

girls who
CODE



Breaking Barriers: Girls and the Future of Cybersecurity



A NOTE FROM JEN EASTERLY, FORMER DIRECTOR OF THE CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

As someone who has spent decades defending our nation's most critical systems, I've learned that cybersecurity is not just about technology—it's about people. And right now, we are leaving too much talent on the sidelines.

This is why the research you're about to read matters so deeply. When I look at a cybersecurity workforce that is only 22% women, I don't just see an engagement problem—I see a national security vulnerability. But this is not just a challenge—it's also an opportunity. By bringing more girls into cybersecurity, we strengthen our workforce, our resilience, and our national security.

My own journey in this field has shown me how much we lose when brilliant minds are discouraged from joining our ranks. While I was fortunate to have mentors who believed in my potential, too many young women never get that chance—not because they lack capability, but because they never see themselves represented in this vital work.



The findings in this report reveal that we're losing potential cyber defenders as early as the teenage years. Girls view cybersecurity as "too technical" or "too stressful"—misconceptions that rob our field of diverse talent precisely when adversaries are becoming more sophisticated and audacious. But the research also illuminates hope: when girls understand what cybersecurity really entails, 85% express interest in the field.

Girls Who Code is leading the way in bringing more girls into the cyber career pipeline. Their work proves that coding is a powerful gateway—but it's only the beginning. As AI increasingly automates routine coding tasks, the uniquely human skills of cybersecurity—critical thinking, creativity, and the ability to outmaneuver active adversaries—become even more essential. That's why introducing girls to cybersecurity now is so powerful: it builds on coding as a foundation while opening doors to protecting the systems that underpin our way of life.

And the research shows that the impact is measurable and profound: Girls Who Code alumni are significantly more interested in continued cybersecurity learning than their peers nationwide. They know more adults working in cybersecurity, creating crucial professional networks, and they practice cyber safety behaviors at substantially higher rates.

The stakes could not be higher. Our digital infrastructure underpins everything from power grids to medical devices to financial systems. Protecting it requires all hands-on deck—and that means ensuring young women see cybersecurity as the critical, creative, collaborative field it truly is.

The research ahead provides a roadmap. Now we must act on it—with urgency, with resources, and with the recognition that our shared future depends on it.

Jen Easterly

Former Director of the Cybersecurity and Infrastructure Security Agency

INTRODUCTION

Women represent only 22% of cybersecurity professionals globally—a gender gap even more pronounced than in the overall tech workforce where 27% of jobs are held by women.¹ While existing research has focused on the barriers facing women in pursuing and thriving in cybersecurity jobs, and what young people know and think about cybersecurity, there is a lack of research specifically focused on girls and cybersecurity.²

To address this gap in the research, Girls Who Code conducted a national survey of 2,105 teens to better understand girls' awareness and attitudes around cybersecurity, as well as what conditions might support them to pursue cybersecurity as a profession.³

Through this research, we learned that the cybersecurity gender gap is not just a workforce problem. The disparities we see in professional cybersecurity are emerging as early as the teenage years, creating an urgent need for interventions that address these gaps before they solidify. Our findings uncover actionable solutions that organizations, educators, and industry professionals should activate to support girls along the cybersecurity pipeline and bolster an industry in need of diverse talent.



Statistically significant gender gaps exist—with boys outpacing girls—in key engagement metrics, including confidence in tech skills, cybersecurity career interest, sense of belonging in the cybersecurity field, and perceptions of cybersecurity as "cool" and attainable.

Misconceptions are creating barriers. Girls view cybersecurity as "too technical," "stressful" and overestimate coding requirements, reflecting widespread misunderstandings about the realities of a cyber career. These misconceptions mask what actually attracts girls to cybersecurity: protecting people, working with technology, and solving problems.

The more girls know about cybersecurity and the realities of working in the sector, the more interested they are in pursuing a career in the field. While half of all girls expressed interest in a cybersecurity career, this number jumped to 85% among girls who "know a lot" about cybersecurity.

There is a peak intervention window to cultivate awareness and interest. Girls' cybersecurity career interest peaks at ages 15-16 before declining in their late teens, creating a critical need for early intervention.

Out-of-school-time programs are essential for fostering knowledge of cybersecurity careers, but they are underutilized. Girls who are very familiar with cybersecurity are 16× more likely than less-familiar peers to have discovered cybersecurity careers through an out-of-school-time (OST) program like Girls Who Code. Yet, these types of high-impact programs reach fewer than 1 in 3 girls.

Girls Who Code is a model of success, with its alumni more likely than other teen girls to be on track to pursuing a cyber career. Girls who have participated in Girls Who Code programs are significantly more interested in continued cyber learning than girls nationally. They also know more adults who work in cybersecurity and, compared to their peers, practice cyber-safety behaviors at higher rates.

DETAILED FINDINGS

GIRLS LAG BEHIND BOYS IN CYBERSECURITY INTEREST BUT SHOW SIMILAR ONLINE SAFETY BEHAVIORS

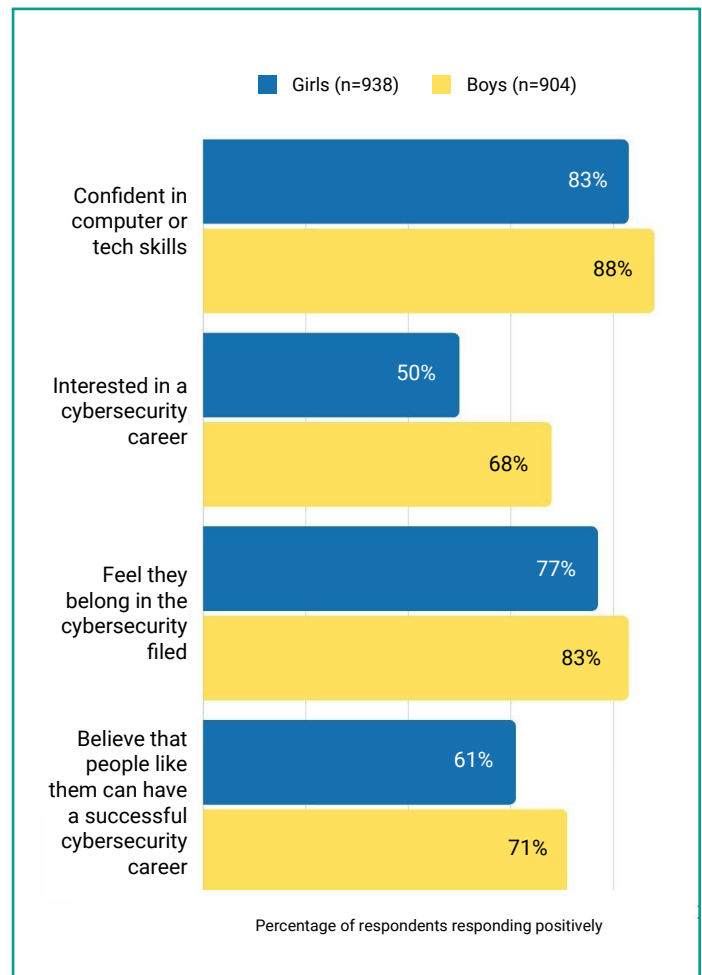
Our research found statistically significant gender gaps—with boys outpacing girls—across several key engagement metrics, including confidence, career interest, and feelings of belonging. Girls consistently showed lower levels across these measures, with the largest gap occurring in cybersecurity career interest (50% compared to 68% of boys).

Importantly, the belonging gap is most pronounced among girls from historically underrepresented groups.⁴ Only 57% of girls from historically underrepresented groups believe people like them can succeed in cybersecurity, compared to 64% of other girls. As this report will continue to discuss, it is key to address these identity and belonging disparities early in order to establish an initial interest in a cyber career.

These gaps are important and build on an existing knowledge base around girls' confidence in their technical skills and feelings of belonging within STEM. Research shows that girls often lose confidence in STEM subjects during early adolescence and are less likely to have a sense of identity and belonging in STEM fields compared to their male peers. These gaps emerge early, persist and often widen throughout the educational pipeline and into the workforce.⁵

These findings do not, however, fully represent the realities of girls' cybersecurity knowledge and online safety practices. Our research found that girls and boys are completing similar basic cybersecurity tasks in their daily lives and completing these tasks at similar rates—from avoiding suspicious links and protecting personal data on social media, to updating software and adjusting privacy settings. This points to a misalignment between girls' confidence in their technical skills and their daily cyber safety practices.

Figure 1: Gender disparities - confidence, interest, and belonging



PERCEPTIONS AND MISCONCEPTIONS OF THE FIELD

Issues of belonging are further compounded by girls’ broader perceptions of the cybersecurity field. Girls are less likely than boys to see cybersecurity as an appealing career and more likely to view it as inaccessible. They are significantly less likely to find cybersecurity “cool and exciting” and more likely to perceive it as “too technical” (33% compared to 22% of boys).

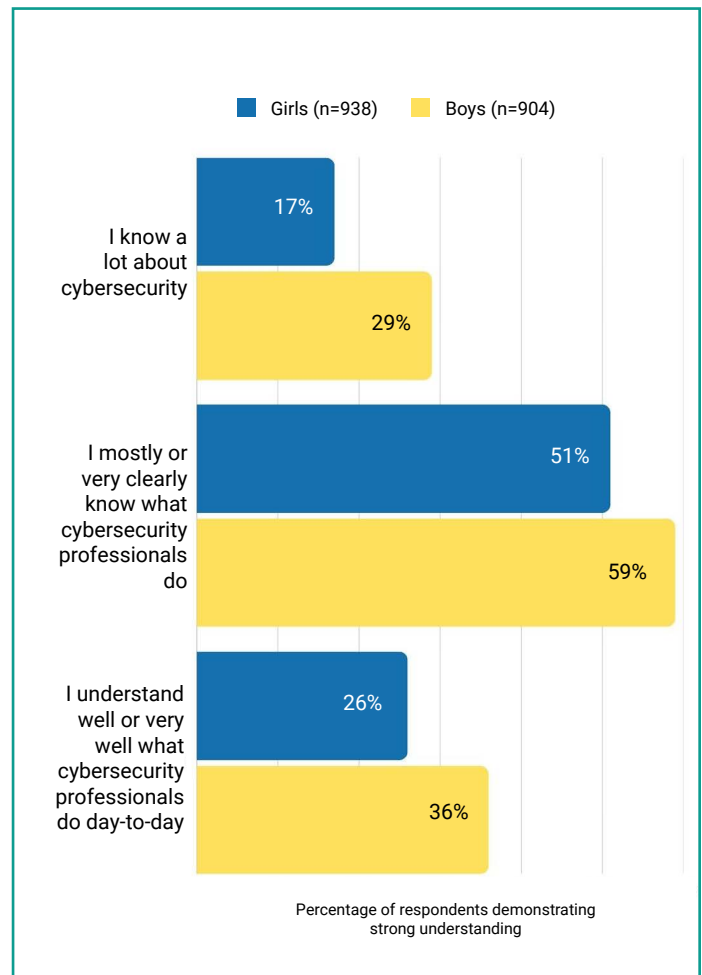
Our research found that these perceptions are grounded in a few common misconceptions around the cybersecurity field. Girls believe that working in cyber is “stressful” and requires a lot of education. There is also a persistent “coding myth” with approximately one out of four girls believing that coding is the most important skill in a cyber career. Efforts to bring more girls into the cyber pipeline must debunk these misconceptions and demystify cybersecurity professions.

BRIDGING THE KNOWLEDGE GAP: FROM AWARENESS TO INTEREST

While nearly all girls (97%) have heard of cybersecurity, this broad awareness masks a critical knowledge gap that is preventing girls from advancing in the cybersecurity pipeline. Compared to boys, girls lack a deeper knowledge of cybersecurity and the work of cybersecurity professionals.

Additionally, approximately one-third of girls have not heard of common cybersecurity job titles like Chief Information Security Officer, Penetration Tester, or Incident Responder—a significantly higher rate than boys (25%). Without this practical knowledge of cybersecurity jobs, many girls may struggle to envision themselves in these roles, regardless of knowing the field exists.

Figure 2: Cybersecurity knowledge, by gender



Awareness alone is not enough—girls need exposure to specific cyber career pathways, an understanding of role responsibilities and daily tasks, and opportunities to observe and learn from cyber professionals. The stakes of closing this knowledge gap are significant. Girls who report knowing “a lot” about the field demonstrate higher tech confidence, stronger comprehension of technical concepts, and—importantly—express greater interest in cybersecurity careers.

WHAT DRAWS GIRLS TO CYBERSECURITY: OPTIMIZING APPROACH AND TIMING

As previously discussed, our research uncovered persistent myths that girls hold about cybersecurity: that cybersecurity jobs require extensive coding skills, advanced math, or tolerance for highly stressful work environments. These misconceptions must be directly addressed by highlighting what actually attracts girls to cybersecurity: protecting people, working with technology, and solving problems.

Specific examples of daily work and hands-on experiences that lead with the aspects of cybersecurity professions that appeal directly to girls will help debunk these misconceptions and enable them to see themselves in the cyber field.

Getting this messaging right is urgent because the window for impact is limited, and these interventions must be timed strategically. Girls' cybersecurity interest peaks at ages 15-16, with 70% very interested or somewhat interested in continued cyber learning and 53% very interested or somewhat interested in a cyber career. Interest then declines in their late teens, mirroring a troubling pattern documented in broader STEM research. This finding aligns with the notion of the "middle school cliff"—the period when girls' interest in computer science declines dramatically while boys' interest grows.⁶ Our research confirms this same dynamic is playing out in the cybersecurity field, revealing a narrow but essential intervention window.

Figure 3: What draws girls to the cybersecurity field?

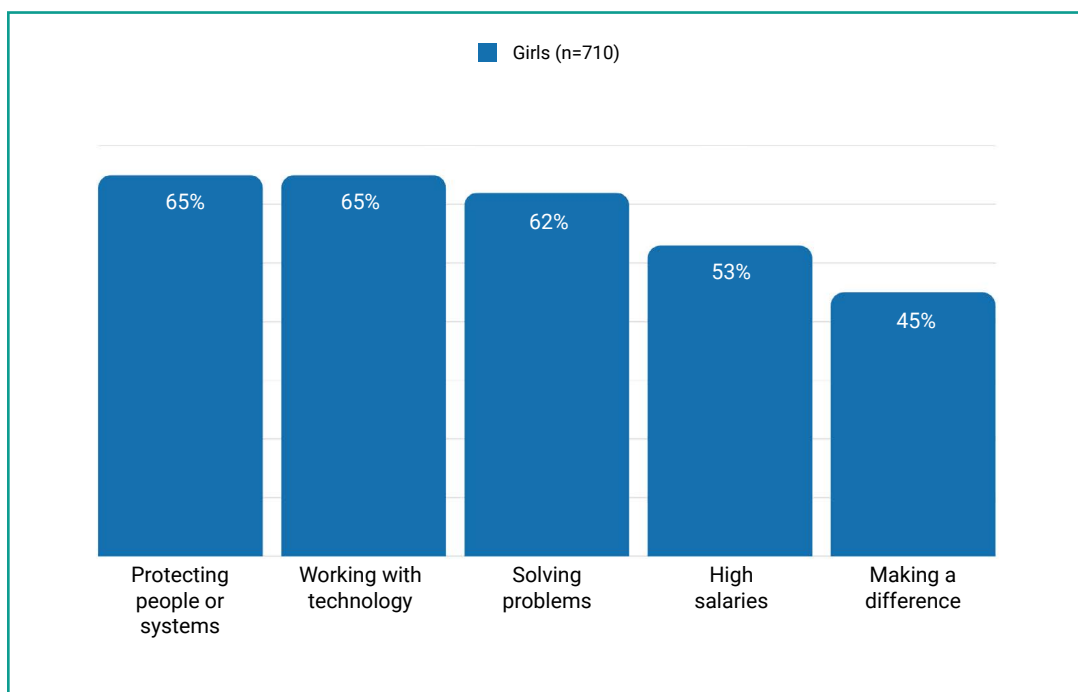


Figure 4: Girls' interest in continued cybersecurity learning, by age

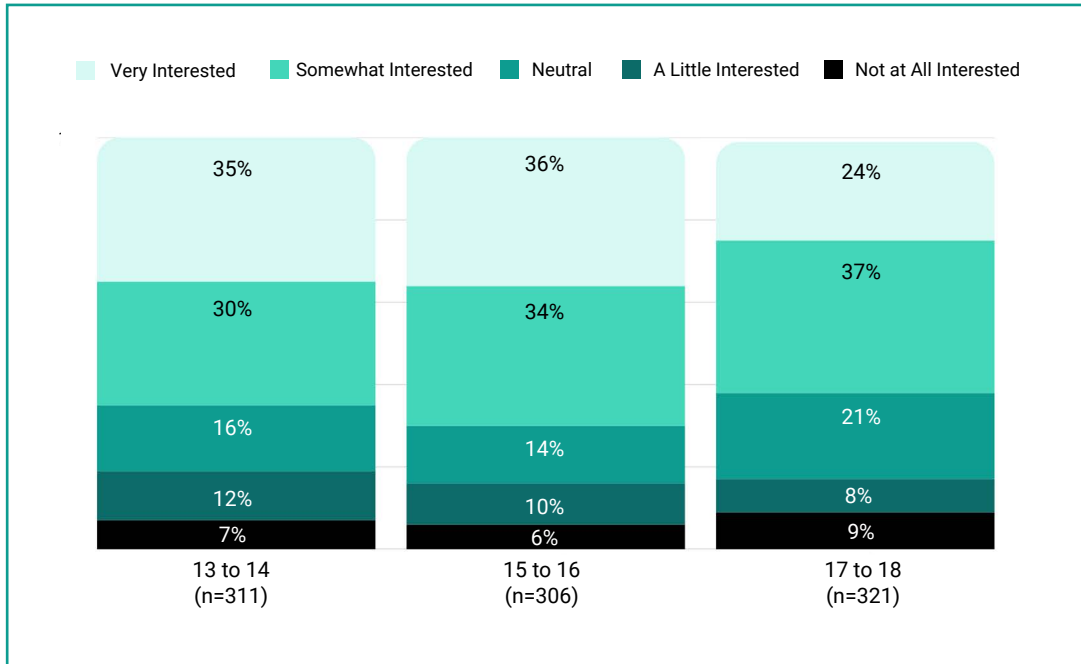
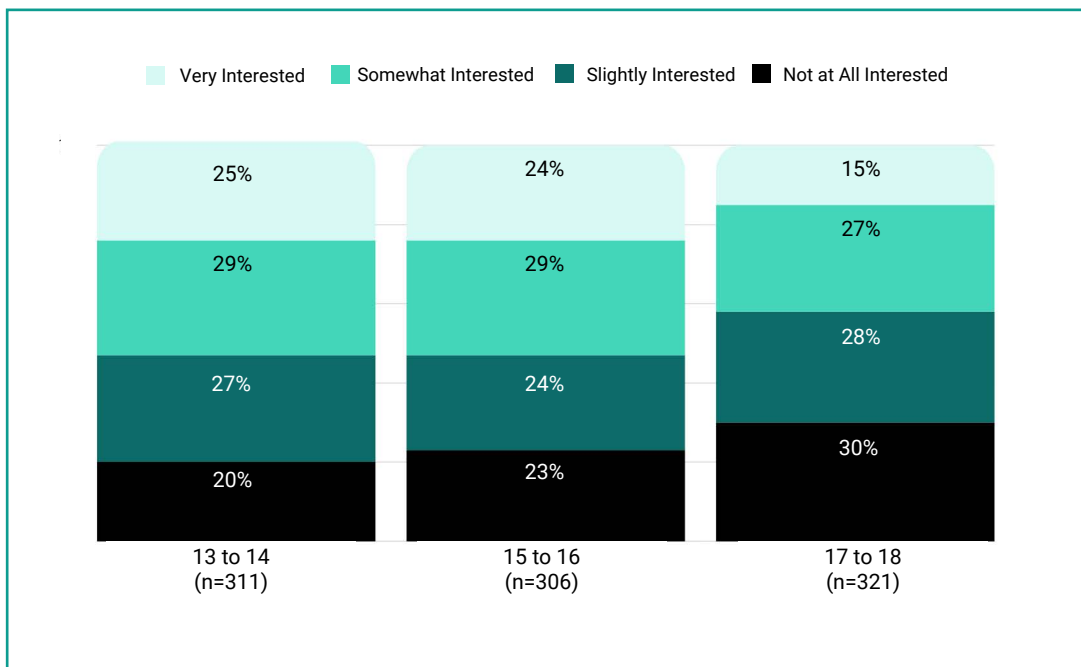


Figure 5: Girls' interest in cybersecurity careers, by age



The implications are clear: ages 13-16 offer a critical window to focus on knowledge-building, address field misconceptions, and nurture feelings of belonging—but only if acted on before interest begins its decline.

Not all girls, though, need the same approach to cultivating interest and building knowledge. Our research reveals that barriers shift depending on where girls are in their journey, with two distinct populations emerging that each require different support and intervention strategies (see "Missing Out" vs. "Cyber-Ready" Girls analysis, to the right).

Girls with low initial interest are more likely to cite concerns that cybersecurity is "too technical," that they "don't belong," or that they "don't understand" the field. For these girls, changing their perceptions is the critical first step to sparking interest.

However, once girls develop initial interest, the barriers change entirely. Now they face practical obstacles: training costs, certification expenses, and lack of mentors. At this stage, removing these friction points becomes essential for converting interest into sustained engagement.



Our research identified two distinct populations of girls that each require different support and intervention strategies.

1

"Missing Out" Girls (19% of sample)

These girls have minimal cybersecurity exposure and need broad-reach, identity-focused interventions before technical content becomes relevant.

What they need:

Demonstrations that cybersecurity professionals look like them and welcome diverse perspectives, with a focus on belonging signals over skill development.

2

"Cyber-Ready" Girls (7% of sample)

These girls show high engagement and confidence but face practical barriers to entry. Despite their readiness, 52% cite training costs as obstacles and 25% lack mentors.

What they need:

Implementation support rather than awareness building—for example, scholarships, micro-credentials, and mentoring programs.

UNTAPPED POTENTIAL: SCALING METHODS THAT WORK

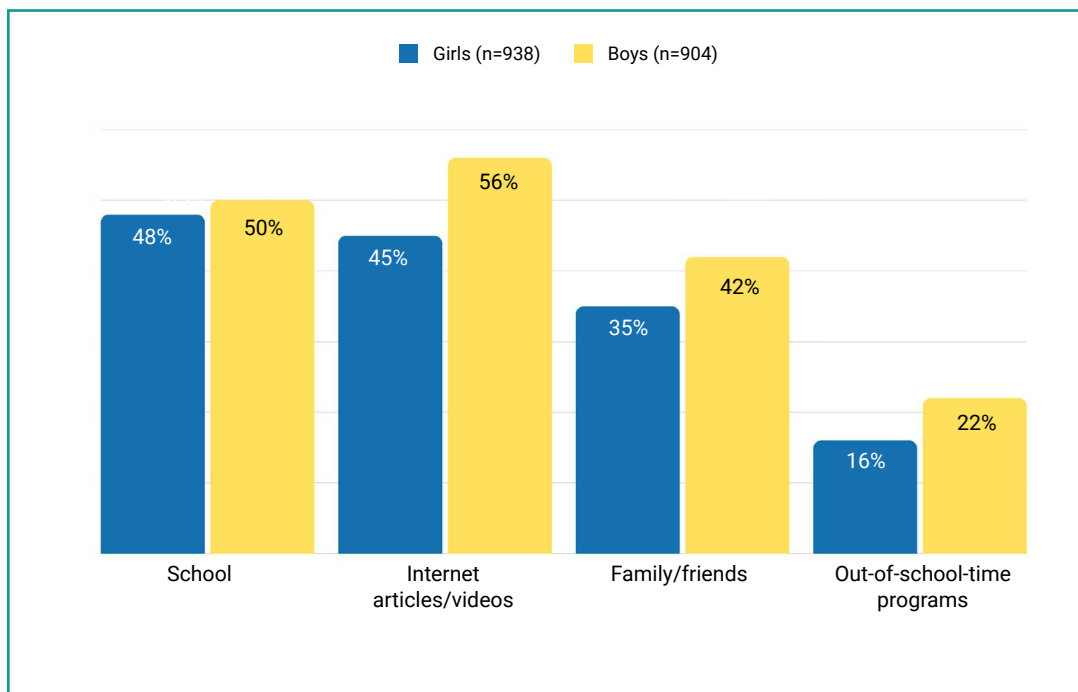
There is another critical piece of the puzzle: not all methods for learning about cybersecurity careers are created equal, and the most effective approaches are reaching the fewest girls.

Both boys and girls tend to hear about cybersecurity careers at school, but our data reveal that girls are less likely than boys to get this information from other common channels, like internet sources, family and friends, and out-of-school-time (OST) programs. For example, only 45% of girls learn about cyber careers via internet articles or videos compared to 56% of boys. This disparity highlights the potential of online initiatives, such as the Cyber Education Alliance led by Girls Who Code, to reach girls at scale and diversify their exposure to cybersecurity career information.

While gender gaps across information channels must be addressed, these channels are not equally effective at building the deep career knowledge girls need to sustain interest through their teens. OST programs stand out dramatically from the rest in their ability to advance and deepen discovery of cyber careers.

While girls typically learn about cybersecurity careers at school, online, or from family and friends, OST programs are a powerful way to connect with a highly motivated subset: girls who are very familiar with cybersecurity are 16× more likely than less-familiar peers to have discovered cybersecurity careers through an OST program. Yet only 28% of girls report participating in these types of programs, revealing a huge intervention opportunity particularly during the critical 13-16 age window.

Figure 6: Where teens learn about cybersecurity careers, by gender

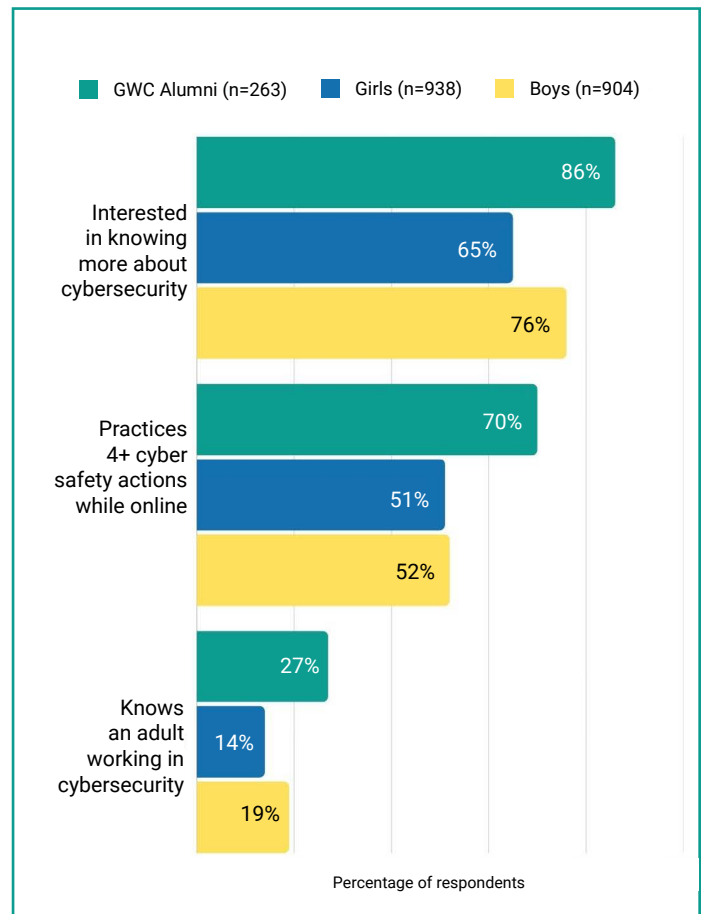


HOW GIRLS WHO CODE IS BRINGING GIRLS INTO THE CYBERSECURITY CAREER PIPELINE

The power of OST programming becomes clear when looking at Girls Who Code alumni. Girls Who Code alumni practice cyber safety behaviors at significantly higher rates than teen girls nationally, know more adults who work in cybersecurity, and show significantly greater interest in continued cybersecurity learning.

What makes programs like Girls Who Code uniquely effective is their ability to bridge a decisive gap. While only 3% of girls have never heard of cybersecurity, 17% have never heard of cybersecurity careers. This reveals how general awareness efforts might successfully introduce the field while failing to connect it to career possibilities. Girls Who Code and other OST programs excel precisely where other interventions fall short: they provide concrete examples of cybersecurity professionals and career pathways, transforming abstract awareness of the field into tangible career understanding.

Figure 7: Spotlight on Girls Who Code alumni



CONCLUSION: A CLEAR PATH FORWARD

The lack of female representation in the cybersecurity workforce requires urgent, meaningful action to engage more girls from an early age, and our research provides a roadmap for this change. The barriers preventing girls from pursuing cybersecurity careers are not insurmountable. They stem from misconceptions, knowledge gaps, and limited access to quality programming during critical developmental years.

Organizations, educators, and industry professionals now have specific, evidence-based strategies to address these challenges and build a more diverse and cybersecurity pipeline.

1. Find ways to attract more girls to out-of-school-time programs that expose them to cybersecurity, like Girls Who Code.

OST programs represent a uniquely effective pathway for advancing cybersecurity career knowledge. Girls very familiar with cybersecurity are 16x more likely to have discovered cyber careers through OST programs, yet only 28% of girls participate in these programs. Expanding access to quality programming that offers hands-on cybersecurity learning, exposure to career pathways and professionals, and meaningful skill-building experiences represents the highest-impact strategy for closing the gender gap in cyber.

2. Target the intervention to ensure girls are engaged in cybersecurity learning at the optimal age of 13-16.

Girls' cybersecurity interest peaks at ages 15-16 before declining, creating a narrow but essential opportunity for impact. Practitioners must strategically aim to reach girls during this critical window when they remain most receptive to career exploration and identity formation around technical fields.

3. While expanding general awareness of cybersecurity is essential to bring girls into the pipeline, practitioners must design offerings that enable girls to build deep knowledge of cybersecurity careers, including the day-to-day work involved.

Surface-level cybersecurity awareness is not enough to sustain career interest. Girls need concrete understanding of what cybersecurity professionals actually do day-to-day, exposure to diverse career pathways, and realistic job previews that emphasize problem-solving, protecting people, and working with technology rather than coding prerequisites.

By implementing these strategies at scale, we can accelerate progress toward gender equity in cybersecurity and build the diverse workforce our digital future demands.



ABOUT GIRLS WHO CODE

Girls Who Code is dedicated to closing the gender gap in technology, with the goal of reaching 5 million girls, women, and nonbinary individuals by 2030. Our mission is to inspire, educate, and champion girls, women, and nonbinary people, with a special focus on historically underrepresented groups, to become changemakers in tech. We are committed to increasing access to the technology field for all, equipping the next generation to thrive in emerging fields like artificial intelligence, cybersecurity, and other transformative technologies shaping the 21st century. Since launching in 2012, Girls Who Code has reached over 760,000 students through our in-person and virtual programming. Of these, 330,000 alumni are now college or career-aged, ready to lead in tech. Learn more at girlswhocode.com.



ABOUT THE CYBER EDUCATION ALLIANCE

Formed in 2024, the Cyber Education Alliance is a coalition led by Girls Who Code composed of organizations dedicated to safeguarding young people online. The Alliance uniquely harnesses the collective power of its members' networks to reach youth, teachers, and parents across the United States, ensuring equitable access to cybersecurity education and resources. Its members include Black Girls Code, Black Girls Hack, CodeHS, Common Sense Media, CYBER.org, CyberTorial, DoSomething, the Geena Davis Institute, Girls Who Code, Girls Who Hack, Girl Scouts of Greater NY, Hack Club, IGNITE Worldwide, Raices Cyber Organization, Startfield, T-ATP, Women in Cybersecurity (WiCYS), Women in Security and Privacy (WiSP), and the Women's Society of Cyberjutsu (WSC). Learn more at getcybersmart.org.



ABOUT TOUCHSTONE RESEARCH

Touchstone Research (TSR) is a full-service market research firm with over 30 years of expertise in engaging kids, teens, young adults, and other hard-to-reach audiences. TSR employs a wide range of COPPA-compliant methodologies, including online surveys, focus groups, in-depth interviews, discussion boards, UX testing, and insight communities, to deliver authentic and actionable insights. Leveraging innovative technologies and rigorous data quality controls, TSR empowers leading global brands, nonprofits, and educational organizations to make informed decisions with confidence. Learn more at touchstoneresearch.com.



END NOTES

METHODOLOGY

Data were collected via an online quantitative survey built and administered by Girls Who Code in collaboration with Touchstone Research. This survey was fielded from June 30, 2025 to July 23, 2025. The population included U.S. teenagers ages 13–18. The total sample of 2,105 respondents comprised two groups: 1,842 general population teens recruited from national online consumer panels and 263 Girls Who Code alumni recruited via email campaigns. The general population sample included 938 girls and other gender identities and 904 boys. The sample was evenly distributed across age groups and nationally representative by region and race/ethnicity.

REFERENCES

- ¹ ISC2 (2024). [“Women in Cyber”](#); NCWIT (2024). [“By the Numbers”](#); CompTIA (2024). [“State of the Tech Workforce 2024.”](#)
- ² CYBER.ORG (2021). [“The State of Cybersecurity Education in K-12 Schools”](#); WiCyS (2023). [“The 2023 State of Inclusion Benchmark in Cybersecurity”](#); World Economic Forum (2022) [“Empowering women can help fix the cybersecurity staff shortage.”](#)
- ³ Online survey of U.S. teens ages 13-18 (N=2,105) administered by Touchstone Research, including nationally representative general population sample (n=1,842) and Girls Who Code alumni (n=263).
- ⁴ This includes respondents who are Black, Latinx, Indigenous, and from other races/ethnicities underrepresented in tech.
- ⁵ Accenture and Girls Who Code (2020). [“Resetting the Tech Culture”](#); Accenture and Girls Who Code (2016). [“Cracking the Gender Code”](#); CompTIA (2024). [“State of the Tech Workforce 2024”](#); Forbes (2024). [“Gender Bias In STEM May Start In Kindergarten”](#); Forbes (2017). [“Why Women Leave the Tech Industry at a 45% Higher Rate Than Men”](#); UNESCO (2024). [“Closing the Gender Gap in Science”](#); Shenouda et al. (2024). [“Who Can Do STEM?: Children’s Gendered Beliefs about STEM and Non-STEM Competence and Learning.”](#)
- ⁶ Accenture and Girls Who Code (2016). [“Cracking the Gender Code.”](#)