STRENGTHENING CYBER RESILIENCE FOR AMERICAN FAMILIES:

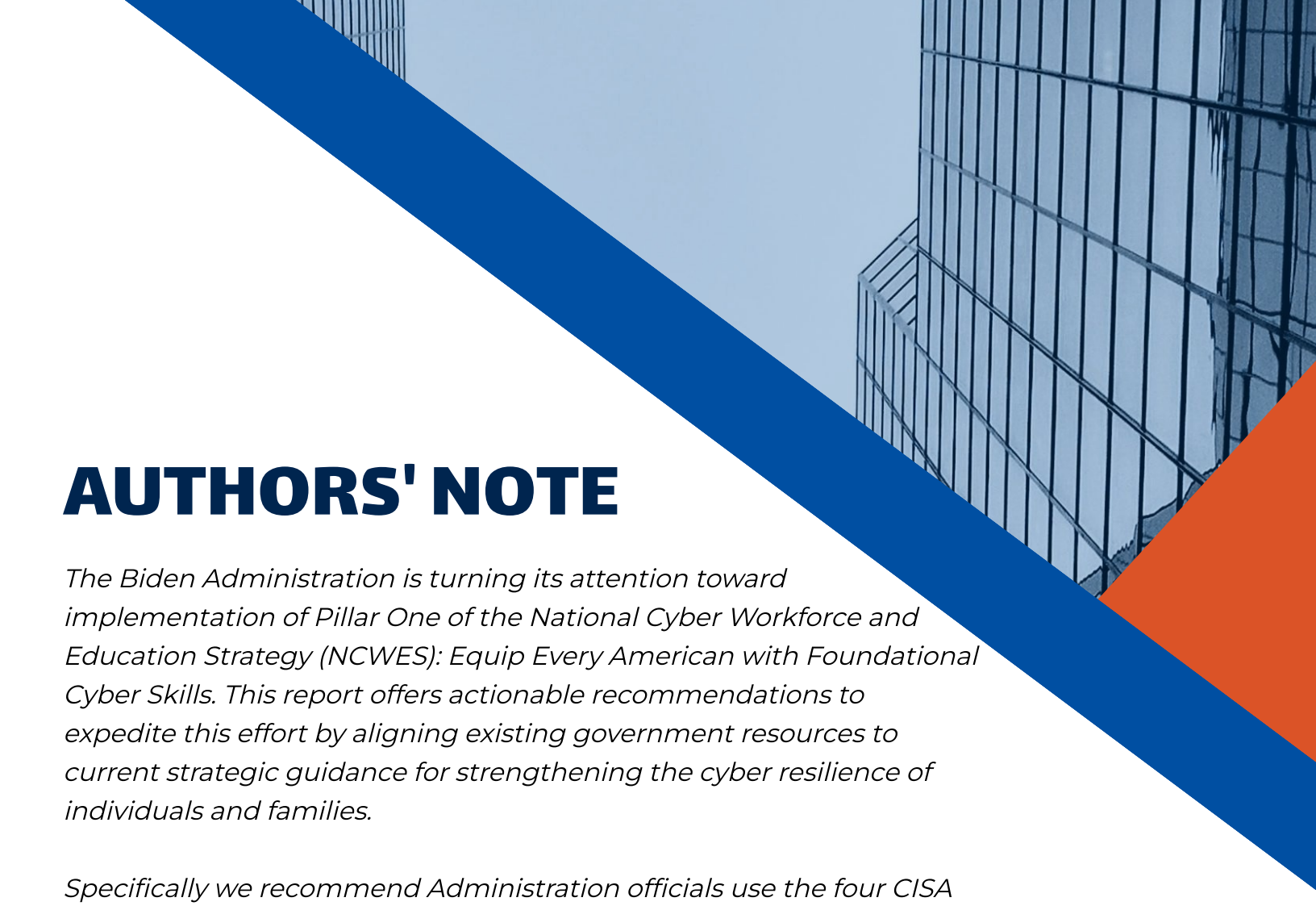
Aligning existing government resources with current government guidance

Dr. Sasha O'Connell & Dr. Diana Burley
American University

September 2023

Sponsored by craig newmark philanthropies

TABLE OF CONTENTS



AUTHORS' NOTE

The Biden Administration is turning its attention toward implementation of Pillar One of the National Cyber Workforce and Education Strategy (NCWES): Equip Every American with Foundational Cyber Skills. This report offers actionable recommendations to expedite this effort by aligning existing government resources to current strategic guidance for strengthening the cyber resilience of individuals and families.

Specifically we recommend Administration officials use the four CISA Shields Up campaign priority areas as a simple branding frame. Shields Up provides guidance and the work summarized in this report couples that guidance with vetted resources to enable immediate action.

We recommend that the Administration leverage prior federal investment in cybersecurity awareness by aligning the resources developed through those efforts with current guidance. Finally, we recommend starting now. Since usable and free resources already exist, implementing an effective campaign to raise cyber resilience can begin immediately. Notably, since the 2023 CSAM theme is Shields Up, the proposed materials can be folded into developing plans for citizen outreach. We look forward to additional opportunities to work with the Biden Administration to support NCWES implementation and strengthen the cyber resilience of all Americans.

BACKGROUND

Protecting America's digital infrastructure has long been a national security imperative[1]. The security of these systems and the data they house drives economic prosperity and is inextricably linked to the provision of essential services, daily transactions, and, increasingly, personal social interaction. Knowing this, nefarious actors ranging from nation-states to criminal enterprises and individuals work to impede and disrupt the flow of information, money, and operations by exploiting vulnerabilities in the systems and the people who use them. While cybersecurity professionals build technical defensive tools and capabilities to meet these threats, they also recognize that people are often the weakest link in the system. A door with the most sophisticated lock will not stop a thief if it is left ajar. As such, proactive measures that strengthen an individual's ability to use these defensive tools, or at least not to render them ineffective, is a necessary component of a holistic cybersecurity strategy.

This is not to say that all citizens should become cybersecurity experts. Rather, it recognizes the role everyone will play in securing systems and suggests having a basic understanding of fundamental measures is a must. This foundational knowledge will both support needed growth in the future cybersecurity workforce and raise the base level of proficiency among the general population. To prepare all citizens for participation in society, the American educational system is designed around developing student proficiency in the 3 "R" of basic education: reading, writing and arithmetic. Given our collective reliance on the viability of digital systems, a fourth "R" for cyber is a logical expansion and the federal resources identified in this report provide a starting point for educating all Americans.

Released in July 2023, the Biden Administration's National Cyber Workforce and Education Strategy[2](NCWES) effectively describes this need to develop foundational cyber skills for all citizens.

Specifically, the strategy asserts that the nation's prosperity, security, and well-being depend in part, on the ability of citizens to use and know digital literacy skills, adapt and grow their digital resilience, and analyze and apply computational literacy skills. This assertion follows the Biden Administration's Cybersecurity Strategy[3] which argues that even with a national directive to "lift and shift" to "ensure that the burden of cybersecurity is allocated toward those who are most able to bear it," **there is and will continue to be residual responsibility for all Americans to improve their cyber resilience and to use this basic knowledge of digital and computational skills in support of societal security.**

But how? Strategies and directives are important first steps. However, for these steps to be implemented, people need to know where to start. Then, once their efforts are focused on priority areas, individuals and families need guidance on finding, understanding, and using resources on how to safely engage online.

Despite the imperative, even motivated Americans do not have easy access to cybersecurity resources that provide information on the digital and computational literacy skills that will enable their cyber resilience. Further, even when identified, the information is offered through a variety of sources which are often unfamiliar and thus, either not trusted or too easily trusted, by the recipient about where to find resources, potentially reducing their risk. In addition, because the resources vary in quality, clarity, and accessibility, the expectation that large segments of the population will understand the content or how to use the resource is unrealistic.

To minimize concerns over the trustworthiness of the resource, American citizens often turn to information provided by the U.S. federal and state governments. Not surprisingly, government efforts to strengthen cyber resilience for individuals and families are plentiful. Federal agencies with both direct and indirect cyber missions as well as the states have produced a broad range of cybersecurity resources.

A few of these resources are linked together through cross-referencing and concept definitions. However, connected or not, no unifying guidance on how to select or how and when to use the resources is readily available. **With the wide array of resources and the lack of guidance on how to select among them, citizens must determine the most appropriate source, reconcile differences, assess the fidelity, relevance, and timeliness of the information, and avoid information overload all on their own.** Of course, these criteria do not account for differences in learning preferences and styles. Thus, individuals must also identify resources delivered in a manner (e.g., text-based vs. video) that most aligns with their learning preferences.

Previous Efforts to Address the Need for Resources

[The authors note here that cyber resilience is an updated term used in the NCWES to convey the desired outcome of cyber awareness initiatives. The prior efforts were labeled as "awareness" rather than "resilience" but target the same desired behavior change. For purposes of this report, the terms are considered interchangeable.]

Multiple USG-coordinated communications campaigns have been created to strengthen cyber resilience including, **Shields Up** (2022, Biden Administration), **Be Cyber Smart** (2019, Trump Administration), **OnguardOnline** (2006/2011, Bush Administration continued under the Obama Administration), and **Stop.Think.Connect.**(2010, Obama Administration and international in scope). In addition to these campaigns, in 2004 the Bush Administration established October as **Cyber Security Awareness** month (CSAM), a high visibility outreach campaign that continues today. CSAM's capacity to drive content creation and dissemination for cybersecurity deserves special mention here. While CSAM activities are widespread across sectors throughout the month, it is not clear where to find resources when the month ends. During these annual campaigns resources are pushed to the public through public service announcements, printed artifacts, targeted training, and specialized events. Messaging across federal and state agencies is uniform, following the theme of the year and the weekly areas of focus.

As the most recent initiative, the Cybersecurity and Infrastructure Security Agency (CISA) launched Shields Up[4] in 2022. The Shields Up Campaign "provides recommendations, products, and resources to increase organizational vigilance and keep stakeholders informed about cybersecurity threats." Shields Up guidance for families provides four simple steps - (1) update software, (2) use strong passwords, (3) implement multi-factor authentication, and (4) think before you click to avoid phishing, that every citizen can take "to improve their cyber hygiene and protect themselves online." **While the cybersecurity priority areas for individuals and families are clearly outlined on the Shields Up website, supporting resources that explain their importance and, importantly, guidance on how to implement the steps are not included.**

Each of these efforts has undoubtedly reached segments of the American public **however, they have also resulted in uncoordinated artifacts positioned across federal and state-run websites.** More confusing for the public, even when resources were repeated, they were often positioned differently with some positioned as consumer protection and others situated within the homeland/national security category. Clearly, cyber resilience can be properly categorized in both areas. Nevertheless, when resources are positioned differently without clear explanation, it can lead to confusion on the part of the recipient, about where to find resources, potentially reducing their use.

The Cyber Civil Defense Intiative to Identify Cyber Resiliency Resources

This report seeks to help answer the Biden Administration's call to elevate cyber resilience for individuals and families by addressing the challenge confronting citizens: How do they prioritize, identify, and assess the resources needed to build their cyber resiliency? And further how can government resources be leveraged to support their development?

To address these questions, the research team sought to prioritize and identify free, accessible, online government resources and provide recommendations for presenting these resources in a manner that supports strengthening cyber resilience among individuals and families. In doing so, the report also answers the call set forth in the NCWES to leverage previous government investments to address the new imperative.

METHOD

Based on this background, the authors developed a three-step methodology to prioritize, identify, and assess (based on the criteria below) cybersecurity resilience resources on federal and state government websites.

PRIORITIZE: To prioritize the resources, the reviewers chose to use the current CISA Shields Up campaign focus areas . As outlined above, Shields Up identifies four priorities for individuals and families seeking to strengthen their cyber resilience. These priorities, along with two additional categories added based on sponsor discussions, form the six categories used to organize resources. They are: (1) update software, (2) use strong passwords/pass keys[5], (3) implement multi-factor authentication, (4) think before you click/avoid phishing, (5) implement mobile/app security, and (6) practice general cyber hygiene.

IDENTIFY: To identify resources, the reviewers assessed the official government websites of the fifty U.S. states and the District of Columbia, and the U.S. federal agencies and sub-agencies identified in the 2020 Government Accountability Office (GAO) report, *Cybersecurity: Clarity of Leadership Urgently Needed to Fully Implement the National Strategy* [6], as having an official role or responsibility for some aspect of cybersecurity.

By limiting the population of resources to those appearing on the official website of the GAO-identified agency or state government, the reviewers moved forward with the expectation that the content was trustworthy. The public consumes information from official government sources with the assumption that it is (1) either created or approved by the government entity, (2) technically accurate, (3) free, and (4) following accessibility requirements as specified in Section 508 of the Rehabilitation Act [7].

The websites were reviewed for relevant content using the following 4 step search process.

- **1- Internal Search:** After navigating to the official website of the federal agency or state, the reviewers utilized the internal search function to find any reference to cybersecurity-related resources using the following key terms selected to mirror the Shields Up priority categories: MFA, passwords, phishing, software updates, digital safety, online safety, cyber training, cyber training, and cybersecurity training.

- **2- Review and Confirmatory Search:** After reviewing over 100 websites using the internal search function, the reviewers conducted a confirmatory search to ensure that the internal search resulted in a full set of applicable resources. For each website, a confirmatory check was performed using the Google search engine by entering the agency or state name along with the associated keywords (e.g., "Department of Commerce" and "passwords"). In every case, the Google search yielded more results. Based on this finding, we decided to move forward using the Google search to identify relevant resources.

- **3- Google Search:** The Google search was performed by entering the agency or state name along with the associated keywords (e.g., "Department of Commerce" and "passwords") All webpages and resources resulting from the keyword search were cataloged and moved to the next step in the process.

- **4- Quality Check:** A sample of websites was selected for a quality check. Websites chosen for the quality check included five randomly selected states and the four federal agency websites with the most identified resources. For this subset, the web pages and resources identified through the Google search were compared with resources identified through a review of the site map. The site map outlines the content of each web page contained within the website. Each site map was searched using the same key work search process listed above. The resources identified through the quality check for each of the sampled websites were materially identical to those discovered through the Google search. The resulting confirmed resources were then assessed based on the process below.

ASSESS: Each resource identified through the steps listed above was assessed for readability, completeness, and format.

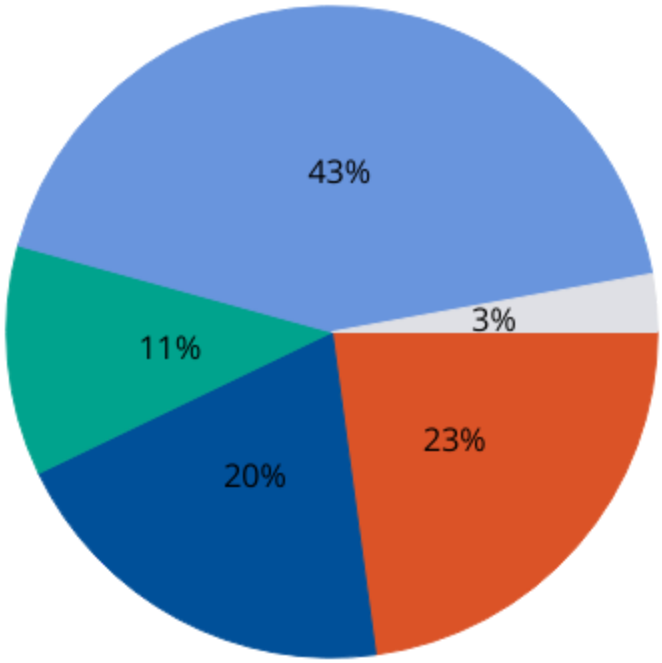
- **Readability** was defined using the 2010 Plain Writing Act[8] enacted under President Obama to establish "a system of transparency, public participation, and collaboration [9]". The federal plain writing act asserts that materials be written such that which requires official government communications to be be written so that the public can find, understand, and use the information [10].
- **Format** was categorized as text-based documents, video resources, graphic depictions, and combined (e.g., text and video). Format was used as an initial step toward connecting resources with learning styles. A detailed investigation of the relationship between learning styles and the modality of content delivery was outside the scope of this project. However, a follow up study to examine the relationship may be valuable.
- **Completeness** was defined as containing the following components: (1) a definition of the focus area (e.g. a definition or explanation of the term phishing), (2) a statement of relevance for individuals and families (Why should they care or what is the potential impact?), and (3) instructions that outline actions and clear steps the reader can take to implement the recommended action to reduce the threat and increase cyber resilience.

FINDINGS

Based on the method outlined above, the reviewers identified 71 government websites across the federal and state levels. The list of these websites is provided in Appendix A.

Across the 71 websites, the team identified 185 resources that addressed the six priority categories (Shields Up four plus two). Following the assess phase, 35 resources were identified as meeting the assessment criteria (see Appendix B for the full list of 35). The content identified through these resources falls into the following single categories:

- **"General" cyber security awareness - 8 resources, (23%) of resources found**
- **Multi-factor authentication - 7 resources, (20%) of resources found**
- **Passwords/pass keys - 4 resources, (11%) of resources found**
- **Phishing - 15 resources, (43%) of resources found**
- **Software updates - 1 resource, (3%) of resources found**
- **Mobile - 0 resources***



**Note: While no resource fell solely in the mobile/app security category, four resources addressing mobile security were found. As shown in Appendix B, two resources were combined with other general cybersecurity awareness resources and two were combined with multi-factor authentication.*

Regarding the full set of 185 resources reviewed

While the 35 resources that passed the assessment for readability and completeness are the focus here, a review of the full set of resources provides additional valuable insights .

Resource Alignment - Federal investment in cybersecurity awareness resources is paying off as states and nonprofits are leveraging federal resources for their own awareness raising campaigns:

- Thirteen states leverage resources from the FTC or Onguard Online initiative.
- Six states and the District of Columbia leverage CISA's resources.
- Four states leverage Common Sense Media resources.

Audience - Vulnerable populations are the target of many cybersecurity awareness resources:

- The websites reviewed provided abundant resources specifically designed to appeal to children and small and medium-sized businesses.
- Notably, there was a distinct absence of resources designed to appeal to senior citizens in the materials reviewed for this study.

Branding - Consumer protection and security (individual and national) are the context for many cybersecurity awareness resources:

- Resources were housed in a variety of locations on the state websites including the Attorney General, information technology, consumer protection, and cybersecurity offices.
- Federal agencies either branded the resources as a consumer protection issue or positioned the content within the context of national or homeland security

RECOMMENDATIONS

Based on the findings, we offer five recommendations to strengthen cyber civil defense.

Leverage existing government resources.

The Biden Administration has articulated the strategic goal of increasing the cyber resiliency of American citizens and their families, and to do so, when possible, by leveraging previous investments of taxpayer dollars. Prior federal initiatives have yielded usable, free resources that are readily available and accessible online.

Select a simple branding strategy.

The message about cybersecurity priorities for lay citizens should be clear and easy to understand. Reduce and/or link initiatives together and to the same source content.

- In the case of cyber resilience for citizens, consumer protection and national security are two sides of the same coin. Link them together using clear messaging. Consumers need to see the relationship between protecting consumers and protecting the homeland.
- Create a branded character and campaign slogan (or reintroduce a federal 2.0 of an existing one– McGruff, Woodsy the Owl, Cyber Florida's Pixel) to help sustain promotion year-round.

Align resources with guidance.

When consumers visit a government site seeking information on what behaviors to prioritize, they should also receive guidance on why the action is important, what it is, and how to take action.

Identify a single owner.

Determine who owns the base content that underpins the resources, will establish joint messaging, and brand consistency. The owner should house resources that all others link back to such that a call to one is a call to all.

- The owner should establish a review cycle and process.
- Clarify how citizen outreach should occur.

Start now.
Since appropriate resources already exist, implementing an effective campaign to raise cyber resilience can begin immediately. The key to effective and quick action will be uniform branding of identified resources to bring them to the attention of all families and individuals.

Finally, we remind all stakeholders that strengthening cyber resilience among individuals and families is a team effort. While these recommendations suggest that the federal government take the lead, only a joint effort that includes state, local, and tribal territories, along with cross-sector participation will enable the United States to achieve true progress in cyber civil defense.

ENDNOTES

1. See for example, the Cyberspace Solarium Commission Report (March 2020) Executive Summary (p. 4) recommends *The U.S. government should promote digital literacy, civics education, and public awareness (3.5) to build societal resilience to foreign, malign cyber-enabled information operations*
2. To access the Biden Administration National Cyber Workforce and Education Strategy, see: Fact Sheet, (July 2023)
3. To access the Biden Administration National Cybersecurity Strategy, (March 2023)
4. To access the CISA Shields Up Campaign Guidance for Individuals and Families, see: https://www.cisa.gov/shields-guidance-families
5. Pass keys: While the term pass keys is not used in the Shields Up categories for individuals and families the research team added this in keeping with the spirit of passwords in order to capture all relevant material
6. To access the GAO report see: https://www.gao.gov/products/gao-20-629
7. To access Section 508, see https://assets.section508.gov/files/rehabilitation-act-of-1973-amended-by-wioa.pdf
8. To access the 2010 Plain Writing Act, see https://www.govinfo.gov/content/pkg/PLAW-111publ274/pdf/PLAW-111publ274.pdf
9. To access the 2009 Memorandum on Transparency and Open Government, see https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2009/m09-12.pdf
10. Ibid

APPENDIX A: REVIEWED WEBSITES

All twenty (20) federal websites identified in the 2020 GAO report were reviewed. They are:

- Department of Homeland Security (DHS)
- Cybersecurity and Infrastructure Agency (CISA)
- Department of Justice (DOJ)
- Federal Bureau of Investigation (FBI)
- Department of State (State)
- Department of Transportation (DOT)
- Department of Treasury (DOT)
- Enivornmental Protection Agency (EPA)
- Federal Chief Information Officers Council (CIO Council)
- Federal Communications Commission (FCC)
- General Services Administration (GSA)
- National Science Foundation (NSF)
- Office of the Director of National Intelligence (ODNI)
- Department of Agriculture (Agriculture)
- Central Intelligence Agency (CIA)
- Department of Commerce - National Institute of Standards and Technology
- Department of Defense (DOD) Defense Logistics Agency
- DOD Office of Small Business Program
- Department of Energy

In addition, the official website for each of the fifty(50) states, and the District of Columbia were reviewed. In total, the study team reviewed seventy-one (71) distinct government websites. While local jurisdictions (e.g. county or city governments) as well as tribal territories likely also contain relevant cyber security awareness-raising resources, the goal here was not to develop a comprehensive listing of all public sector web-based resources. Rather, the goal was to identify a robust set of quality, free resources to form the foundation of collective effort to increase the cyber resilience of individuals and families.

APPENDIX B: SELECTED GOVERNMENT RESOURCES

Category	Source	Link
General Awareness	CA	https://oag.ca.gov/privacy/facts/online-privacy/protect-your-computer
General Awareness	CISA	https://www.cisa.gov/shields-guidance-families
General Awareness	CISA	https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Awareness%2520Month%25202021%2520-%2520Phishing%2520Tip%2520Sheet.pdf
General Awareness	PA	https://www.pa.gov/guides/cybersecurity/#BrowseSafely
General Awareness	PA	https://www.ready.pa.gov/Are-You-Ready-PA/Pages/Article.aspx?post=29
General Awareness	TX	https://dir.texas.gov/cybersecurity-information-texans?id=161
General Awareness (including mobile security)	MN	https://www.ag.state.mn.us/Consumer/Publications/HowtoProtectYourselfAgainstHackers.asp
General Awareness (including mobile security)	AL	https://cybersecurity.alabama.gov/cybersecurity-resources/
MFA	CISA	https://www.cisa.gov/resources-tools/resources/multi-factor-authentication-mfa
MFA	FTC	https://consumer.ftc.gov/articles/use-two-factor-authentication-protect-your-accounts
MFA	NY	https://its.ny.gov/multi-factor-authentication
MFA	TX	https://dir.texas.gov/sites/default/files/2023-04/DIR%20OCISO%20Multi-Factor%20Authentication%20%28MFA%29%20Best%20Practices.pdf
MFA	NIST	https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication
MFA (including mobile security)	CISA	https://www.cisa.gov/be-cyber-smart
MFA (including mobile security)	FTC	https://consumer.ftc.gov/identity-theft-and-online-security/online-privacy-and-security
Passwords	FTC	https://consumer.ftc.gov/articles/password-checklist
Passwords	CISA	https://www.cisa.gov/news-events/news/choosing-and-protecting-passwords
Passwords	IN	https://www.in.gov/cybersecurity/blog/posts/one-password-to-rule-them-all/
Passwords	NE	https://protectthegoodlife.nebraska.gov/choosing-and-securing-your-passwords
Phishing	CISA	https://www.cisa.gov/sites/default/files/2023-02/phishing-infographic-508c.pdf
Phishing	NC	https://ncdoj.gov/internet-safety/phishing/
Phishing	SC	https://consumer.sc.gov/sites/consumer/files/Documents/Spotlight/Phishing_Scams.pdf
Phishing	WI	https://datcp.wi.gov/Pages/Publications/Phishing402.aspx
Phishing	NC	https://it.nc.gov/resources/online-safety-privacy/tips-guidance/avoiding-phishing-attacks
Phishing	TN	https://www.tn.gov/content/dam/tn/cybersecurity/state-cybersecurity-newsletter-archive/STS_Risk_Bulletin_Phishing.pdf
Phishing	CISA	https://www.cisa.gov/sites/default/files/publications/Phishing%20General%20Security%20Postcard_6.24.2021_508cV2.pdf
Phishing	CISA	https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks
Phishing	FBI	https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/spoofing-and-phishing
Phishing	FTC	https://consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams
Phishing	Dept of Ag	https://www.fsis.usda.gov/sites/default/files/media_file/documents/Food-Defense-Cyber-Security-Phishing.pdf
Phishing (holidays)	DE	https://news.delaware.gov/2018/12/07/avoid-getting-reeled-phishing-scams-holiday-season/
Phishing (SMS)	MA	https://www.mass.gov/info-details/smstext-message-phishing
Software Updates	CISA	https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates

Project Team & Contacts

PROJECT TEAM

Sasha O' Connell	Project Co-lead
Diana Burley	Project Co-lead
Denise King	Senior Learning Design Consultant
Colleen McInerney	Project Manager

Sasha Cohen O'Connell, Ph.D. is an Executive in Residence in the Department of Justice, Law & Criminology, School of Public Affairs (SPA), American University where she currently teaches cyber policy at the graduate and undergraduate levels. Additionally, she serves as the Director of the Terrorism and Homeland Security Policy Master's program at SPA. O'Connell's career in public service includes time in the executive branch. She has spent the majority of her career at the FBI where she served most recently as the organization's Chief Policy Advisory, Science and Technology and as the Section Chief of Office of National Policy for the FBI's Deputy Director where she led policy engagement with the National Security Council on a wide breadth of issues.

Diana Burley, Ph.D. is Vice Provost for Research & Innovation at American University where she also directs the Shahal M. Khan Cyber and Economic Security Institute and serves as Professor of IT & Analytics and Professor of Public Administration & Policy. She has nearly 30 years of experience driving digital transformation and regularly advises global executives on building digital workforce programs, inclusive security cultures, and an equitable global tech community. She led the ACM taskforce to establish global cybersecurity educational standards and directed the US cyber corps program. Diana speaks regularly at CISO forums, serves on several boards including the Cyber Future Foundation, and has been recognized by EWF, GET Cities, and SC Magazine for her efforts to build the cybersecurity workforce. She earned her PhD from Carnegie Mellon University.

This report was made possible by the generous support of craig newmark philanthropies.

Sponsored by craig newmark philanthropies