersecurity awareness of local underserved populations to gain a baseline understanding of their specific situation. They can do this by designing and directing funds towards surveys or informational workshops to assess major areas of interest and/or lack of knowledge among residents. Based on my experience, I recommend partnering with local community organizations that serve low-income residents, English language learners, and senior citizens. In addition to assessing cybersecurity awareness, use this initial outreach as an opportunity to assess what modes of training (e.g. one-hour workshops, half-day workshops, etc.) might be most suitable for different constituencies. It is also

important to identify what translation or technology resources might be required to facilitate trainings for the largest number of underserved citizens.

DEVELOP TAILORED TRAININGS TO BOOST CYBERSECURITY AWARENESS

Many cities already offer (or are planning to offer) digital literacy trainings. My findings suggest that such programs should include explicit targeted cybersecurity awareness and training components, which the Federal government can direct funds towards. A customized cybersecurity awareness program that is tailored to the specific needs of the community—with topics and content prioritized on research-based understanding of the local community's specific needs—could help improve the knowledge and skill level of participants, which would improve cybersecurity outcomes and increase internet service engagement. Potential long-term benefits include improved economic and social indicators for members of the underserved population.

Trainings should be customized for different audiences, and should target areas where citizens possess lower levels of digital literacy. Trainers should also incorporate an awareness of the cultural sensitivities and trust habits of the disparate communities. Analysis of survey responses from San Francisco, for example, suggests that respondents from different communities access different knowledge sources. For example, while a larger percentage of Hispanic/Latino respondents rely on teachers for advice on matters of cybersecurity, African American and Caucasian respondents said they are more likely to refer to websites, while Asian respondents are more likely to refer to friends and relatives.

DEVELOP A PUBLIC SERVICE CYBER-HYGIENE CAMPAIGN

The Federal government can promote cyber-hygiene awareness and suggest best-practices through public service announcements and a cybersecurity campaign on television, in schools, digital platforms, public libraries, radio, and other communication channels.

PUBLIC-PRIVATE PARTNERSHIPS

In addition to providing training to residents directly, the Federal government has the opportunity to partner with private-sector technology companies and service providers to address system-level cybersecurity concerns, such as the technological protections that are built into devices and systems. Effective system-level protections make it easier for residents to maintain good cyber-hygiene.

DEVELOP A CYBERSECURITY ADVICE WEBSITE

Members of the public already have access to reliable and free resources for cybersecurity, including the United States Computer Emergency Readiness Team

advice website[10]. Yet in many cities, information about cybersecurity and related resources is disaggregated and difficult to find.

The Federal government can work with private-technology firms to develop reliable websites that provide cybersecurity advice. It may be feasible to develop a phone chatbot that can help residents with basic information security questions[11]. Such chatbots can be designed to communicate in several languages, and provide clearly defined answers on core cybersecurity knowledge questions, as well as offer step-by-step instructions based upon best-practices. Chatbots should also be designed to be highly secure and transparent, with reminders to users not to share personally identifiable information, as this software could in theory be vulnerable to attacks aimed at capturing data and subverting the quality of information provided[12].

PARTNER WITH COMPANIES TO DEVELOP APPS FOR USE ON OLDER AND UNSUPPORTED PHONES

Underserved populations tend to use older smartphones that are often unsupported by software makers. As a result, older smartphones are not guaranteed to get new security updates, and some software updates for older devices are not compatible with new phones[13]. This is especially a problem for users with Android phones, where the market consists of hundreds of smartphone manufacturers using different and modified versions of Android's OS. According to Google's own figures, two-thirds of Android devices worldwide run older versions of the OS that are no longer receiving security updates[14]. For Apple's iOS devices, that figure is five percent[15]. Apple does provide software updates to phones older than five years. Even if they follow best practices in cyber-hygiene, users with older smartphones are still highly vulnerable to cybercrime because patches are not automatically installed for known vulnerabilities.

The Federal government should engage smartphone manufacturers like Apple, Google, and Samsung to develop workarounds that protect older smartphones that cannot accept the latest round of security updates. These workarounds could include prompting older smartphones to activate device encryption settings, password manager apps,

---

[10] "Tips." Virus Basics | US-CERT. Accessed September 11, 2018. https://www.us-cert.gov/ncas/tips.

[11] Security chatbots have become increasingly popular over the last few years. For example, Endgame developed Artemis, a language agnostic platform that integrates to Amazon's virtual assistant Alexa and provides cybersecurity advice to analysts . See "Four Ways Chatbots Are Transforming Cybersecurity." Endgame. June 16, 2017. Accessed September 11, 2018. http://www.endgame.com/blog/executive-blog/four-ways-chatbots-are-transforming-cybersecurity.

[12] "Expect a New Battle in Cyber Security: AI versus AI." Symantec. Accessed September 11, 2018. http://www.symantec. com/blogs/expert-perspectives/ai-versus-ai.

[13] For more on security updates and smartphone compatibility, refer to Emspak, Jesse. "When Does an Old Smartphone Become Unsafe to Use?" Tom's Guide. April 09, 2017. Accessed September 11, 2018. http://www.tomsguide.com/us/oldphones-unsafe,news-24846.html.

[14] "Distribution Dashboard | Android Developers." Android Developers. Accessed September 11, 2018. https://developer. android.com/about/dashboards/.

[15] Apple Inc. "App Store." Purchase and Activation - Support - Apple Developer. Accessed September 11, 2018. https:// developer.apple.com/support/app-store/

virtual private networks (VPN), and two-factor authentication software. Companies that develop operating systems should also be asked to develop stricter app security review and enforcement guidelines that can review the catalog of existing apps as well as newly submitted apps for security bugs.

As a potential challenge, Google has little control over the updates sent to Android phones in which the OS has been heavily modified by the manufacturer, who in many cases retains control over software updates. The Federal government will need to develop a strategy with Google to reach smartphone manufacturers who are outside of the Google software update landscape.

CREATE A DIGITAL PHISHING/SCAM COALITION

More than half of all emails are spam[16]—and that figure continues to rise. Spam is the primary delivery mechanism for cyber-attacks like phishing and malware[17]. And while phishing attacks disguised as fake invoice emails are a popular form of phishing, there are nine other forms of phishing emails that are harder to spot, such as Mail Delivery Failure emails and order emails. In fact, reports of W-2 tax filer phishing scams—one of the most dangerous and effective email phishing scams, according to the IRS[18]—increased by 870 percent between 2016 and 2017.

To address this challenge, the Federal government should build coalitions of organizations that can target popular and successful phishing scams. Models for such public-private initiatives include the Digital PhishNet initiative, developed jointly by the FBI's National Cyber-Forensics & Training Alliance[19], and the Advance Fee Fraud Coalition, developed by African Development Bank, Microsoft, Yahoo, and the Western Union Company[20]. Companies should target overlapping scams and phishing efforts by utilizing contacts in the private sector.

Federal government officials can also partner with international initiatives such as the Unsolicited Communications Enforcement Network (UCENET)[21], which identifies and shares threats to the broad online community and facilitates enforcement compliance

---

[16] "Latest Intelligence for August 2017." Symantec. Accessed September 11, 2018. https://www.symantec.com/connect/ blogs/latest-intelligence-august-2017.

[17] "2018 Internet Security Threat Report." Symantec. Accessed September 11, 2018. http://www.symantec.com/securitycenter/threat-report.

[18] "Dangerous W-2 Phishing Scam Evolving; Targeting Schools, Restaurants, Hospitals, Tribal Groups and Others." Internal Revenue Service. Accessed September 11, 2018. http://www.irs.gov/newsroom/dangerous-w-2-phishing-scam-evolvingtargeting-schools-restaurants-hospitals-tribal-groups-and-others.

[19] The Digital Phishnet (DPN) collects and develops intelligence regarding high priority and sophisticated phishing and identify theft schemes. DPN uses threat intelligence received from approximately 300 companies. For more visit: http:// www.ncfta.net/

[20] 0 The collaborative effort was designed to educate internet users so they are better able to protect themselves against fraudulent activities online and to improve INTERPOL's data collection efforts on cyber fraud. For more on this: http:// www.affcoalition.org/

[21] Formerly known as the London Action Plan (LAP): https://www.ucenet.org/history/

checks. Private-sector representatives are encouraged to designate a spam enforcement contact, coordinate with law enforcement agencies, and report on new technology trends that affect anti-spam strategies.

CONCLUSION

It has been an honor to appear before this distinguished panel of policymakers and practitioners. Thank you, Chairman Richmond and Ranking Member Katko, for your dedication to addressing cybersecurity vulnerabilities, and for thinking about ways in which the Federal government can assist state and local efforts.

Promoting cyber-hygiene through trainings, public service initiatives, and public-private partnerships can lead to significant gains in the lives of underserved populations and protect businesses as well as government systems from cyber threats. But to achieve these gains, state and local governments will require support and guidance from the Federal government. It is my hope that policy makers recognize the challenges ahead and rise to the occasion. Thank you and I will be happy to answer any of your questions.

TESTIMONY

Ahmad Sultan
Affiliated Researcher, Center for Long-Term Cybersecurity

Before the 116th United States Congress, House of Representatives
Committee on Homeland Security, Subcommittee on Cybersecurity, Infrastructure Protection and Innovation
"Cybersecurity Challenges for State and Local Governments: Assessing How the Federal Government Can Help."
Cannon House Office Building, Room 310
Tuesday, June 25, 2019

Table 1: Cybersecurity Knowledge between Underserved and Comparison Group respondents

Cybersecurity Knowledge	Underserved	Comparison Group
Know what Online Crime/ or Scams are	80%	96%
Know what Email Spam is	79%	96%
Know what Computer or Phone viruses are	74%	98%
Know what anti-virus software are	69%	93%

Table 2: Phishing Prevention Best-Practices between Underserved and Comparison Group respondents

Best-Practice	Underserved	Comparison Group
Do not check to see if the email address of the sender is suspicious?	35%	5.0%
Do not check the grammar of the email to see if it is suspicious?	35%	7%
Do not hover the mouse arrow over a link to check if it is suspicious?	57%	25%

Do not inspect the 'Subject line' to check if it is suspicious?	37%	9.0%

Figure 1: Withdrawal from Online Services between Underserved (US), Low-Confidence Underserved (LC), and Comparison Group (CG) respondents

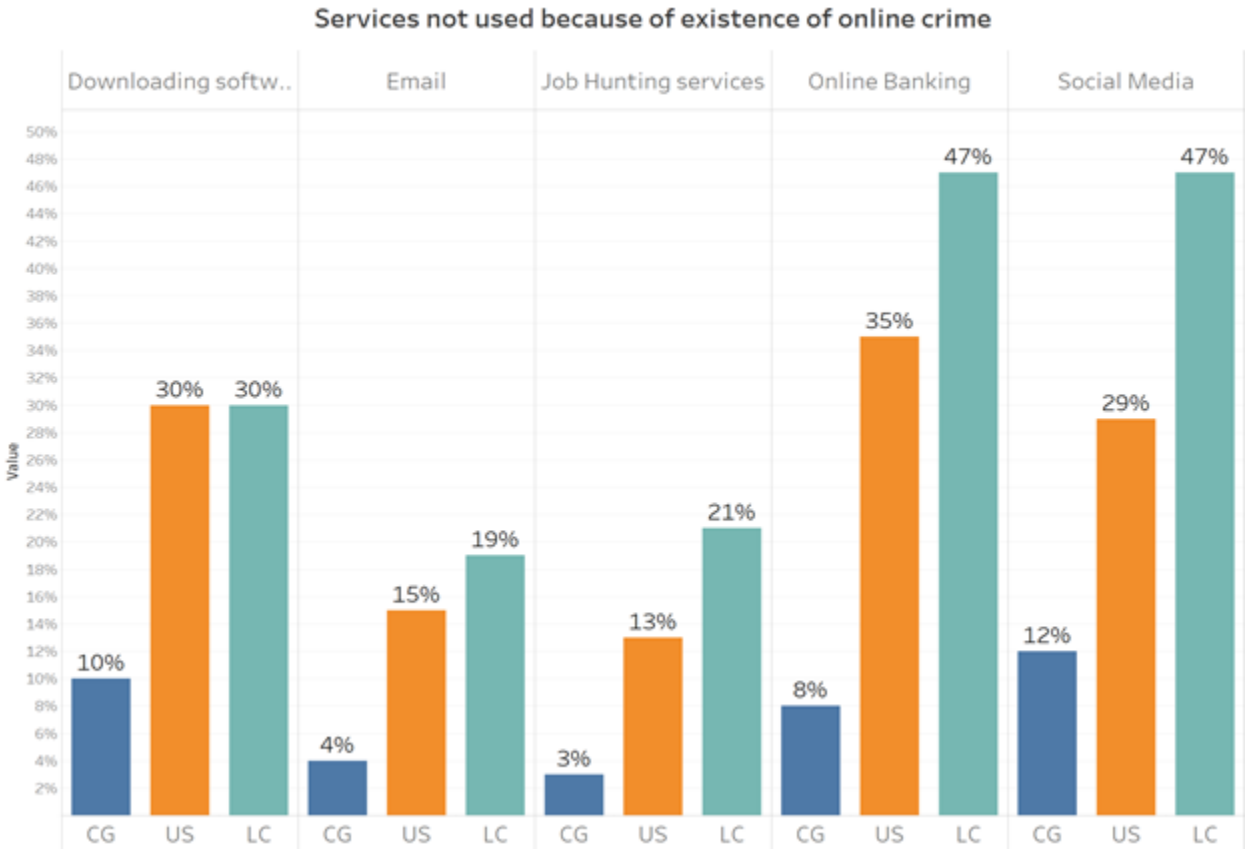

Table 3: Requirements for a successful cybersecurity training program

Before Training	
1	Target training location by income and digital literacy and cybersecurity outcomes
2	Engage with community leaders to finalize training locations
3	Training-of-Trainers

4	Course Design
During Training	
5	Provide realistic information on threat landscape
6	Avoid “Fear Appeals”
7	Explain benefits of best-practices
8	Provide credible, reliable and trust-worthy advice resources
9	Provide advice resources that distinguish between OS and device
10	Collect endline data on cybersecurity Knowledge and Skill in last session
After Training	
11	Use endline data to choose next training locations
12	Use endline data to further refine cybersecurity trainings curriculum