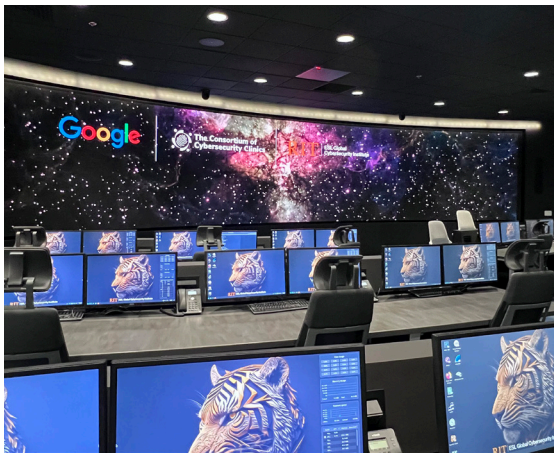
Google.org

2026 Impact Report

Google.org's Cybersecurity Clinics Fund

Investing in America's Cybersecurity Infrastructure



BUILDING STRONGER, SAFER, MORE RESILIENT COMMUNITIES

For two and a half decades, Google's investments in technology and talent have fueled growth in communities across the country. While the creation of technology can create new threats, it can also help us fight them. Security has always been at the core of our products, and we've long worked to protect people, businesses and governments by sharing our expertise and advancing cybersecurity tools and resources.

We know that cyber attacks on vital neighborhood resources, like hospitals, power grids, and emergency response services, can wreak havoc on the everyday lives of those who depend on them. That's why, in 2023, amidst historic investments in national infrastructure and the rapid adoption of AI, Google identified a real and urgent need—**to equip communities to guard against cyber attacks and ensure a robust pipeline of talent to serve the diverse cybersecurity needs of communities nationwide.**

To meet the needs of the moment, we established the **Google Cybersecurity Clinics Fund and awarded more than $36 million to support the creation and expansion of cybersecurity clinics at 35 educational institutions across the U.S.** Cybersecurity clinics function much like clinics at law schools or medical schools, delivering free security services and critical support to K-12 schools, healthcare systems, local governments, nonprofits, small businesses, and more. From Washington, D.C. to Hawaii, hundreds of students have been deployed into their communities to address critical vulnerabilities. Institutions selected to be part of the fund have also received access to in-kind resources, including the Google Cybersecurity Certificate, Passkeys and mentorship from Google security subject matter experts.

In collaboration with the Consortium for Cybersecurity Clinics, the fund brings together college and university students, industry professionals, local governments, nonprofits, and small businesses to help communities stay ahead of new and evolving threats.

We're now seeing the impacts of this work firsthand. For example:

- A local water authority in San Diego improved its security configurations, threat detection, and response processes with the support of the San Diego Cyber Clinic
- The County Manager in rural Georgia, who doubled as his county's IT Manager, became equipped to protect his constituents and their services with support from University of Georgia's cybersecurity clinic
- A power grid serving 80,000 residents in Indiana strengthened its defenses with the assistance of Indiana University's Cybersecurity Clinic

As a longtime champion of computer science education, academic research, and applied learning, I know well that these hands-on experiences not only help students gain valuable real world experience, but provide organizations and communities with valuable tools and resources—and we're thrilled to see economic opportunity born of this work.

As we build an AI-enabled future, this work has never been more important. Thank you to the cyber clinics and local organizations who are working together to build a more safe and secure future. We can't do this alone—and your partnership has made this work possible for communities big and small.

Maggie Johnson
Google.org

ADDRESSING THREATS TO CRITICAL INFRASTRUCTURE:
The Pressing Need for Cybersecurity Talent

Cybersecurity is central to our daily lives and protects our most critical systems—from our hospitals and schools to our power grids and financial systems. While AI is accelerating innovation, research, advances in critical sectors like healthcare, it's also accelerating the speed, scale, and sophistication of cyberattacks, vulnerabilities are multiplying faster than organizations can respond.

At the same time, more than half a million cybersecurity jobs in the U.S. remain unfilled, leaving critical infrastructure exposed—and economic opportunity on the table.

$4.4M

is the average cost of a data breach in the U.S.[1]

77%

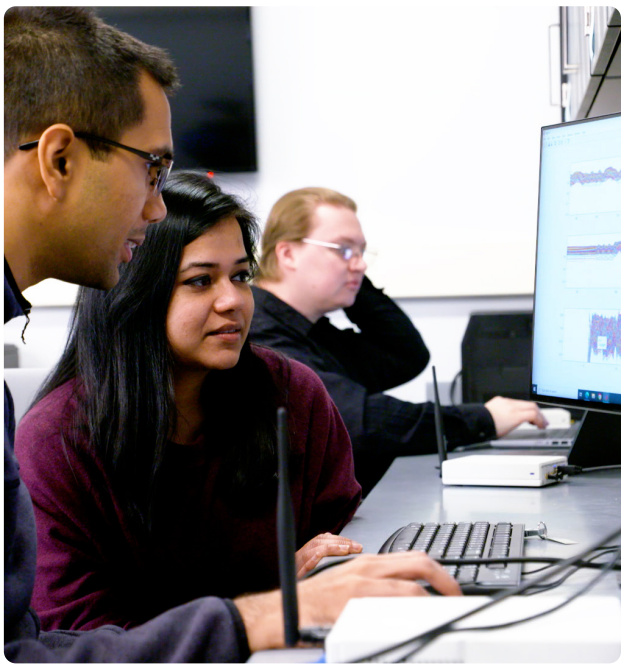
of organizations lack the data and AI security practices needed to safeguard critical infrastructure[2]

16%

of cybersecurity breaches in 2025 involved attackers using AI[3]

514,000

unfilled cybersecurity jobs in the United States[4]



1 IBM Security, Cost of a Data Breach Report 2024–2025, https://www.ibm.com/reports/data-breach.
2 Accenture, State of Cybersecurity Resilience 2025, https://www.accenture.com/content/dam/accenture/final/accenture-com/document-3/State-of-Cybersecurity-report.pdf.
3 IBM Security, Cost of a Data Breach Report 2025, https://www.ibm.com/reports/data-breach.
4 National Institute of Standards and Technology (NIST) and CyberSeek, "New CyberSeek Updates Reveal 57,000 Increase in Cybersecurity Job Openings," June 2025, https://www.nist.gov/news-events/news/2025/06/new-cyberseek-updates-reveal-57000-increase-cybersecurity-job-opening.

GROWING CYBERSECURITY RESILIENCE:
Google.org's Cybersecurity Clinics Fund

Security has always been at the core of Google's products, as we've long worked to protect people, businesses, and governments by sharing our expertise and advancing cybersecurity tools and resources. Our Cybersecurity Clinics Fund was established in 2023 to help secure critical infrastructure and equip academic institutions to create and expand education and work-based learning opportunities for students interested in a career in cybersecurity. The $36M investment will help grow 35 cybersecurity clinics across the and will provide:

The $36 million investment will help grow and launch 35 cybersecurity clinics across the country.

7,600+

students with hands-on learning and cybersecurity skills

1,250+

community-based organizations with support to secure their critical systems

"At Google, we feel a deep sense of responsibility to help people find good paying jobs in technology. We also want to make sure that, as a nation, we have a strong cybersecurity workforce to help us stay ahead of new and evolving threats. That is why we launched the Cybersecurity Clinics Fund—to give students the opportunity to learn and improve their skills, while helping to protect critical infrastructure such as hospitals, schools and energy grids.

Sundar Pichai, CEO of Google and Alphabet

BRIDGING LEARNING AND IMPACT:
Core Components of Clinics

1

Interdisciplinary, Cybersecurity Curriculum

The heart of cybersecurity clinic operations is the curriculum. Each cyber clinic has an interdisciplinary approach and tailors its courses to the needs of their students and community. Typical curricula topics include: common types of cybersecurity attacks, AI in cybersecurity defense, risk assessment, network security, incident detection, and cloud security.

2

Hands-on Experience with a Community-based Client

Each clinic identifies public interest institutions and community-based organizations that are typically at high-risk for cyber attacks and might not be able to afford comprehensive, costly consulting services. Student teams work alongside these organizations to provide high-quality cybersecurity services, which may include standardized risk assessments, compliance audits, policy development and staff training, to strengthen their security posture.

3

Google.org Supports

For institutions who have received funding to expand or create a cybersecurity clinic, Google.org also offers access to Google mentors and volunteers, Passkeys, and Google Cybersecurity Career Certifications. These supports help accelerate the impact of each clinic.

96%

of clinics offer free access to Google Cybersecurity Certifications

90%

of clinics use Passkeys donated by Google

72%

of clinics leverage Google mentors and volunteers

The Consortium of Cybersecurity Clinics

Building a Network of Support: The Consortium of Cybersecurity Clinics

Founded in May 2021, the Consortium of Cybersecurity Clinics serves as a forum for clinicians, trainers, students, and advocates to share knowledge, expand the reach of cybersecurity clinics, and lower the barriers for other institutions to establish their own clinics. The Consortium was founded after multiple member universities came together organically to support each other's work and help other institutions launch cybersecurity clinics of their own. Today, the Consortium is led by faculty and staff at MIT and UC Berkeley and has a network of 59 national and international institutional members.

"Without the Consortium of Cybersecurity Clinics and Google.org's funding, we would have not been able to launch our clinic this fall," said Meredith M. Quinn, Ph.D., Executive Director at the Center for Computing and Interdisciplinary Technology at Franklin Cummings Tech. "The Consortium provided legal templates, curriculum guidance, and best practices for working with small business that provided catalytic support for our two-year college to launch a best-in-class clinic in record time."

The Consortium has provided critical support to institutions in launching and growing their clinics' impact. Google.org is proud to support the Consortium's capacity to serve more institutions, including Franklin Cummings Tech.

"Every community should have access to cybersecurity expertise—and we are working to see a clinic in every state by 2030. The consortium can aggregate knowledge and collectively advocate for resources that make it more than the sum of its parts. By working together, we are creating scaffolding that underpins the sustainability of all the clinics—something no one clinic could do alone.

Ann Cleveland, Executive Director of Center for Long-Term Cybersecurity at UC Berkeley and co-chair of the Consortium of Cybersecurity Clinics

CLIENT SPOTLIGHT

FROM POLICE DEPARTMENTS TO PUBLIC UTILITIES: Safeguarding the City of Bloomington's Systems Serving 80,000 Residents

INDIANA UNIVERSITY
CYBERSECURITY CLINIC

Strong and secure digital infrastructure is essential to protect the services communities rely on every day—from clean water and emergency response to public safety and energy. Indiana University's Cybersecurity Clinic has partnered with the City of Bloomington over the past two years to ensure vital city functions run smoothly for its 80,000 residents, including public safety, utilities, and emergency response services.

A team of six cybersecurity clinic students supported the City of Bloomington's Fire Department to ensure the security and continuity of emergency services. At the time, the department was understaffed by approximately 20 firefighters, straining both resources and operational capacity. This gap, coupled with the integration of new technologies to improve efficiency, heightened their vulnerability to cyber threats.

The team developed a customized business continuity plan, addressing key risks to critical systems like 911 call centers, emergency dispatch software, and server access. Their work included designing redundancies to mitigate potential service disruptions, such as ensuring backup communication protocols in the event of a system outage.

At the same time, another team of six cybersecurity clinic students designed risk management frameworks for the City of Bloomington's IT department. With over 1,000 city employees working across 40 sites—from police and fire departments to public utilities—Bloomington's digital network must operate seamlessly. The students' work has been instrumental in identifying potential vulnerabilities and bolstering security protocols for their systems, making Bloomington more resilient to cyber threats.

The collaboration inspired several students to pursue internships with the City of Bloomington and careers in local government—and exemplifies how innovative, community-driven solutions can empower both students and municipalities, creating a model of mutual benefit and security for all.

GOOGLE MENTOR SPOTLIGHT

PREPARING THE WORKFORCE OF TOMORROW:

How Google.org Mentors Strengthen the Cyber Clinics Experience

At the San Diego Cyber Clinic, a collaboration between the Cyber Center of Excellence (CCOE), San Diego State University, California State University San Marcos, and National University, Google.org mentor Ben Trachtenberg has become a force multiplier—helping students sharpen their technical skills, understand real-world threats, and navigate a rapidly evolving cybersecurity job market. As a manager within Google Cloud, Ben has worked in tech and cybersecurity for more than 15 years. Now in his second year as a mentor, Ben supports the clinic through monthly office hours and quarterly webinars that draw more than 200 student registrants and give them unprecedented access to industry expertise.

Ben was immediately drawn to the clinic's model: students providing pro-bono cybersecurity assessments to small businesses and community organizations that rarely have the resources to hire cybersecurity professionals. "It's incredible to see students doing real consulting work, strengthening the security of the local organizations people rely on every day," he shared.

A consistent theme in his sessions is students' eagerness to understand the tools practitioners actually use. During these conversations, Ben bridges the gap between classroom learning and the realities he sees at Google supporting hundreds of companies each year. He helps students understand both enterprise-level challenges and the constraints of resource-strapped small businesses.

A highlight for Ben was participating in a recent clinic event where students and one of their client partners—a medical research center—shared their experience on stage. "Hearing students walk through their assessment, side by side with an organization they helped protect, was a powerful moment. You could see their confidence grow in real time."

Reflecting on his experience, Ben shared: "Everyone has someone who went above and beyond for them early in their career. This program lets us do that for the next generation. It's rewarding, it's energizing, and it builds the kind of talent the field needs."

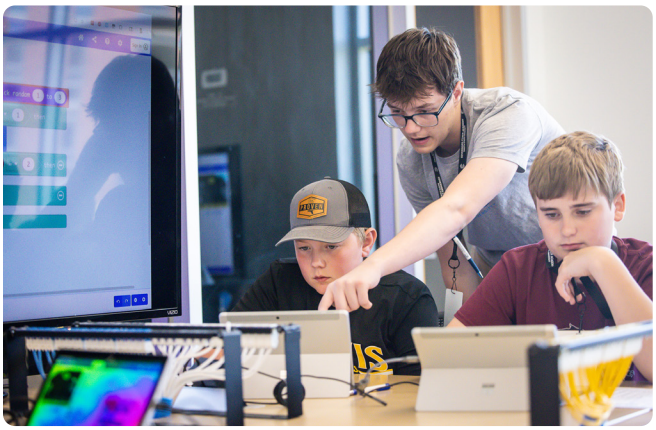
> It's incredible to see students doing real consulting work, strengthening the security of the local organizations people rely on every day.

BY THE NUMBERS:
Building Nationwide Resilience

Through Google.org's initial investment in cybersecurity clinics, they will equip more than 7,600 students across the U.S. with meaningful skills in cybersecurity and hands-on learning experiences. In addition, the funding will support more than 1,250 community-based institutions with critical public infrastructure and cybersecurity assessments and tools.

100%

of clinics surveyed said Google.org funds enabled their communities to be safer and more secure through increased access to cybersecurity expertise



96%

of clinics surveyed said Google.org funds allowed them to expand their impact in local communities

90%

of clinics surveyed said Google.org funds increase the amount of hands on training students receive

AI AND CYBER:
Highlighting Clinic Innovations

Emerging technologies like AI are reshaping the cybersecurity landscape—creating both unprecedented opportunities and evolving threats. In response, cybersecurity clinics are ensuring that the next generation is equipped to navigate a future where AI will play a defining role in both protecting and challenging digital systems.

AI-Enabled Tools to Support Organizations With Limited Resources

San Diego Cyber Clinic's CCOE helped develop My eCISO, a generative AI tool that provides scalable cybersecurity assessments based on the National Institute of Standards and Technology (NIST) framework. The tool, provided by the City of San Diego's Regional Cyber Lab has been leveraged by over 150 users and accelerates impact by supporting organizations with limited resources to more efficiently bolster their defenses.

Embedding AI into the Classroom

The University of Hawaii has added modules like large language models and prompt engineering into their curriculum to prepare students to detect and deter cyber threats. Similarly, Dakota State University is teaching students how bad actors use AI to enhance attacks. These efforts not only improve local cybersecurity readiness but also contribute to a global understanding of AI's potential to shape the cybersecurity landscape.

Google.org is proud to support these institutions leveraging innovative AI technologies to strengthen communities and protect critical infrastructure.

CLINIC SPOTLIGHT

PRACTICING DURABLE SKILLS:
How an AI-Enabled VR Lab is Transforming Cybersecurity Education

UNC GREENSBORO

Before University of North Carolina-Greensboro (UNCG) students meet a client, they meet someone else first: a lifelike virtual avatar that challenges their clarity, confidence, and communication skills. Under the supervision of Dr. Pourbehzadi, UNCG's cybersecurity clinic has built one of the country's first AI-enabled virtual reality labs designed to help cybersecurity students master the hardest part of client engagements: communicating clearly, confidently, and collaboratively with client executives.

Every semester begins with a six-week onboarding that blends technical foundations—NIST-aligned frameworks, rigorous curriculum, and workshops with a Google.org mentor—with UNCG's immersive VR durable skills experience. Inside the simulation, students interview lifelike avatars who behave like actual executives—pushing for clarity, asking follow-ups, and challenging jargon. After each session, an AI coach scores performance and gives comprehensive feedback. The result: students practice, repeat, and refine the human-centered communication skills essential for the workforce.

The model is already delivering measurable impact. In its first year, 98 students supported nearly 20 local organizations, including Forge Greensboro, the largest community makerspace in the Southeast.

"The team asked thoughtful questions and identified practical steps we could take immediately," said Executive Director Tiffany Jacobs. "They even made us aware of cybersecurity insurance—something we didn't realize existed—and helped us strengthen protections for our staff and members. Programs like this are an invaluable resource for community organizations."

By practicing authentic client interactions using AI and VR, students arrive on-site prepared not just to analyze systems—but to build trust, communicate risk, and help community partners build resilience.

STUDENT SPOTLIGHT

FROM CLASSROOM TO COMMUNITY:
Safeguarding Boston's Small Businesses

Franklin Cummings Tech

Franklin Cummings Tech—a two-year technical college deeply aligned with employer demand—designed its cybersecurity clinic around a simple idea: students learn best when they are solving real problems in their community. Ashanti DeJesus proved just how powerful that can be.

When Ashanti joined the clinic, she expected a class assignment; she didn't expect to help protect 30 neighborhood businesses in just ten weeks. Through a Google.org–funded partnership with the Boston Main Streets Foundation, Ashanti and a classmate conducted rapid, interview-based cybersecurity assessments for local shops, restaurants, and community-serving organizations that typically can not afford this support. They also delivered a virtual training to help business owners take immediate action on the findings.

The experience reframed cybersecurity as a form of community care. "It felt like helping keep the heart of the neighborhood beating," she shared.

The clinic also accelerated Ashanti's professional trajectory. Selected to present her work at the National Science Foundation conference in Washington, D.C., she gained visibility, confidence, and industry connections. Today, she works as a Security Operations Center Analyst at CyberTrust Massachusetts—a path aligned with the college's strong outcomes: 80% of Franklin Cummings Tech graduates secure employment within a year.

Ashanti now hopes to launch her own cybersecurity venture to support small businesses—a full-circle moment that reflects the promise of Franklin Cummings Tech cybersecurity clinic: when students learn by protecting their own communities, everyone becomes more resilient.

> "It felt like helping keep the heart of the neighborhood beating."

CYBERSECURITY CLINICS FUND FOOTPRINT

> In partnership with the Consortium of Cybersecurity Clinics, we have a simple yet bold goal: a cybersecurity clinic in every state by 2030. Cybersecurity clinics build resilience where it's needed most—preparing students for high-growth careers while helping communities stay secure.

Shanika Hope, Google.org

BUILDING TOGETHER: Our Trusted Clinic Partners

Spelman College

University of Hawai'i Maui College

Eastern Washington University

Trident Technical College

Turtle Mountain Community College

The University of Arizona

Tougaloo College

The University of Texas at El Paso

West Virginia State University Cybersecurity Innovation Center

Franklin Cummings Tech

UNC Greensboro

Northeastern State University

Berkeley University of California

UNLV

University of Georgia CyberArch

Indiana University Cybersecurity Clinic

Massachusetts Institute of Technology

RIT Rochester Institute of Technology

Stillman College

Texas The University of Texas at Austin

CIAS Center for Infrastructure Assurance and Security UTSA

UA Little Rock

Institute of Data and Analytics

The University of Oklahoma

Lewis & Clark College

Champlain College

LSU

Dakota State University

CCOE

with

California State University San Marcos

SDSU San Diego State University

National University

NSI Cyber and Tech Center

&

Howard University

CLIENT SPOTLIGHT

FROM SERVICE TO CYBERSECURITY:
Veterans Protecting Critical Infrastructure

In 2024, CCOE received a grant from Google.org to launch a cybersecurity clinic in partnership with their higher education institutional partners, including National University. National University was founded to support deployed soldiers and veterans, and as a leading educator of U.S. military personnel, the cyber clinic has engaged nearly 200 students in hands-on projects to safeguard critical infrastructure.

Securing a Local Water District

A team of students conducted a cybersecurity assessment for a municipal water district serving approximately 8,000 water and 3,000 sewer customers across an 80-square-mile area in California. This district manages critical infrastructure, including water mains, pump stations, and reservoirs, making it a vital service provider for the community. The assessment included social engineering exercises to mitigate phishing and insider threats, penetration testing to identify vulnerabilities, and the creation of essential resilience plans—like a disaster recovery plan. The work culminated in briefing the Chief Information Officer (CIO), providing actionable recommendations. Without these measures, the water district faced risks, including potential cyberattacks that could disrupt water supply, contaminate drinking water, or compromise sanitation services. By addressing these vulnerabilities, the students not only enhanced the district's resilience but also ensured the continued reliability of critical services for the communities.

Supporting Small Businesses

A veteran-led student team supported a small, family-owned trucking company transporting sensitive materials for the Department of Defense (DoD). Facing stringent cybersecurity requirements under the Cybersecurity Maturity Model Certification (CMMC), the business relied on the clinic's expertise to ensure its compliance and grow the business. The students conducted a comprehensive assessment, including a physical walkthrough of the office, and provided recommendations, such as securing laptops to prevent sensitive scheduling information from being compromised. This support helped the business achieve compliance and better protect sensitive DoD-related operations. Building on this success, the clinic is now developing a CMMC baseline program to offer free resources to small businesses across San Diego. This initiative ensures organizations can meet DoD requirements, fostering greater resilience in the defense supply chain.

STUDENT SPOTLIGHT

FROM CLINIC TO CAREER:

How Hands-on Clinic Experience Delivered A Dream Job

UNIVERSITY OF GEORGIA
CyberArch

When Hannah Brown first arrived at the University of Georgia, she knew she liked technology but thought her only pathway into a career in tech was through the School of Engineering. Everything changed when she joined CyberArch, a hands-on cybersecurity clinic at UGA's Carl Vinson Institute of Government. Through this program, students tackle real-world challenges—helping K-12 school districts, local governments, rural hospitals, and small businesses across Georgia improve their cybersecurity posture and fortify their digital infrastructure.

For Hannah, CyberArch became the turning point in her college journey. She worked with three county governments and a small business, helping them address critical cybersecurity vulnerabilities. Recognizing common struggles among counties, Hannah stepped up as a leader, creating and hosting a six-part webinar series in collaboration with the Association of County Commissioners of Georgia (ACCG). The series equipped government officials with practical strategies to apply the National Institute of Standards and Technology (NIST) Cybersecurity Framework—filling a knowledge gap in resource-strapped local agencies.

Hannah's leadership extended beyond the classroom. She helped create a summer camp curriculum to inspire the next generation of cybersecurity professionals. "My experience at CyberArch wasn't just about learning technical skills—it was about teamwork, leadership, and gaining the confidence to work with real-world clients," she said.

After graduating, Hannah joined Coalfire, a leading cybersecurity and compliance firm, as an associate. She credits her time at CyberArch with preparing her for the job. **"CyberArch introduced me to a career path I didn't even know existed and gave me the skills to succeed."** Hannah's story is a testament to the transformative power of cybersecurity clinics like CyberArch, which not only build the workforce of tomorrow but also strengthen the resilience of communities today.

CLINIC SPOTLIGHT

TURNING ADVERSITY INTO OPPORTUNITY:

How a Cyberattack Sparked Innovation at Stillman College

When the historically Black institution based in Tuscaloosa, Alabama faced a ransomware attack on its own campus network, Stillman College quickly recognized a critical need to protect its own systems and empower a new generation of skilled cybersecurity professionals. After the attack in 2017, Stillman College established the Cybersecurity DEI Clinic to equip its students to enter careers in cybersecurity and provide free cybersecurity services to community organizations and small businesses in the mid-south, particularly minority-owned businesses in Alabama and Tennessee. To further prepare its students to tackle emerging cyber threats, Stillman College facilitated "AI bootcamps" for students, giving them foundational skills in artificial intelligence and its applications in cybersecurity.

With a transformative $500,000 grant from Google.org, Stillman College was able to grow its impact and reach within the community. The clinic provides Stillman College students with education and real-world projects with local community organizations and small businesses in their community, often the hardest hit by cyber threats due to limited resources. Through partnerships with these community organizations, Stillman College students apply their classroom knowledge to protect vulnerable systems, enhancing their skills while providing critical services.

Today, Stillman College serves as a mentor to other Historically Black Colleges and Universities (HBCUs) launching cyber clinics within their own communities. By supporting HBCUs to create similar programs, Stillman College is helping to expand opportunities for underrepresented talent and strengthen cybersecurity nationwide.

For Stillman College, a cyberattack wasn't just a wake-up call—it was a catalyst for change.

In memory of Dr. Kevin Harris, the founding executive director of Stillman's Cybersecurity DEI Clinic and leading pioneer in the ecosystem.

STUDENT SPOTLIGHT

FROM PASSION TO PURPOSE:
Jose Torres' Journey to Cybersecurity

TEXAS
The University of Texas at Austin

For Jose Torres, a native of Houston, Texas, joining the cybersecurity clinic at the University of Texas at Austin was more than just a chance to develop new skills—it was a turning point that fueled his confidence and built his interest in pursuing cybersecurity as a career. Jose has been fascinated by computers since the age of three, spending hours exploring and learning the basics of technology. As a student in the School of Information, he was initially uncertain about his career direction, but an info session about the clinic sparked his interest. Motivated by the program's hands-on approach and the ability to have tangible community impact, he joined the inaugural class in 2023.

As part of the clinic, Jose worked on a project supporting a local city government outside of San Antonio, where he helped assess and strengthen the city's cybersecurity protocols to protect against potential threats. Working alongside classmates, Jose analyzed vulnerabilities and provided recommendations to enhance the city's digital systems that support more than 100,000 residents.

Reflecting on his journey, Jose now brings his skills full circle, often helping his mother check her computer for bugs and security issues. From a young child working with computers to a cybersecurity advocate, Jose is determined to make technology safer for all communities—starting at home.

> **For students from lower-income backgrounds like mine, cybersecurity can seem out of reach. But programs like this, supported by a leading tech company like Google, not only open new doors for students but also strengthen entire communities by working with local businesses, nonprofits, and governments. It's a win for students, leaders, and everyone involved.**

Jose Torres,
Student at University of Texas at Austin,
School of Information

CLINIC SPOTLIGHT

WHEN YOUR DATA IS YOUR BUSINESS:

A Student Managed Clinic Securing Nevada's Small Businesses

UNLV

Founded in 2021, the UNLV Cyber Clinic is a unique model that is student-managed and faculty-directed. It works to protect and educate small businesses while building the foundation for tomorrow's cybersecurity professionals.

"The cybersecurity clinic is not just about protecting systems—it's about empowering communities," said Mehdi Abid, the Cyber Program Coordinator at UNLV and a faculty member in UNLV's Cybersecurity BS program. "By partnering with organizations that often lack the resources for robust cybersecurity, we're able to provide meaningful support while giving our students the hands-on experience they need. This work prepares them to make a real impact, whether they're securing small towns or global networks.

To date, the Cyber Clinic has dedicated **10,200+** hours supporting small businesses by providing accessible, high-quality cybersecurity to help organizations safeguard their assets and customer information. In collaboration with the various partners, including the Nevada Small Business Development Center (SBDC), student-teams provide crucial cybersecurity assessments, vulnerability testing, and incident response planning at no cost to small businesses selected.

"These small businesses have one to 20 employees and often lack IT expertise," said Dr. Yoohwan Kim, Professor of Computer Science at the University of Nevada - Las Vegas and Clinic Founder and Director. "Their founders are usually busy with other responsibilities, leaving them vulnerable to cyberattacks."

The UNLV Cyber Clinic is addressing immediate security needs in the greater Las Vegas areas while simultaneously developing tomorrow's workforce into leaders today.

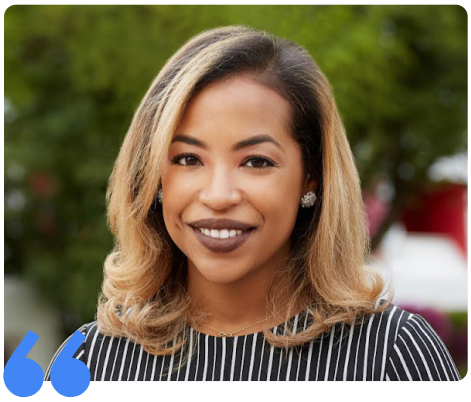
63% of small business owners report having been a victim of a cyber attack.[5]

5 SBA. "Entrepreneurs Need to Stay Aware: Cybersecurity Threats May Directly Impact Bottom Line." Accessed October 30, 2024. https://www.sba.gov/article/2024/10/03/entrepreneurs-need-stay-aware-cybersecurity-threats-may-directly-impact-bottom-line.

EMPOWERING STUDENTS, PROTECTING COMMUNITIES:
How Cybersecurity Clinics Are Making A Difference

As we look to the next decade of innovations in AI, we must stay ahead of new and evolving threats and take advantage of the opportunities it presents. Continued investments in our local communities, our academic institutions and the education of future generations are essential in delivering a reliable, safe and secure infrastructure—and a thriving workforce in every corner of the U.S.

We look forward to the continued impact of the 30 cybersecurity clinics nationwide—and continuing to codify a model that is replicated across institutions. 96% of clinics supported to date aspire to grow and increase their impact in the coming years. Today's leaders and learnings will be tomorrow's innovations.



As we navigate rapidly evolving technologies, staying ahead of emerging threats and harnessing the transformative potential of AI is more critical than ever. By increasing investments in cyber clinics, we can build a more secure digital future for all. Together, we can ensure that every community has the tools and resources to safeguard their communities.

Maab Ibrahim, Knowledge, Skills and Learning Lead for the Americas at Google.org

JOIN US AS WE BUILD FOR THE FUTURE—A FUTURE BUILT FOR OUR COMMUNITIES, IN OUR COMMUNITIES AND WITH OUR COMMUNITIES.

LEARN MORE