CENTER FOR LONG-TERM CYBERSECURITY

CLTC WHITE PAPER SERIES

Improving Cybersecurity Awareness in Underserved Populations

AHMAD SULTAN

Front cover art © Kathy Anselmo

CLTC WHITE PAPER SERIES

Improving Cybersecurity Awareness in Underserved Populations

AHMAD SULTAN

CLTC
Center for Long-Term Cybersecurity

CENTER FOR LONG-TERM CYBERSECURITY

Contents

Executive Summary

Thanks to the rise of mobile devices, the “digital divide”—the gap between those who have access to online services and those who do not—has been shrinking. Yet 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.

Indeed, while the rising frequency of cyberattacks—including the distribution of malware, phishing, and data breaches[1]—has led organizations and nation-states to invest billions of dollars in their cyber-defense and offense capabilities, very little of that effort has been aimed at under-resourced communities where residents are extraordinarily vulnerable to cyber-crime—and may suffer disproportionately from its consequences.[2]

This paper, published in partnership with the UC Berkeley Center for Long-Term Cybersecurity, highlights research indicating that “underserved” residents in San Francisco, California—including low-income residents, seniors, and foreign language speakers—face higher-than-average risks of being victims of cyber attacks. They are less likely to know whether they have even been victimized by a cyber attack, and they have lower awareness of cybersecurity risks. Partly as a result, they are less likely to access online services. This cybersecurity gap is a new “digital divide” that needs to be addressed—with urgency—by the public and private sectors alike.

We offer a framework of recommendations for how officials in U.S. cities can promote cybersecurity awareness among vulnerable undeserved populations. Drawing on our research in San Francisco, we provide a summary of our research methodology and findings, an implementation strategy for training, and a discussion of potential challenges that cities may face. The report is intended to help city leaders understand how they could better understand this issue in their own cities, and how they might forge public-private partnerships to address cybersecurity concerns at the system level.

Assessing the Challenge: San Francisco

Cybersecurity is a major concern for individual citizens, as digital technologies are increasingly essential for navigating everyday life. Digital technologies are necessary to gain access to banking, health services, educational programs, and other resources. As more services are made available only to those with mobile phones, those citizens who do not have access to these services risk falling behind economically.

To understand the scope and nature of the underserved communities' cybersecurity outcomes, we conducted a survey of 'underserved' residents in the City and County of San Francisco (CCSF). 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. The survey questionnaire was targeted at two different respondent-types: representatives of underserved groups in San Francisco, as well as members of a comparison group (CG).

Underserved Residents: The questionnaire was provided to eight San Francisco-based, community-focused non-profit organizations. These organizations cater to residents from low-income households, foreign-born and foreign-language speakers, and seniors. The questionnaire was translated into Spanish and Chinese for foreign-language speakers. The total survey response target for this population was 153 respondents.

Comparison Group: For comparison, we surveyed a group of respondents who are less likely to be in any of the "underserved" categories. Results from this group were collected using an online Google form and an Amazon Mechanical Turk ("MTurk") form. The Google form was distributed to students at the University of California, Berkeley Goldman School of Public Policy and to the staff of CCSF-based, community-focused non-profit organizations. The MTurk form was distributed to users. The comparison group sample was composed of 142 people.

FIGURE 1 **Characteristics of Survey Groups**

	Underserved (US)	Comparison Group (CG)
Household income less than $25,000/year	45%	20%
65 years of age or older	35%	8%
Primary spoken language not English	38%	2%
College Graduate/Advanced Degree	42%	74%
Android Owners	50%	54%
Apple Owners	37%	37%

FIGURE 2 **Survey Uptake Results: Community Organizations**

Non-Profit Organization	Survey Format	Respondents
San Francisco Public Library	In-person, Single session	21
Code Tenderloin	In-person, Single session	17
Onlok Senior Center	In-person, Single session	21
Tenderloin Tech Lab	In-person, Multiple sessions	24
San Francisco Community Living Campaign	In-person, Multiple sessions	23
Cameron House	In-person, Multiple sessions	20
The Women’s Building	In-person, Multiple sessions	1
Chinese Newcomers Service Center	Online Google Form survey	26
Total Respondent Count		**153**

Our findings[3] suggest that:

- A significant percentage of underserved residents likely have been victim of a cyber scam, and many may have been scammed multiple times.
- Underserved residents often possess an incomplete understanding or distorted view of the online security landscape. A large number of respondents were unable to comment on cyber-crime impact because they did not understand basic cybersecurity concepts. Respondents who said they were confident in their ability to protect themselves online are often not in fact taking basic security precautions that could justify some of that confidence.
- Underserved residents generally suffer from low levels of confidence in their ability to protect themselves online and have low trust in technology companies to secure their data. As a result, they are deterred from using online services, such as banking or social services, that can bring important economic and social benefits.

- While many internet users have had the benefit of years of experience and have built their knowledge and skill level through time, effort, and education, members of underserved communities have in most cases not had these experiences and privileges. In the absence of help, they are more likely to fall further behind than they are to converge and catch up.
- Underserved citizens whose primary language is not English often struggle to find resources on cybersecurity in their own language, and many do not know what resources to trust. Residents often turn to friends or relatives and receive partially accurate information at best.

POOR CYBERSECURITY KNOWLEDGE AND SKILL LEVEL

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.

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.

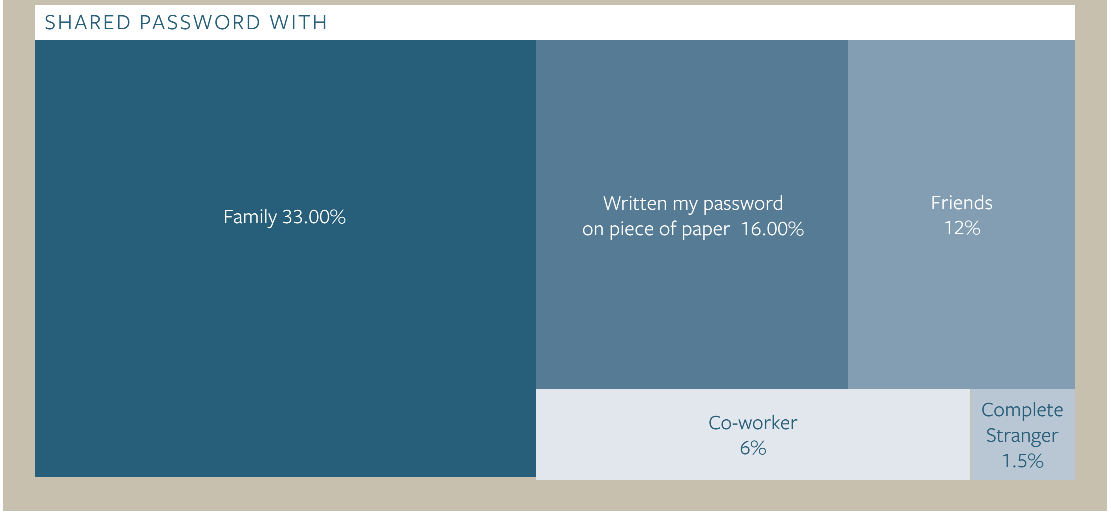
FIGURE 3 **Phishing Prevention Best-Practices**

Best-Practice	Underserved Communities	Control Group
Do not check to see if the email address of the sender is suspicious:	35%	5%
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%

VICTIMS OF CYBERCRIME

A large number of respondents from the underserved group reported that they have fallen victim to cyber scams[4] and internet viruses. Respondents provided information about the types of personal information that has either been stolen from them online, or that they

FIGURE 4 Password Protection Behavior



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 victim 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.

TRUST IN ONLINE SERVICE PROVIDERS

Respondents were asked to assess their trust that various digital services providers—including Facebook, Twitter, Yahoo, Instagram, Microsoft, Apple, the federal government, and online banks—would keep their data secure. Roughly 34 percent of underserved respondents do not trust any of the organizations keep their personal data secure, compared to 28 percent of comparison group respondents. Instagram, Microsoft, Yahoo, and Twitter in particular attract very low levels of trust. Apple, Facebook, the federal government, and online banks perform marginally better, but still gained trust from less than 30 percent of underserved respondents. Facebook and online banks highlighted the largest delta in trust between the two survey groups, with the comparison group 27 percentage points more trusting of both than the underserved respondents.

A large percentage of the underserved respondents do not use important online services because of cybercrime, as evidenced in Figure 6. These services include online banking, social media, downloading software, and email. Although trust in online service organizations is generally low across both the comparison group and the underserved respondents, the results suggest that underserved respondents are more likely to withdraw from using an important online service if they perceive a threat of online crime on a platform. This suggests that trust and security play a larger role in determining online service use for the underserved.

CONFIDENCE

A significant portion of the underserved sample self-assess as having either "high confidence" (HC) (36 percent) or "low confidence" (LC) (38 percent) in their ability to protect themselves from online crime.[5] High-confidence respondents[6] 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.

More high-confidence respondents have never installed a security update and do not know how to install anti-virus software when compared to the underserved sample. Forty-three percent of high-confidence respondents also do not check the encryption security seal when visiting a website (see Figure 8).

Having low confidence in one's own ability to defend against cybercrime correlates with low trust in online service-providers' ability to protect user data. Self-assessed "low-confidence" respondents are more concerned about the existence of cybercrime than other groups.

FIGURE 5 **Cybersecurity Impact Outcomes**

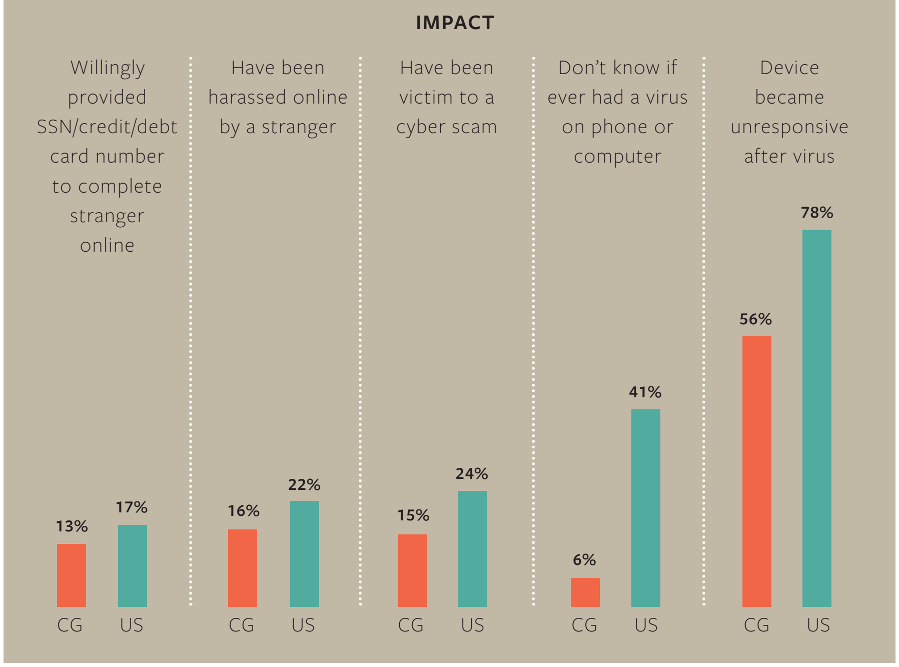


FIGURE 6 **Trust in Online Service Providers**

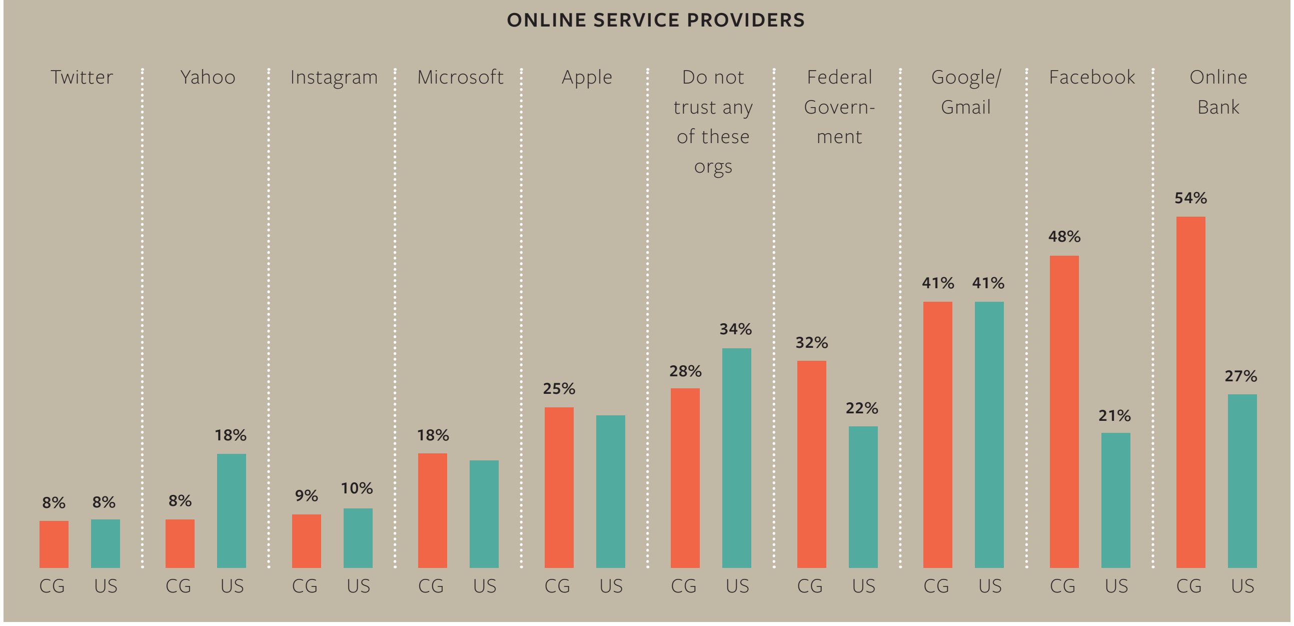
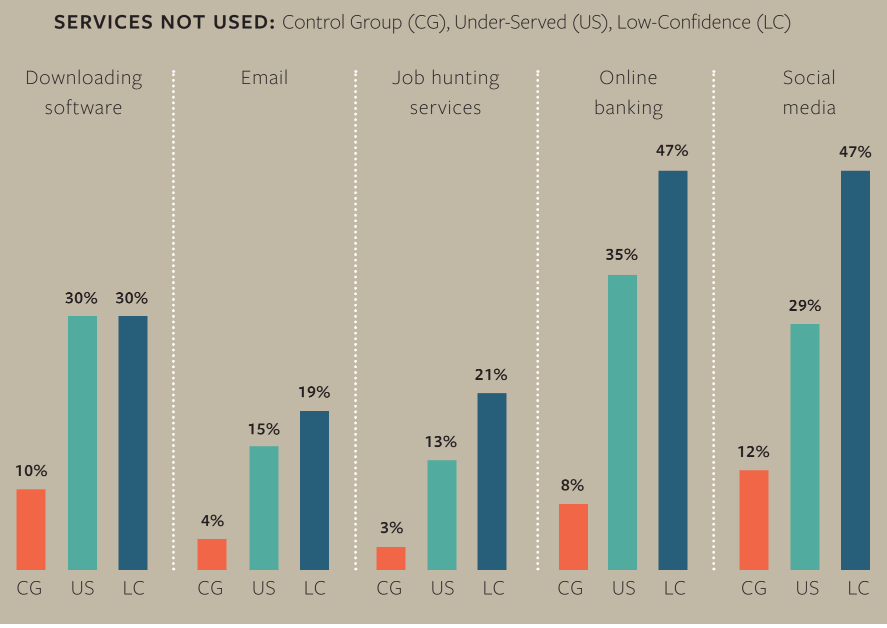


FIGURE 7 Services Not Used Due to Threat of Online Crime



For example, 47 percent of low-confidence 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. Although trust in online service providers is generally low across both the comparison group and underserved respondents, the underserved respondents are more likely to withdraw from using important online services. This suggests that trust and security play a larger role in determining online service usage for the underserved as compared to the comparison group. In fact, very few respondents from the comparison group have been deterred from using online banking, email, or job hunting services, even though 45 percent of comparison group respondents indicate they do not trust online banks, 64 percent do not trust Google/Gmail, 82 percent do not trust Yahoo, and 90 percent do not trust Microsoft to keep user data secure.

SOURCES OF CYBERSECURITY ADVICE

Respondents from the underserved group were more likely to refer to friends and relatives for advice on cybersecurity issues than any other resource, with 39 percent of respondents choosing the friends/relatives option. Only 21 percent of underserved respondents refer to websites, and seven percent refer to government websites. More than a third of respondents

FIGURE 8 **Adoption of Cybersecurity Best Practices**

	Underserved	High Confidence
Never installed a security update	14 percent	20 percent
Do not know how to get rid of a virus	43 percent	59 percent
Do not know how to install anti-virus software	31 percent	33 percent
Do not generally set a complex password	39 percent	30 percent
Do not check email address of the sender to assess if the email is suspicious	35 percent	30 percent
Do not check security seal when visiting a website	49 percent	43 percent

(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).

Our results indicate that the use of websites (including government websites) is positively correlated with cybersecurity index scores.[7] 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.

Respondents with higher Knowledge and Skills index scores have higher average income and educational attainment and rely more on websites for advice, while lower-skilled respondents have lower average income and lower educational attainment and rely more on family, friends, and teachers for advice. The data also shows that a large number of respondents do not try to access any advice source on cybersecurity.

ANDROID SMART PHONE OWNERS MORE VULNERABLE TO CYBERATTACK

In comparison to respondents who own an Apple iPhone, respondents who own an Android smart phone are likely to be more vulnerable to cyberattacks, more likely to withdraw from using important online services, and also more likely to trust Google to keep their data secure. This will have important implications for cities providing cybersecurity and privacy trainings and advice resources, as they will have to be tailored according to the operating system of the users.

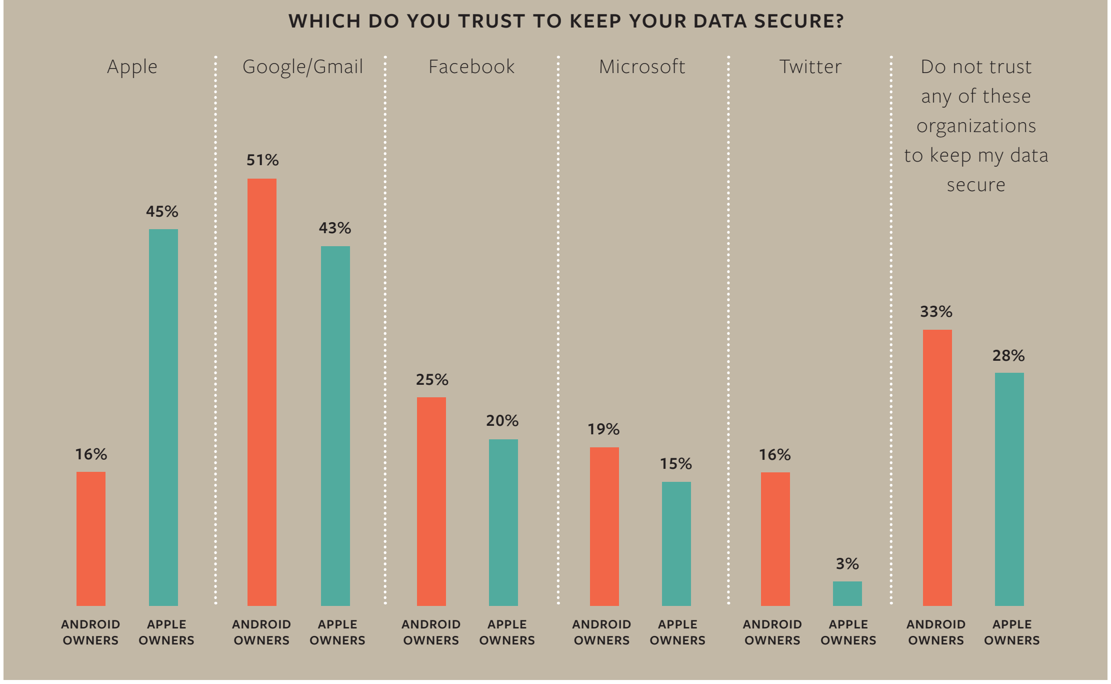
- Fifty-three percent of Android owners and 31 percent of Apple owners have reported that their devices have been infected by a virus at least once.
- Sixty-one percent of Android owners and 41 percent of Apple owners have stopped using a key online service due to the threat of cyber-crime.

Respondents also place a significantly higher level of trust in the company that developed the operating system (OS) of their smart phone:

- Fifty percent of Android owners trust Google to keep their data secure.
- Forty-five percent of Apple owners trust Apple to keep their data secure.

While Apple owners place a high level of trust in Google as well (43 percent), Android owners place a low level of trust in Apple (16 percent). These findings hint at the existence of biases that inform device and service use as well as responses related to trust. Apple owners are likely to access Gmail services offered by Google, which could explain the comparatively high levels of trust placed in Google. Meanwhile, Android owners are unlikely to use an Apple-offered service, as Apple services are tied to Apple device ownership, which could explain the low levels of trust placed in Apple.

FIGURE 9 Trust in Online Service Providers by Smartphone OS



RECOMMENDATIONS

Local governments have a variety of approaches available to improve the cybersecurity awareness of underserved populations.

GAIN AN UNDERSTANDING OF THE SITUATION IN YOUR COMMUNITY

Cities seeking to improve the cybersecurity awareness of local underserved populations may first want to gain a baseline understanding of their specific situation, for example by conducting surveys or informational workshops to assess their major areas of interest and/or lack of knowledge among residents. Based on our experience, we 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 (see Figure 10). Our findings suggest that such programs should include explicit targeted cybersecurity awareness and training component. A customized cybersecurity awareness program that is tailored to the specific needs of your community—with topics and content prioritized based on a 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.

A sample structure for a four-hour cybersecurity training might include:

- Key cybersecurity terms and concepts like spam, viruses, and phishing (one hour);
- Cyber-hygiene and best practices (one hour);
- Downloading, installing, and use of anti-virus and malware software (one hour);
- Cybersecurity recap and Q&A (one hour).

FIGURE 10 Digital Literacy Initiatives

A growing number of cities across the United States have invested in digital literacy training initiatives that aim to educate underserved populations in the basics of computer usage and commonly used software. 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 non-profits and local governments and aim to improve citizens' skills and confidence, as well as increase their motivation to engage in online activity.

The National Digital Inclusion Alliance (NDIA) maintains a list of **Digital Inclusion Trailblazers**, a public inventory of local government initiatives promoting digital literacy and broadband access for underserved residents. This resource is intended in part to provide examples and contacts for communities interested in launching similar initiatives. Learn more at https://www.digitalinclusionorg.

Digital literacy initiatives generally focus on basic skills, and rarely include training focused explicitly on cybersecurity. Here are a few notable exceptions:

Chicago DigiSeniors (https://blogs.microsoft.com/chicago/2016/08/08/introducing-the-digiseniors-program/): The City of Chicago partnered with Microsoft to create a cybersecurity program called "DigiSeniors" designed to teach senior residents on responsibly navigating the internet and avoiding scammers. This program has been launched in other cities, and "train the trainer" resources are available to get started.

Los Angeles Cyber Lab (https://www.lacyberlab.org): Launched in August 2017, the Los Angeles Cyber Lab is a non-profit organization that promotes innovation, education, and information sharing between Los Angeles' public and private sectors for the benefit of businesses and residents. The website includes basic educational resources on password management, avoiding scams, etc.

New York Secure (https://secure.nyc/): A public-private partnership meant to provide cybersecurity to New York City residents, the New York Secure app alerts users to unsecure Wi-Fi networks, unsafe apps in Android, system tampering, and more.

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

FIGURE 11 **The Importance of Avoiding Fear in Building Cybersecurity Awareness**

The phenomenon of using fear in awareness campaigns has been covered extensively in public health literature and is known as "fear appeal." Protection Motivation Theory (PTM) offers a framework to study the behavioral determinants of "fear appeal" that motivate people to protect themselves. Academics have applied PTM to cybersecurity in a variety of ways.

For cybersecurity trainings, "fear appeal" on its own is not an effective strategy because it discourages those who can least afford to take risks (i.e. underserved populations) from using the internet. Instead of fear, positive security behaviors that increase the perceived utility of cybersecurity would be more effective. Training to help over-confident users become aware of the likelihood and consequences of cyber-threats would also be useful to encourage cyber-hygiene.

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.

Organizers should not encourage cyber-hygiene through an appeal to fear, but rather should leave participants feeling equipped to deal with the cyber threat landscape, as opposed to withdrawing from it (see Figure 11).

DEVELOP AND DISSEMINATE RESOURCES FOR SELF-TEACHING

Through trainings and other communication channels, cities can promote cybersecurity awareness by sharing links to reliable online resources that are easy to interpret and access. Officials should recognize the differences in educational attainment and digital literacy skills in their training cohort, and work to make all respondents feel comfortable in accessing reputable online resources for advice on cybersecurity questions.

Officials can customize advice resources for each audience by pre-screening for preferences for advice resource, signal the credibility of the resources by reassuring them that the advice has been verified and that the source of advice is not trying to market a service or product, and address privacy concerns. They should also aim to provide straightforward, accessible advice with step-by-step instructions that avoid jargon, and provide information about apps and threats specific to Android users and iOS users respectively.

Trainers can provide a one-hour session explaining fundamental cybersecurity concepts and threats—explaining terms like phishing, viruses, and malware—before recommending specific best practices. As these trainings are likely to attract participants with a wide range of digital literacy and educational attainment, trainers should not assume that participants will understand the importance or relevance of their suggestions. Trainers should not merely train through basic rules or heuristics, but rather should ensure that participants understand the underlying reasoning behind the recommendations.

Trainers should make the instruction digestible and up-to-date, but not over-simplify it to the point that participants cannot adapt their knowledge, as technologies change in the future. Once the program begins, city officials should continue to survey the population on digital literacy and cybersecurity. Evaluating progress will inform where future trainings are needed.

PUBLIC-PRIVATE PARTNERSHIPS

In addition to providing training to residents directly, cities have opportunities 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,[8] and residents of select cities may have access to online resources for reporting incidents; for example, San Francisco residents can report and resolve cybercrime by calling the San Francisco Police Financial Crimes Unit.[9] Yet in many cities, information about cybersecurity and related resources is disaggregated and difficult to find.

Cities 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.[10] 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.[11]

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.[12] As a result, older smartphones are not guaranteed to get new security updates, and some software updates for older devices are not compatible on 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.

Cities 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, 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. Local governments 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, cities have opportunities to 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 the overlapping scams and phishing efforts by utilizing contacts in the private sector.

Local 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 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. SignalSpam is another public-private partnership; it acts as a national spam reporting center in France by collecting spam reports from end-users through email client and web browser plugins. While SignalSpam is specific to France, city officials across America can learn from the development, rollout, and impact of this program. (Note that cities may receive pushback from the private-sector on any proposed partnership that would allow them to access user-data.)

Conclusion

Research and government intervention efforts aimed at improving online security have not effectively reached underserved populations, who (as shown in this study) frequently suffer from poor cybersecurity outcomes, including being victimized by cyber-scams and avoiding the use of online services due to the threat of cybercrime.

Investing in programs that improve cybersecurity hygiene could have far-reaching social and economic benefits. Citizens will be more cognizant of their web browsing behavior if they know what a cyber scam is and are aware of the types of cyber scams that exist. They will be able to prevent cyber scams like phishing attacks by practicing proper cyber-hygiene when interacting with emails from unknown sources. And they will be able to deal with the repercussions of scams if they understand the legal recourse available (such as cyber-fraud bank insurance), understand the effects of a virus/malware (such as making phones/computers unresponsive), or have installed anti-virus software that can delete malware or viruses downloaded through a phishing link.

Further research is needed to fully understand the scope of this challenge on a national level, and particularly to assess how underserved residents secure themselves online and how they have been affected by cyber-criminals. While the field of cybersecurity impact evaluation is young, experiences in the field of public health can serve as a helpful guide for city leaders hoping to chip away and define the future of cybersecurity for underserved residents. Cities should continue to invest in research that combines primary survey data, rigorous analysis, and actionable recommendations.

Cities have opportunities to work together to develop joint cybersecurity initiatives, including digital literacy trainings to improve cybersecurity outcomes, while also creating strong, sustainable, and actionable partnerships with private-technology firms to address system-level cybersecurity concerns.

Endnotes

[1] 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.

[2] Through countless hours of research, I could only find one report and one draft paper exploring cybersecurity outcomes for low socioeconomic status individuals.

[3] All results relate to underserved respondents, unless explicitly stated to represent results from the comparison group.

[4] A cyber scam is defined as the use of Internet services or software with internet access to defraud victims or to otherwise take advantage of them.

[5] Respondents were asked to rate their ability to protect themselves from online crime on a Likert scale of 1 to 5.

[6] "Over-confidence" is reflected within the responses of the Underserved population that has self-identified as having "High-confidence" in their ability to protect themselves from cybercrime. Self-assessed "High-confidence" respondents think that they have a higher level of cybersecurity knowledge while some of their survey responses say otherwise. The "High-confidence" population has similar if not lower scores on certain knowledge and skills questions compared to the Underserved sample average. Respondents who self-assessed themselves as 1 or 2 form the "Low-confidence" group, and respondents who self-assessed themselves as 4 or 5 form the "High-confidence group".

[7] Correlation and multiple regression analyses were conducted to examine the relationship between the Cybersecurity Index score and various potential predictors, such as types of resource used for cybersecurity advice, education level, public computer use, being a senior (65 years or older), being from a low-income household ($25,000 household income or less), the non-profit organization where the respondent took the survey, and the respondent's race. The multiple regression model shows a positive and statistically significant relationship between the use of websites for advice on cybersecurity and the cybersecurity index score. The multiple regression model with all 10 predictors produced $R^2 = .428$, $F(21, 131) = 4.662$, $p < .0001$.

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

[9] "Police Department." Vision Statement | Police Department. Accessed September 11, 2018. https://sanfranciscopolice.org/financial-crimes-unit-fraud., (415)553-1521

[10] 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.

[11] "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.

[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/old-phones-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/.

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/security-center/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-evolving-targeting-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 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/

Acknowledgments

I would like to thank the Center for Long-Term Cybersecurity for the grant, support, and guidance that helped make this project a reality, as well as Alex Banh and Matthias Jaime at the Committee on Information Technology for guiding my efforts and providing me the resources I needed to complete this report.

About the Author

Ahmad Sultan is the Associate Director for Research, Advocacy and Technology Policy at the Anti-Defamation League's Center for Technology and Society. His background in technology policy focuses on underserved and vulnerable populations and his policy expertise includes the fields of cybersecurity, cyber harassment, and data privacy. He has worked with the Committee on Information Technology (COIT), the City and County of San Francisco technology policy body, where he helped shape the City's cybersecurity initiatives. Currently he is also advising the Berkeley Research on Autonomous Vehicle Opportunities (BRAVO) team on privacy and security matters. Previously, he has led poverty alleviation projects at the World Bank and the Center for Economic Research in Pakistan. Ahmad has a Master of Public Policy degree from UC Berkeley's Goldman School of Public Policy, where his Master's Thesis was a finalist for the Smolinsky Prize for Best Thesis. He also has a Master of Arts degree in Economics from the University of Glasgow.

CLTC

Center for Long-Term Cybersecurity

UC Berkeley

Center for Long-Term Cybersecurity
cltc.berkeley.edu
@CLTCBerkeley