Safer Together: Inclusive Cybersecurity

By Camille Stewart Gloster

Foreword by Samantha F. Ravich, Ph.D.

"To err is human," Alexander Pope, poet of the Enlightenment, said in his 1711 treatise *An Essay on Criticism*. Pope understood that error is the basis of human nature, and civilization would be stronger if it recognized and mitigated such fallibility rather than dismissing it. The world of cybersecurity would be wise to relearn Pope's observation.

In today's world, a vast, globally connected, digital platform is the foundation of an individual's ability to participate in society and prosper. From ensuring one's shelter, food, utilities, communications, education, medical care, and income to casting a vote, driving a car, or receiving government benefits, internet-enabled technology is indispensable to modern life. At the same time, this digital network is extraordinarily vulnerable to the actions of any one person. This is not hyperbole or a theoretical risk. It is a reality that shows itself every day.

In 2014, an IBM Security Services report concluded that human error was a contributing factor in 95 percent of all cyber incidents.[1] Human error today can have serious national economic and security consequences.

In the spring of 2020, a large-scale spear-phishing campaign tricked numerous employees of U.S. defense and aerospace contractors into opening emails disguised as job offers. Malware infected their devices, and North Korean hackers exfiltrated defense technology.[2] A single person could have allowed a hostile foreign government to gain critical intelligence on the F-22 fighter jet program. The targets of this cyberattack were experienced technicians and engineers, well versed on operational security and aware they could be under foreign surveillance. And even *they* erred.

Cyberattacks are growing in volume and intensity. Governments and companies are spending billions of dollars to create and deploy new layers of cybersecurity technology. But not enough attention or resources are deployed to understanding the human element in this equation. Employees will yearn for better jobs and continue opening emails that suggest such an opportunity is in the offing. People, tired of the dozens of passwords they are forced to create, will continue to select passwords they can remember.

Conventional wisdom states the user is the weakest link in cybersecurity. But perhaps this is incorrect. Perhaps the problem lies with the security community failing users by not accounting for the people at the center of this work. The security community may be assuming an ideal, hyper-informed user or at least modeling a homogenous user population.[3] This paper posits that the lack of life experience diversity in the developer and technical communities results in a paucity of consideration of the users — and how they interact with technology — when building cybersecurity protocols.[4] Developers may be creating technology *by them for them* while users who click on the email that contains malware or select and reuse weak passwords are blamed for their ignorance or laziness. This equation must change.

The reality is that cybersecurity best practices are not meeting the population where they are — where and how they live, how they understand and interact with technology in their lives and lifestyles, and even how they participate in their communities. The security technology community promotes multifactor authentication as the solution to many cybersecurity ills, for example, but fails to recognize that in poorer communities, users may not be able to afford

1. "IBM Security Services 2014 Cyber Security Intelligence Index," *IBM Global Technology Services*, May 2014, page 3. (https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF)

2. Sergiu Gatlan, "US defense contractors targeted by North Korean phishing attacks," *Bleeping Computer,* July 30, 2020. (https://www.bleepingcomputer.com/news/security/us-defense-contractors-targeted-by-north-korean-phishing-attacks)

3. Tatum Hunter, "The government isn't great at explaining cyberthreats to Americans," *The Washington Post,* April 6, 2022. (https://www.washingtonpost.com/politics/2022/04/06/government-isnt-great-explaining-cyberthreats-americans)

4. Lauren Zabierek and Algirde Pipikaite, "Why cybersecurity needs a more diverse and inclusive workforce," *World Economic Forum,* October 26, 2021. (https://www.weforum.org/agenda/2021/10/why-cybersecurity-needs-a-more-diverse-and-inclusive-workforce)

multiple devices or may be sharing a single cell phone with other friends or family members. A better understanding of the user community and how different users interact with technology, their risk tolerance, perception of the threat, and level of trust/distrust in, and historical interaction with, various institutions can help drive a cultural change towards more positive cybersecurity behaviors and reduce national cyber risk.

What follows is a bold challenge to the cybersecurity community — "inclusive cybersecurity" must become the norm if our society is going to give itself a fighting chance to protect our networks going forward. The paper begins with an exploration of the relationship between cultural identity and cybersecurity. And while Camille Stewart Gloster brings to bear both qualitative and quantitative research to aid in this exploration, she acknowledges this barely scratches the surface of what needs to be studied. Still, the findings are robust enough to start building a framework for more inclusive cybersecurity. To repurpose Benjamin Franklin's comment at the time of the signing of the Declaration of Independence for today's need for cybersecurity, "We must all hang together, or, most assuredly, we shall all hang separately."

Executive Summary

As the frequency and severity of cyberattacks grow, countermeasures have proliferated to protect against digital extortion, disinformation, fraud, and other malign activities. These countermeasures are critical for protecting everything from national security systems to consumer devices. The technology deployed to counter these threats is often rooted in a strictly technical understanding of the challenge.

Ignoring the individuals that use the systems, or assuming all individuals interact with security measures in the same way, creates new vulnerabilities. The individual is not "the weakest link in security." Rather, the systems we have created have failed to account for a range of human behavior. Numerous studies have confirmed that cultural identity and cultural norms can have an influence on a given individual's risk posture. This includes the level of trust in authoritative experts and the willingness to adopt new security protocols. Gender, ethnicity, age, education level, and economic status may all impact how and to what extent an individual adheres to cybersecurity best practices.

This paper posits that a user-centric, inclusive focus can significantly enhance cybersecurity. If cyberspace comprises technology, people, and processes, then cybersecurity and risk mitigation must consider the sum of those elements. Owing to cultural nuances in the use of technology, it is essential to understand these differences to build effective user-centric security programs that include a holistic view of the threat and opportunity landscape. Accounting for the economic, ethnic, and cultural backgrounds of individuals and communities is necessary to properly combat cyber threats.

This paper probes several questions surrounding the relationship between cultural identity and cybersecurity, drawing upon two original, small-scale studies conducted by the author. The first is a survey of participants roughly representative of the U.S. population, which aims to assess trends in cybersecurity behavior based on identity attributes. This study asked participants a series of demographic questions and ran regression analysis to identify trends relating to cybersecurity. It found differences in cybersecurity practices based on age, sex, and education level, with some limited differences based on race.

The second study collected anecdotal information about participants' cyber behaviors and explored how they were influenced by their cultural identities and experiences. This diary study identified indications of connections between cybersecurity behavior, risk tolerance, and cultural identities.

With these insights, this paper proposes the notion that user-centric solutions that allow for a socio-technical view of the threat landscape could improve cybersecurity. The paper explores five principles upon which to build an inclusive cybersecurity framework. These principles focus on the perils of groupthink and the necessity of diversity and inclusion, individual-centrism, and clear communication. The paper concludes with examples of how applying these principles could provide a better outcome than traditional, technology-centric solutions.

Safer Together: Inclusive Cybersecurity

The Need to Factor the Individual Into Cybersecurity

Two decades ago, cybersecurity risks were largely mitigated through training and policies implemented by internal security teams in the "in-office" environment. Organizations created prescriptive security programs that dictated how, when, where, and why an employee could engage with the company network and technology. These programs viewed users solely through the lens of their employment status.

However, legacy cybersecurity programs became outmoded and ineffectual as technology migrated to homes and personal lives.[5] Remote work has further blurred the line between the personal and professional.[6] Citizens move throughout the day with few, if any, borders between work and personal technology, especially with their mobile devices. The corporate data security team can no longer control network access when employees rely on personal devices to do their jobs. The risks compound as those employees use corporate systems for personal activities. A 2021 survey found that younger people increasingly use corporate email for personal use, including online shopping.[7] Given the threat landscape, security teams cannot rely solely on how a corporate system is *supposed* to operate.

According to a 2021 PricewaterhouseCoopers survey, "employees — especially those of the millennial generation (51%) and generation Z (45%) — admit to using applications and programs on their work devices that their employer has expressly prohibited."[8] The use of personal VPNs, file sharing applications, or personal file storage (e.g., DropBox, Box, Google Drive), and the use of unauthorized USBs quickly create vulnerabilities in the corporate network defense.

This inclination to skirt corporate cybersecurity rules is driven by a desire for convenience, the disconnect from the often rigid instructions from security teams, real-world workflow demands, and cultural norms. For example, the forensic investigation into a 2008 breach of U.S. military systems found the initial access point came from a single flash drive. A soldier needed to move information from one system to another. Despite having been trained on the cybersecurity risks of moving the information via a thumb drive instead of the usual, more cumbersome, data transfer process, battlefield tempo necessitated taking the risk. The individual assessed the immediate need to provide information to assist his comrades under fire outweighed a possible cybersecurity threat lurking in the data. After detection, it took the Pentagon another 14 months to remove the malware and the hackers — likely Russian — from U.S. systems.[9]

In a study by Brigham Young University's Marriott School of Business, three rationales accounted for 85 percent of intentional rule-breaking: "to better accomplish tasks for my job," "to get something I needed," and "to help others get their work done."[10] Individuals do what they always do when confronted with rules and regulations that appear to make their lives more difficult: they improvise workarounds. Cybersecurity best practices often ignore this basic human instinct and, by doing so, fail the user and the broader ecosystem.

Instead of basing threat evaluations on how a system should work, security teams must "account for unexpected user behavior," concluded the Lawfare Institute's Trusted Hardware and Software Working Group. This concept of "socio-

5. Thulani Mashiane and Elmarie Kritzinger, "Identifying Behavioral Constructs In Relation To User Cybersecurity Behavior." *Eurasian Journal of Social Sciences*, 2021, pages 98-122. (https://ideas.repec.org/a/ejn/ejssjr/v9y2021i2p98-122.html)

6. "The cyber-threat landscape: The digital rush left many exposed," *PricewaterhouseCoopers,* April 2021. (https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/2021-digital-trust-insights/cyber-threat-landscape.html)

7. SailPoint, Press Release, "New SailPoint Survey Exposes Concerning Generational Differences Regarding Corporate Email Use and Cybersecurity Posture," November 3, 2021. (https://www.sailpoint.com/press-releases/new-sailpoint-survey-exposes-concerning-generational-differences-regarding-corporate-email-use-and-cybersecurity-posture)

8. "The cyber-threat landscape: The digital rush left many exposed," *PricewaterhouseCoopers,* April 2021. (https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/2021-digital-trust-insights/cyber-threat-landscape.html)

9. "Agent.btz," *Council on Foreign Relations,* November 2008. (https://www.cfr.org/cyber-operations/agentbtz)

10. Clay Posey and Mindy Shoss, "Research: Why Employees Violate Cybersecurity Policies," *Harvard Business Review*, January 20, 2022. (https://hbr.org/2022/01/research-why-employees-violate-cybersecurity-policies)

technical integration considers how people interact with the system."[11] Security teams can better mitigate "unexpected user behavior" when they better understand the user. The unexpected can then become more predictable.

Inclusivity as the Core of a User-Centric Security Program

Understanding user behavior requires understanding and appreciating how users' identities (economic, cultural, racial, ethnic, gender, and age) affect cybersecurity decisions. Researchers are now exploring how cultural identity correlates with poor security behaviors and increased susceptibility to cybercrimes, such as phishing or social engineering.[12] The work in this area is limited, however, especially as it relates to racial identity and ethnicity.

The nature of a user's identity is complex and layered. It is possible, however, to ascertain trends. Cultural norms often impact how and when individuals engage with technology and develop cybersecurity behaviors. Groups with shared identity attributes and shared experiences often behave similarly in cyberspace. According to Reinier Moquete, the co-founder of the Latino STEM Alliance, "Latinos often have reservations when it comes to asking for computer-related help, particularly when it may be necessary to go outside their immediate circle to get that assistance. Exacerbating that situation is the fact that despite being united by a common language, the Latino community is comprised [*sic*] of many distinct cultures. These cultural differences, along with a sense of safety and belonging by staying close to what's familiar, keep [the community] segregated into ethnic pockets that ultimately further limit the knowledge base within each group."[13] This cultural dynamic can influence how members of the community learn and adopt cybersecurity best practices.

American Indian, Alaska native, and indigenous native peoples have a unique government-to-government relationship with Washington. Sovereignty and culture inform their use and adaptation of contemporary communication technologies.[14] Tribal elders may be especially leery of the damage technology can bring indirectly to traditional culture and community through the exposure to content viewed as harmful in a cultural context and directly to public health and safety through cyberattacks on their critical infrastructure.

A 2019 cyberattack highlighted the intersection of these threats. On December 7, 2019, Russian cybercriminals attacked the IT infrastructure of the town of Cherokee, capital of the Eastern Band of Cherokee Indians (EBCI), a federally recognized tribe of more than 16,000 members.[15] The criminals were most likely hoping to access the accounts of the Cherokee Nation Business, a tribally owned holding company of the Cherokee Nation that generates nearly $2 billion in annual revenue.[16] Among other damage inflicted by the ransomware attack was the loss of a library of irreplaceable Cherokee language audio and video files the tribe had invested 15 years in collecting. Richard Sneed, principal chief of the EBCI said at the time, "There is a way to speak the language and we've only got 160-some fluent speakers left...

11. Paul Rosenzweig et al., "Creating a Framework for Supply Chain Trust in Hardware and Software," *Lawfare*, May 2022, page 16. (https://s3.documentcloud.org/documents/21831749/creating-a-framework-for-supply-chain-trust-in-hardware-and-software.pdf)

12. Serge Egelman and Eyal Peer, "Scaling the Security Wall: Developing a Security Behavior Intentions Scale (SeBIS)," *Association for Computing Machinery*, April 2015, pages 2,873-2,882. (https://dl.acm.org/doi/10.1145/2702123.2702249); Margaret Gratian, Sruthi Bandi, Michel Cukier, Josiah Dykstra, and Amy Ginther, "Correlating human traits and cyber security behavior intentions," *Computers & Security*, March, 2018, pages 345-358. (https://www.sciencedirect.com/science/article/pii/S0167404817302523)

13. Reinier Moquete, "Barriers to cyber security in Latino community," *Boston Business Journal*, September 14, 2012. (https://www.bizjournals.com/boston/print-edition/2012/09/14/barriers-to-cyber-security-in-latino.html)

14. Marisa Elena Duarte, *Network Sovereignty: Building the Internet across Indian Country* (Seattle: University of Washington Press, 2017). (https://uwapress.uw.edu/book/9780295741826/network-sovereignty)

15. Bill Briggs, "After a devastating cyberattack, the Eastern Band of Cherokee Indians became a technologically advanced nation," *Microsoft*, September 13, 2022. (https://news.microsoft.com/source/features/digital-transformation/after-a-devastating-cyberattack-eastern-band-of-cherokee-indians-most-technologically-advanced-nations)

16. "Our Company," Cherokee Nation Businesses, accessed March 6, 2023. (https://cherokeenationbusinesses.com/our-company)

Safer Together: Inclusive Cybersecurity

That data is lost and gone forever. It's priceless. It carries a long-term cultural impact that I don't think most people give thought to."[17]

Improperly staffed security teams and the complexity in the relationship and data sharing with federal law enforcement contributed to the attack and the ensuing destruction. "Tribal Nations cyber security preparedness and maturity continues to fall well short of state and local governments," the National Congress of American Indians affirmed citing the National Cybersecurity Review.[18] According to a study by the law firm Holland & Knight, "tribal governments continue to be largely left out of federal opportunities to build critical cybersecurity infrastructure and internal protocols that keep tribal data safe."[19]

Different populations face different threats. Ethnic and gender minorities, for example, often face more severe cyber threats, making effective cybersecurity even more important.[20] A study by Recorded Future, one of the world's largest cyber threat intelligence companies, found that the Black community is more susceptible to fraud campaigns compared to other racial and ethnic groups. Hackers use phishing lures based on trending current events, including movements such as Black Lives Matter. Organizations advocating for racial justice and equality are frequently targets for distributed denial of service attacks. Foreign information operations also target the Black community to further polarize U.S. politics and sour the community on the political process.[21]

Indeed, a 2021 Aspen Institute study on disinformation concluded that "false information, which proliferates on social media, disproportionately impacts marginalized communities."[22] Russian disinformation during the 2016 presidential election specifically targeted Black Americans.[23] Other mis- and disinformation campaigns around the census and the 2020 U.S. election targeted Latino Americans through the explosion of Spanish-language misinformation campaigns on social media.[24] Mis- and disinformation related to the COVID-19 pandemic led to an increase in physical violence and hate speech against Asian American communities.[25] Foreign and domestic actors also leverage disinformation and smear campaigns to perpetuate online abuse against women and gender minorities.[26]

Additional or nontraditional support is needed to counter these threats and to bridge the systemic digital divide. Meanwhile, understanding a particular community's cultural and historic context — how they interact with the judicial

---

17. Bill Briggs, "After a devastating cyberattack, the Eastern Band of Cherokee Indians became a technologically advanced nation," *Microsoft*, September 13, 2022. (https://news.microsoft.com/source/features/digital-transformation/after-a-devastating-cyberattack-eastern-band-of-cherokee-indians-most-technologically-advanced-nations)

18. National Congress of American Indians, Resolution #DEN-18-012 "Support for Tribal Nations' Access to Cyber Security Services and Funding," October 21-26, 2018. (https://www.ncai.org/resources/resolutions/support-for-tribal-nations-access-to-cyber-security-services-and-funding)

19. Kayla Gebeck Carroll and Marissa C. Serafino, "Tribal Governments Advocate for Cybersecurity Funding in Next COVID-19 Package," Holland & Knight, June 2, 2020. (https://www.hklaw.com/en/insights/publications/2020/06/tribal-governments-advocate-for-cybersecurity-funding)

20. Nina Jankowicz, Jillian Hunchak, Alexandra Pavliuc, Celia Davies, Shannon Pierson, and Zoe Kaufmann, "Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online," *Wilson Center,* January 2021. (https://www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online)

21. Insikt Group, "Cyber Threats to the Black Community," *Recorded Future,* March 2, 2021. (https://go.recordedfuture.com/hubfs/reports/cta-2021-0302.pdf?hsCtaTracking=fc239c11-547b-4007-a722-ef6fa33c715c%7C94208a21-e8ca-42f0-ab71-65d083461fa0)

22. "The Commission on Information Disorder Final Report," *The Aspen Institute,* November 2021. (https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute_Commission-on-Information-Disorder_Final-Report.pdf)

23. Naima Green-Riley and Camille Stewart, "A Clapback to Russian Trolls," *The Root*, February 28, 2020. (https://www.theroot.com/a-clapback-to-russian-trolls-1841932843); Janell Ross, "Russia's election interference exposes America's Achilles' heel: Race," *NBC News,* December 19, 2018. (https://www.nbcnews.com/news/nbcblk/russia-s-election-interference-exposes-america-s-achilles-heel-race-n949796)

24. Amanda Seitz and Will Weissert, "Inside the 'big wave' of misinformation targeted at Latinos," *Associated Press,* December 1, 2021. (https://apnews.com/article/latinos-misinformation-election-334d779a4ec41aa0eef9ea80636f9595)

25. Jonathan Corpus Ong, "Online Disinformation Against AAPI Communities During the COVID-19 Pandemic," *Carnegie Endowment for International Peace,* October 19, 2021. (https://carnegieendowment.org/2021/10/19/online-disinformation-against-aapi-communities-during-covid-19-pandemic-pub-85515)

26. Nina Jankowicz, Jillian Hunchak, Alexandra Pavliuc, Celia Davies, Shannon Pierson, and Zoe Kaufmann, "Malign Creativity: How Gender, Sex, and Lies are Weaponized Against Women Online, *Wilson Center,* January 2021. (https://www.wilsoncenter.org/publication/malign-creativity-how-gender-sex-and-lies-are-weaponized-against-women-online)

and education systems, for example — is essential to combating cyber-enabled information operations targeting the community.[27]

The Research: The correlation Between Individual Identity and Cybersecurity Behavior

To better understand the correlation between cultural identity and cybersecurity behaviors, the author conducted two small-scale studies. The first was a social media survey to determine if differences in cybersecurity behavior correlate with identity. The second was a limited diary study to further explore the correlation between identity and cybersecurity behaviors.[28] While the entire topic deserves much more study, the initial findings suggest an urgent need for security controls and programs to ensure that marginalized groups (whether due to race, culture, gender, or even age) are not excluded from cybersecurity.

Social Media Survey Observations

In the first study, rather than conducting a traditional phone survey, participants were recruited on social media. The 853 participants represented a diverse group based on sex, age, race, and region. They answered questions about their cybersecurity behavior, including knowledge of phishing, password protection, email best practices, and two-factor authentication (2FA).

Analysis of the findings pointed to three trends indicating a potential link between certain cybersecurity behaviors and demographics. (Appendix A lists all significant findings.)

The findings indicate that gender may influence cybersecurity behavior.[29] Men were more likely to use public Wi-Fi, reuse passwords, and use weak passwords. At the same time, men were more likely to use password storage software, enable automatic software updates, and demonstrate familiarity about 2FA and phishing. Taken together, these behaviors may sound contradictory, but they align with other, better studied trends observed among males. For example, men are three times more likely to engage in risky online behavior compared to women, according to a study by SecurityAdvisor in 20 different countries.[30]

Age also appears to influence cybersecurity behavior. Younger people were more likely to use strong passwords (but reuse those passwords) and to be familiar with 2FA. Additionally, younger people were more likely to use public Wi-Fi, although this may be related more to lifestyle habits (how often a population works from public areas) rather than a cybersecurity choice.

This correlation between age and cybersecurity behavior aligns with other studies on the topic.[31] Studies show, for example, that Gen Z — a born-digital generation — is technologically savvy yet prone to sacrificing privacy and security for personalized experiences, e.g., by providing websites and applications with personal data in exchange for more tailored content or advertisements.[32] Younger generations also seem to have less of an understanding of cybersecurity

27. Charles M. Blow, "How Black People Learned Not to Trust," *The New York Times,* December 6, 2020. (https://www.nytimes.com/2020/12/06/opinion/blacks-vaccinations-health.html)

28. A diary study collects qualitative data about user behaviors, activities, and experiences over time — ranging from a few days to even a month or longer. See: Kim Salazar, "Diary Studies: Understanding Long-Term User Behavior and Experiences," *Nielsen Norman Group,* June 5, 2016. (https://www.nngroup.com/articles/diary-studies)

29. The survey asked respondents to identify as male or female. The sample did not explicitly include gender minorities (e.g., nonbinary people, trans men, trans women). Understanding cybersecurity behavior trends amongst gender minorities, however, is an important part of understanding how gender affects or influences cybersecurity. This knowledge will help address unique threats and challenges faced by women and the LGBTQIA community members.

30. "Support the Human Firewall by Identifying the Riskiest Users and Their Most Dangerous Online Behaviors," *SecurityAdvisor,* accessed March 16, 2023. (https://www.securityadvisor.io/risky-behavior-report)

31. Abe Selig, "Generation Influence: Reaching Gen Z in the New Digital Paradigm," *WP Engine,* December 9, 2022. (https://wpengine.com/gen-z-us)

32. Eileen Brown, "Gen Z willing to provide their personal data for more personalized experiences," *ZDNet*, March 6, 2019. (https://www.zdnet.com/article/gen-z-willing-to-provide-their-personal-data-for-more-personalized-experiences)

threats, including phishing. A 2021 study by enterprise security company SailPoint found that while all respondents were confident in their ability to identify a phishing email, the majority did not know to report it to corporate IT security. Remarkably, 46 percent of Gen Z respondents said they would open a phishing link or attachment, compared to 29 percent of Millennials, four percent of Gen X, and just one percent of Baby Boomers.[33]

This trend of risk-tolerant behaviors appears to continue with the next generation. While there are few studies on the cybersecurity behaviors of children, a 2021 National Institute of Standards and Technology study found that children are embracing many cybersecurity best practices yet still demonstrating bad password habits.[34]

Education and income also appear to be determinants of cybersecurity behavior. Higher income individuals were more likely to use automatic software updates, change their passwords regularly, use password storage software, and demonstrate a willingness to use 2FA. Those who continued schooling past high school were more likely to use strong passwords, to be familiar with phishing, and to have avoided phishing in the past.

Diary Study Highlights

Building on the insights from the survey, the author commissioned a diary study in an attempt to better understand user behavior, identify trends, and collect personal anecdotes about whether and how cultural identity informs cybersecurity. The study was conducted over the course of two weeks in 2021. It included 37 people in the United States with varied ethnic backgrounds, gender identities, age, income, and education. With such a small group, the study could not examine a full range of cultural identities.[35] Nor did the diary study consider other behavioral factors.[36]

Identity "categories only serve the purpose of classification; in the real world, differences between these categories are blurred," caution Harvard's Celia de Anca and Salvador Aragón in a 2018 Harvard Business Review article.[37] However, these categories are useful constructs that help explain how identity informs behavior and may help create a better security culture.

The anecdotal evidence of the diary study illuminated how cybersecurity intersects with cultural identity and underscored the need for more rigorous research regarding ethnicity, gender identity, parental status (rearing children or not), and immigrant ties (either being an immigrant or having an immigrant parent or grandparent) on cybersecurity awareness and implementation of best practices. (See Appendix B.)

Study participants said their ethnic identity informs their risk tolerance in general and cybersecurity behavior specifically. One participant noted, "being a Black woman definitely heavily influences...my security and my privacy... I feel like as a woman, security is extremely important. And so I make sure that I'm extra vigilant."[38] Another African American woman said, "I have a son and a daughter, and we all identify as African-Americans... We have to take all types of security extremely serious."[39]

---

33. SailPoint, Press Release, "New SailPoint Survey Exposes Concerning Generational Differences Regarding Corporate Email Use and Cybersecurity Posture," November 3, 2021. (https://www.sailpoint.com/press-releases/new-sailpoint-survey-exposes-concerning-generational-differences-regarding-corporate-email-use-and-cybersecurity-posture)

34. "NIST Study on Kids' Passwords Shows Gap Between Knowledge of Password Best Practices and Behavior," *National Institute of Standards and Technology,* August 11, 2021. (https://www.nist.gov/news-events/news/2021/08/nist-study-kids-passwords-shows-gap-between-knowledge-password-best)

35. Celia de Anca and Salvador Aragón, "The 3 Types of Diversity That Shape Our Identities," *Harvard Business Review,* May 24, 2018. (https://hbr.org/2018/05/the-3-types-of-diversity-that-shape-our-identities)

36. Thulani Mashiane and Elmarie Kritzinger, "Identifying Behavioral Constructs In Relation To User Cybersecurity Behavior." *Eurasian Journal of Social Sciences*, 2021, pages 98-122. (https://ideas.repec.org/a/ejn/ejssjr/v9y2021i2p98-122.html)

37. Celia de Anca and Salvador Aragón, "The 3 Types of Diversity That Shape Our Identities," *Harvard Business Review,* May 24, 2018. (https://hbr.org/2018/05/the-3-types-of-diversity-that-shape-our-identities)

38. Twenty-nine-year-old Black woman from Richmond VA, college educated, full-time employment in entertainment and leisure, diary study respondent.

39. Thirty-nine-year-old woman, Detroit Michigan, some college, single with kids, entrepreneur, diary study respondent.

An Asian American participant also emphasized the connection between race and privacy. She said, "I think my race and my upbringing has a lot of influence on my privacy and security habits online. Growing up, I had my parents always ensuring that I'm posting stuff online that is not going to incriminate me for the future. In a way, they have been kind of strict about my online presence. So in turn, as I have gotten older, I make sure that I keep a lot of things about me like personal things very, very private. And now that I am an adult with a daughter, I make sure that [with] her presence online also, she stays safe and private."[40]

Another participant, a Middle Eastern and North African American woman, noted the influence of religion on her cybersecurity practices. "I'm a lot more private about what I post online since I do wear the veil, the scarf. I don't post pictures of me without my scarf online, so I was careful with that and I don't reveal a lot of information online. I keep my personal life pretty much personal."[41]

Wariness of posting personal information is often associated with good cybersecurity hygiene. A heightened sense of risk, however, can have a perverse effect of making an individual less cybersecure. This imbalance can be seen within the immigrant and diaspora communities who do not necessarily trust the tools that are commonly associated with cybersecurity.[42] As one first-generation American from Colombia remarked, "being an immigrant made me more skeptical and careful having to start life somewhere else and figure things out and kind of get messed over and taken advantage of in some situations and made me just kind of question things, you know, like when they say, like, 'Oh, use a password manager,' I'm like, 'Whatever, the password manager gets hacked.'"[43]

As might be expected, work and school are still the best sources of cybersecurity and privacy information for most users. In this regard, the diary study mirrored findings in other studies. Indeed, users encounter the most security structure and guidance in the workplace and classroom. And while these institutions have the greatest potential to drive a change in individual cyber behavior, the focus must shift to include those individuals who do not benefit from these structures.

Inclusive Cybersecurity Principles

Cyberattacks succeed when defenses fail and normal users are manipulated.[44] According to Peiter "Mudge" Zatko, a network security expert, this can occur when attackers exploit scenarios where diversity is not considered or understood, providing an operational weakness.[45] The Aspen Institute report on disinformation, for example, concludes that a "persistent root cause" driving mis- and disinformation to affect marginalized communities disproportionally is "a lack of diverse perspectives in positions of power and homogenous decision making within platform companies and news media."[46]

Jon Kaltwasser, who has led cybersecurity efforts within the U.S. government and private sector, has come to similar conclusions best illustrated by his participation in a hack-a-thon. He explained to the author how his team weaponized a lack of diversity to win a prominent Capture the Flag hacking competition at DefCon, one of the best known and largest computer security competitions.[47] Kaltwasser and his team saw that the opposing teams were entirely male. Jon's team

40. Thirty-two-year-old Asian American woman, Alexandria, VA, married with children, post-grad coursework, student, diary study respondent.

41. Thirty-eight-year-old MENA American woman, Dearborn Heights, MI, college educated, full-time employment, married with children, diary study respondent.

42. Shabnam Etemadi Brady and Michelle C. Stevens, "Is immigration a culture? A qualitative approach to exploring immigrant student experiences within the United States," *Translational Issues in Psychological Science,* March 1, 2019, pages 17-28. (https://www.scinapse.io/papers/2920870421)

43. Twenty-five-year-old man from Cypress, TX, Colombian American (Latin American), high school graduate, full-time employment, diary study respondent.

44. James Hadley, "The defensive power of diversity in cybersecurity," *TechCrunch,* December 6, 2021. (https://techcrunch.com/2021/12/06/the-defensive-power-of-diversity-in-cybersecurity)

45. Interview with Peiter "Mudge" Zatko on April 21, 2022.

46. "The Commission on Information Disorder Final Report," *The Aspen Institute,* November 2021. (https://www.aspeninstitute.org/wp-content/uploads/2021/11/Aspen-Institute_Commission-on-Information-Disorder_Final-Report.pdf)

47. Interview with Jon Kaltwasser on April 27, 2022.

baited opponents by having a female member of their team dress a bit risqué and spend day one asking the other teams for help. She asked questions about their defenses and pretended to be new and eager to learn. The men jumped to be of assistance. They revealed details about their defensive strategy and left her alone with systems such that she could insert USB drives and install software onto their machines. By the end of the day, Kaltwasser's team had mapped out how the opposing teams, and each of their individual players, functioned. Kaltwasser credits his team's win in part to this social engineering exercise.

Kaltwasser notes, "the lack of diversity creates bias and as an attacker you want to identify those gaps and leverage them. On the red teaming side, you are always looking for bias because it equals a blind spot. Diversity is a deterrent." In subsequent years, opposing teams were more diverse, and Kaltwasser's team could no longer employ the same tactic.

The following inclusive cybersecurity principles are fundamental precepts from which a user-centric security program can be derived. These principles are informed by research on product inclusion, scientific bias doctrine, diversifying the cyber workforce, and standard security frameworks and programs.[48] When applied together, these principles are a force multiplier for the work of an already strong security program.

1. Cybersecurity must center on the people it serves.

While it is easy to focus on technology when trying to solve cybersecurity challenges, technology is only as effective as its users, who operate in a specific social environment. Understanding that environment — the social factors (political, economic, and cultural) and the stakeholders involved (technology operators, technology developers, malicious actors, and users) — enhances security.

To balance operational needs, security, and convenience, security practitioners must work harder to understand users and the way they interact with technology.[49] The differing behaviors and risk tolerances across user groups undermines the traditional one-size-fits-all cybersecurity solution mentality. A new approach to research, including usability testing, trend analysis of the user base, user feedback, product and process improvement sprints, and periodic reviews can better identify solutions that enable security for all users.

Usability testing is already a common practice, where companies put products in the hands of users to measure how they interact with them.[50] This testing could also assess how different communities interact differently with a new product or new security feature.

2. Human biases must be recognized and minimized in cybersecurity.

The lack of diversity within the cybersecurity developer corps may lead to security practices that cannot easily be applied in all scenarios for all individuals. An apt analogy: The large corpus of research on non-diverse medical trials has shown that "many groups underrepresented and excluded in clinical research can have distinct disease presentations or health circumstances that affect how they will respond to an investigational drug or therapy."[51] A 2022 report, commissioned by Congress and conducted by the National Academies of Sciences, Engineering, and Medicine, found that "hundreds of

48. Annie Jean-Baptiste, *Building For Everyone: Expand Your Market With Design Practices From Google's Product Inclusion Team* (New York: Wiley, 2020). (https://www.wiley.com/en-us/Building+For+Everyone%3A+Expand+Your+Market+With+Design+Practices+From+Google%27s+Product+Inclusion+Team-p-9781119646228)

49. "Creating a Framework for Supply Chain Trust in Hardware and Software," *Lawfare*, May 2022, page 16. (https://s3.documentcloud.org/documents/21831749/creating-a-framework-for-supply-chain-trust-in-hardware-and-software.pdf)

50. Ellen Merryweather, "Product Management Skills: User Research," *Product School,* September 19, 2020. (https://productschool.com/blog/product-management-2/product-management-skills-user-research)

51. *Improving Representation in Clinical Trials and Research: Building Research Equity for Women and Underrepresented Groups,* Eds. Kirsten Bibbins-Domingo and Alex Helman (Washington: National Academies Press, 2022). (https://nap.nationalacademies.org/read/26479/chapter/2)

billions of dollars will be lost over the next 25 years due to reduced life expectancy, shortened disability-free lives, and fewer years working among populations that are not proportionately represented in clinical trials."[52]

One of the root causes for the lack of diversity in medical trials is the lack of diversity in the medical research teams themselves, leading to acknowledged and unacknowledged biases.[53] The use of artificial intelligence may be compounding these problems. As William Greig Mitchell, of the Harvard T.H. Chan School of Public Health in Boston has written, "Repeatedly feeding models with relatively homogeneous data, suffering from a lack of diversity in terms of underlying patient populations and often curated from restricted clinical settings, can severely limit the generalizability of results and yield biased AI-based decisions."[54]

Both human and machine processes of cybersecurity programs may reflect similar biases, eroding their efficiency. Insider threat programs, for example, often suffer from a lack of diversity of life experience. When reviewers see demographic data (e.g., race, gender, nationality) about employees with access to sensitive systems, confirmation bias may cause them to forego fully investigating some incidents while diverting attention to lower risks.[55] Some programs have elevated the level of risk assigned to employees based on their visa status, country of origin, or nationality.[56] While this may be relevant for certain projects or programs, especially where related to the U.S. federal government, at other times it can lead to wasted resources investigating false positives, erosion of employee trust, potential legal liability, and impairment of an organization's ability to hire and retain staff.[57]

Bias training and tools like red teaming can help build awareness and create opportunities to mitigate bias. In addition to conducting bias awareness training and building diverse teams, insider threat programs and other cybersecurity efforts should focus on technical steps that address bias, like anonymizing data to decrease the chances that demographic information will influence decision-making. Security programs achieve better outcomes when they do not presuppose certain threats while overlooking others.

3. Groupthink in cybersecurity is fatal. The antidote is diversity.

In 1972, Irving Janis published his seminal work on "groupthink" and the Bay of Pigs disaster. Although writing decades before the internet age and the scourge of cyberattacks, Janis accurately pinpointed what has become a failure in cyber security research, design, and implementation. Janis wrote that there is a "mode of thinking that persons engage in when *concurrence-seeking* becomes so dominant in a cohesive ingroup that it tends to override realistic appraisal of alternative courses of action."[58] "Equal is not always equitable" is a common product inclusion principle and an important reminder in security.[59] Applying the same security controls across communities and user groups may not yield the same or similar outcomes. Greater efficacy in cybersecurity requires modifying or redesigning to consider and account for the unique needs, perspectives, and preferences of certain user groups, particularly historically underrepresented users, older

52. Dana Goldman, PhD, Edith A. Perez, MD, and Carlos del Rio, MD, "Lack of Diversity in Clinical Trials Costs Billions of Dollars. Incentives Can Spur Innovation," *Leonard D. Schaeffer Center for Health Policy & Economics*, August 5, 2022. (https://healthpolicy.usc.edu/article/lack-of-diversity-in-clinical-trials-costs-billions-of-dollars-incentives-can-spur-innovation)

53. "New Study Finds Severe Lack of Diversity in the Health Care Workforce," *GW Today*, March 30, 2021. (https://gwtoday.gwu.edu/new-study-finds-severe-lack-diversity-health-care-workforce)

54. Hannah Murphy, "Lack of diverse datasets in AI research puts patients at risk, experts suggest," *Health Imagining*, April 11, 2022. (https://healthimaging.com/topics/artificial-intelligence/lack-diverse-datasets-ai-research-puts-patients-risk-experts-suggest)

55. Jason Barnhart, "A Research Review, Countering Insider Threat: Understanding the Bias Mindset While Determining a Response to an Insider Event," *Security Awareness,* April 18, 2021. (See archived version at: https://web.archive.org/web/20211027044408/https:/securityawareness.usalearning.gov/cdse/itawareness/documents/BarnhartJ-NITAM-Essay.pdf)

56. Interview with Michael Sinno on April 19, 2022.

57. INSA's Insider Threats Committee, "Strategies for Addressing Bias in Insider Threat Programs," *Intelligence and National Security Alliance,* January 2022. (https://www.insaonline.org/docs/default-source/default-document-library/2022-white-papers/bias-and-insider-threat-programs-paper.pdf)

58. Irving Janis, *Victims of Groupthink: a Psychological Study of Foreign-Policy Decisions and Fiascoes* (Boston: Houghton Mifflin Company, 1972).

59. Annie Jean-Baptiste, *Building For Everyone: Expand Your Market With Design Practices From Google's Product Inclusion Team,* (New York: Wiley, 2020).

users, or users with special needs. For example, if the primary or only means to add additional security is through two-factor or multifactor authentication, this could cause disproportionate harm to communities that cannot afford multiple devices, may be sharing a device with others, and are most often interacting exclusively on a cell phone. Understanding where controls fall short requires understanding individual communities and being attuned to the disproportionate harm that certain policies can have on them.

Red teaming with a lens for bias, along with reviews and tabletop exercises conducted by a diverse group of experts, can help prevent groupthink and bias. Ensuring the cybersecurity developer corps, alongside the infosec and cyber policy teams, has the requisite diversity of life experience and thought can often have a positive impact on business growth and performance. A May 2020 McKinsey study noted, "Diverse teams are more innovative—stronger at anticipating shifts in consumer needs and consumption patterns that make new products and services possible, potentially generating a competitive edge."[60] Additionally, user reports (or external comments, in the case of a cyber policy) can provide important information to better understand potential impacts on different communities.

In the context of building the cybersecurity technology, protocols, and best practices to counter disinformation, for instance, understanding how disinformation is received and perceived is best done through the creation of more diverse and inclusive teams.

4. Building inclusive cybersecurity requires continuous investment.

Not every demographic can be represented on every team. However, cultivating teams that are conscious of diversity, think outside of their personal circumstances, and consider the cultures and experiences of others can help achieve better levels of cybersecurity. Teams and companies must be intentionally and proactively inclusive when forming teams and in the execution of responsibilities across functions.[61] Structures and processes that reinforce inclusivity and diverse perspectives should check for understanding of unintended impacts and outcomes and identify sources of bias, including bias in data and models. The structures and processes should also consciously recognize that technology is continuously evolving meaning that the individual, and the communities in which they live, have shifting relationships with it. A "set it and forget it" approach to inclusivity and diversity meant to help ensure a better, safer, cybersecurity environment for our citizenry will not succeed.

5. Clear communication is essential to building trust.

Communication between user communities and IT security departments often fails because of misunderstandings. Security practitioners regularly believe security is "too technical for users and communicating to them is not a priority," according to a 2015 study from the University of North Texas.[62] In some cases, users simply do not follow protocols even when they are told how to protect themselves. Meanwhile, when cybersecurity teams focus on securing technology as the primary strategy for preventing cyber threats, they can leave people vulnerable. This myopic focus on technology perpetuates the users' misperception that "cyber-security is mostly a threat at the organization or state-level" and not a personal concern.

60. Kevin Dolan, Dame Vivian Hunt, Sara Prince, and Sandra Sancier-Sultan, "Diversity still matters," *McKinsey and Company*, May 19, 2020. (https://www.mckinsey.com/featured-insights/diversity-and-inclusion/diversity-still-matters)

61. Fostering belonging and psychological safety are integral. See: Henrik Bresman and Amy C. Edmondson, "Research: To Excel, Diverse Teams Need Psychological Safety," *Harvard Business Review*, March 17, 2022. (https://hbr.org/2022/03/research-to-excel-diverse-teams-need-psychological-safety)

62. Susan Squires and Molly Shade, "People, the Weak Link in Cyber-security: Can Ethnography Bridge the Gap?," *American Anthropological Association,* December 1, 2015. (https://anthrosource.onlinelibrary.wiley.com/doi/full/10.1111/1559-8918.2015.01039)

The study concluded, "Effective cyber-threat interventions must begin by using a systemic, ethnographic approach to identify the perspectives and communication styles of both IT groups and that of the communities of users they serve."[63] This starts with understanding the user/stakeholder groups, educating users about threats, and clearly communicating with users and stakeholders. Distilling complex security concepts is an essential part of clear communication. That clarity will help create a shared understanding so user groups can start to develop informed perspectives that contribute to positive outcomes.

Conclusion

Technical teams building controls, operational teams performing security functions, policy teams writing national or internal policy, and research teams seeking to understand security issues should incorporate inclusive principles. To truly be effective, adoption will require a whole-of-organization effort that translates principles into process changes, training, culture changes, and accountability mechanisms. The following list outlines where and how a company could begin implementing the principles:

- **User-focused Cybersecurity Reviews** — Companies can adopt questions in prelaunch and periodic reviews to assess how a technology, policy, product, or tool impacts diverse users.
- **Cybersecurity Inclusivity Review Board** — Companies can form a review board to identify the implications for different groups prior to the launch of new products or policies. Reviewers should be cognizant that new security policies may impact different groups differently, particularly historically underserved groups.
- **User Research** — Companies can conduct usability testing, trend analysis of their user base, solicit user feedback and periodic reviews, and launch product and process improvement sprints to understand how users engage with the security program.

The application of inclusive cybersecurity principles can help shift the culture around cybersecurity. #ShareTheMicInCyber, a grassroots campaign highlighting and amplifying Black cyber practitioners on social media, has begun this important work, but more research and socialization is needed.[64] The campaign began with a single tweet[65] and has catalyzed a movement around diversifying the industry, breaking down barriers, having conversations about cybersecurity inequity, creating space for underrepresented colleagues, and emphasizing the power of individual action.

Government and industry must also move towards adopting inclusive cybersecurity principles into their security programs, policies, operational processes, and product development. This will require leadership and stakeholder buy-in as well as investment from human resources, legal, product, and policy teams. This will take time. To begin, individual companies should pilot and build upon the tools outlined in this paper to develop programs that work for their unique needs. When companies conduct these pilots, they should share best practices and data with academia, across industry, and with the U.S. government to raise the collective level of understanding and investment in user-centric programs.

The work begun here is merely a beginning effort to better understand the implications of user identity and cybersecurity. As a first step, more research is needed on the correlation between user identity and cybersecurity behaviors. The result will be a fuller fleshing out and embrace of the inclusive principles intended to make all of society and its citizens more secure.

63. Ibid.

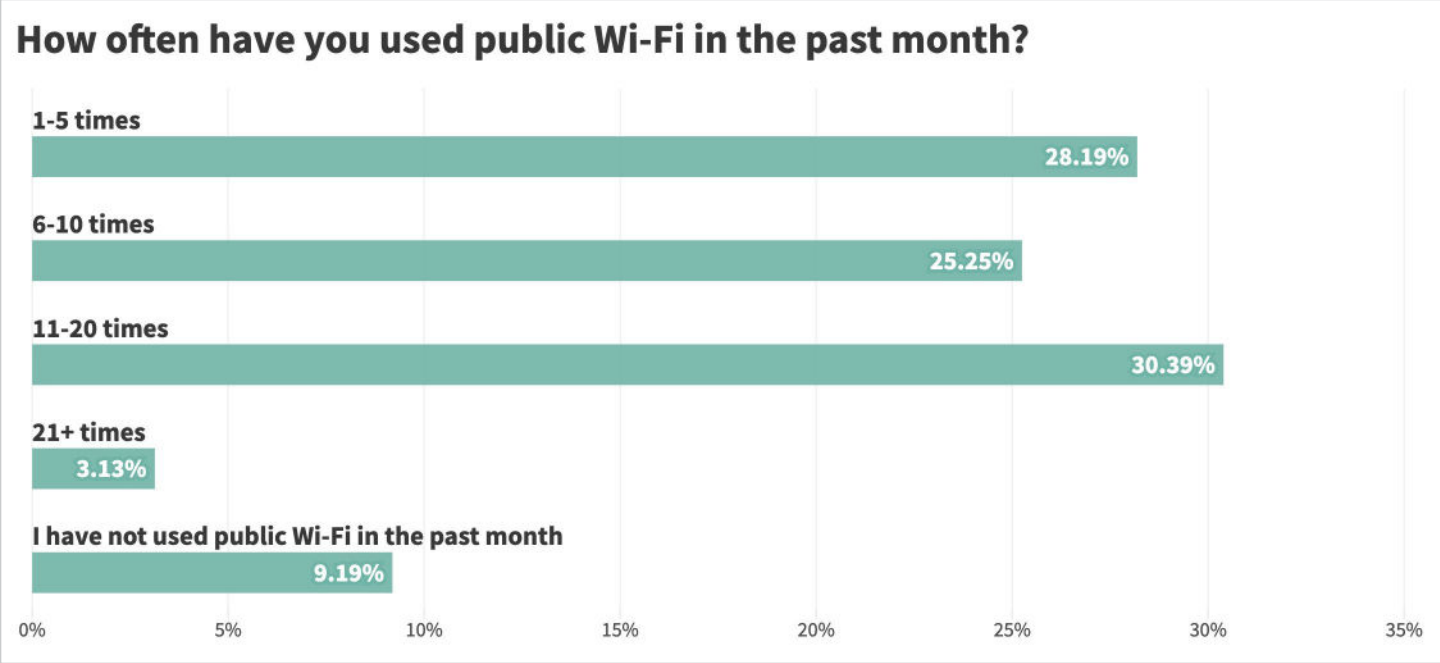
64. "#ShareTheMicInCyber," *Share the Mic in Cyber,* accessed February 28, 2023. (https://www.sharethemicincyber.com)

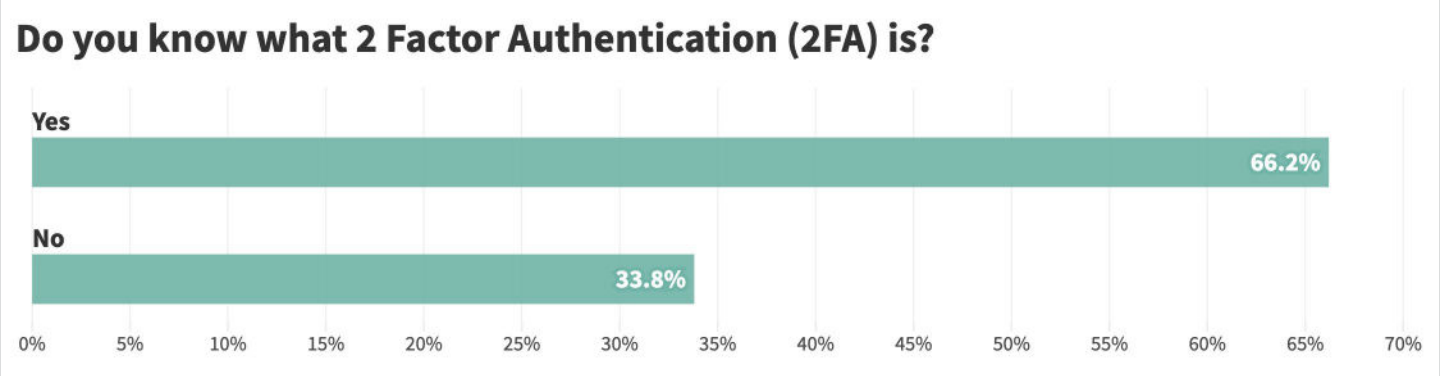
65. CamilleEsq, *Twitter,* June 9, 2020. (https://twitter.com/CamilleEsq/status/1270492873209724928)

Appendix A: Cybersecurity Survey: Results of Regression Analysis

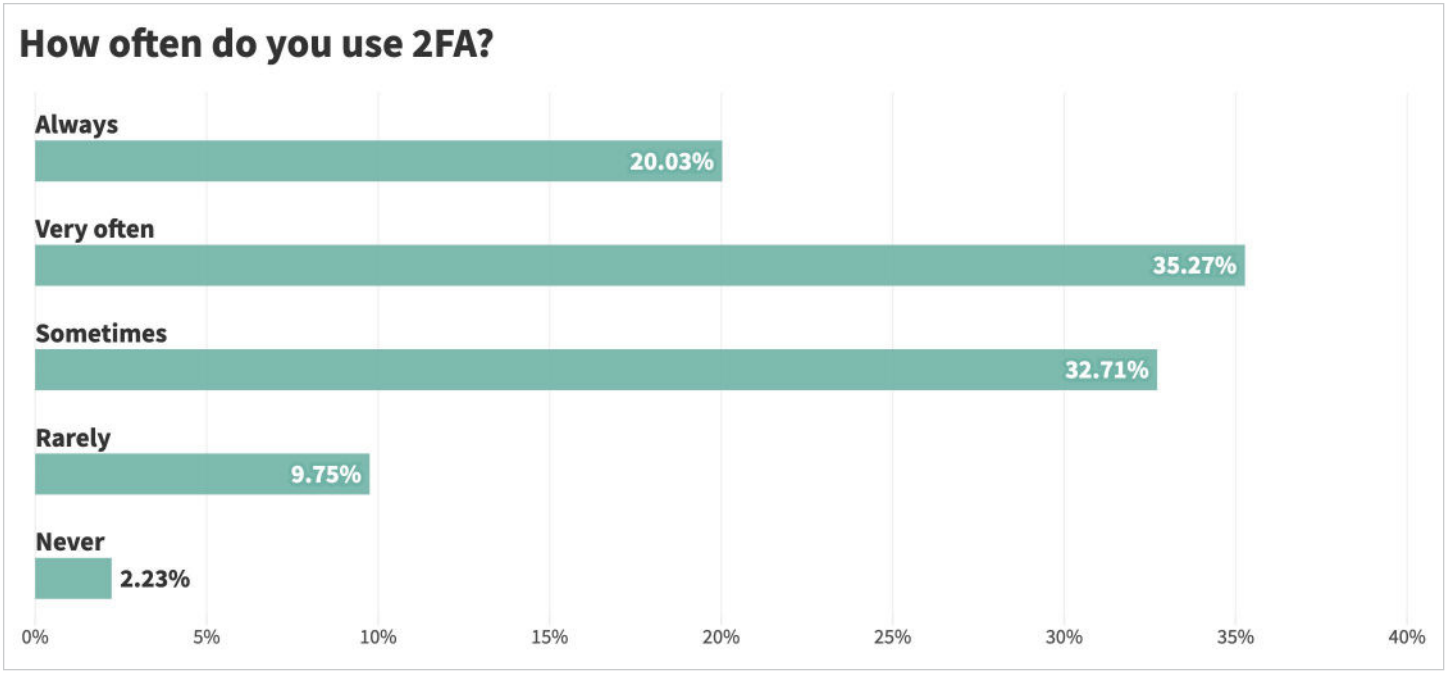
Survey conducted on December 23, 2020, via Pollfish

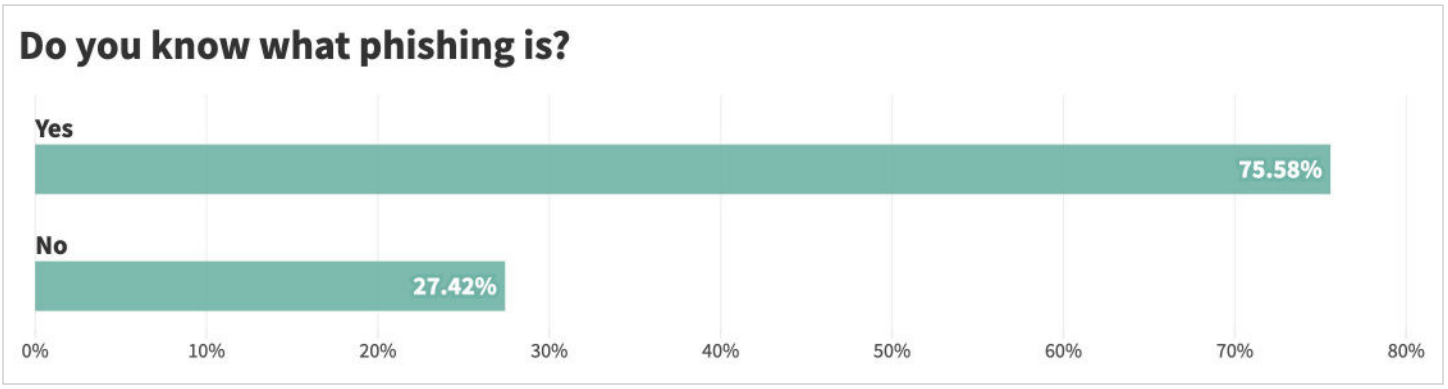
- Survey of 853 U.S. individuals conducted via PollFish. Stratification by age and region
- Gender: 481 Female (56%), 372 Male (44%)
- Race: 587 White (69%), 87 Black (10%), 71 Latino (8%), 43 Asian (5%), 1 Arab (<1%), 64 Other (7.5%)

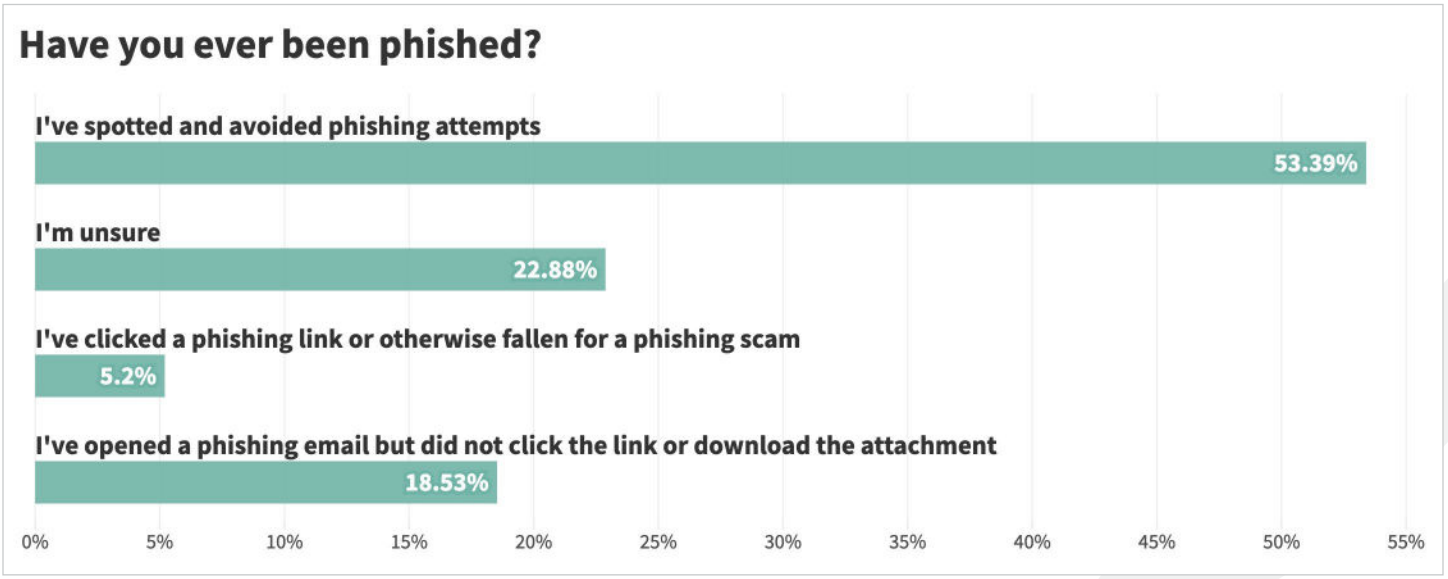




Safer Together: Inclusive Cybersecurity

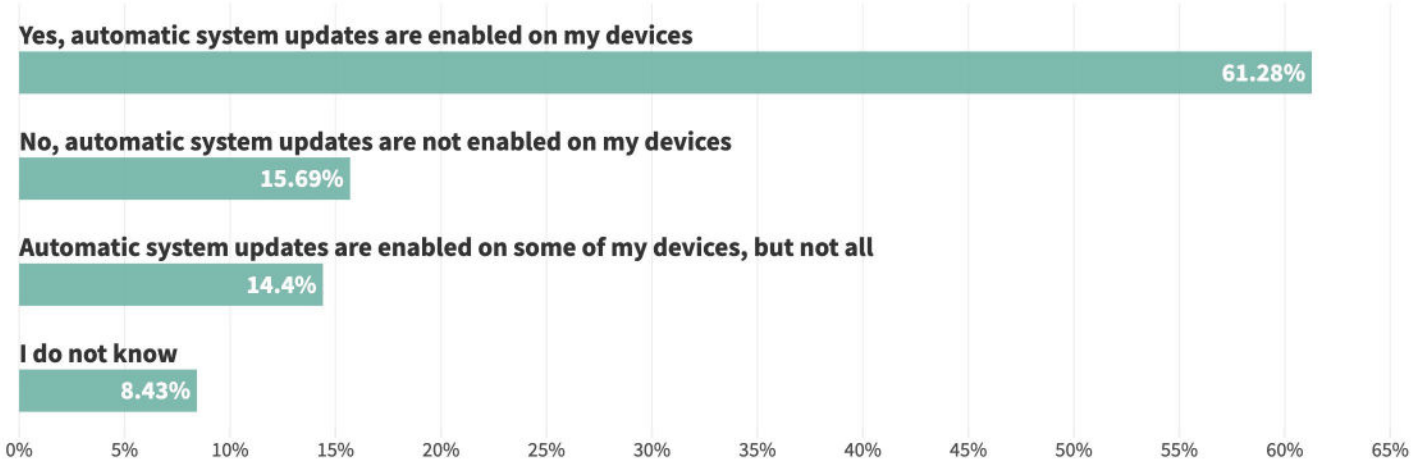




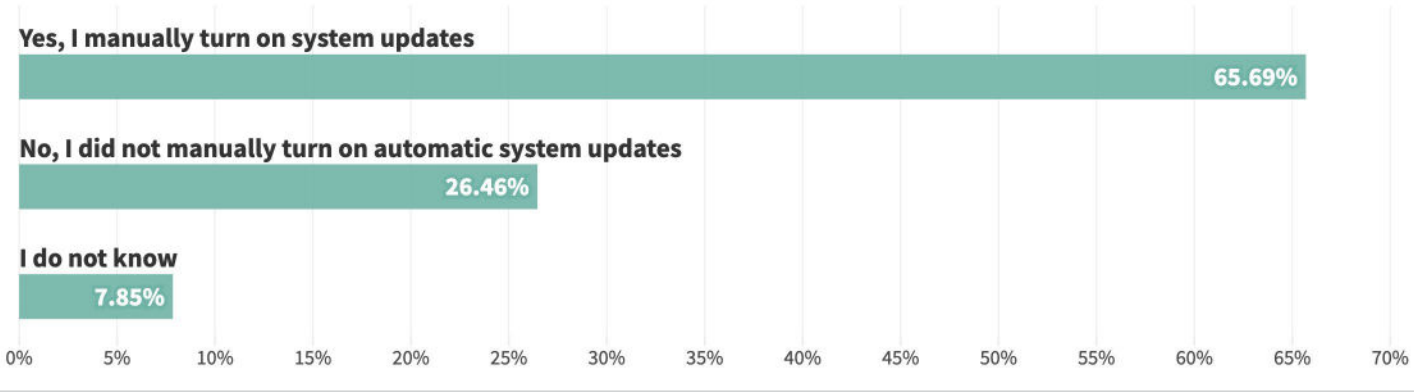


Safer Together: Inclusive Cybersecurity

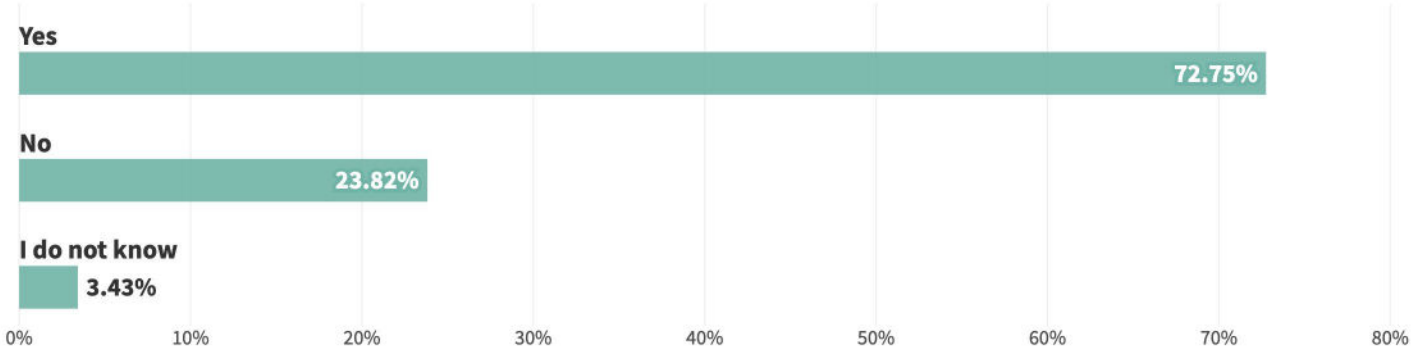
Do you know if automatic system updates are turned on for any of your devices?

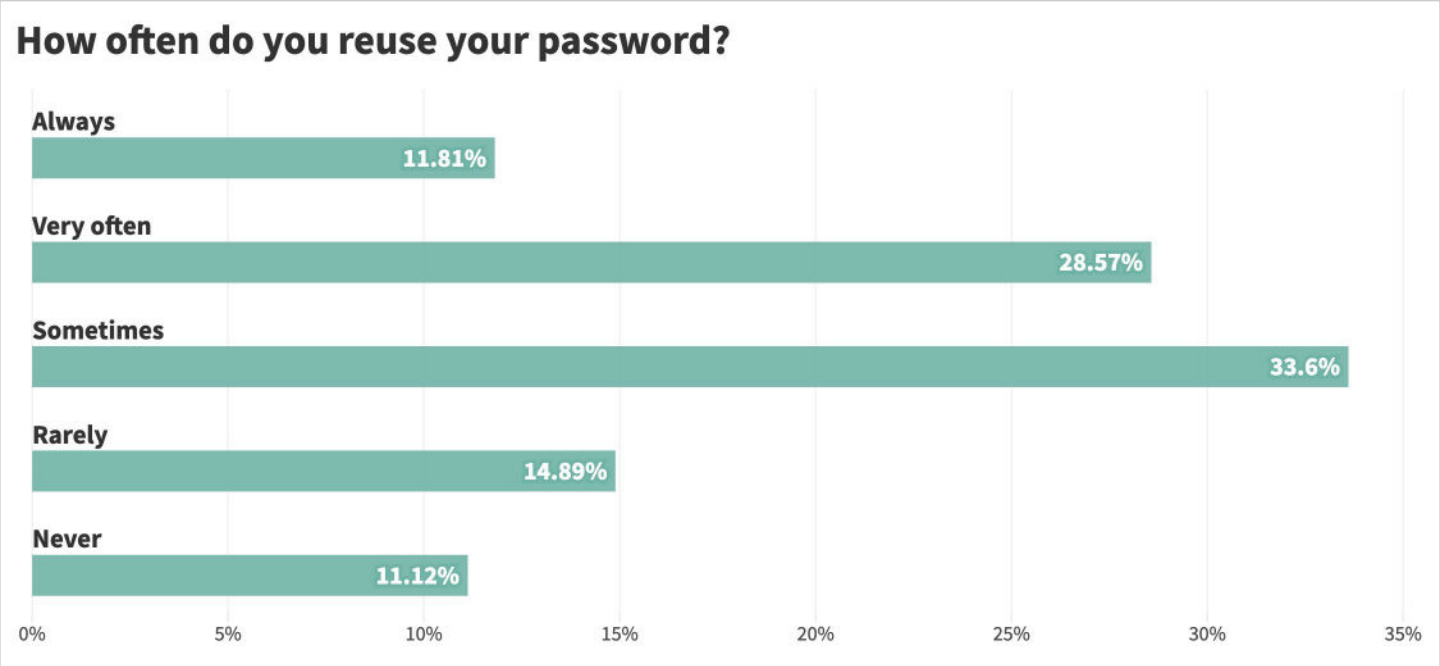


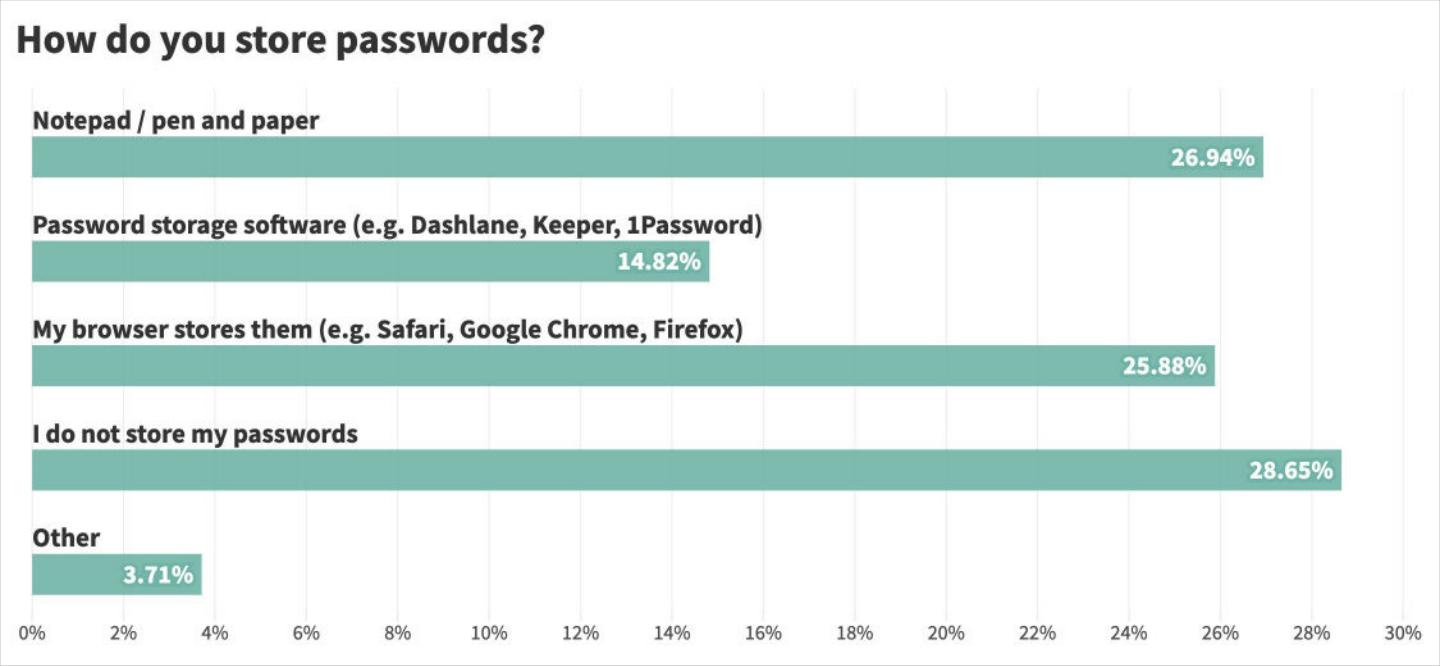
Did you turn them on yourself?

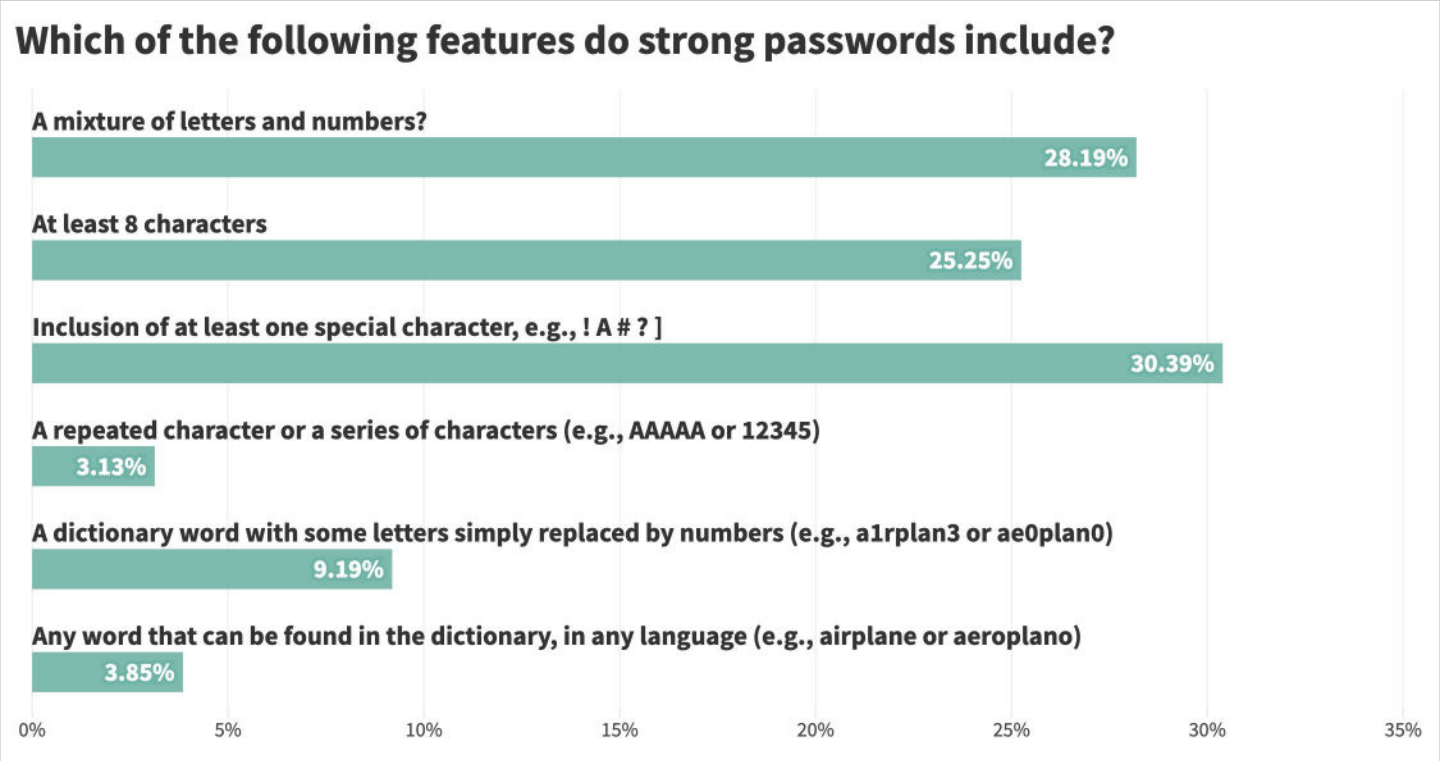


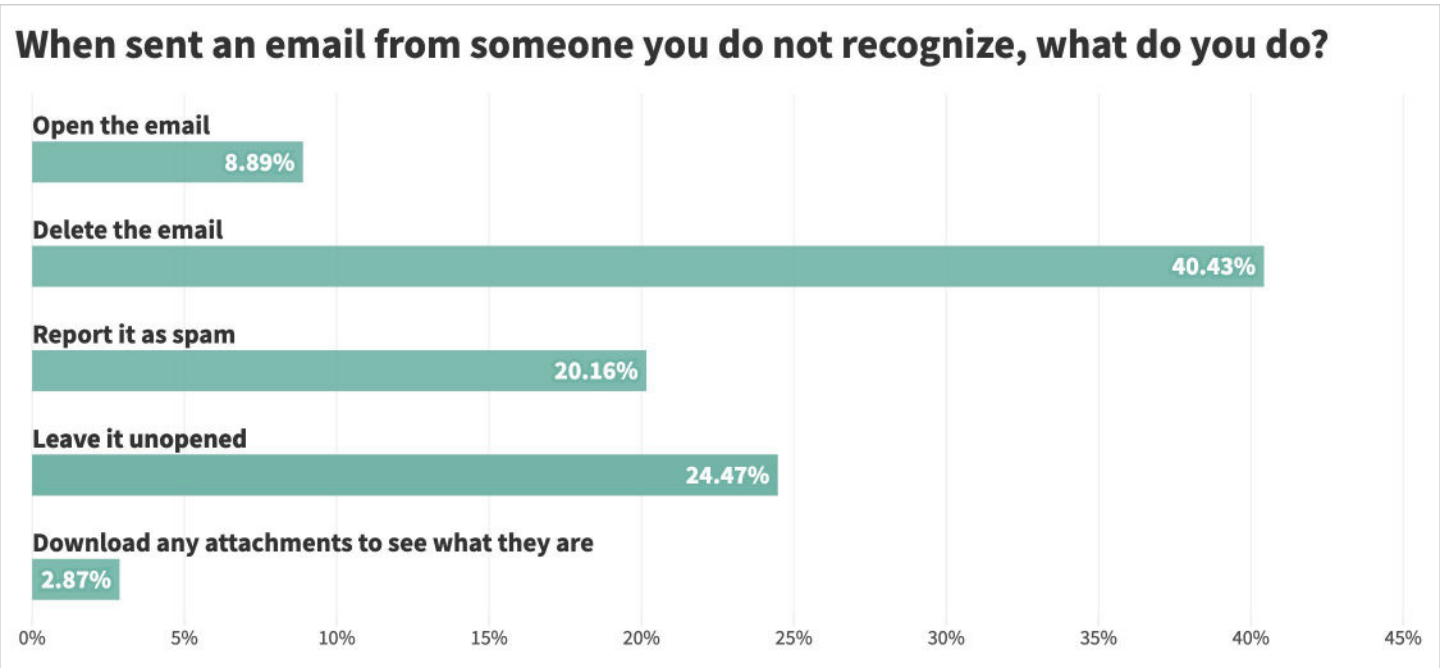
Have you used the same password more than once?




How often do you reuse your password?
Always
11.81%
Very often
28.57%
Sometimes
33.6%
Rarely
14.89%
Never
11.12%
0%
5%
10%
15%
20%
25%
30%
35%

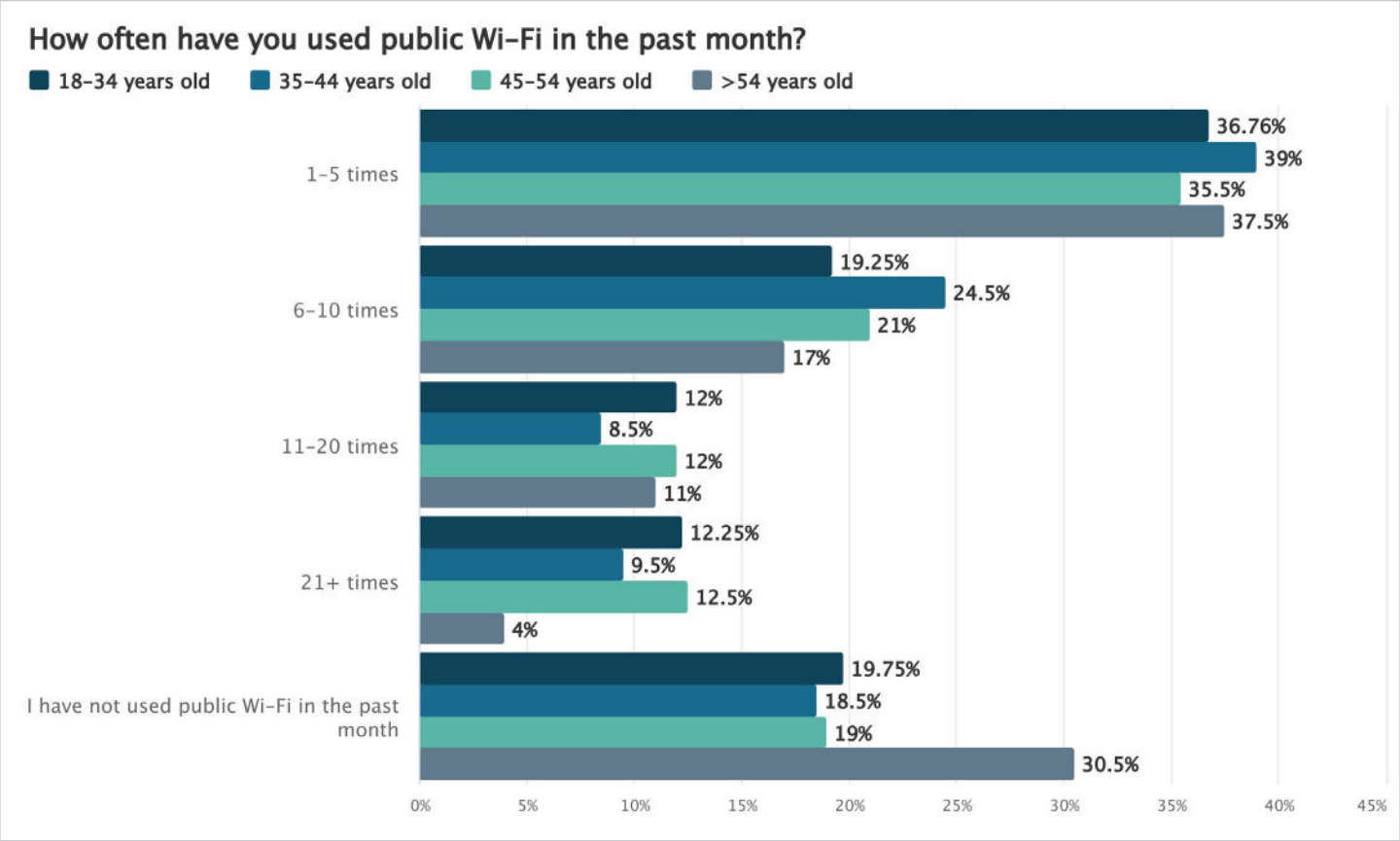

How do you store passwords?
Notepad / pen and paper
26.94%
Password storage software (e.g. Dashlane, Keeper, 1Password)
14.82%
My browser stores them (e.g. Safari, Google Chrome, Firefox)
25.88%
I do not store my passwords
28.65%
Other
3.71%
0%
2%
4%
6%
8%
10%
12%
14%
16%
18%
20%
22%
24%
26%
28%
30%

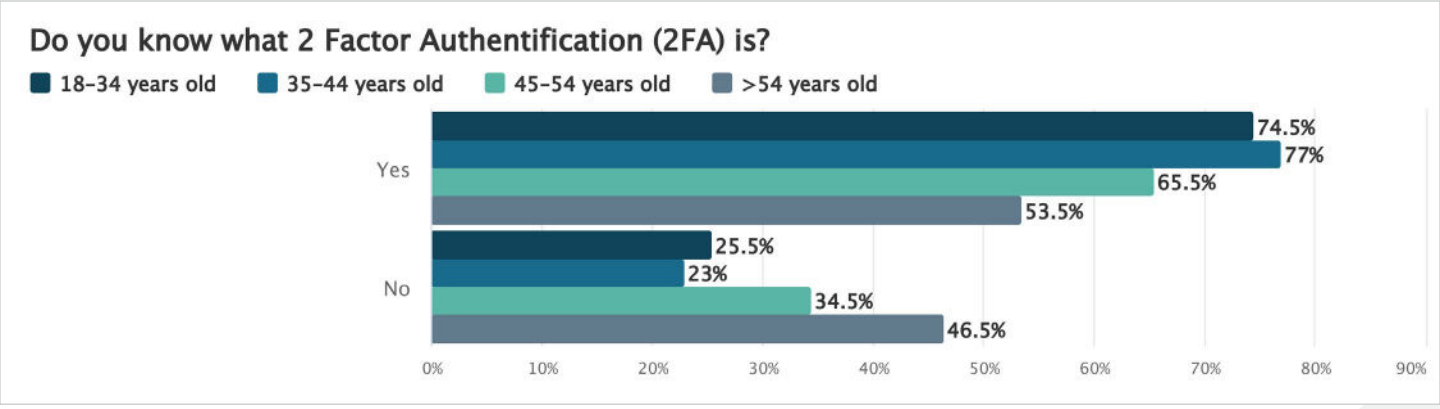

Which of the following features do strong passwords include?
A mixture of letters and numbers?
28.19%
At least 8 characters
25.25%
Inclusion of at least one special character, e.g., ! A # ?]
30.39%
A repeated character or a series of characters (e.g., AAAAA or 12345)
3.13%
A dictionary word with some letters simply replaced by numbers (e.g., a1rplan3 or ae0plan0)
9.19%
Any word that can be found in the dictionary, in any language (e.g., airplane or aeroplano)
3.85%
0%
5%
10%
15%
20%
25%
30%
35%


When sent an email from someone you do not recognize, what do you do?
Open the email
8.89%
Delete the email
40.43%
Report it as spam
20.16%
Leave it unopened
24.47%
Download any attachments to see what they are
2.87%
0%
5%
10%
15%
20%
25%
30%
35%
40%
45%

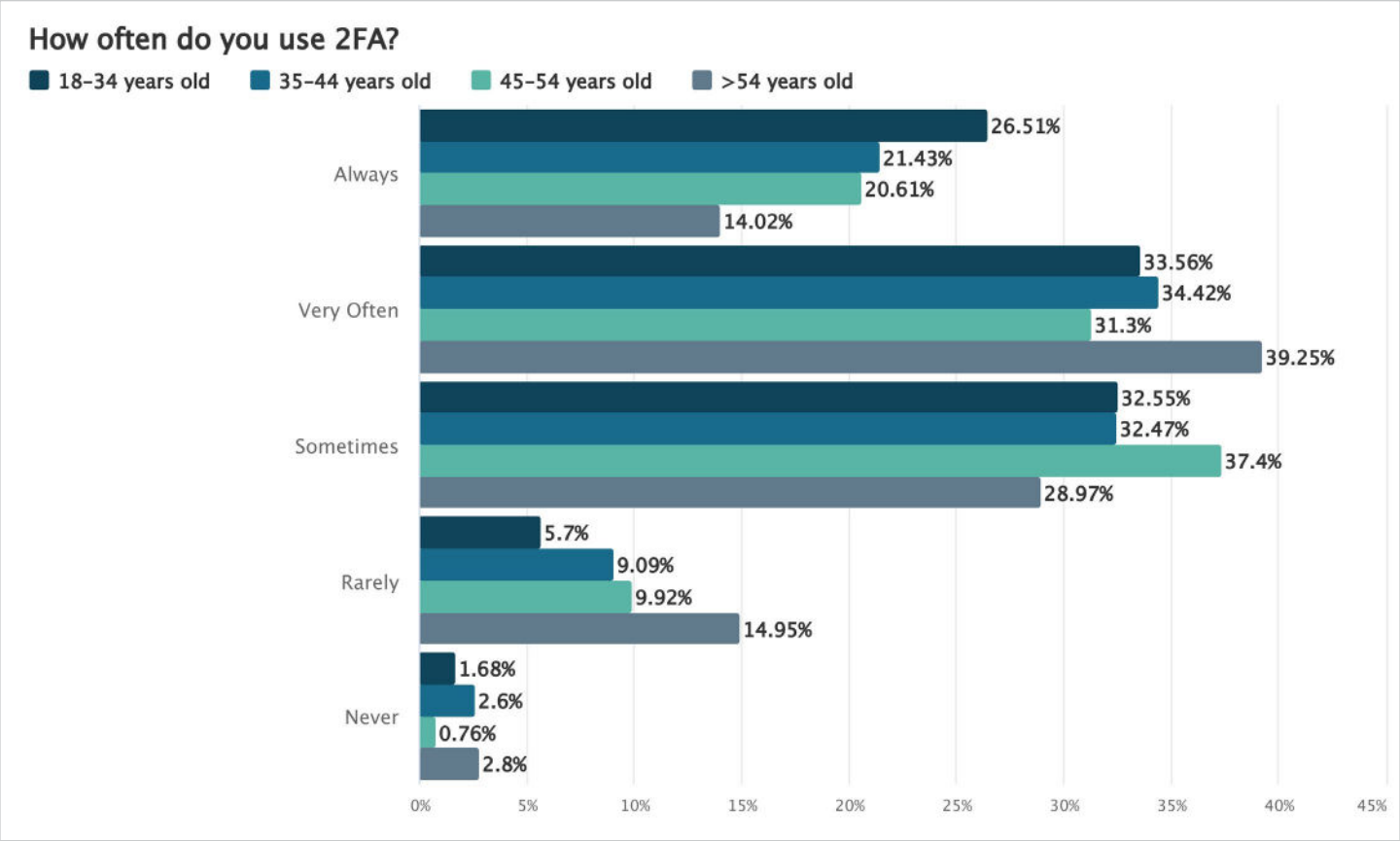
Safer Together: Inclusive Cybersecurity

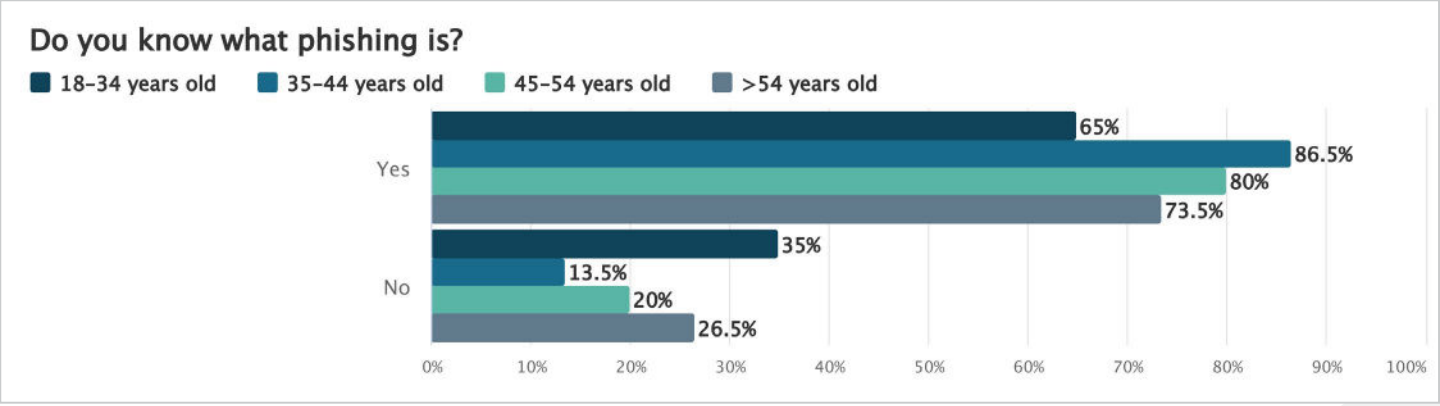
Responses by Age



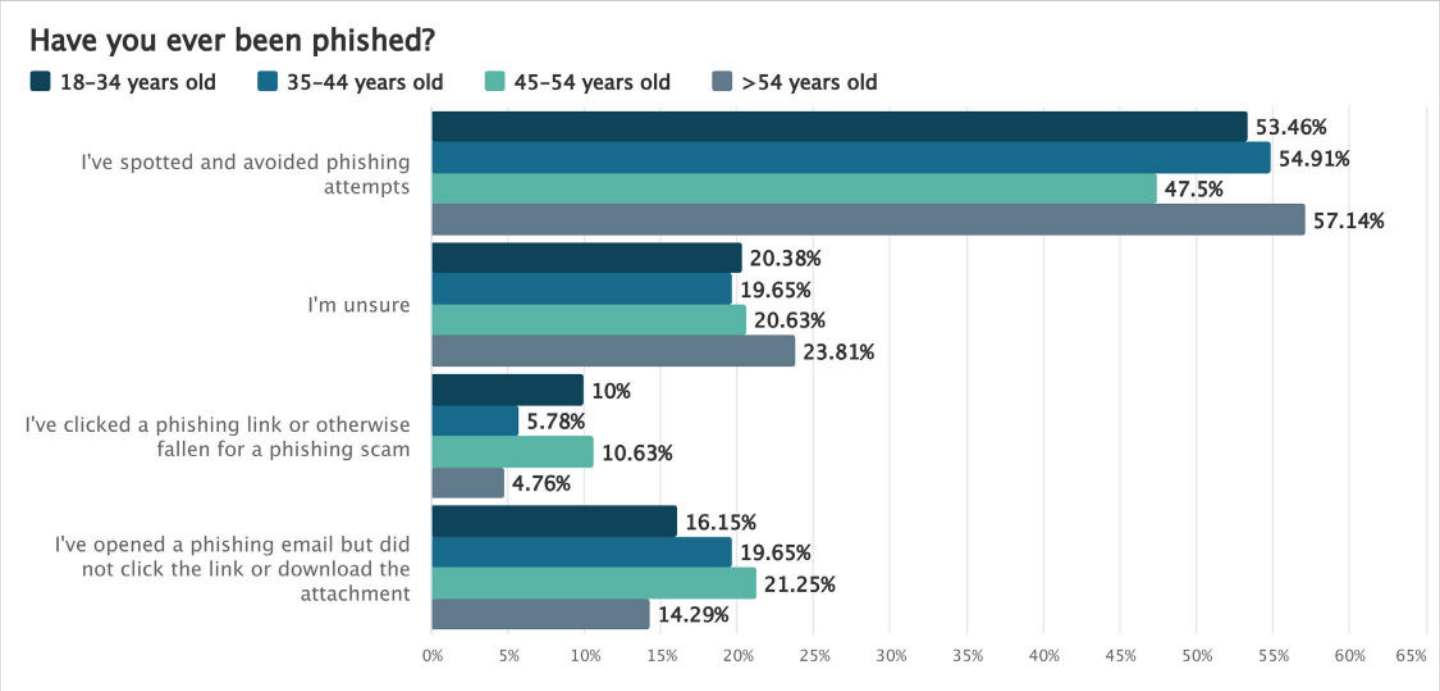


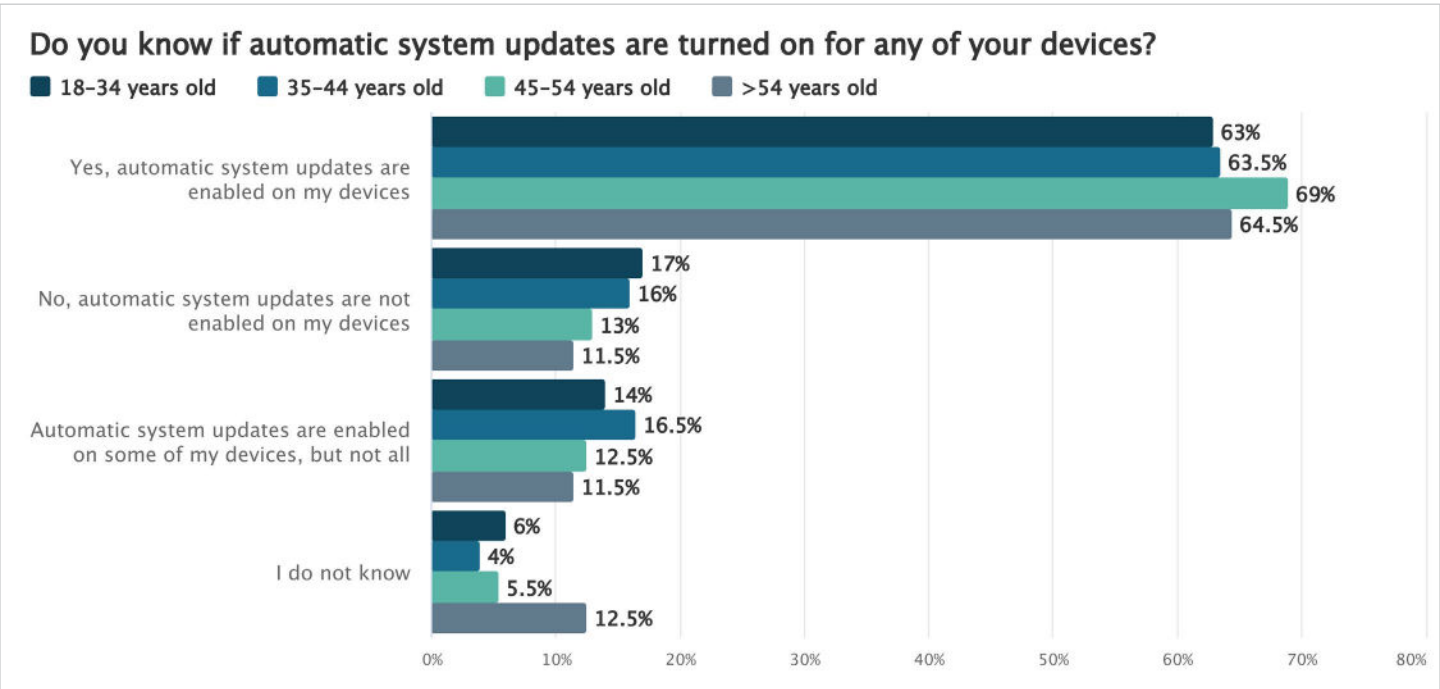
Safer Together: Inclusive Cybersecurity



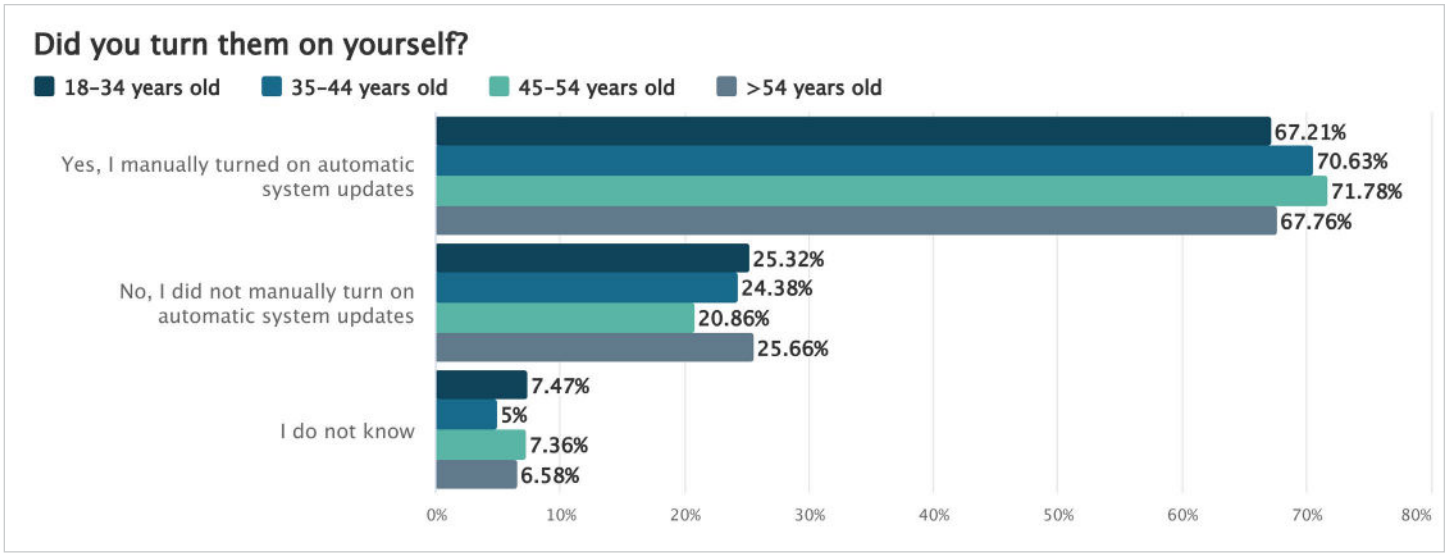


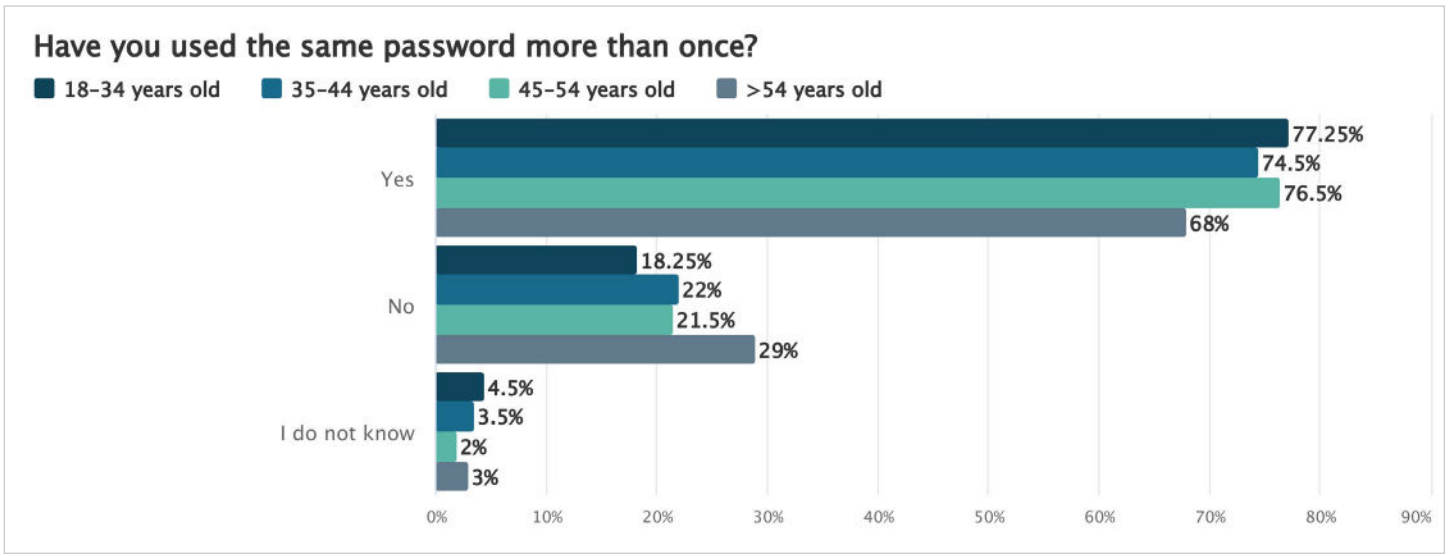
Safer Together: Inclusive Cybersecurity



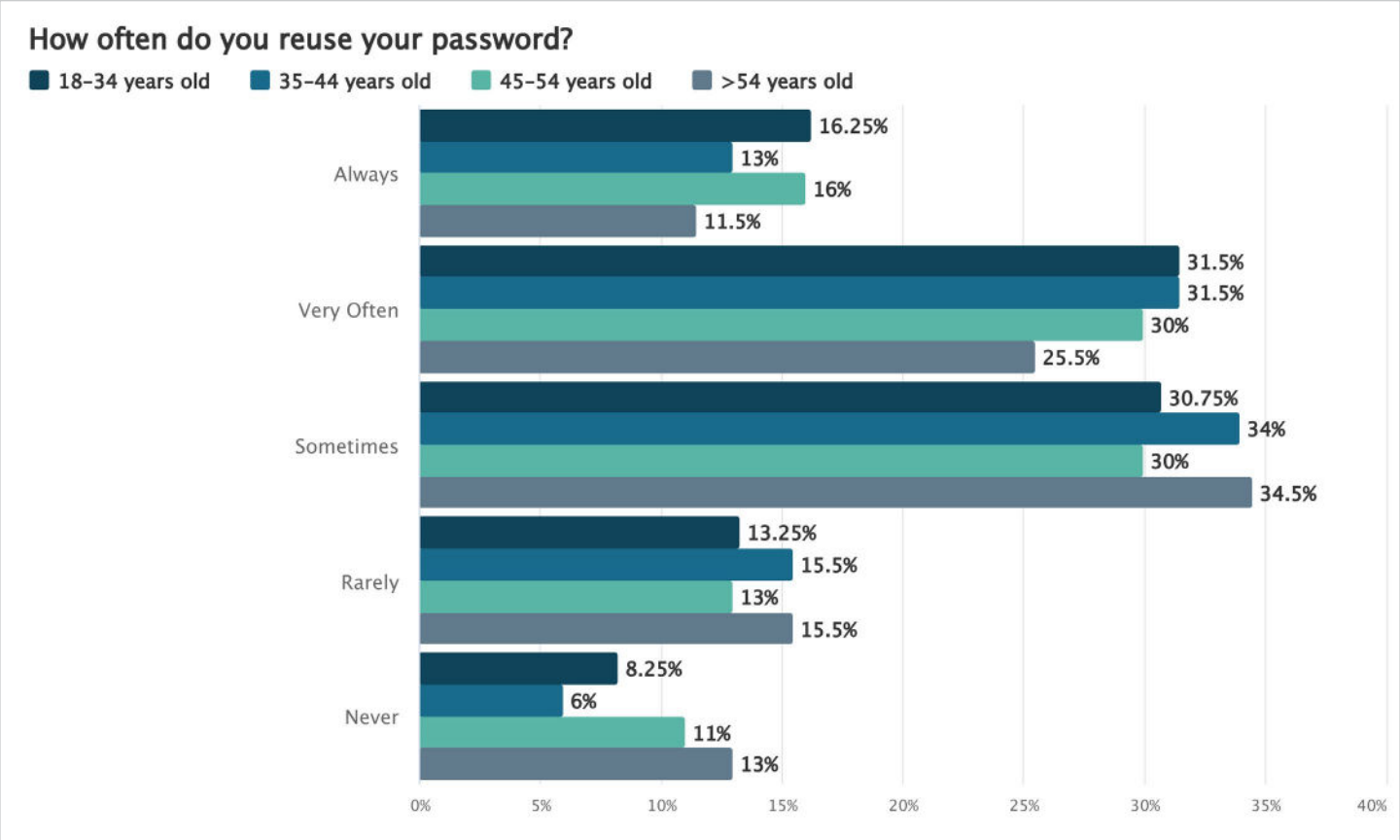


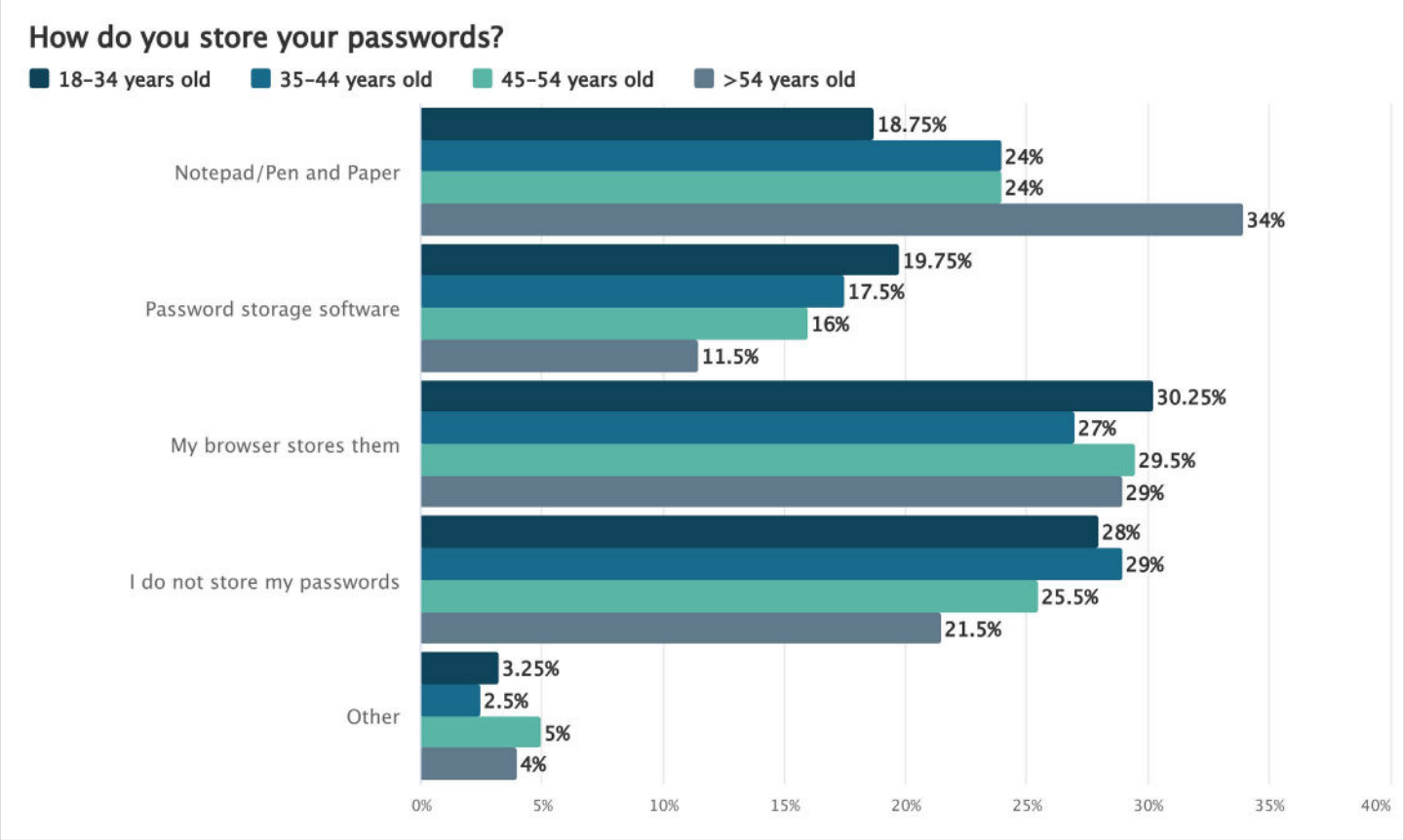
Safer Together: Inclusive Cybersecurity





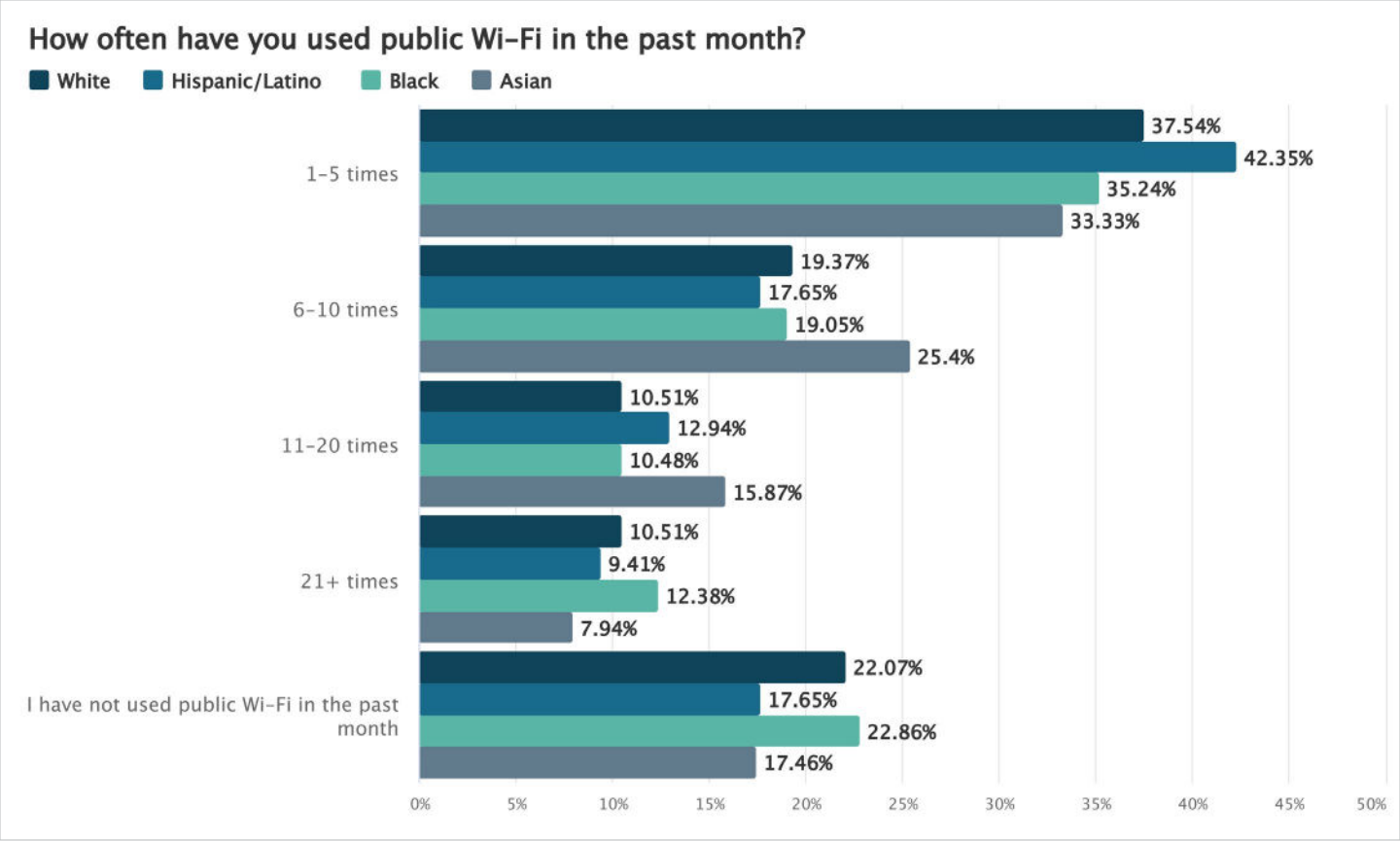
Safer Together: Inclusive Cybersecurity

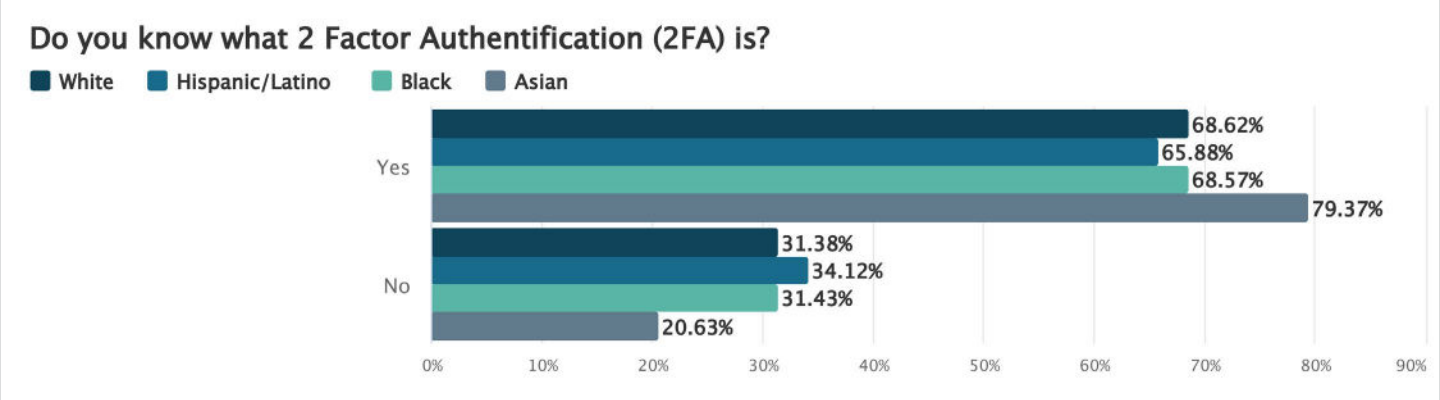




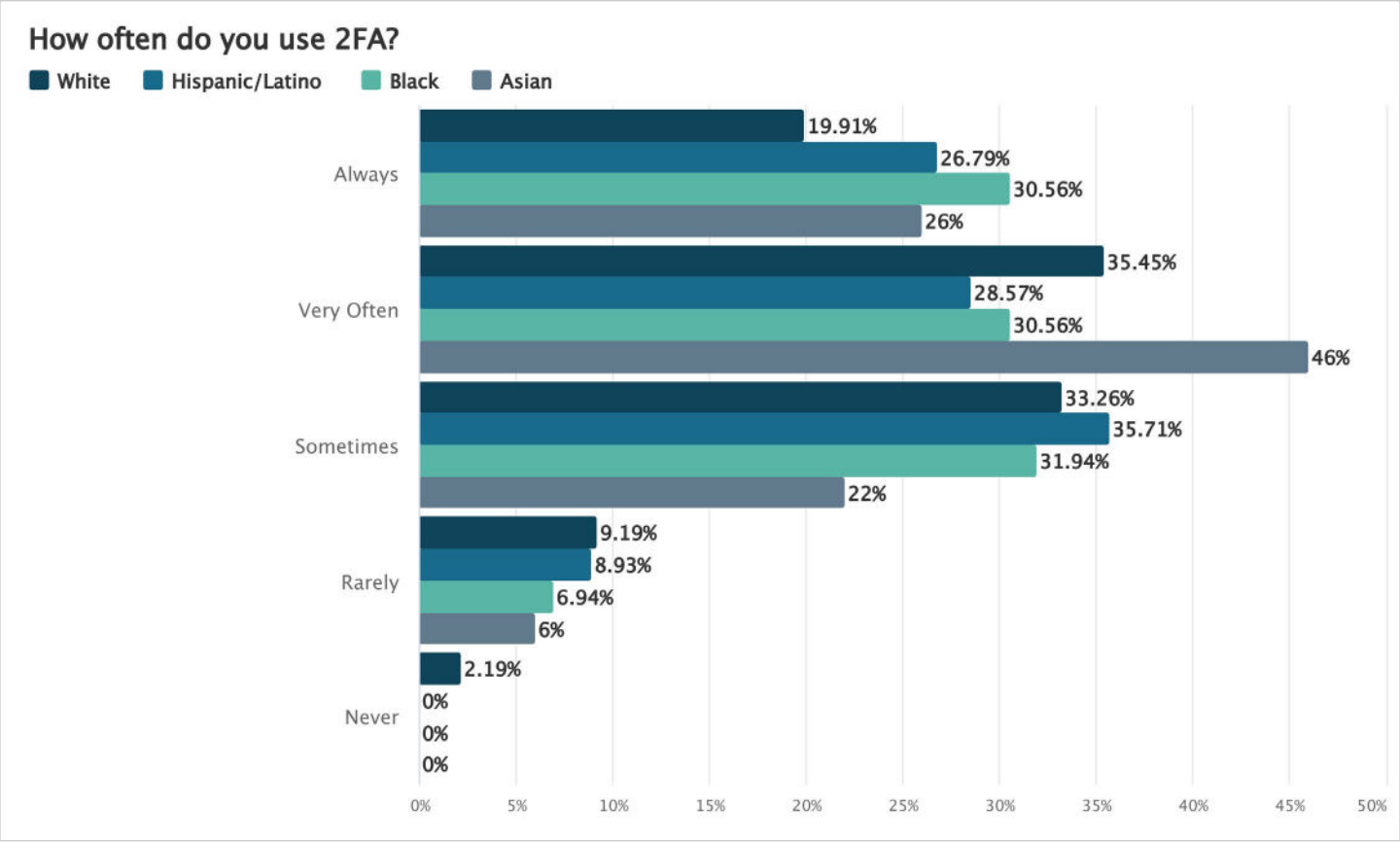
Safer Together: Inclusive Cybersecurity

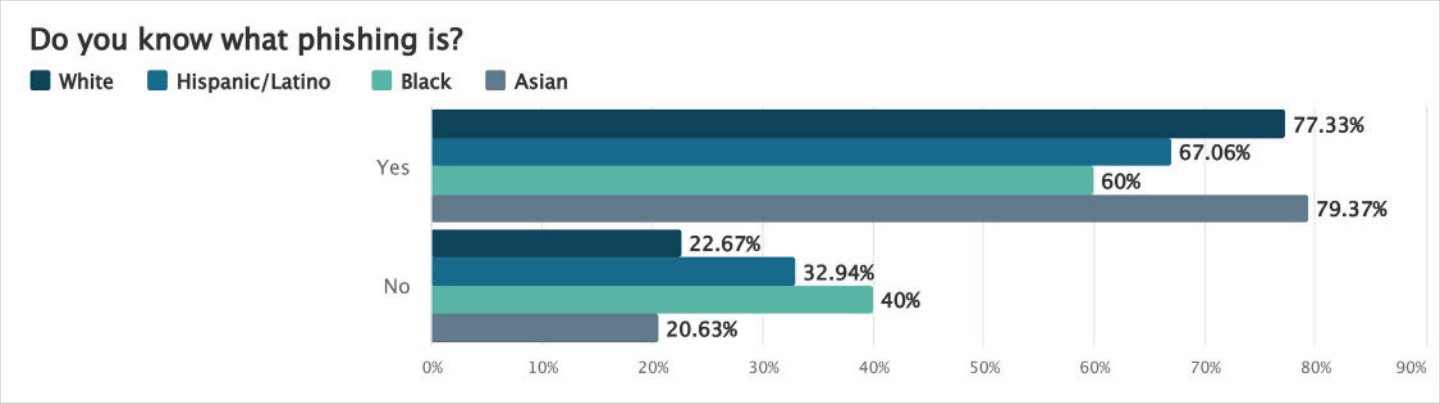
Responses by Race



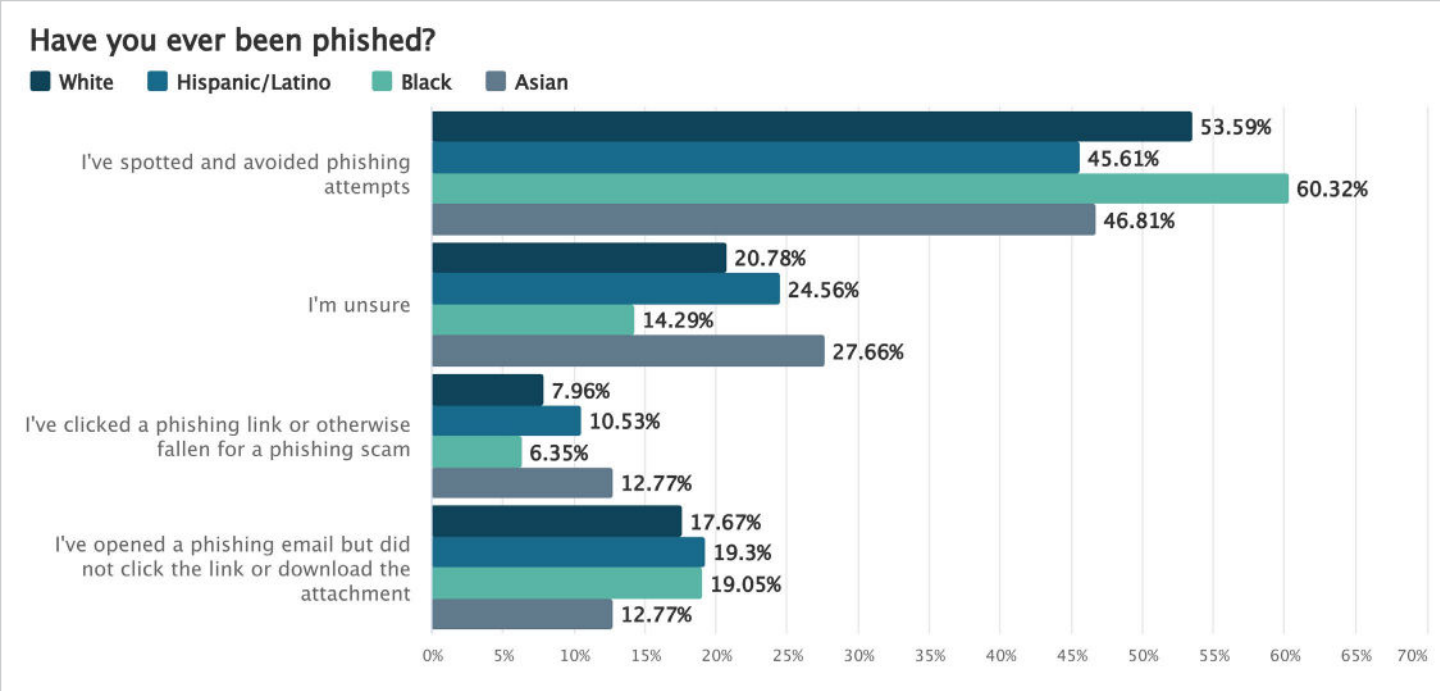


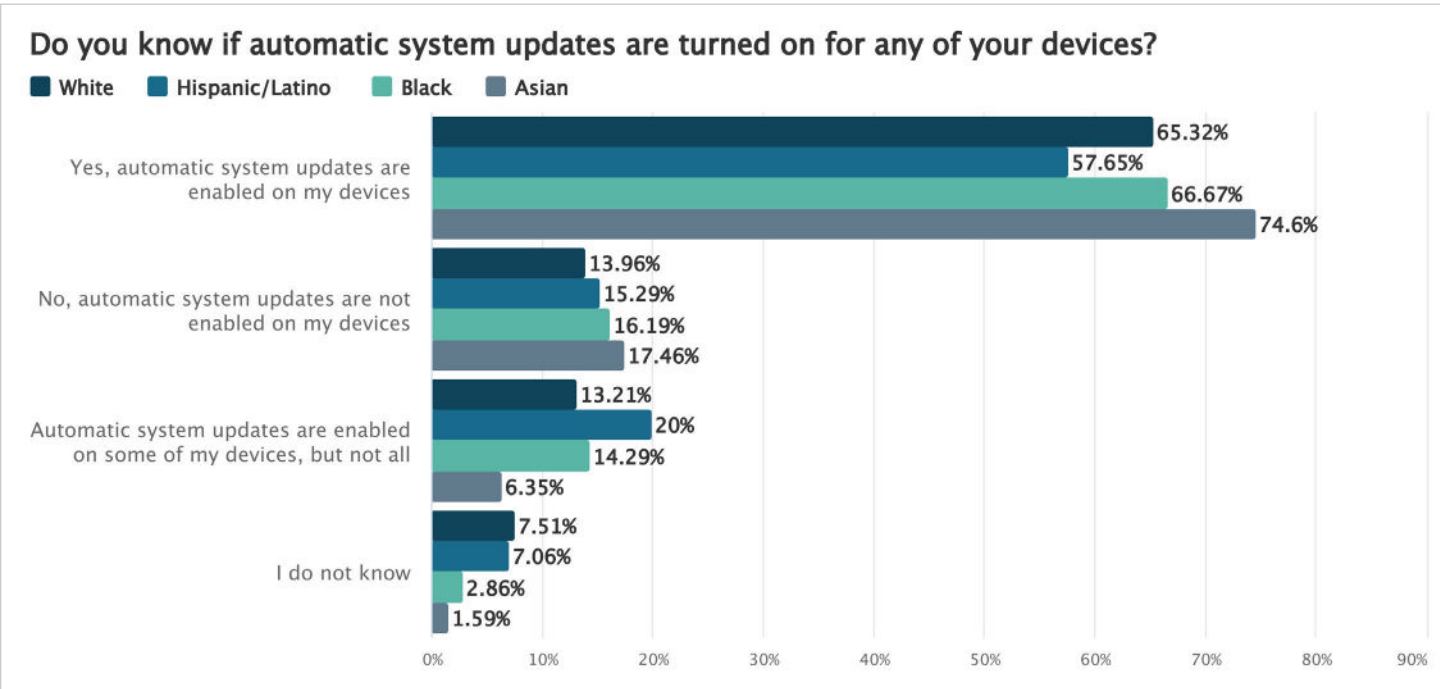
Safer Together: Inclusive Cybersecurity



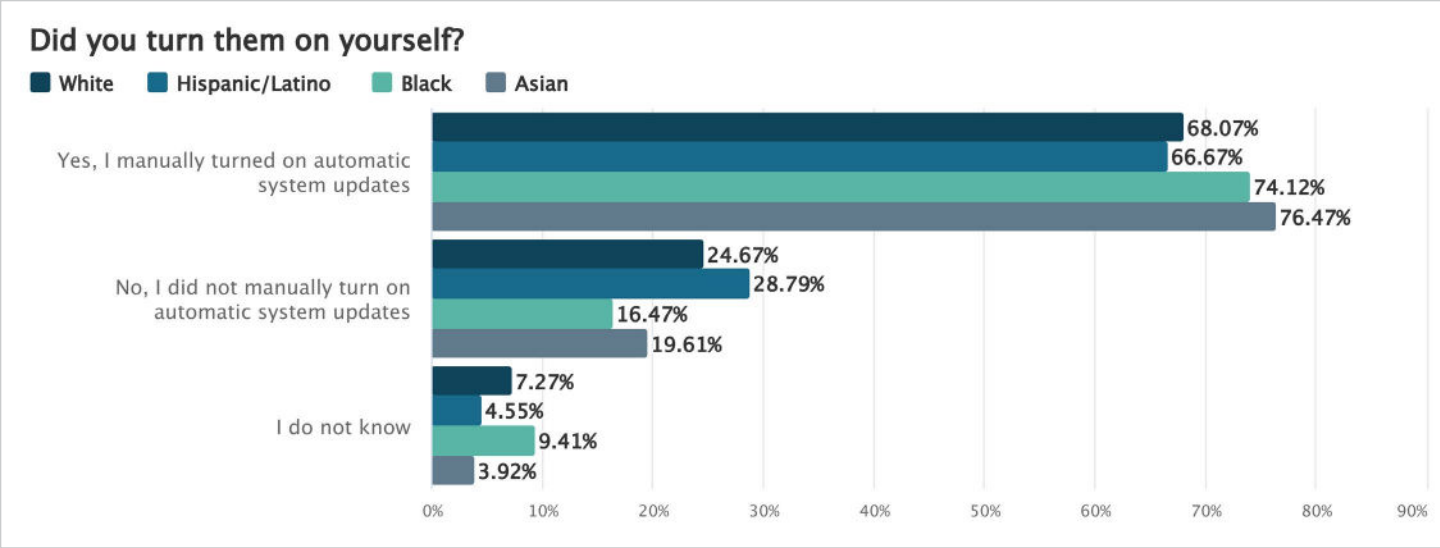


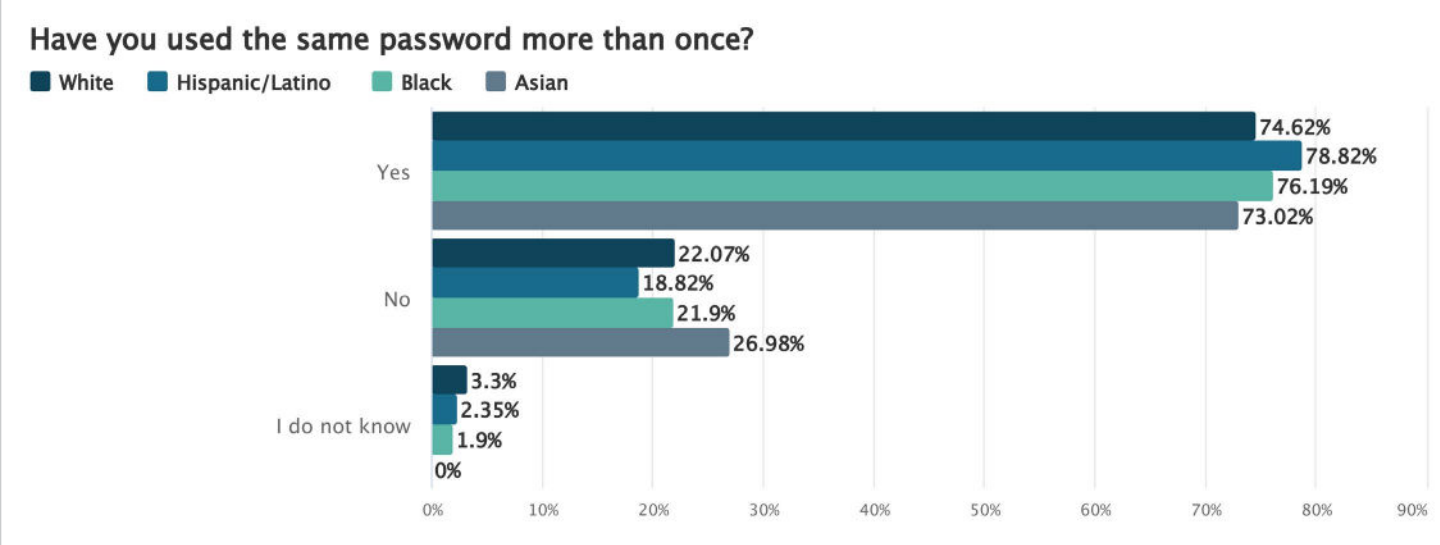
Safer Together: Inclusive Cybersecurity



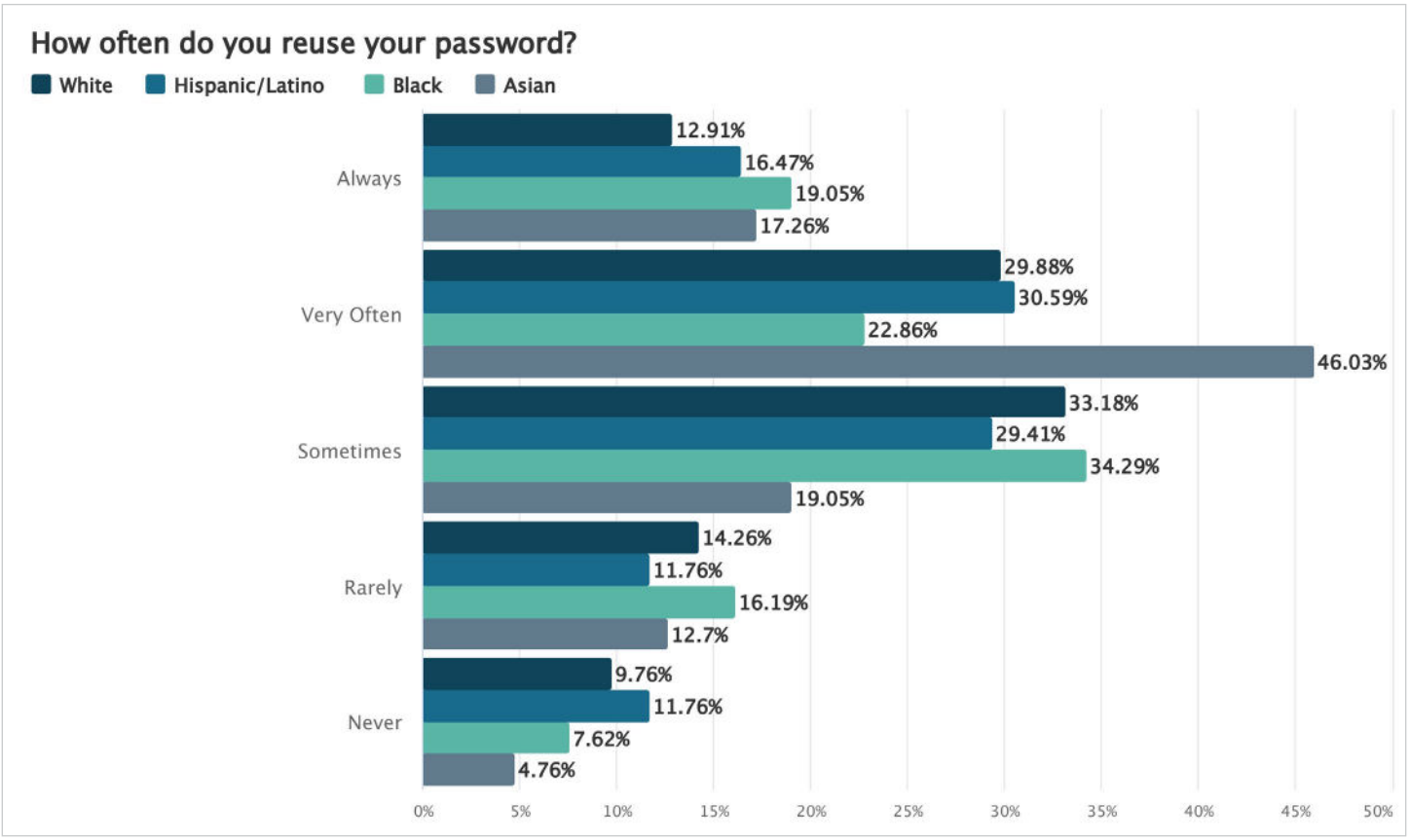


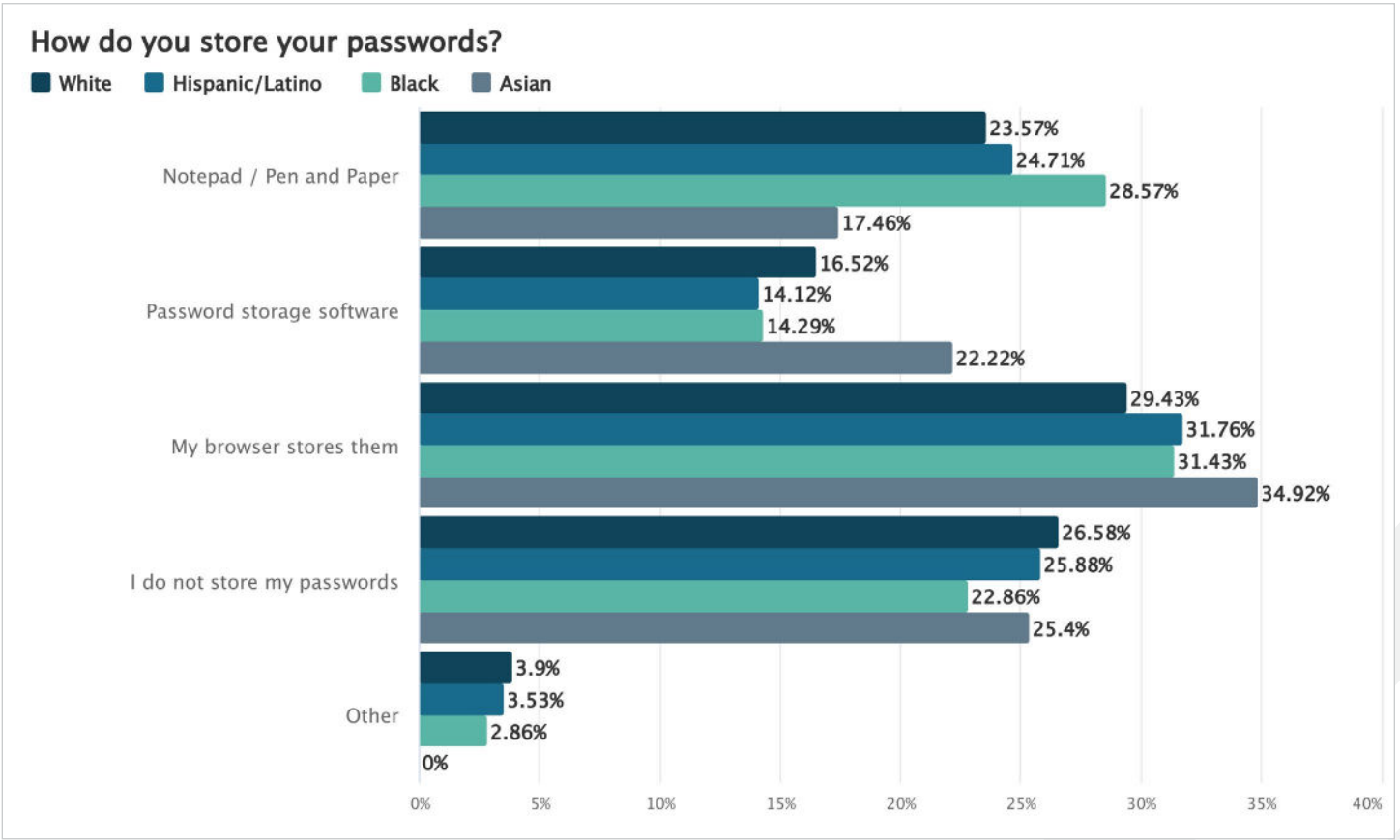
Safer Together: Inclusive Cybersecurity





Safer Together: Inclusive Cybersecurity





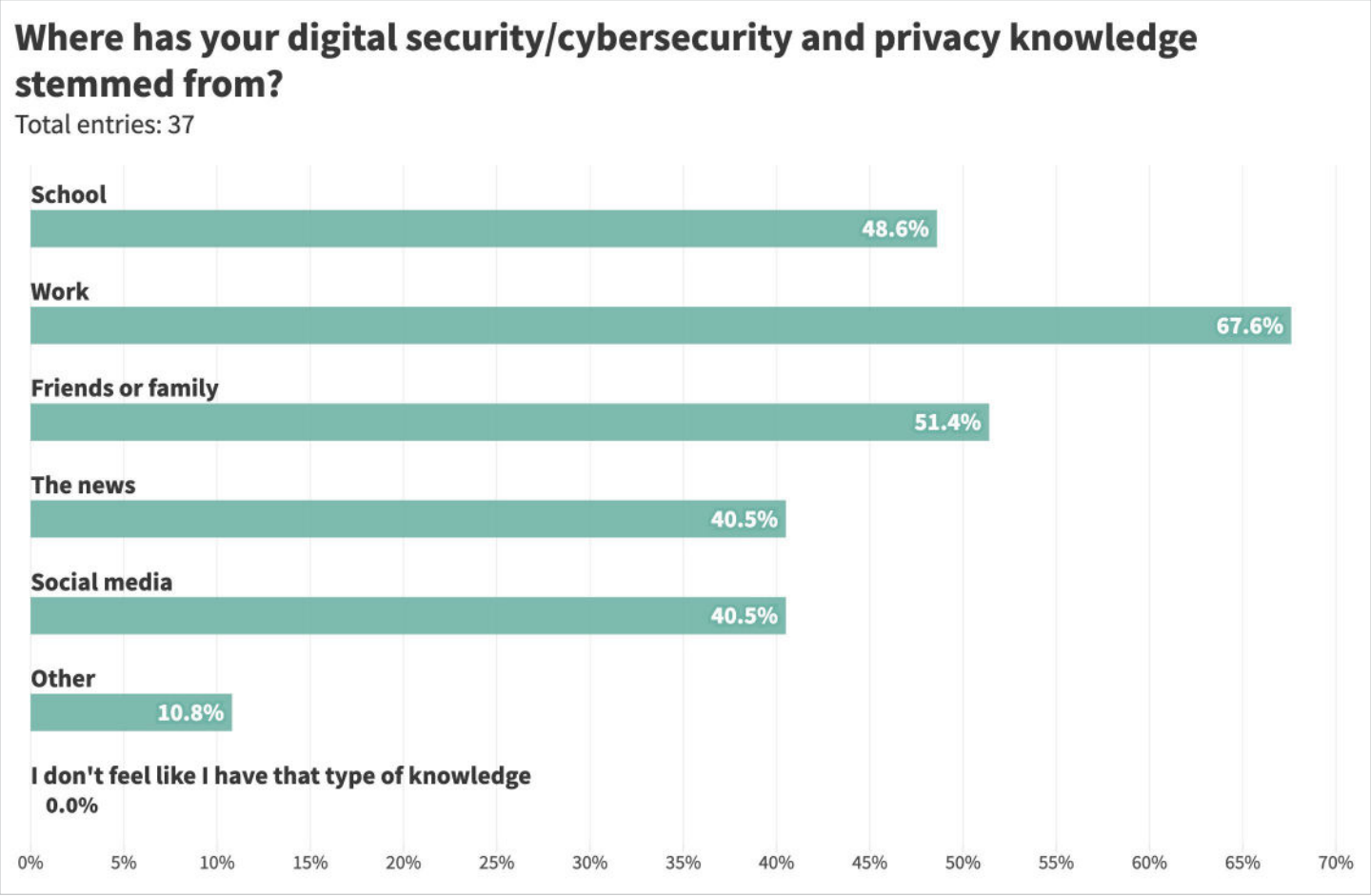
Safer Together: Inclusive Cybersecurity

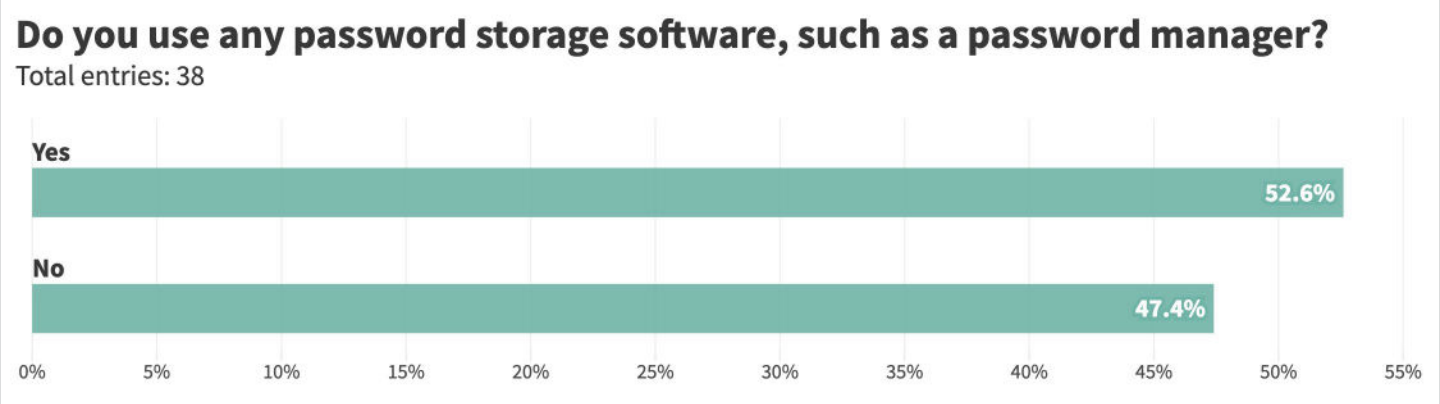
Appendix B: Diary Study Data

Study conducted October 6-11, 2021

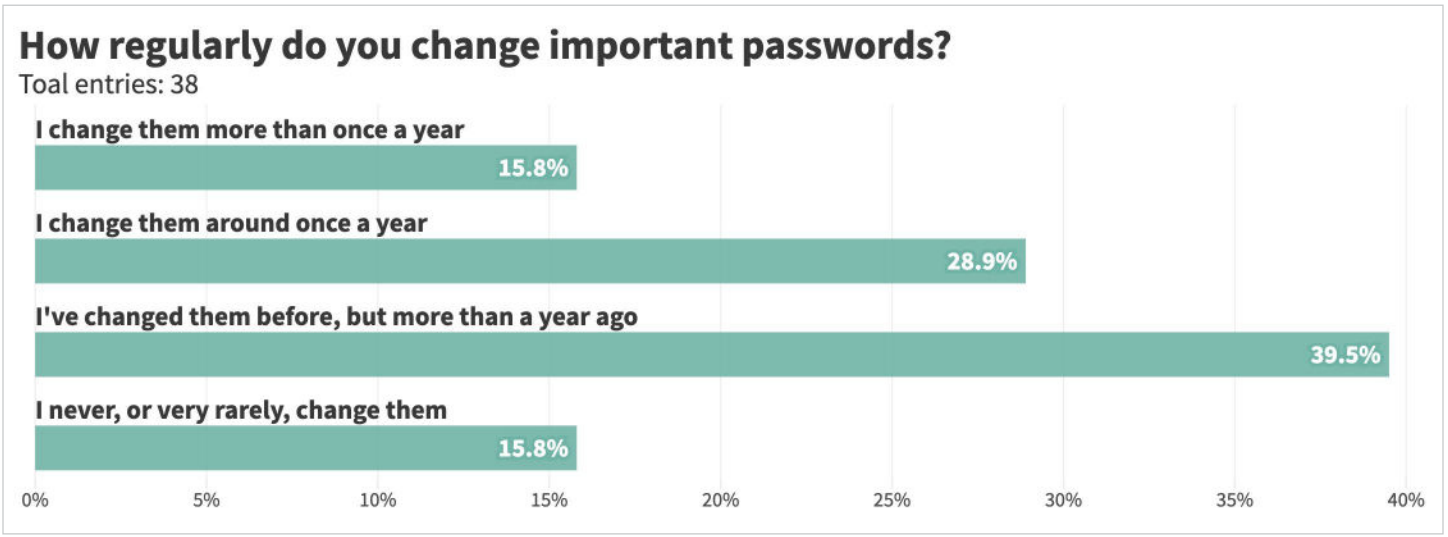
Security basics

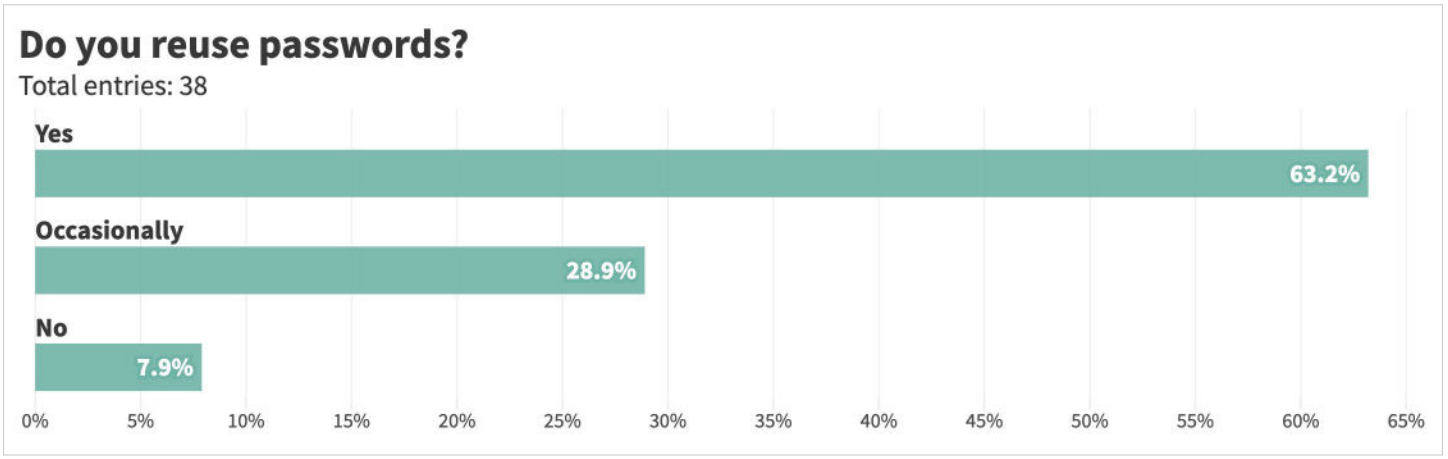
While participants are generally aware of the security and privacy tools available to them, e.g., MFA and password managers, they are still reusing passwords, using public Wi-Fi, not using these tools, and otherwise not adopting security best practices and tools. However, security incidents do impact behavior.

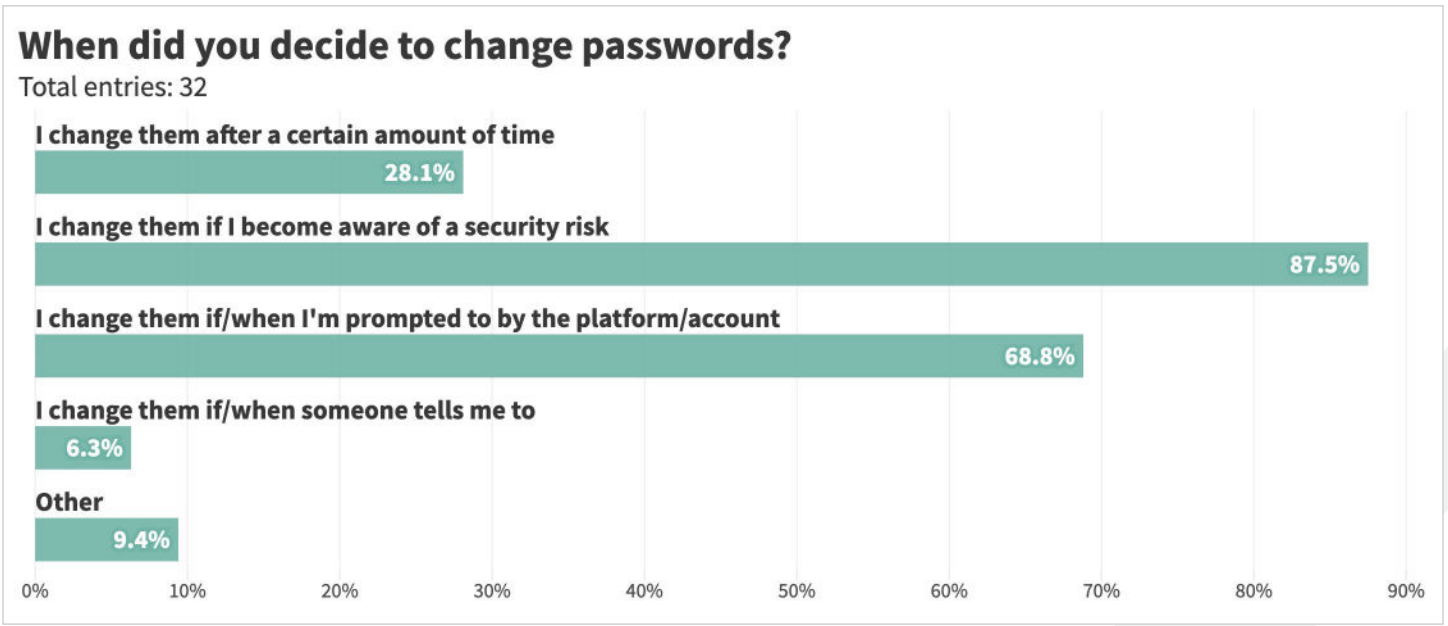




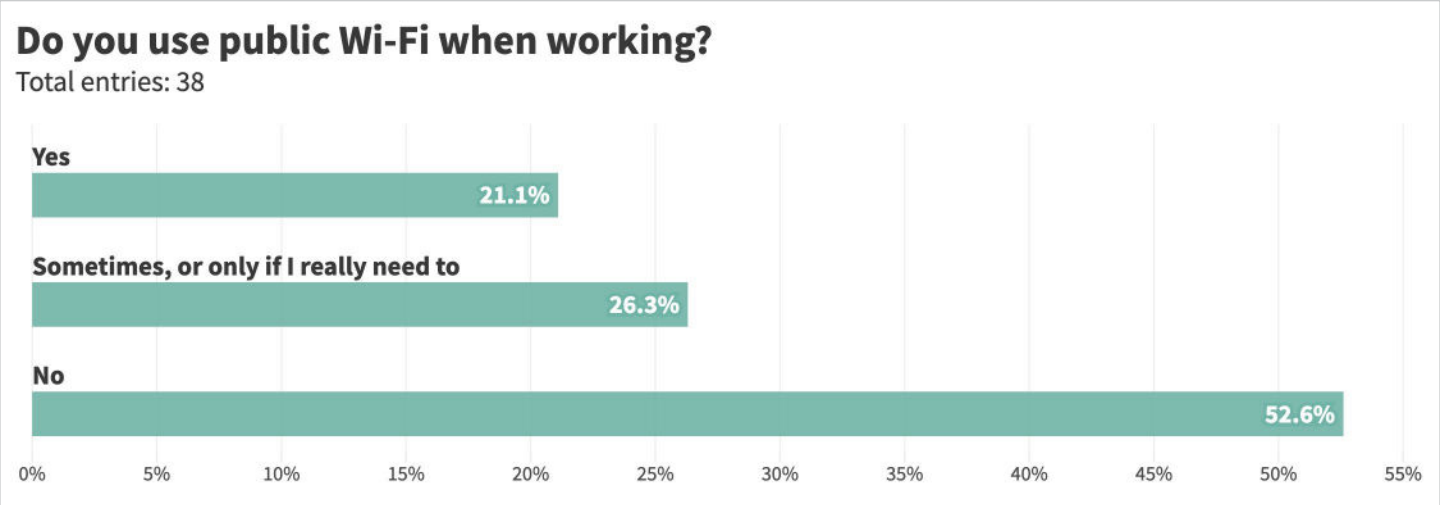
Safer Together: Inclusive Cybersecurity

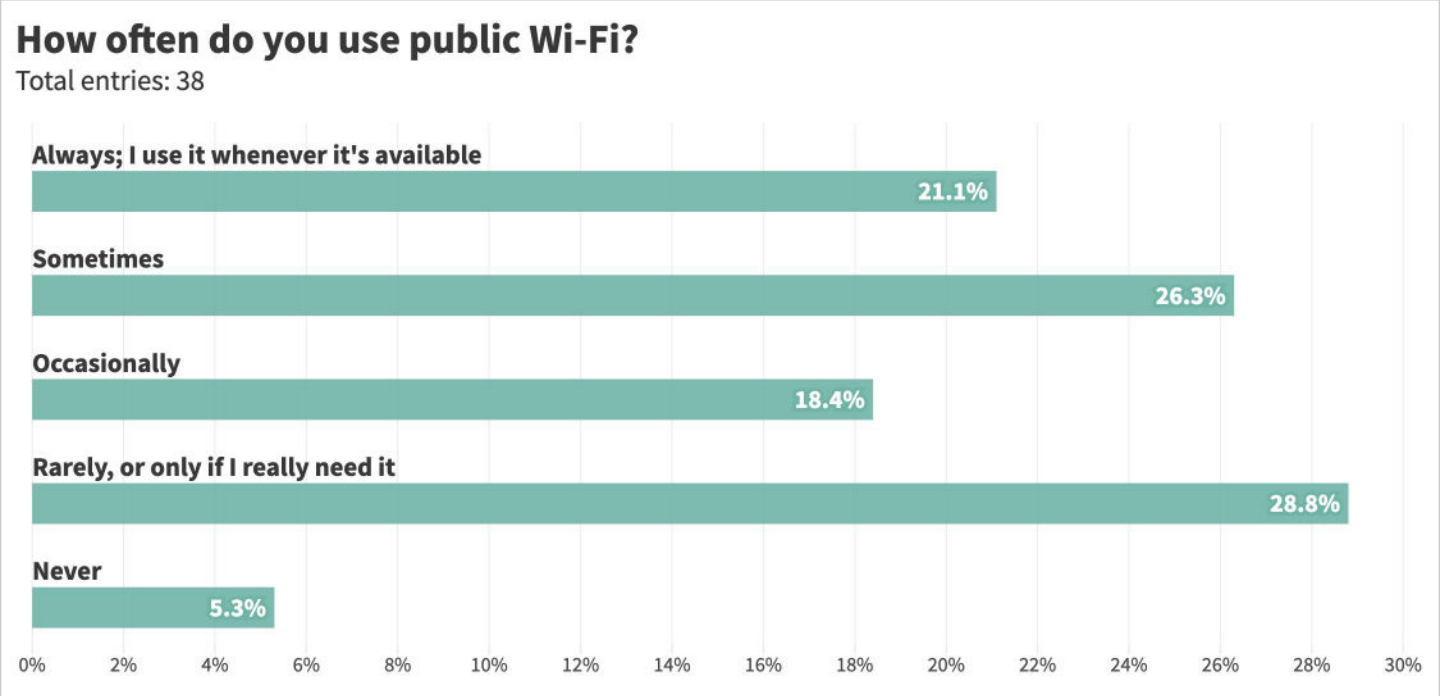






Safer Together: Inclusive Cybersecurity

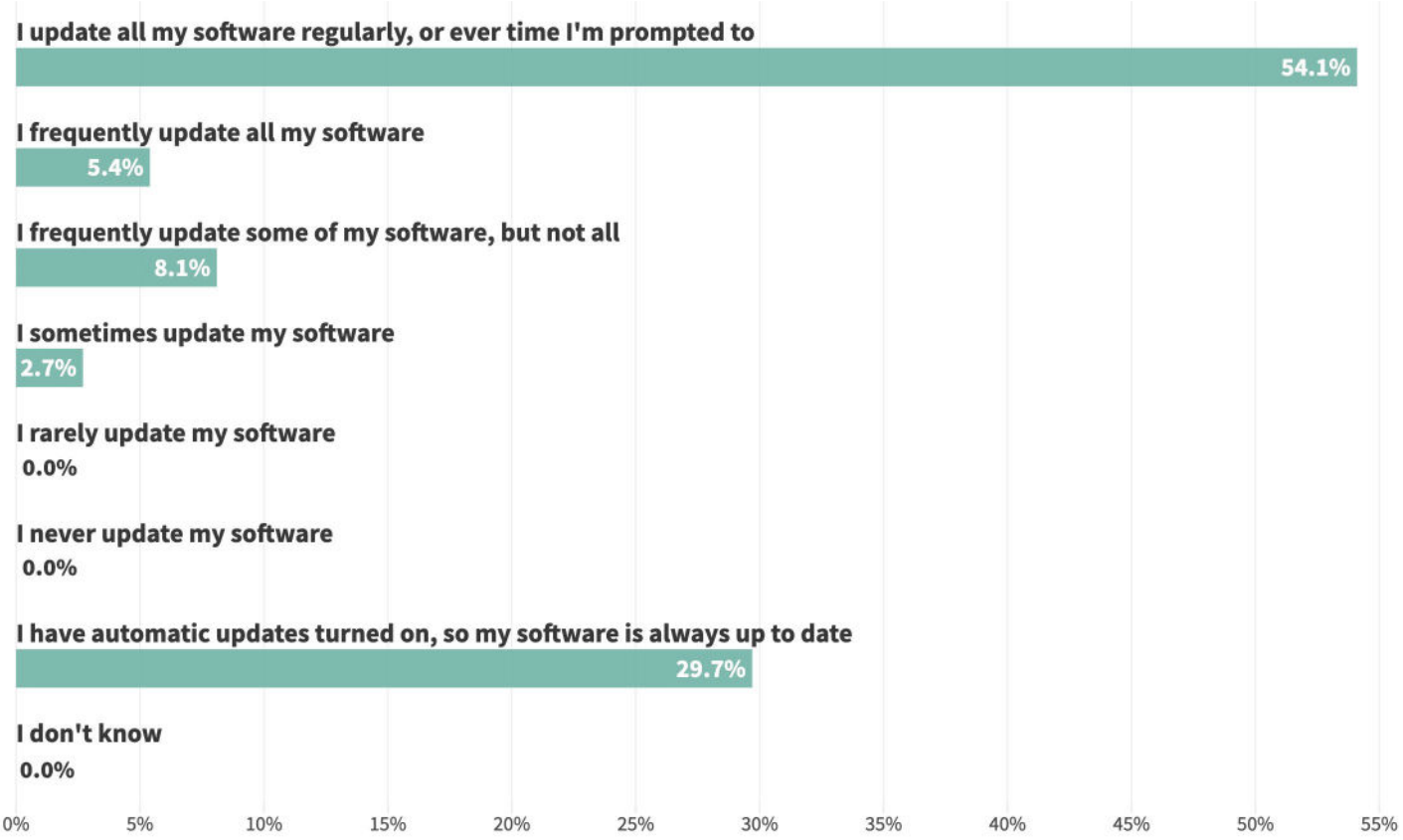




Safer Together: Inclusive Cybersecurity

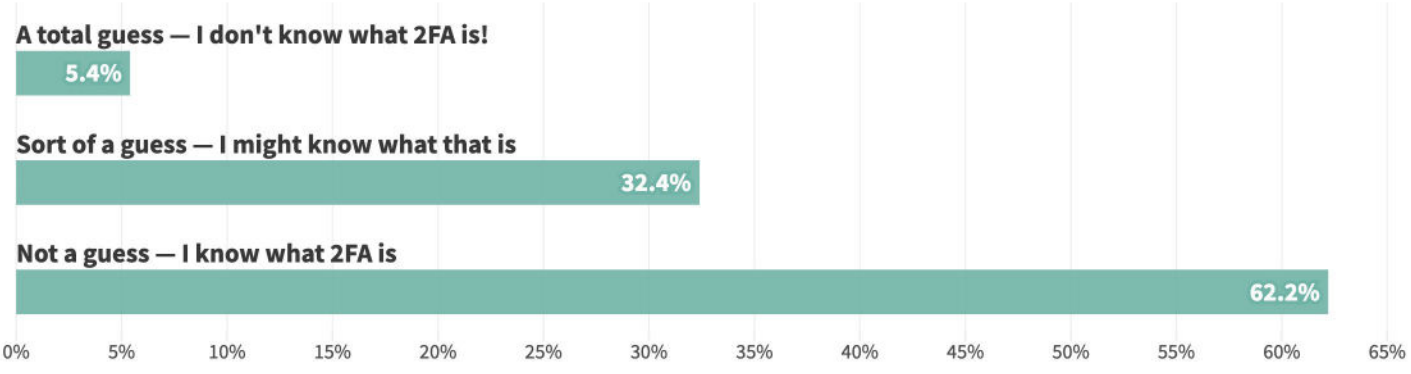
Do you regularly update your software? Or do you have automatic updates activated on your electronic devices? Select which answer fits you best.

Total entries: 37



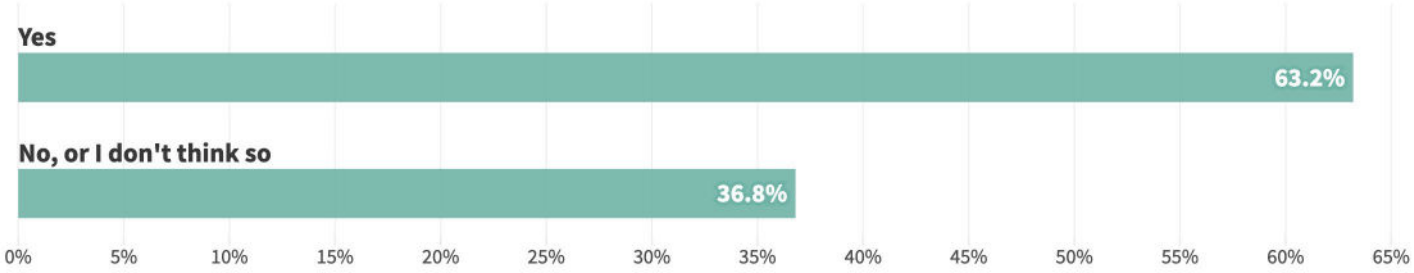
You correctly selected the definition of 2FA from a multiple-choice list. Be honest; was that a guess or do you already know the definition?

Total entries: 37



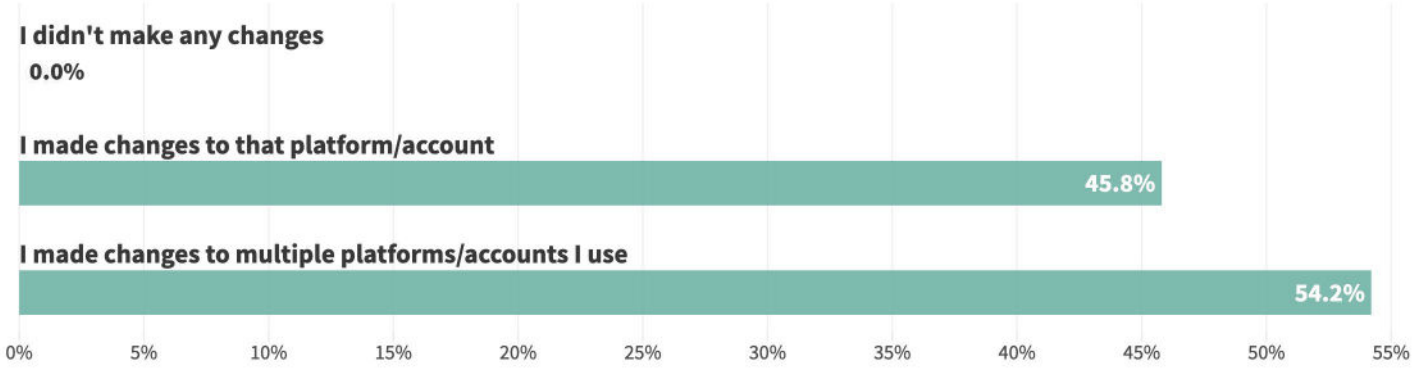
Has any event (e.g., company breach like Target, having your identity stolen, ransomware attack like Baltimore schools) ever caused you to change your security behavior?

Total entries: 38



Did you change your security behavior on just that platform/account (e.g. changed your password, added security questions), or more broadly (e.g. change passwords to other accounts as well, updated settings for multiple accounts)?

Total entries: 24



Safer Together: Inclusive Cybersecurity

Freeform Question Response Highlights

Generally, participants acknowledge or demonstrate that their identity (e.g., family structure - parents, upbringing, race, ethnicity, gender, age) informed either their views on security and privacy or their risk tolerance.

"I have a son and a daughter, and we all identify as African-Americans here in America. We have to take all types of security extremely serious because, you know, there's nothing we can do that can't get us in some type of trouble. Then when we get in trouble, we get the extreme version of that trouble. So most definitely explain to them how to be safe while online so that they don't get in trouble. Be careful of who you speak to online because you don't know who it really is, you know, and things like that. So I just make sure to teach them everything that I've figured out since the beginning of the internet. But also, I grew up with the internet when computers first became a thing and internet came out and hanging out online, I try to teach them all my safety rules so that they know them and they can follow most of."
— **39-year-old woman, Detroit, Michigan, some college, single with kids, entrepreneur**

"I think my race and my upbringing has a lot of influence on my privacy and security habits online. Growing up, I had my parents always ensuring that I'm posting stuff online that are not going to incriminate me for the future. In a way, they have been kind of been strict about my online presence. So in turn, as I have gotten older, I make sure that I keep a lot of things about me like personal things very, very private. And now that I am an adult with a daughter, I make sure that her presence online also, she stays safe and private"
— **32-year-old Asian American woman, Alexandria, VA, married with children, post-grad coursework, student**

"So being a black woman definitely heavily influences how my security and my privacy have it, I feel like as a woman, security's extremely important. And so I make sure that I'm extra vigilant."
— **29-year-old Black woman from Richmond, VA, college educated, full-time employment in entertainment and leisure**

"Hello. So I feel that my family background and identity affects my identity because as a Chinese-American child of immigrants, I feel as if everything I know about the internet and security and privacy habits I learned by myself. I learned through Googling or through listening to podcasts and through choosing my own sources because I feel as if my parents didn't really ... know that much about the internet and didn't teach me that much. And as a child, I also don't feel as if my time on the internet was very supervised. However, I feel like the bigger influence is my own personality. I think I am inherently a little bit naturally suspicious. And I also feel like the idea that other people can find my information and find my habits is just really startling and uncomfortable to me because I, as a person really value privacy. So I feel as if, while like my family identity did affect me, in some ways, I think the larger influence is definitely my own natural inclinations towards privacy and security. So." — **22-year-old Chinese American woman, college educated, temporarily unemployed, Chicago, IL, no spouse or kids**

"I've never really thought that much about these factories having an impact on my security and privacy habits. My father's side of the family definitely has a little bit more of an impact from a race perspective because they are Chinese and I'm half Chinese. So especially in the last year, with all of the rise in Asian hate with the pandemic, that's been something that's been on my mind. I have not really experienced a lot of it myself because my appearance is a little less obvious, but that is something that I have continued to think about when it comes to personal security. As a woman, though, that is something that impacts my behavior on a daily basis. More specifically in terms of physical security, like being out alone at night, making sure that I'm carrying some sort of alarm, that I am aware of my surroundings, I don't have earbuds in otherwise. Things like religion has [*sic*] not really had a big impact on my security or privacy habits, either. Generally, I just consider myself to be a pretty aware person when it comes to those issues."
— 23-year-old Chinese & White mixed woman, Washington, DC, college graduate, no spouse or kids, works in international development

Safer Together: Inclusive Cybersecurity

"So how my family influenced my view [of] security, I would say ... both my parents are baby boomers, even though I'm a younger millennial, and so I think with that comes a very healthy skepticism of internet security... So, um, as far as being black and being a woman in the inner city, I don't know if I feel like that influences my view. I think it influences my view of those who run those companies. And I view, like cybersecurity in the whole world of tech is a very like white, male centric space. And so therefore, I feel like it is a very privileged space and I don't trust it." — **26-year-old Black woman from Minneapolis, MN, college educated, full-time employment**

"All right, so I am ... Spanish. Specifically Colombian, I'm a first generation immigrant, and I think that being an immigrant made me more skeptical and careful having to start life somewhere else and figure things out and kind of get messed over and taken advantage of in some situations and made me just kind of question things, you know, like when they say, like, 'Oh, use a password manager,' I'm like, 'Whatever the password manager gets hacked,' you know, like question and be skeptical. And I think that my upbringing and where I'm from and how things are in Third World countries made me more of a survivalist." — **25-year-old man from Cypresse, TX, Colombian American (Latin American), high school graduate, full-time employment**

"So, the only thing I can think of is how my religion influences security and my privacy habits. I'm a lot more private about what I post online since I do wear the veil, the scarf. I don't post pictures of me without my scarf online, so I was careful with that and I don't reveal a lot of information online. I keep my personal life pretty much personal." — **38-year-old MENA American woman, Dearborn Heights, MI, college educated, full-time employment, married with children**

Acknowledgments

A big thank you to Kris Yun for her support as my research assistant during the initial survey and diary study. You added an intergenerational lens to the work and your commitment to supporting this vision was essential.

Thank you so much Juan Carlos Chavez and Itsa Dan Hawk for their candor and welcoming spirit. I appreciate your guidance and support as I ventured to share a peek into the American Indian, Alaska native, indigenous native peoples experience.

Thank you Peiter "Mudge" Zatko, Jon Kaltwasser, Wendy Nather Anita D'Amico, Kelley Mistra, Amanda Krauss, and Paul Rosenzweig for being part of the brain trust that helped shape and inform this work.

Thank you to the FDD team, especially Samantha Ravich and Annie Fixler for their support, editing, and contributions to this project.

Thank you, Lauren Zabierek, for your continued support and partnership on #ShareTheMicInCyber and your keen eye on this paper.

Thank you to my husband for his support and encouragement.

About the Author

Camille Stewart Gloster, Esq. is the deputy national cyber director for technology and ecosystem for the White House. In her role, Camille leads technology, supply chain, data security, and cyber workforce and education efforts for the Office of the National Cyber Director (ONCD). Camille is a cyber, technology, and national security strategist and policy leader whose career has spanned the private, public, and non-profit sectors. She joined ONCD from Google, where she most recently served as global head of product security strategy and before that as head of security policy and election integrity for Google Play and Android. Prior to working at Google, Camille led cyber diplomacy, technology policy, privacy, and technical policy areas as the senior policy advisor for cyber, infrastructure & resilience at the U.S. Department of Homeland Security (DHS). During her time at DHS, Camille led campaigns, international engagements, and policy development that bolstered national and international cyber resilience.

Camille authored this report in her personal capacity and concluded her work on it prior to joining ONCD.

About the Foundation for Defense of Democracies

FDD is a Washington, DC-based, nonpartisan 501(c)(3) research institute focusing on national security and foreign policy.

About FDD's Transformative Cyber Innovation Lab

TCIL finds and nurtures technologically feasible, testable pilot projects which begin to solve some of the hardest cyber problems afflicting the national security industrial base and the United States. TCIL's mission is to help shorten the lag between idea and piloting and between piloting and the adoption of potential solutions to the thorniest of cyber problems. TCIL seeks to drive revolutionary, society-wide improvement in cyber resilience through the innovative synthesis of technology, policy, and governance.

For more information, visit: https://www.fdd.org/projects/transformative-cyber-innovation-lab