bugcrowd

INSIDE THE MIND OF A HACKER

2020

The most extensive study of global hackers and the economics of security research

Contents

Introduction

Security researchers might not share the same history, but they all share a destiny.

Casey Ellis
Founder, Chairman and CTO

We are living in a time of unprecedented change and uncertainty. Despite global economies screeching to a halt, the **$5.2 trillion** economy of cybercrime continues to thrive, with bad actors attacking a new web application every **39 seconds**. The rise of commercial cybercrime has also outpaced traditional security teams, making it harder for them to maintain productivity and reduce risk proactively.

Rivaling these mercenary forces is a new economy of cybersecurity powered by Bugcrowd, which gives organizations flexible access to more security testing and expansive skillsets on-demand. At the heart of this economy are security researchers, also known as ethical hackers, who collaborate around the world in building lucrative, often unsung, careers that serve to protect the biggest brands and most vulnerable people in our society.

These security researchers come from all walks of life and live in countries spanning six of the world's seven continents. They possess varied skills, ranging from conventional techniques to specialist expertise, and act with an abundance of positive intent. While stereotypes might lead you to think of a hacker as a formidable hooded character, real security researchers have more in common with everyday people than you might think.

Diversity happens to be the one thing security researchers have in common. Once thought of as an underground hobby, ethical hacking has since become a mainstream career choice that offers diverse individuals the means of generating a sustainable livelihood from anywhere in the world.

While security researchers might not share the same history, they all share a destiny at Bugcrowd. Together they help organizations face the unknown, unexamined, and unsolved challenges of tomorrow through their differences—not just their similarities.

Humans have sought to overcome contemporary challenges by examining modern problems through the lens of history for centuries. So, it's unsurprising that organizations typically perceive cybersecurity through contexts similar to the Industrial Revolution, with tales of innovation, automation, and commercialization. While similarities exist, the latest research indicates the next era of cybersecurity has more in common with the Renaissance, sharing its characteristics of humanism, exploration, and warfare.

39sec
until the next cyberattack†

Notwithstanding this period of transformation, security researchers remain trusted professionals who strongly value the ethic of their craft and strive to earn the trust of the organizations with which they work. Through crowdsourced security programs, these researchers offer organizations greater depth and breadth in testing by leveraging their collective experience to uncover critical vulnerabilities before bad actors can exploit them. They also help to establish a level of adversarial intuition within internal security teams that automation and tools simply cannot replicate.

▶ **But who exactly are these security researchers, and can organizations trust them? In this report, we take a look inside the minds of 3,493 hackers to find out.**

†According a Clark School **study** at the University of Maryland.

Executive Summary

*Bugcrowd prevented **$8.9B** in cybercrime in 2019 and helped hackers earn **38% more**.*

This report highlights the latest composition of Bugcrowd's vast on-demand cybersecurity workforce. It provides organizations with insight into who they are, the skills they have, what they care about, and much more.

Furthermore, new links between diversity and cybersecurity resilience suggest that engaging security researchers as part of agile release cycles make applications more enduring to evolving risks. Through extensive survey data and unique perspectives on long-standing stereotypes, the report takes organizations into the everyday lives of 3,493 security researchers to get answers for questions they previously had nobody to ask.

Organizations of all sizes, geographic locations, and industries face the financial, reputational, and regulatory consequences of a breach. In 2019, Bugcrowd prevented $8.9B in cybercrime[‡], and security researchers earned 38% more in bounty payments.

Social responsibility has also increased exponentially, with organizations making 5x the number of coordinated disclosures. This growth signals the value security transparency provides to an organization's stakeholders, including the general public, and demonstrates the good intentions with which researchers lead.

While there are a few million-dollar hackers out there (including those who made their fortune on Bugcrowd), these security researchers represent less than 1% of the global community. Most come from large working-class families, and three-quarters speak at least two or three languages. According to the National Average Wage Index, their traditional incomes of less than USD 25,000 per year mean the majority of researchers enjoy an easygoing lifestyle that costs less than half of what is considered a median salary in the United States. However, researchers don't report being disadvantaged, with 47% reporting that their Bugcrowd earnings were exceeding expectations.

This data illustrates that there isn't a one-size-fits-all approach when it comes to benchmarking the varied earning expectations of skilled security researchers.

The report also considers how the economy of cybersecurity leverages sociological experience at scale, and enables anyone to affect global change for economic rewards that are commensurate with the value provided. Although one-fifth of security researchers confessed they only hack for money, it's teamwork and learning opportunities that drive most to the profession. This trade-off is reflected in another statistic: 56% of security researchers said hacking on Bugcrowd helped them get a job. Earlier in the year, one security researcher's creative problem-solving even set a new record of 12 minutes and 54 seconds between a program launching and the submission of a valid P1 "Business Critical" discovery.

When offered additional rewards like more money or increased public recognition, 62% of security researchers still chose self-development as their primary motivation to hack.

Interestingly, this finding has perdured in both quantitative and qualitative studies, highlighting that it is not from the benevolence of security researchers that organizations expect to discover more critical vulnerabilities but from a regard for their self-development. Crowdsourced security programs appeal not just to their humanity but also to their self-interest. Consequently, organizations never talk to security researchers about their needs, but rather their advantages.

Inside the Mind of a Hacker 2020 recognizes that significant opportunites exist for security researchers at the crossroads of diversity and self-development. As a career, it's helping them to realize autonomy, purpose, and mastery through a professional framework that doesn't discriminate against their gender, race, upbringing, or nationality. After all, an organization's next critical vulnerability could be inside the mind of someone who isn't empowered to share their unique technical skillset or instinctive approach to discovery.

Security researchers are extraordinarily ordinary heroes, and organizations stand only to gain from their disparate worlds of thought.

▶ **These are their stories...**

[‡]# of valid P1 findings made on the platform multiplied by the average cost of a breach, according to **IBM** in 2019.

REPORT HIGHLIGHTS

$8.9B
of cybercrime prevented by hackers on the Bugcrowd platform in the last 12 months.

78%
of hackers believe they will outmaneuver AI for the next 10 years.

53%
of hackers are Gen Z or Millennials below the age of 24.

75%
of hackers speak two or three languages.

5x
as many coordinated disclosures made.

12m 54s
Fastest time to valid P1 after program launch.

13%
of hackers experience neurodiversity.

47%
earn more hacking than expected.

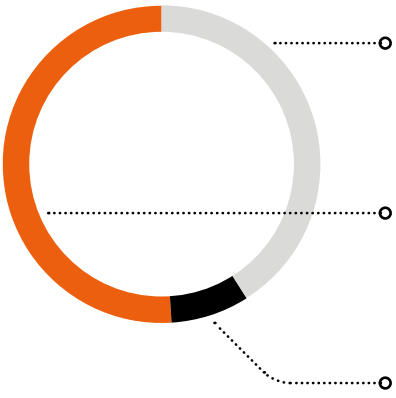
7.7M
platform hacking interactions analyzed.

Methodology

The 2020 edition of **Inside the Mind of a Hacker** analyzes 3,493 survey responses plus ethical hacking activity on the Bugcrowd platform from May 1, 2019, to April 30, 2020, in addition to data from 1,549 successful programs and 7.7 million platform interactions.

Inside the Mind of a Hacker uses a mixed-methods research approach. While the findings might not be indicative of the world's entire hacker population, the report provides a large body of data that organizations can leverage to better understand the impact of crowdsourced cybersecurity and the people behind the work. In this report, the term *security researcher* is used interchangeably with *ethical hacker,* or simply *hacker,* to describe the subject of this study.

3,493 *respondents*



41%

Newcomers

The Newcomers group represents the latest cohort of ethical hackers, with security researchers who signed up to the Bugcrowd platform and completed I.D. verification within the last 12 months.

51%

Regulars

The Regulars group best describes the everyday security researcher on the Bugcrowd platform, with the majority of these ethical hackers having made five or more valid submissions through the platform.

8%

Elite

The Elite group comprises individuals from the top 500 researchers on the Bugcrowd platform, who are continuously measured against the consistent impact of their submissions, demonstrable experience, and verified trustworthiness.

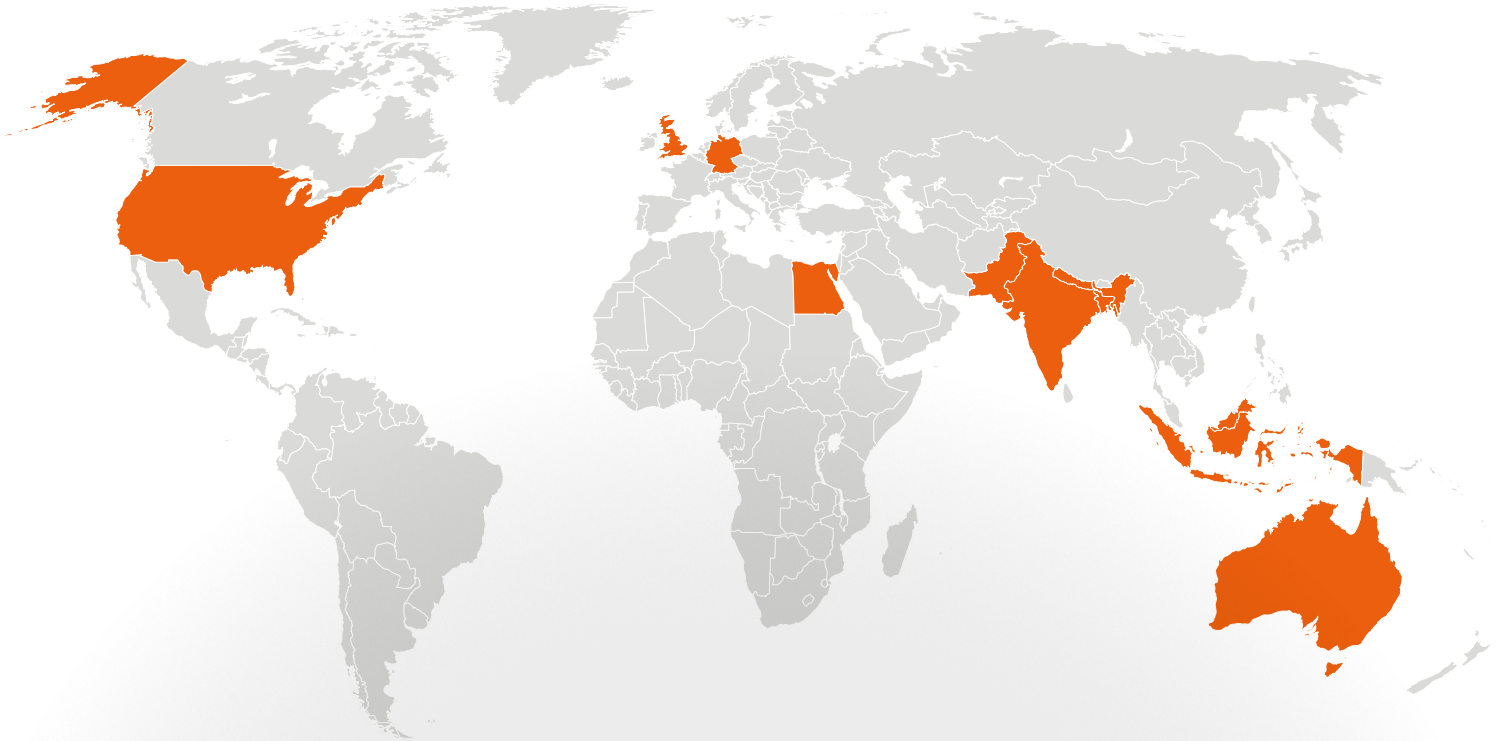
Geographics

*Hackers live on **six** of the world's seven continents and **open new doors** to rich perspectives that accelerate innovation.*

B-roll news footage would have you believe that security researchers work in underground lairs with holographic screens and cinematic lighting. The reality is far less futuristic. Typically, they're familiar neighbors in the global community and live family-oriented lifestyles everywhere from Azerbaijan, to Canada, Morocco, and Sweden. The majority of security researchers who responded reside in India and the United States, while a small group also hold dual U.S. citizenship. They are everyday people who represent the values, attitudes, and lifestyles of more than 100 different countries. Their varied perspectives boost intellectual potential in organizations and help security teams question assumptions faster, enabling them to fix vulnerabilities sooner.

Security researchers work from every corner of the world, bringing together the essential ingredients of innovation, including nonlinear thinking and adaptability. However, acknowledging their international distribution is more than a parade of flags. Research shows that engaging a diverse team translates into better overall financial performance. In a **study** conducted by the Boston Consulting Group, organizations with teams of above-average diversity produced a higher proportion of revenue from innovation (45% of total) than from those with below-average diversity (26%). These findings highlight a significant market-growth opportunity for organizations and demonstrates the considerable impact security researchers can make on their bottom line.

TOP 10 COUNTRIES WHERE RESPONDENTS REPORT LIVING



1. India
2. United States
3. Pakistan
4. Bangladesh
5. Indonesia
6. United Kingdom
7. Egypt
8. Australia
9. Nepal
10. Germany

$8.9B
in cybercrime prevented

2,286 valid P1 submissions x $3.9M, the average cost of a breach in 2019 = $8.9B

Compared to last year's report, Bugcrowd observed an 83% increase in the number of respondents who report living in India. This uptick has caused a thought-provoking shift in the average geographic distribution of security researchers that are examined in the latest edition, with further expansion also seen in Australia and the United Kingdom. While the explosive representation of South Asia is diluting the growing populations of some countries, North America and Europe also continue to see strong year-over-year participation.

For example, in 2019, 27% of respondents said they lived in the United States, yet only 10% reported living there in 2020. Such a significant drop might appear to indicate that the number of security researchers who respond from these countries is shrinking. However, a closer examination of the data shows that the number of respondents from India are merely increasing exponentially faster than other countries that are also experiencing growth. The geographic diversity of the hacker community is a powerful advantage that helped Bugcrowd fortify organizations against $8.9B in cybercrime in the past year.

*Hackers are citizens of the world, but there's no place like **home**.*

⅓
of security researchers have more than one nationality.

14%
of security researchers have the right to a U.S. passport.

Most
dual nationals still live in their country of birth.

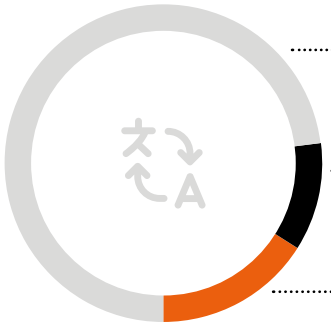
*Hackers speak **multiple** languages and live in sunny urban areas.*

One of the most rewarding aspects of the human experience is the ability to communicate with others, and most security researchers do so effortlessly in at least two languages. Remarkably, the majority are more likely to be fluent in three languages rather than just one.

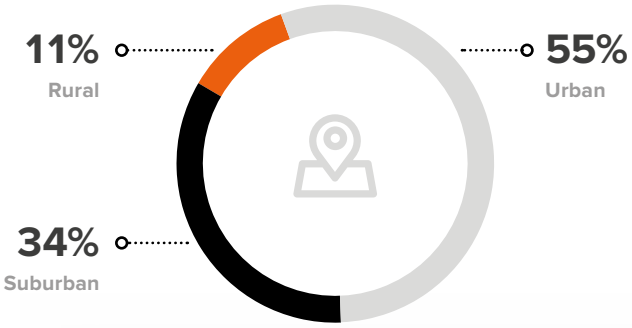
Studies show that speaking more than one language enhances cognitive abilities such as memory, concentration, problem-solving, and critical-thinking skills. Unsurprisingly, these cognitive strengths make multilingual people uniquely suited to work as security researchers because they generally possess superior creativity and logical flexibility.

Data also suggests that decisions made by security researchers in their auxiliary language are more likely to be reason-driven. These findings indicate the adaptive way security researchers can deliberate in a second or third language to minimize emotional biases and make systematic decisions.

NUMBER OF LANGUAGES SPOKEN BY HACKERS



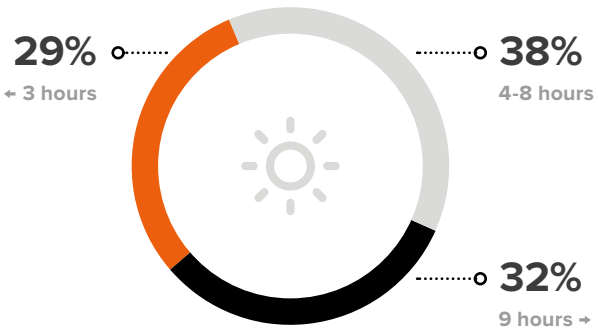
TYPICAL ENVIRONMENTAL CHARACTERISTICS FOR HACKERS



Few divides exist across urban, suburban, and rural areas when it comes to ethical hacking. Most security researchers reside in metropolitan areas, but 11% report living outside of built-up areas in villages, farms, and other isolated dwellings. While developed cities typically provide a more extensive selection of career choices, these findings demonstrate that virtually anyone has the power to earn an income from the cybersecurity economy, regardless of their socioeconomic status.

The majority of security researchers typically enjoy the same amount of sunlight per year as someone living in San Francisco, California. However, 29% observe fewer than three hours per day, which suggests there may be some truth behind the stereotype of hackers working in dimly lit environments.

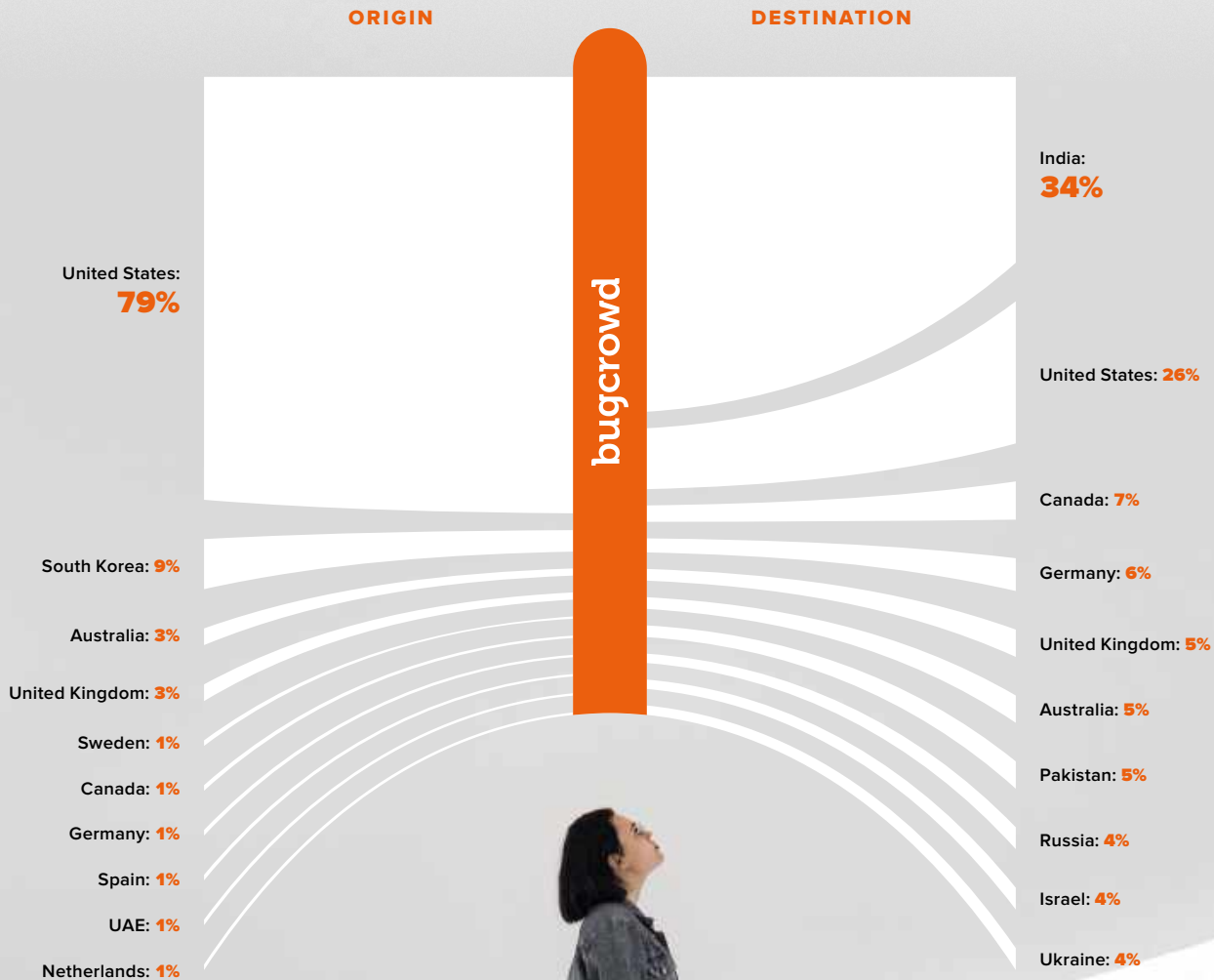
SUNSHINE OBSERVED BY HACKERS AROUND THE WORLD



bugcrowd

GEOGRAPHIC DISTRIBUTION OF CASH FROM HACKING†

Traction among new researchers in emerging markets like India and Bangladesh signal that Bugcrowd's economy of cybersecurity is advancing at a speed relative to the shadow economy of cybercrime. Security researchers live in 109 countries, but most of the cash they earned last year came from organizations in the United States, South Korea, and Australia. In contrast, the majority who collected bounty payments live in India, the United States, and Canada.



†Figure reflects material bounty payments processed on the Bugcrowd platform during the period.

bugcrowd

Hacker Spotlight

Rachel Tobac
Hacker and CEO of SocialProof Security

Rachel is a hacker and the CEO of SocialProof Security, where she helps people and companies keep their data safe by training and pentesting them on social engineering risks. Rachel was also a winner of DEF CON's wild spectator sport, the Social Engineering Capture the Flag contest, three years in a row. Rachel has shared her real-life social engineering stories with NPR, Last Week Tonight with John Oliver, Huffington Post, Business Insider, CNN, USA Today, and many more. In her remaining spare time, Rachel works as the Chair of the Board for the nonprofit Women in Security and Privacy (WISP), where she works to advance women in their fields.

RachelTobac

How would you describe yourself in 100 words or less?

I can do it in one word: curious. But for the sake of the question, let's say: a curious puzzle solver. I want to understand how everything and everyone works. When given a target, I'll keep mapping and branching until I find what I'm looking for, then I'll call to be sure what I found is right.

Tell us about the first–and last–time you hacked something.

Nice try, but I can't disclose details about my clients' pentest work. What I can say is that when hacking, I typically target client-facing team members through email and phone attacks first. They can be anyone in finance, customer support, to hiring managers, recruiters, event planners, office managers, help desk, vendor management, and executive assistants. So, make sure that the client-facing members of your organization are well trained on social engineering threats, and have technical tools to support them when they make mistakes.

Check out **this video** to see how I hacked a CNN reporter, siphoned away his reward points, and contemplated turning off his electricity. Alternatively, you can see how I would attack an election security system via social engineering in this **HBO clip**.

Why do you think learning and creating are more compelling incentives for security researchers?

The security researchers that I know tend to be interested in puzzle-solving, finding that journey to be intellectually challenging and inherently fulfilling. Making money is an essential goal of that challenge, but the problem of hacking is compelling by itself. As an autotelic activity, the learning and creativity involved with the work make it feel worthwhile, even when you're stuck at different moments.

What advice can you give to new researchers on talking about what they do so that others understand the profession better?

It's going to take time to shed the social stigma around hacking, but we're already starting to see the mainstream media portray hackers as "helpers". I hope the increase in positive representation continues to change the old-fashioned sentiments about hacking.

Here's a tip. I always say: "I'm a hacker, not a criminal. As a hacker, I'm hired by people and organizations to use the methods that criminals use to break into their systems so that they can protect themselves before criminals can successfully do what I do. I then test, train, and educate on the exploits I leverage so organizations can fix them before criminals try to use those vulnerabilities."

What can organizations do to better support security researchers going forward?

In terms of security awareness, I hope organizations continue to educate their teams, especially the client-facing employees that I go after first, using the same tactics that criminals use to socially engineer them into handing over their data and money. That first line of defense education, coupled with technical tools to back them up when they inevitably make a human error, is essential to protecting against successful attacks.

Education for security researchers is just as essential! These are the folks who are at the forefront of protecting the tools we all depend upon and use. Without the budget for or access to up-to-date training on the latest methodologies, your security team won't be able to operate to the best of their abilities. Hire the best, then give them access to education to stay the best.

How can the ethical hacking community continue to support women in their cybersecurity careers?

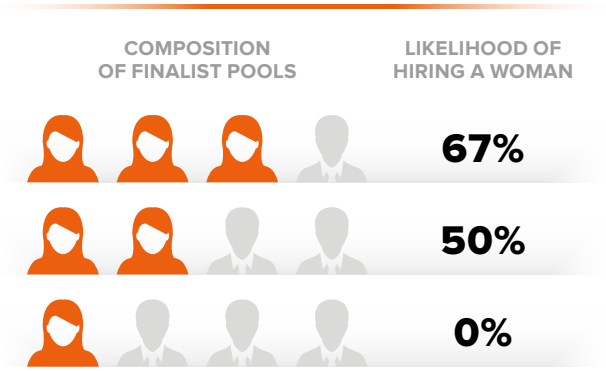
I stumbled upon one of the best tips for hiring underrepresented groups in the Harvard Business Review (HBR). They published a fascinating study in 2016 about hiring pools called the "Two in the Pool" effect. HBR found that if there's only one woman in your final candidate pool, there is statistically no chance she'll be hired.

Some people may look at the chart in the next column and think, "Hmm, those odds make sense. When you have 50% women, you have a 50% chance of picking a woman"; however, we aren't operating under chance-based conditions here! We're talking about merit and experience-based hiring decisions.

If there are four finalists in a candidate pool, and there are three men and one woman, the woman has a 0% chance of being selected due to unconscious bias called in-group favoritism. If there are two women, their chances increase to 50%, and three women brought it to a 67% chance. So, do you want one way to increase your likelihood of bringing an underrepresented person onto your team? Strive to have at least two (hopefully three) underrepresented folks in the finalist pool during the hiring process.

THE RELATIONSHIP BETWEEN FINALIST POOLS AND ACTUAL HIRING DECISIONS

According to one study of 598 finalists for university teaching positions.



Source: Stephanie K. Johnson © HBR.ORG

What impact do you think the coronavirus pandemic will have on the 2020 U.S. presidential election?

The coronavirus pandemic has already disrupted almost every element of life as we know it, and the 2020 U.S. presidential election will undoubtedly face disruption too. We're seeing groups attempting to suggest ballot alternatives that are not recommended by security experts, like blockchain or app-based voting. We also see increased misinformation campaigns across social media, designed to create COVID-19 related chaos. After reading work by Matt Blaze, Maggie McAlpine, and **@commoncause**, I think forcing people to vote in-person during a pandemic is voter suppression (people can't vote if they're sick, immunocompromised, or if it's not safe, etc.).

We have to urge elected officials and lawmakers to adopt emergency measures to protect every Americans' right to vote in the 2020 election. These include: expanding vote-by-mail programs and absentee voting, including mailing absentee ballot applications to all active voters, and for states that require an excuse to vote absentee, issue legislation to allow issues related to COVID-19 to grant the right to vote in absentia.

What words of advice do you have for a future female CISO reading this interview?

The path through leadership in security can be long and challenging. Keep going because you're brilliant and deserve the role. Your representation will demonstrate to others who see themselves in you that it is possible to continue. Remember to bring other underrepresented folks along with you on your journey to leadership. I'm excited to learn from you and your team soon.

Photo • Stephen Hiltner *The New York Times.*

Demographics

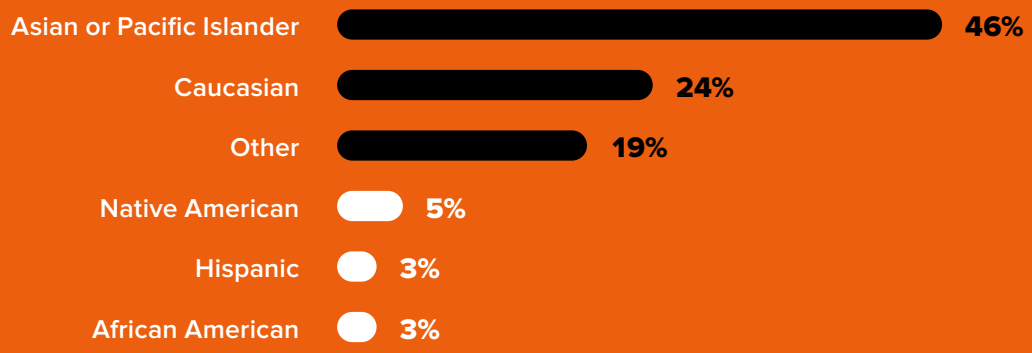
*Hackers are **dynamic**, **young** individuals who come from **all walks** of life.*

Forget about stereotypes of hackers being nefarious masterminds. Bugcrowd security researchers are a vibrant group of Millennials and Gen Z who live family-oriented lifestyles and earn more than they expected. 53% are under the age of 24, and only a quarter of them report having another occupation unrelated to information technology or security.

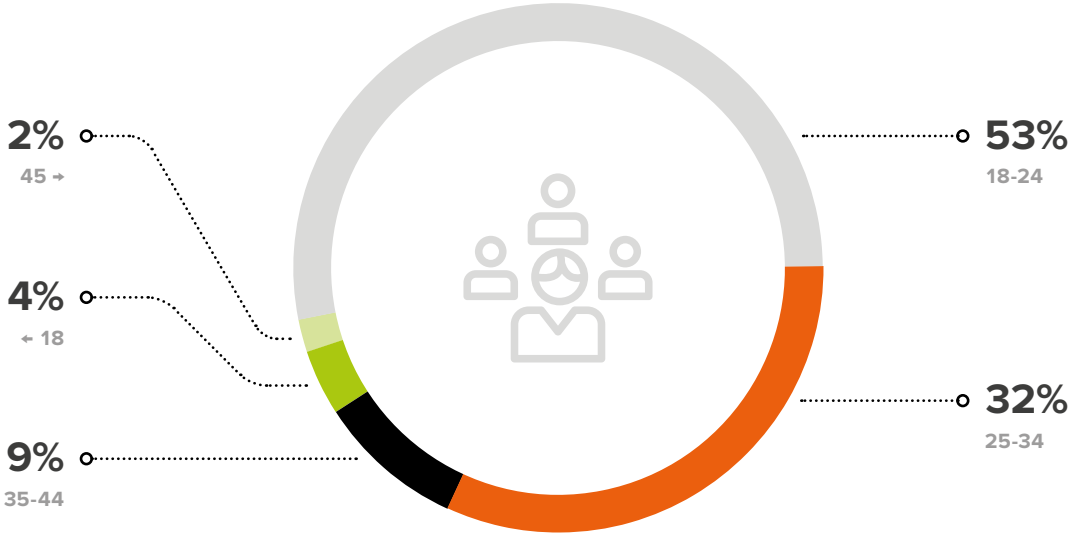
While most security researchers only reached adulthood in the early 21st century, they're helping brands like Mastercard and Atlassian save up to $200,000 in triage hours every year. Five million vacant cybersecurity jobs mean most organizations face a growing skills shortage, and research from **(ISC)²** reveals many are struggling to meet the demands of their evolving threat landscape.

The economy of cybercrime never sleeps, and critical gaps in the workforce offer bad actors more opportunities to commit attacks. Understandably, organizations increasingly trust Bugcrowd to connect them with security researchers who can secure a never-ending list of assets and safeguard their customer experience.

ETHNIC DIVERSITY AMONG HACKERS



AVERAGE AGE OF HACKERS

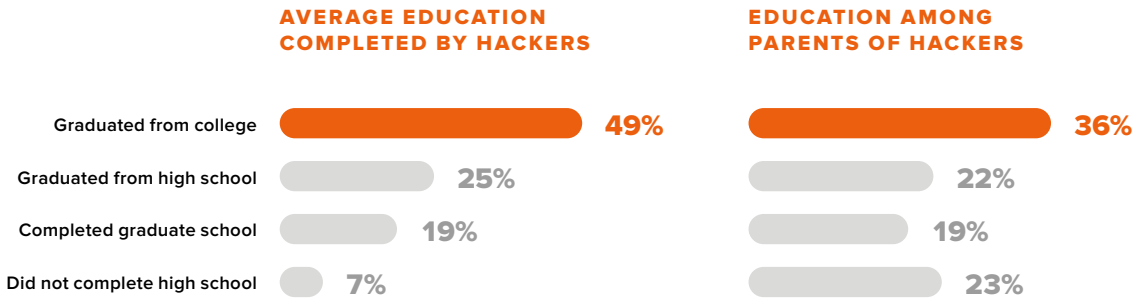


GENDER DIFFERENCES IN HACKERS

94%
MALE

6%
FEMALE

*Hackers are **degree-qualified** and come from scholarly families.*



Security researchers are 3x less likely to drop out of high school than their parents, and 68% have a bachelor's degree. Following in the footsteps of their family, many have also completed graduate programs and possess expert knowledge in at least one professional discipline.

The majority of security researchers' parents graduated from college, with 19% having also completed graduate school. This data suggests most security researchers are degree-qualified because they come from educated families that value the acquisition of worldly knowledge, skills, values, beliefs, and habits.

IMPACT OF INTERNATIONAL EDUCATION STANDARDS

The next generation of security researchers includes hackers living in emerging markets; however, research shows they still possess the same quality of education that organizations have come to expect in developed countries like Australia and the United States.

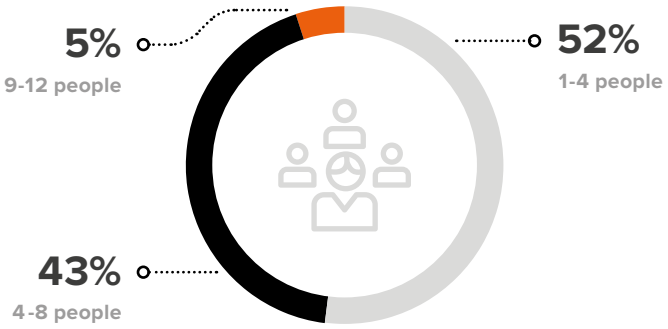
For example, universities in India, like the Indian Institute of Science, are internationally recognized for providing some of the highest standards of engineering education. Research institutes in South Asia are among the world's most reputable for science and mathematics, and advance many of the fundamental disciplines that underpin ethical hacking.

These insights provide meaningful assurance to organizations concerned about the skills of foreign security researchers, highlighting the considerable degree of education most have completed.

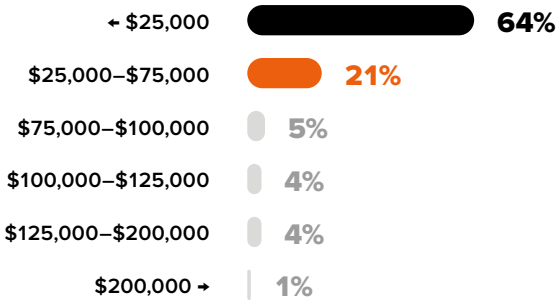
bugcrowd

*Hackers work hard to support their **large households**.*

TYPICAL HOUSEHOLD SIZE OF A HACKER



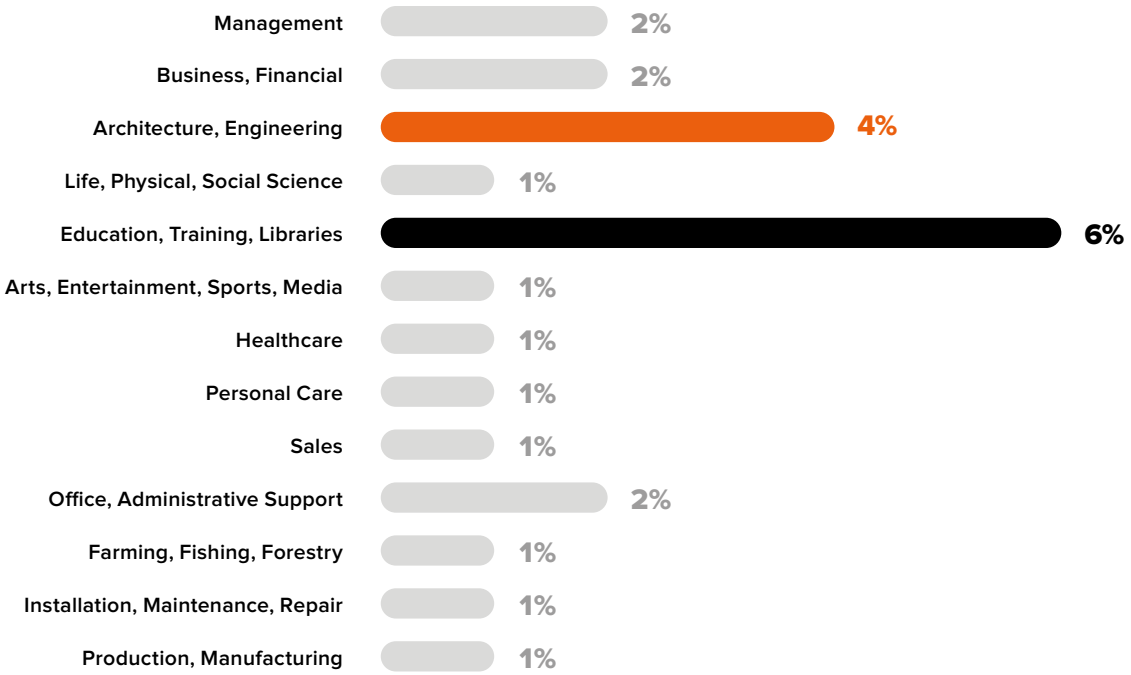
MEDIAN INCOME OF A HACKER



The average American household has steadily decreased in size for the last six decades down to 2.52 people in 2019, according to the U.S. Census Bureau. In contrast, 48% of security researchers report living in households roughly twice that size, with 5% including as many as 12 people. Even increasing the baseline threshold to 4.9 people, the average household size in India, does little to influence considerable data indicating that security researchers come from large working-class families.

In 2020, the majority of security researchers earned more from ethical hacking than they might have otherwise in traditional careers. They typically take home an international equivalent of less than USD 25,000 per year and enjoy varied lifestyles relative to their unique economic climates. According to the Bureau of Labor Statistics, 35% of security researchers earn median incomes higher than their counterparts, while another 9% net staggering six-figure incomes.

OCCUPATIONS HELD BY HACKERS UNRELATED TO IT OR SECURITY



bugcrowd

Psychographics

*Hacker lifestyles are **many** and varied, but all security researchers have **good intentions**.*

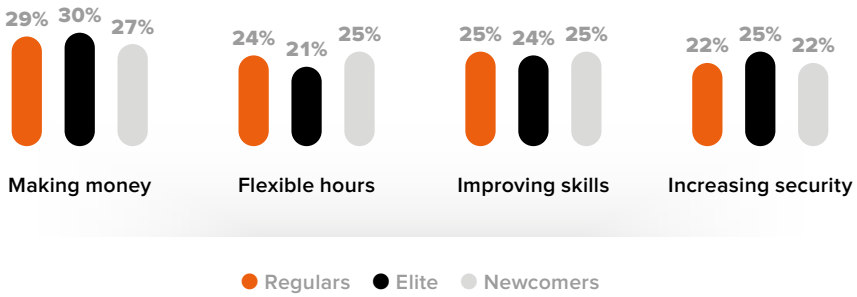
In this section, we further examine the intentions of security researchers by exploring the beliefs and goals that motivate them to hack. Organizations might think of hackers as self-serving people motivated by money; however, 93% of security researchers primarily hack out of care for the well-being of the organizations with which they work. Given few are hacking with intent contrary to this, the data suggests the majority of security researchers are unwavering in judgment and extremely disciplined in their professional conduct.

Data also reveals that 13% of security researchers are neurodiverse and possess varied advantages in non-pathological functions, including learning and concentration. Nearly half live with attention-deficit/hyperactivity disorder (AD/HD), which, according to the experts, helps them thrive in ethical hacking with their unique cognitive strengths in creativity and pattern recognition.

Across all surveyed groups, the #1 consideration observed among security researchers was defending organizations against cybercrime, rather than committing it. 77% of security researchers say web applications are their favorite target to hack, and 17% want to improve their skills in testing server/cloud targets. Unsurprisingly, more than a third of security researchers follow news about cybersecurity and the latest breaches for information that might help them find more vulnerabilities. These insights undermine traditional stereotypes of ethical hackers being corrupt or untrustworthy and paint a clear picture of the professional ethics with which they act.

*Hackers are **empathetic** and have extraordinary **pattern recognition** and **memory** skills.*

MOST IMPORTANT ISSUES FOR HACKERS



Security researchers care about their digital footprint, and the majority said maintaining personal privacy (29%) is critical when hacking. Unsurprisingly, security researchers also appreciate getting quick responses from program owners (25%) and receiving constructive feedback on their submissions (23%). These results reinforce their growth mindsets and underline the quality of privacy that Bugcrowd offers them when hacking on Crowdcontrol™.

NEUROLOGICAL DIFFERENCES AMONG HACKERS

13%
NEURODIVERSITY

Neurodiversity 101

The term *neurodiversity* refers to variations in the human brain regarding sociability, learning, attention, mood, and other non-pathological mental functions.

When people think about diversity, things like race and gender typically come to mind, but another quality also diversifies ethical hackers: neurodiversity. The attribute is worth considering given that 13% of security researchers report experiencing distinct neurodevelopmental conditions that include dyspraxia, dyslexia, attention-deficit/hyperactivity disorder (AD/HD), dyscalculia, autistic spectrum, and tourette syndrome. According to Dr. Devon MacEachron, a psychologist specializing in twice-exceptional and gifted learners, neurodiversity is a genetic property related to the evolution of humans as a species. Consequently, these differences are not flaws, but instead natural variations in the human genome that can provide unique advantages in contexts like hacking.

Nearly half of neurodiverse security researchers live with AD/HD (6%). Experts say individuals with this condition thrive in environments of rapid change and variety that reward creativity and out-of-the-box thinking. These qualities underpin ethical hacking, making them highly suited to work as a security researcher.

Unsurprisingly, security researchers with AD/HD often possess different neurological strengths that enable them to provide exceptional depth and dimension in testing. These superior abilities have links to DRD4, an associated novelty-seeking gene that arrived on the human evolutionary scene more than 10,000 years ago. The long-standing prevalence of genetic variants like AD/HD suggests they remain in the gene pool because they are advantageous mechanisms.

Leading authorities on the subject believe neurodiverse attributes were positively selected during human evolution for contributing exceptional memory skills, heightened perception, a precise eye for detail, and an enhanced understanding of systems. As both a profession and subculture, ethical hacking allows the cognitive strengths of neurodiverse security researchers to shine without prejudice as to the challenges they face. While anomalies in neurodevelopment might otherwise limit their professional or social prosperity, Bugcrowd proudly recognizes and accommodates the tremendous value these researchers can offer to organizations' security programs.

Hacker Spotlight

Anna Westelius
Sr. Manager for Security Products at Cruise Automation

Anna Westelius is the Senior Manager for Security Products at Cruise Automation, where her team works on solving the complex problems their engineers face by providing security tooling, systems, and solutions. Previously, Anna has experience in both security research, and leading engineering organizations to build defensive and offensive security-centric technologies.

bubblewire

Tell us about the first time you hacked something.

First? Hard to say and even harder to remember. There may or may not have been an incident involving bypassing the BIOS passwords and modifying the default boot image in my early school days to avoid certain restrictions. Still, I can neither confirm or deny that.

Tell us who your top 3 female role models are in infosec and why?

Anne-Marie Eklund Löwinder (**@amelsec**). Swedish internet pioneer and CISO of the Swedish Internet Foundation, a local hero in my book.

Amanda Rousseau (**@malwareunicorn**). Amanda, and her reversing skills need no introduction; I have always admired her ability to explain complex security concepts, which she reflects in all of her training and workshop content.

Marion Marschalek (**@pinkflawd**) has done and presented tons of incredible research. I have always been very impressed with her work and will go out of my way to see her present.

What do you think will motivate more female security researchers to join Bugcrowd, and how can the ethical hacking community continue to support women in their cybersecurity careers?

Representation. On the global conference stage, in the media, and at the top of large companies. We, as a community, can support women and other minorities by continuing to highlight great work and provide safe spaces for everyone.

What do you think the modern woman represents in security research today, and what opportunity is in store for her over the next 12 months?

Change to the corporate security environment. Hacking, as a community, has, to me, always represented openness to the odd, unusual, and unconventional. Meanwhile, the corporate security industry has (historically) consisted of a very homogenous group, a "boy's club," you could say. As the lines between these environments blur, and we see more security researchers working in organizations, we'll see a shift in the perception of the appearance of hackers. As women, who have previously struggled to be part of this environment, we have an opportunity to further push for and uplift otherwise underrepresented people.

Tell us about your experience speaking multiple languages, and how this diverse attribute helped facilitate more impact in your career

→ Anna speaks Swedish, Danish, English, and Japanese

I have always attributed a lot of my "computer skills" to multilingualism. Learning new languages felt the same as learning a new syntax; at least for me, it's the same thought process. However, I'd also argue that the statistic could be a representation of how global the security research community is. As a non-native English speaker, you have to learn at least two languages to do the work.

What tips do you have for early-career security researchers?

I recommend looking for security-adjacent jobs, like IT, support, network/system/security analysis, or administration. These jobs not only pay the bills, but they also teach great fundamentals and understanding of the systems you'd want to research later on. In general, I suggest learning networks and system fundamentals. Knowledge about TCP/IP will get you a long way!

What application and interview advice do you have for other job seekers, especially women or those from minority groups?

Not everyone has the time or option to build a vast portfolio of cool research, but we interviewers do love some additional content to take a look at before proceeding with an interview.

If you participate in projects or events, make sure you highlight them in the application. If you've built a lab at home, talk about it. Do you participate in bug bounty programs? We'd love to know more. Anything that helps highlight that you'll be able to do the things asked of you on the job—especially if you don't have a lot of experience. You should be sure to do the following as well:

- Research and attempt to understand the job you are applying for and relate your application and adjust your content accordingly.
- Be humble. It's okay not to know everything, particularly when you're new.

Experience

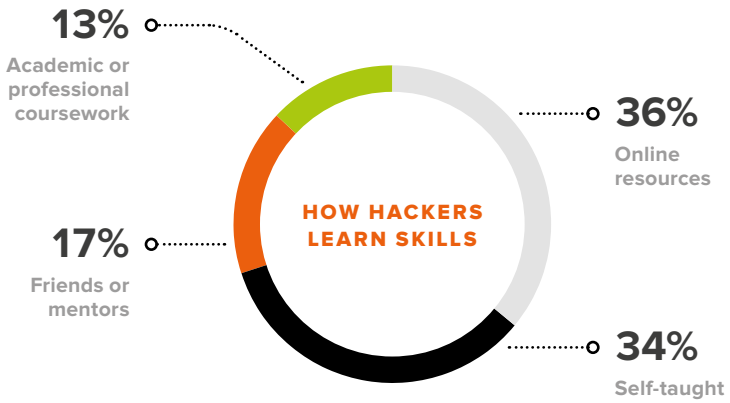
*Hackers **teach themselves** skills online that translate into **real-world** jobs.*

It's not uncommon for organizations to express concern about the potential for external security researchers to be incompatible with their technology stack, application, or use case. Fortunately, the CrowdMatch™ sourcing engine analyzes historical program insights within Crowdcontrol™ to ensure organizations rapidly connect with researchers that have the specific skills, reliability, and experience they need.

Remarkably, most security researchers taught themselves how to hack using online resources, but 13% also report having completed academic or professional coursework related to cybersecurity in the last 12 months. They describe their strongest hacking skills as web application testing (70%), network pentesting (7%), and recon/asset discovery (6%).

True to the entrepreneurial nature of their demographic cohorts, more than half of security researchers say Bugcrowd helped them land a professional job in the real world.

Another 18% indicated they are already hacking full-time, which may explain why they typically do most of their testing in the evening. The majority say they dedicate up to 14 hours every week to the platform, while 60% of Elite hackers confess they mostly work on Bugcrowd. Platform activity also increases Thursday through to a Saturday peak (19% of total), suggesting security researchers prefer to hack outside traditional working hours and in their free time.



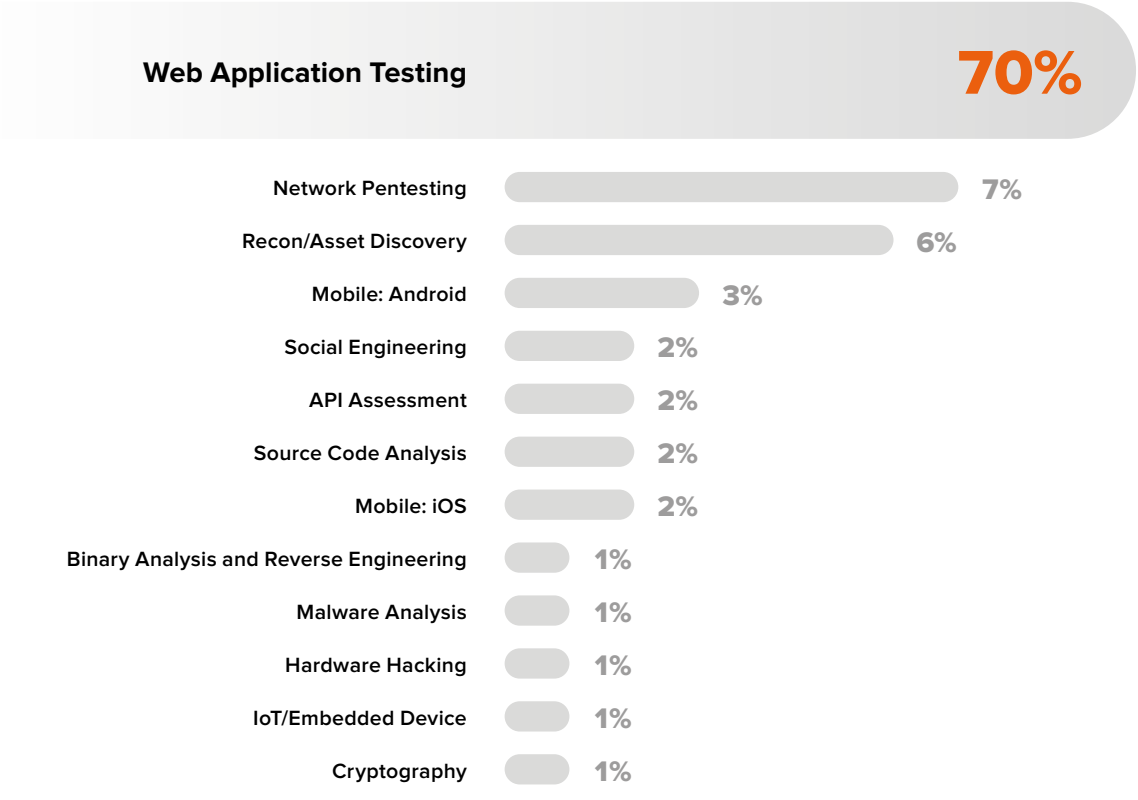
Most security researchers learned how to hack using online resources, while 36% report being entirely self-taught. Only 13% completed academic or professional coursework related to cybersecurity, highlighting their preference for online resources and community support.

Bugcrowd University is one such resource that helps security researchers learn the basics of hacking or uplevel their hacking skills with videos, tutorials, and community-driven best practices. Remarkably, videos in Bugcrowd University have been viewed by security researchers more than a million times, underscoring their voracious appetite for education and learning.

HACKERS' STRONGEST SKILLS

According to a report from **Avast**, the attack surface is growing faster than it has at any other time; however, despite web applications being at an increased risk, organizations still find themselves needing to secure more than 400 of them. Fortunately, 70% of security researchers are highly skilled in web application testing and unburden internal teams so that they can remediate risk earlier in the development lifecycle. While less prevalent overall, other hacking skills, like network pentesting (7%) and recon/asset discovery (6%), are also increasing among security researchers.

In a recession of expertise, cybersecurity has become a high-interest debt that's becoming impossible for organizations to pay down. Bugcrowd bridges the gap between security testing that must be done, and the shortage of human expertise needed to do it, by plugging today's organizations into the cybersecurity economy of tomorrow. As a result, 56% of security researchers report securing further professional employment thanks to the skills and experience they acquired while hacking on Bugcrowd.

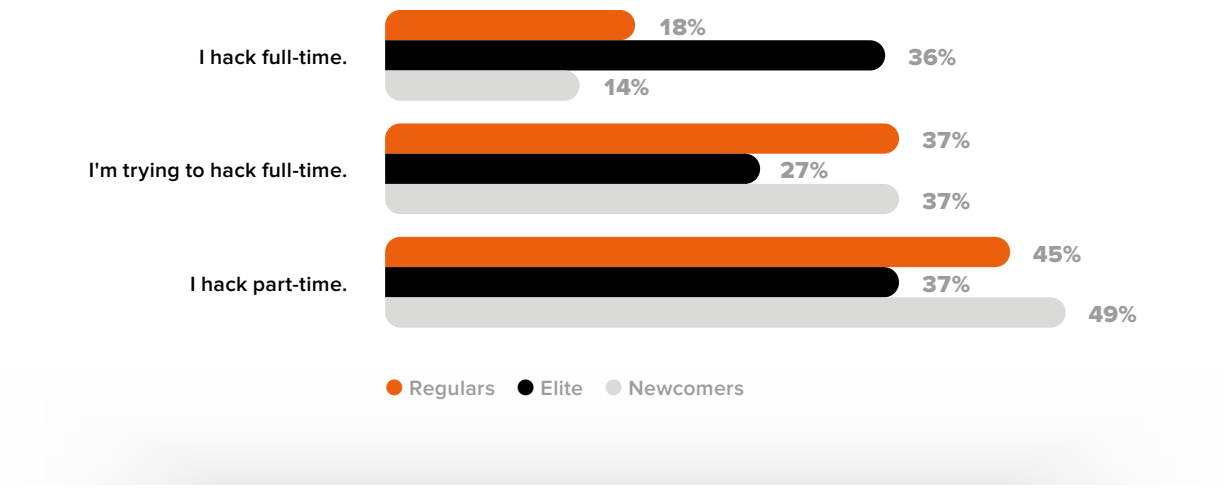


bugcrowd

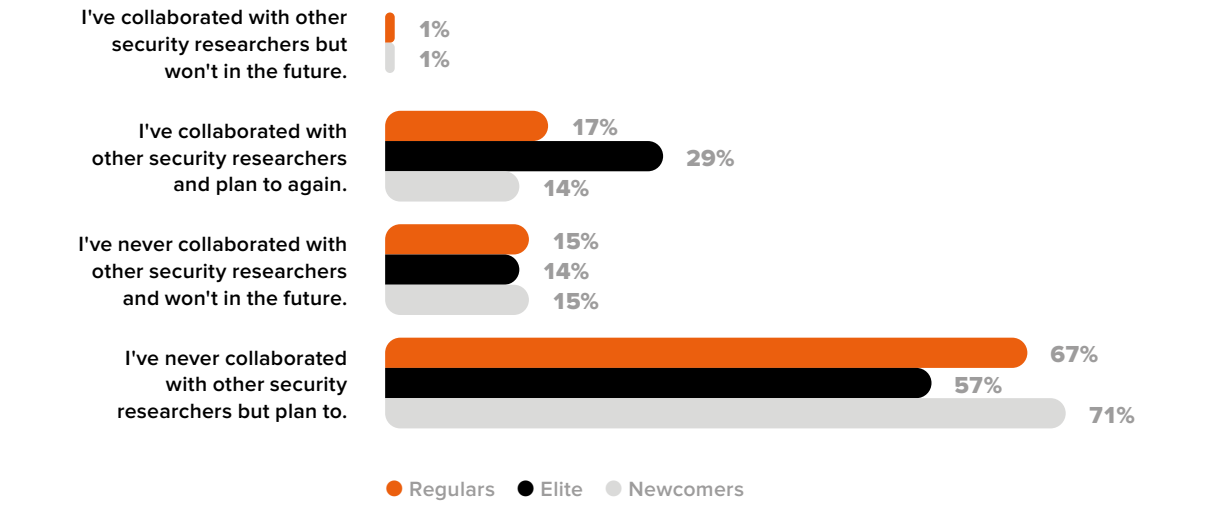
*Hackers are going **full-time** and love to collaborate.*

The Elite group hack full-time the most, with 36% reporting it as their primary occupation, while Regulars and Newcomers similarly hope to turn their part-time hacking work into a professional career. As leaders of the ethical hacking community, it also comes as no surprise that the Elite group has a long history of collaboration that data shows they plan to continue. In the same vein, 68% of all security researchers said they plan on collaborating with other hackers to test targets on Bugcrowd in the future.

EMPLOYMENT STATUS OF HACKERS



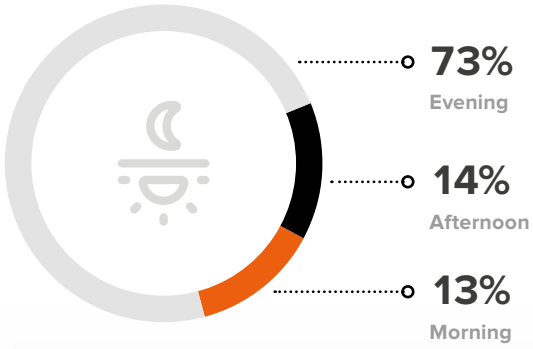
COLLABORATION AMONG HACKERS



bugcrowd

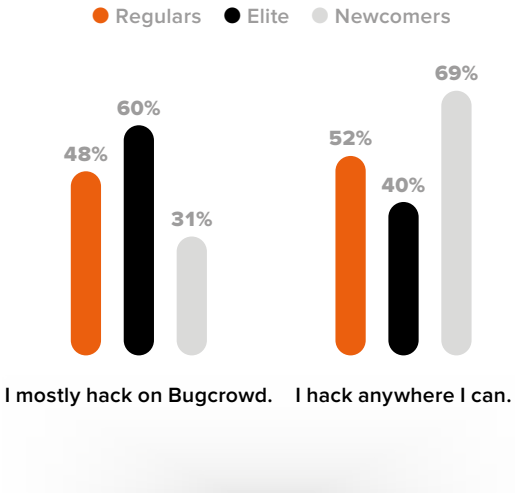
Hackers do the majority of their work at night, and the best do it ***mostly on Bugcrowd****.*

TIME SPENT HACKING BY TIME OF DAY



19%↑
more hacking on Saturdays

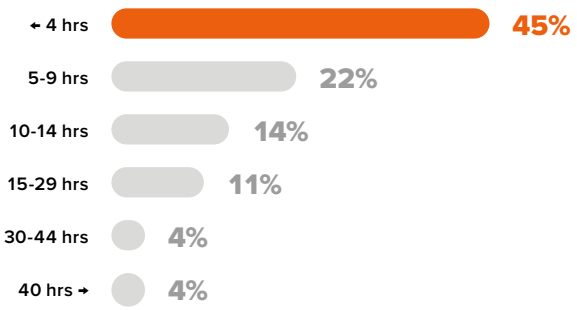
WHAT THEY HACK ON



Data shows that 42% of all security researchers choose to hack on Bugcrowd, but closer examination of the groups that make up the wider population offers additional insight. For example, nearly half of Regulars and 60% of the Elite group prefer Bugcrowd compared to other hacking outlets. Interestingly, this data indicates a trend that as Newcomers mature on the platform, they also grow less interested in hacking elsewhere. These findings provide a rare glimpse into the mind of security researchers who, despite having no shortage of opportunities, increasingly devote the time they spend hacking to programs on Bugcrowd.

The majority of security researchers spend a part-time equivalent hacking, with 81% committing up to 14 hours per week to the platform. While some reported working close to full-time hours (8%), historical submission data indicates that security researchers can work fewer hours while still earning an income similar to their salaried peers. Even when done on the side, ethical hacking often provides a level of professional flexibility that allows them to spend more time doing things they enjoy without forgoing new opportunities to advance their careers.

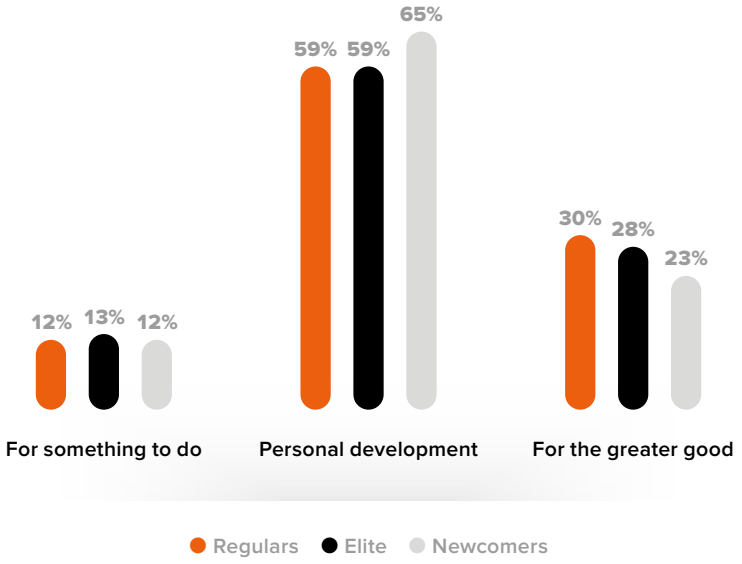
HOURS DEVOTED TO HACKING PER WEEK ON BUGCROWD



bugcrowd

*Hackers have similar **growth mindsets**, but hunt differently.*

WHY DO THEY HACK ON BUGCROWD



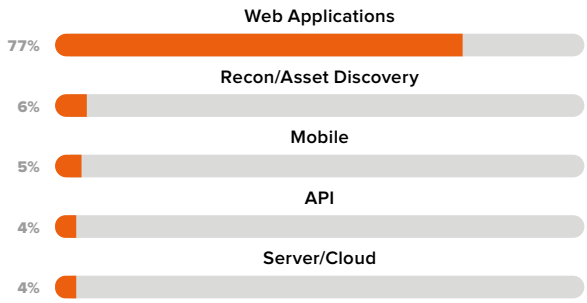
Across all surveyed groups, 61% of security researchers say they hack for reasons of personal development, like realizing new talents, facilitating employability, and enhancing their quality of life. In contrast, 27% say they do it mostly for the greater good. These statistics acknowledge the authentic interest security researchers have in defending the organizations with which they work and show the profession is helping most of them realize their aspirations.

17%
of hackers want to improve their skill at testing server/cloud targets.

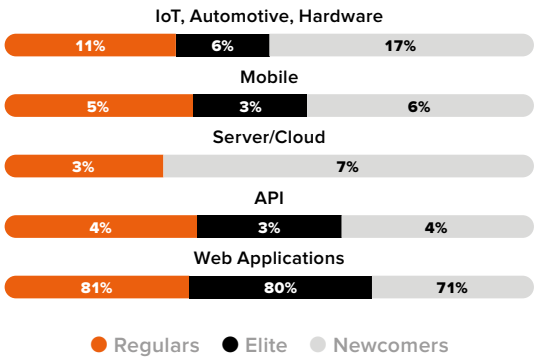
16%
of hackers want more experience testing mobile targets.

11%
of hackers want opportunities to test automotive and vehicle targets.

TARGETS THAT HACKERS ENJOY WORKING ON THE MOST



FAVOURITE TARGETS ACROSS DIFFERENT GROUPS OF HACKERS

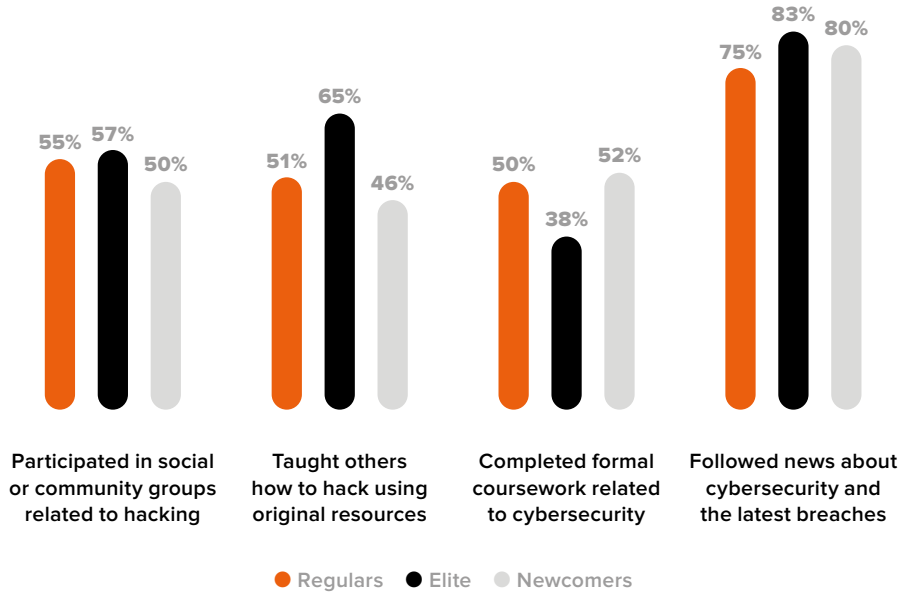


Organizations increasingly task their security teams to oversee hundreds of web applications. While many are unprotected, some assets also remain unknown to their relevant stakeholders. Fortunately, 77% of security researchers say that web applications are their favorite targets to hack, while another 6% describe recon/asset discovery as a top pursuit. Mobile (5%) hacking maintains a marginal lead over server/cloud (4%) and API (4%), with the remaining population distributing evenly.

bugcrowd

*Hackers follow the latest breaches to find more **unknown assets**.*

WHAT HACKERS WERE UP TO IN THE LAST 12 MONTHS

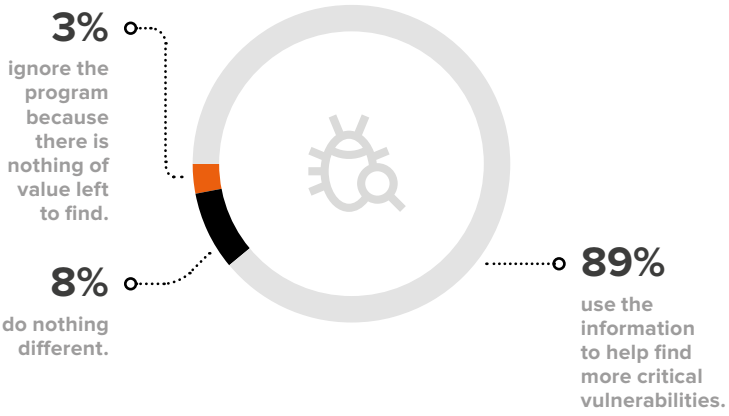


News about cybersecurity and the latest breaches can be a rich source of intelligence in ethical hacking. Naturally, 34% of all security researchers follow mainstream publications, hoping to find tips that may lead them to more high-impact discoveries. Besides completing the least amount of academic or professional study, the Elite were most active in the ethical hacking community outside of Bugcrowd. In the last 12 months, 57% of the Elite participated in online or in-person social groups related to hacking. This insight goes hand-in-hand with the 65% that also taught another person how to hack with original materials.

In the last 12 months, Crowdcontrol™ facilitated 5x more coordinated disclosure than it did in any other year. Managed by the platform, coordinated disclosure enables program owners and researchers to agree upon a date, and the scope of the information they will reveal, before publicly disclosing a vulnerability or exploit. The exponential growth of these disclosures highlights the value of transparency to stakeholders and demonstrates that organizations are taking social responsibility more seriously than ever.

When organizations publicly disclose a vulnerability identified through Bugcrowd, 89% of security researchers use the details released to help find more critical issues in the same or similar programs, whereas, 3% feel such transparency indicates less value for them to find and pursue other programs as a result.

WHAT HACKERS DO WHEN ORGANIZATIONS DISCLOSE VULNERABILITIES FOUND ON BUGCROWD



78%
of hackers say AI-powered cybersecurity alone isn't enough to outmaneuver cyber attacks over the next decade.

93%
of hackers care about the well-being of end-users and the organizations with which they work.

87%
of hackers agree that vulnerability scanners can't find as many critical or unknown assets as they can.

bugcrowd

Defending Defenders

Michael Skelton
aka codingo

Global Head of Security Ops & Researcher Enablement

Michael went from being a Top-50 security researcher on the platform to leading the international triage team at Bugcrowd. In his free time, he writes and maintains several open-source tools like Reconnoitre, NoSQLMap, VHostScan, and Interlace.

codingo_

Bugcrowd has witnessed government agencies become practical and optical leaders in cybersecurity over the last few years. Since 2014, our world-class security researchers have provided advisory for the creation of programs, including the FDA post-market cybersecurity guidance around vulnerability disclosure, the DHS Binding Operational Directive on government-wide adoption of VDP, the UK NCSC's vulnerability disclosure and Bug Bounty programs, and efforts from the EAC and Capitol Hill around the role of ethical hacking in the 2020 elections. It's also one of the reasons that Paladin Capital invested in Bugcrowd during its seed round.

When the U.S. Department of Defense launched Hack the Pentagon in 2016, it was a watershed moment for the perception of contemporary hackers and the crowdsourced security category that Bugcrowd pioneered. After all, hackers must be both helpful and trustworthy if one of the most prominent military organizations on the planet was deciding to enlist their help. Their public support for crowdsourced security also influenced other organizations in just about every industry to adopt the model.

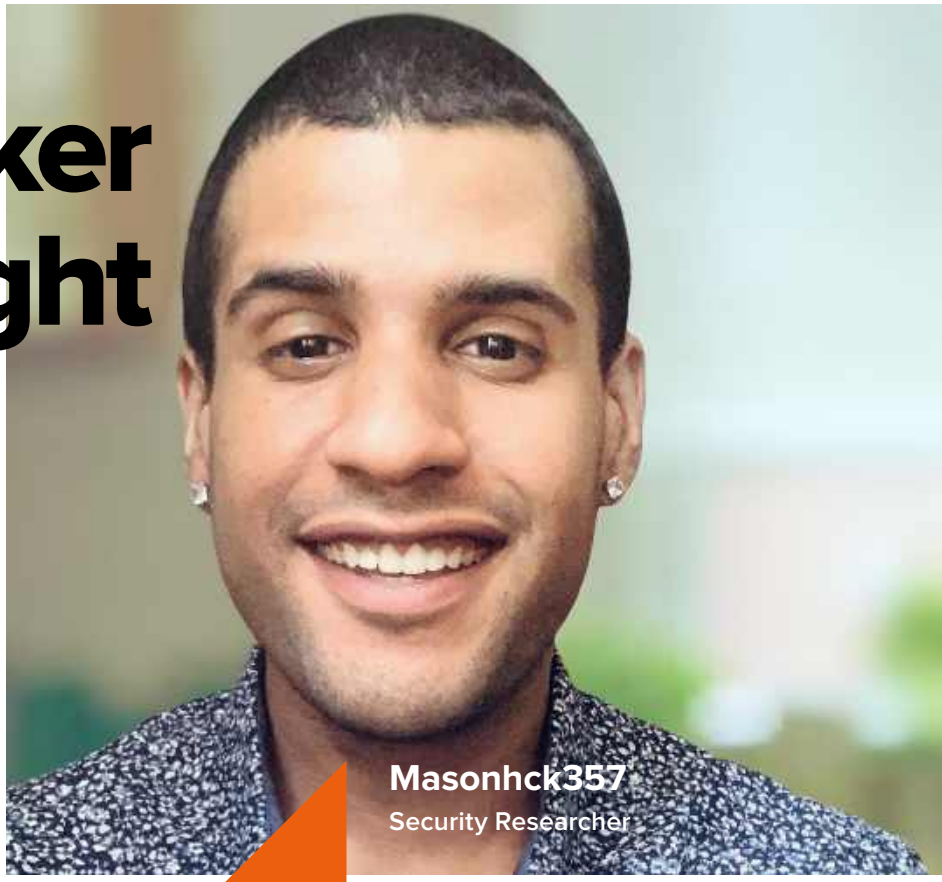
At the same time, Bugcrowd initiated the Open Source Vulnerability Disclosure Framework (OSVDF), which was later subsumed into the **disclose.io** project. It has since evolved into a viral movement driving simple, safe, and standardized vulnerability disclosure. The grassroots initiative is also working to reform anti-hacking laws to accommodate the role of "digital locksmiths" for the future health of the Internet. Today, disclose.io covers four jurisdictions, it's language has been used in countless briefs around the world, and the disclosure Safe Harbor logo is becoming recognized as a "green padlock" representing Neighbourhood Watch for the Internet.

While the term *hacker* still conjures up a familiar mental montage of hooded characters for some, the reality is that top government agencies trust Bugcrowd security researchers. These hackers aren't working below a waterfall of green matrix code; they're providing expert skills and intelligence on some of the most sensitive cybersecurity testing scenarios in the world.

GOVERNMENT BODIES TRUST BUGCROWD HACKERS

bugcrowd

Hacker Spotlight



Masonhck357 is an active security researcher on the Bugcrowd platform. He describes himself as a "pretty dope human," with a survivalist mentality that doesn't shy away from hard work. In his personal and professional life, he likes to be innovative and think outside of the box. He loves hacking, music, gaming, animals, and never giving up!

Masonhck357

Tell us about the first–and last–time you hacked something.

I first hacked Tesla after watching a video by Jason Haddix. Needless to say that within five minutes, I got my I.P. banned and had to move on (lol).

The last time I hacked was just a few moments ago! I was parsing through Javascript files in hopes of finding an XSS that will allow me to pull access tokens out of LocalStorage.

Who are your top role models in ethical hacking, and why?

- Jason Haddix **@Jhaddix**: He's the one that started it all for me. I religiously watched the Bug Bounty Hunter Methodology series when it first began–I appreciated his solid understanding of the basics when learning!
- James Kettle **@albinowax**: I had the opportunity to watch his HTTP request smuggling presentation live at DEF CON, and he blew my mind. His research is incredible, thorough, and inspiring. Although at the time, I had no idea what he was talking about, I grew to enjoy his thought process in approaching novel ideas.

Why do you think learning and creativity are more compelling incentives for security researchers?

Let me answer that question with a question. Once you have more money than you need (which is possible in ethical hacking), what will motivate you to continue hunting? For me, every new program provides a new creative way to hack. The chance to replicate the work you did the day before is slim. With continued drive and a commitment to learning, the sky's the limit!

Recently, I completed a JavaScript course, which has completely changed my thought process when hunting. It has also helped solidify my understanding of XSS and exploiting the vulnerability. Learning JavaScript has also pushed me to become more familiar with how the DOM works, as well as shifted my testing environment to Chrome Dev Tools.

Research shows that 73% of security researchers speak two or three languages; what languages do you speak?

I speak English and Spanish. Unfortunately, I haven't yet had the opportunity to use Spanish in my work as a security researcher–but maybe I will soon!

How is the coronavirus pandemic affecting your life as a security researcher?

Other than a few programs pausing and slower responses, it hasn't affected me all that much. Bugcrowd has done an excellent job handling the changes that have occurred over the last few months. I want to give a big shout out to the triage team for doing a great job during this time–you're fantastic!

How has diversity impacted the work you do as a security researcher?

People from different backgrounds have varied ways of speaking, distinct habits, and unique methods of doing things. I believe these individual differences make us stronger as a team. For example, I know that my experience in the military (retail analyst, I.T.) had a big part in helping me get to where I am in a short amount of time.

Do you have any concerns about the 2020 U.S. Presidential election about privacy and cybersecurity?

I just read this morning that the State of Georgia recently spent $107 million dollars on voting machines with (redundant) Windows 7 installed. So yes! Unfortunately, our politicians are extremely out of touch when it comes to privacy and cybersecurity.

What words of advice do you have for a future hacker reading this interview?

Prioritize learning over hacking, and don't give up!

Is there a memorable program you participated in on Bugcrowd that you'd like to share?

I can't. It's private...just kidding!

Once, I joined a 3-year-old private program that had double bounty activated. In 2 months, I was able to perform unique account takeovers in 3 different portals. I saw four RXSS, chained with CSRF, that turned one of their forms into a Phishing Campaign. I would say this program was what got the ball rolling for me.

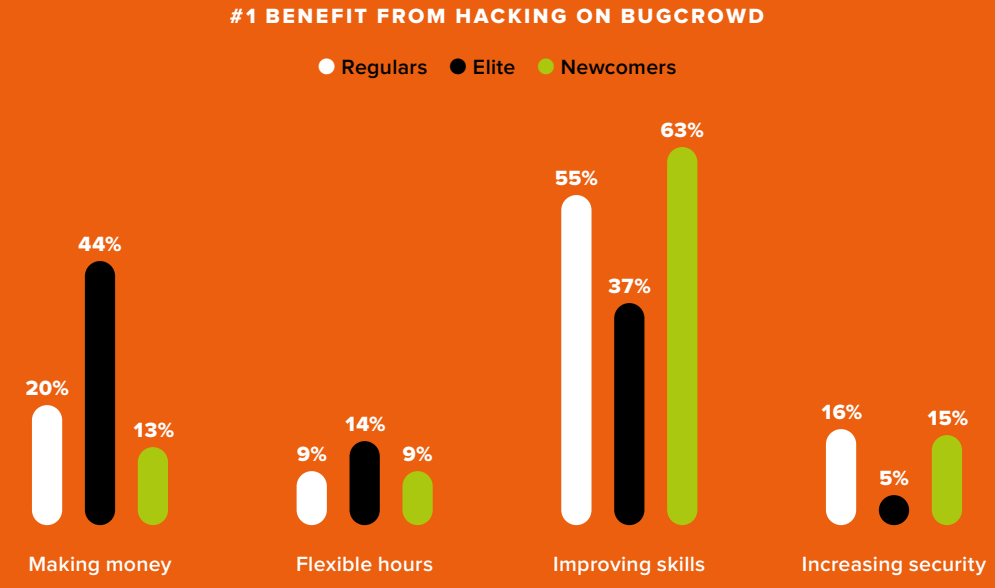
Motivations

*Hackers earn U.S. dollars, but transact in the currency of **self-development**.*

Teamwork and learning opportunities drive most to ethical hacking, although one-fifth say they're primarily motivated by monetary rewards. Even when tempted with more cash and extra recognition, 62% still selected personal development as their primary incentive to hack. These findings indicate security researchers generally value their long-term professional skills above short-term financial gain.

In the economy of cybersecurity, anyone has the power to affect global change in exchange for rewards. The majority of security researchers describe their earnings as good or better than expected, while half have full-time earning expectations that are less than what is considered a median salary in the United States. Another 56% say hacking on Bugcrowd even helped them get a job in the real world.

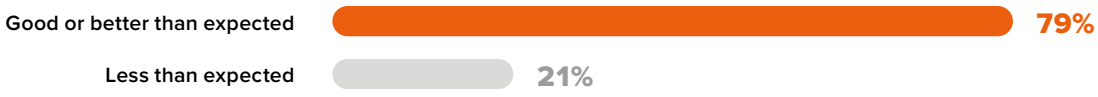
57% of all security researchers reported improved technical skills as the primary benefit they received from Bugcrowd. More security researchers also prioritized their role in increasing the security of information over the perk of working flexible hours. Unsurprisingly, the Elite group tended to focus more on their bottom line, with 44% saying money is their main benefit.



bugcrowd

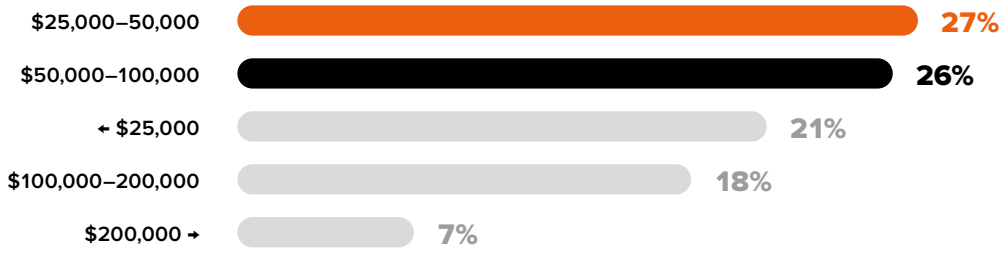
HACKERS EARN MORE THAN EXPECTED AND WORK FULL-TIME FOR LESS THAN YOU MIGHT THINK

PERCEPTIONS OF EARNINGS FROM HACKING



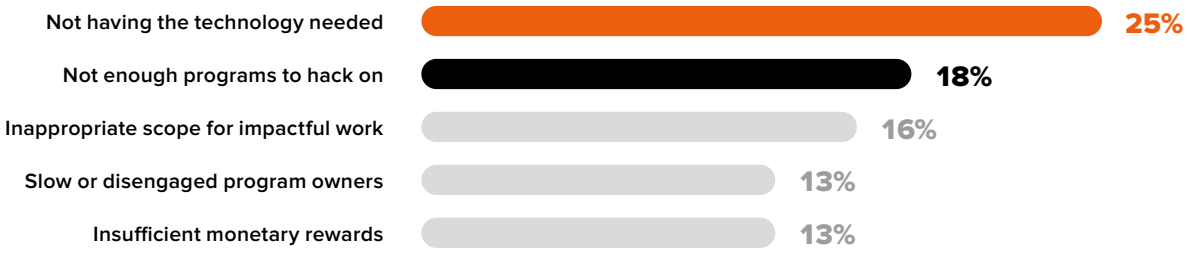
79% of security researchers say earnings from Bugcrowd were good or better than expected, highlighting the competitive market bounty rates they have come to expect on the platform. Crowdcontrol™ maintains unrivaled ROI from its bounty payments by layering data from across the ecosystem to build incentivization frameworks, optimizing the quality and price of submissions that organizations receive.

EARNING EXPECTATIONS AMONG HACKERS GOING FULL-TIME



A quarter of security researchers have ambitious six-figure earning expectations that are comparable to their professional counterparts working as application security engineers in the United States. However, nearly half of casual hackers say they would go full-time for earnings of less than $50,000. By dynamically managing the varied earning expectations of international security researchers in different economic climates, Bugcrowd can variabilize security spend that organizations might otherwise have considered a fixed cost.

TOP BARRIERS TO HACKER SUCCESS



bugcrowd

Expert Opinion

Dr. Sylvie Studente

Creativity Expert

Dr. Studente is a Senior Lecturer in Information Systems for the Faculty of Business & Management at Regent's University London. She is a published expert on creativity and has an extensive background in human-computer interaction.

Why do you think organizations should consider creativity when conducting security research?

Scholars have acknowledged "cybersecurity creativity" in attempting to address the threat of cybercrime, with many pointing to proactive and creative solutions as the optimal response to growing attacks. Recent literature within the area also suggests using attack simulation and other interactive types of learning that engage targets in "real-world" scenarios.

Given the research in support of these approaches, organizations would be remiss not to explore the value creativity offers to problem-solving in security programs.

What impact, if any, does diversity have on creativity?

On an implicit level, humans approach creative endeavors as influenced by concepts of the culture in which they find themselves immersed. However, in the context of cybersecurity, I feel that organizations can better understand the individual differences of [ethical hackers] through the context of learning.

As reported in the research I've undertaken, we can consider creativity as a subset of learning. In that way, individual and cultural differences associated with creativity may play a crucial role in the problem-solving involved in security testing.

Can you tell our readers about the relationship, if any, between learning and creativity?

Contemporary research discusses creativity as inherent to the learning process. A widely accepted view on creativity is that creative potential is possessed by all, and differs between individuals based on psychological and environmental factors. Creativity commences with inspiration, the joining together of concepts in novel ways, and the production of an output.

Similarly, the process of learning also differs between individuals based on cognitive thinking styles, preferred learning methods, knowledge level, and environmental factors. Similar to the creative process, learning commences with the introduction of concepts that are linked to prior knowledge so that they can be understood, culminating in new understandings.

How do you think online platforms, like Bugcrowd, can facilitate and motivate written and technical creativity in security research?

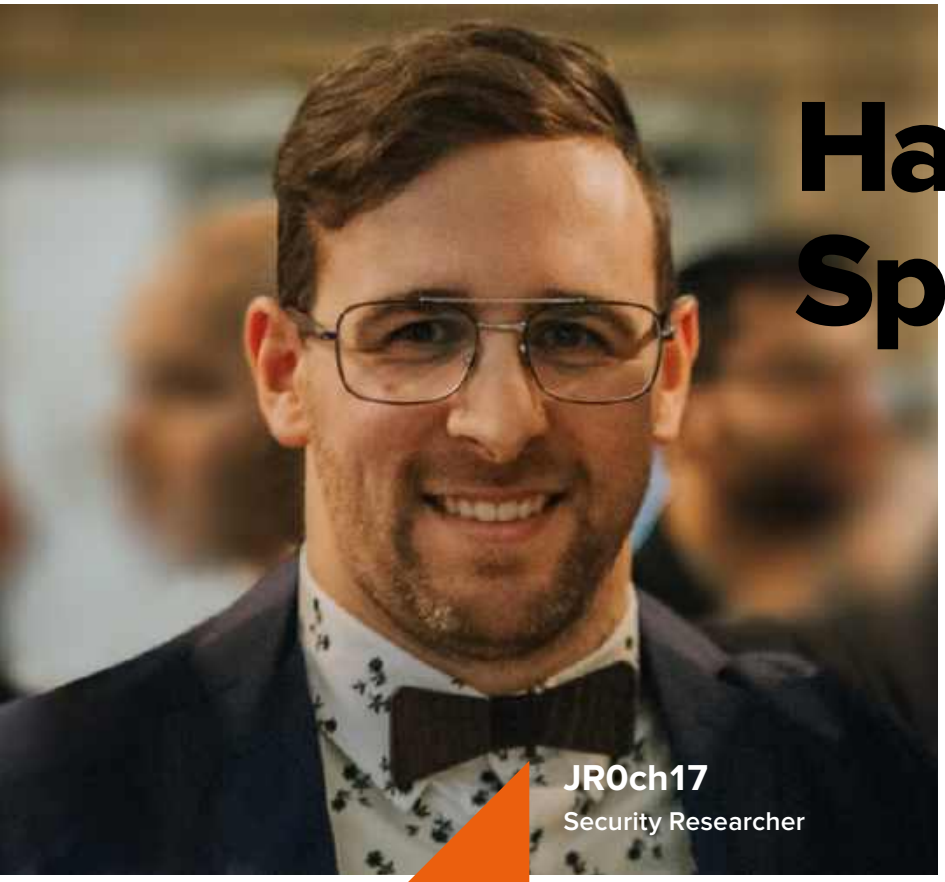
There is an inherent social element to any creative endeavor, which makes a platform like Bugcrowd conducive to both creativity and learning. Unsurprisingly, considerable research exists on the benefits of collaborative learning in developing shared understandings and negotiating new meanings. Additionally, collaborative creativity facilitates the ability to form multiple perceptions of a problem.

Collaborative approaches enable individuals with differing backgrounds, knowledge, skillsets, and experience levels to build on current levels of knowledge in forming solutions.

From a learning perspective, Bugcrowd also relates to Vygotsky's zone of proximal development (ZPD) in that security researchers can learn from each other concepts which they may not have understood alone.

How do you think community-driven learning encourages creativity and enhances cybersecurity?

I think Bugcrowd offers organizations a clear advantage in knowledge-sharing and the co-creation of security resources. Naturally, this encourages more creativity and helps organizations arrive at solutions to their problems sooner.



Hacker Spotlight

JR0ch17
Security Researcher

JR0ch17 is an active security researcher on the Bugcrowd platform. He started hacking about three years ago while he was working as a system administrator. His mantra is "Make your dreams become a reality," and true to that sentiment, he now works full-time as a security researcher. When he's not hunting bugs, you'll find him playing hockey, soccer, and golf.

JR0ch17

What advice do you have for security researchers trying to go full-time?

I started my full-time ethical hacking journey after attending a Bug Bash by Bugcrowd at RSA Conference. My best advice would be the following:

- Make sure you have a lot of bugs in your backlog waiting to be paid out so that you don't get stressed out financially and are still able to pay bills.
- Have a plan and schedule in place so that you work specific hours and do other activities to avoid burn out.
- Set up automated recon so you can spend more time hacking rather than doing asset discovery.
- Work on programs with which you're already familiar.
- If you have reached your monthly goal early in the month, spend some time tweaking your tools, working on recon, and looking for 0-days so that you can also be successful in the future months to come.

→ JR0ch17 is ranked #47 on the platform at the time of publication.

What are the top 5 tools that help you most when you're hacking?

If I could, I'd probably put Burp Suite in positions 1-3 as I do most of my work from there. That said, here are four other tools that help me the most when I'm hacking:

- Burp Suite (+all of the extensions that I use)
- The recon framework that I built (/am still building)
- Nuclei (when I find a misconfig or vuln on a product, I can test it out on every single subdomain I've gathered in my recon)
- Dirsearch/ffuf
- sqlmap

Identity

Hackers have identities characterized by learning and ***problem-solving****.*

Identity encompasses the perceptions, experiences, and values that create a hacker's sense of self. It's what makes security researchers and their techniques appear familiar to others over time, even as they evolve. The way security researchers think of themselves, in contrast to how they believe others think of them, also provides an interesting perspective as to who they are.

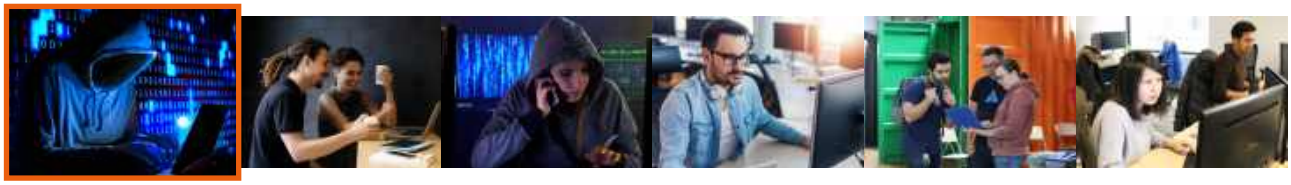
Results show that the majority of security researchers believe others presume their appearance will align with stereotypical images of hackers wearing hoods. In contrast, when asked to describe themselves, 40% of security researchers chose a picture of two everyday people high-fiving. This choice suggests security researchers aren't space-age specialists, but rather, ordinary people that just so happen to have extraordinary skills in cybersecurity.

Identity is worth considering because it influences how ethical hackers moderate their behavior and interactions with others. Interestingly, depictions of material success like a job offer (10%) and public recognition (4%) conflicted with security researchers' desire to maintain a self-identity characterized by learning (30%) and problem-solving (20%). These findings indicate security researchers effortlessly straddle the divide between their diversities and self-development.

As a career, ethical hacking is enabling them to realize their aspirational identities through professional attributes of autonomy, purpose, and mastery. These characteristics empower them to share their unique expertise with organizations from anywhere in the world.

*Hackers are still heavily stereotyped despite looking **more relatable than ever**.*

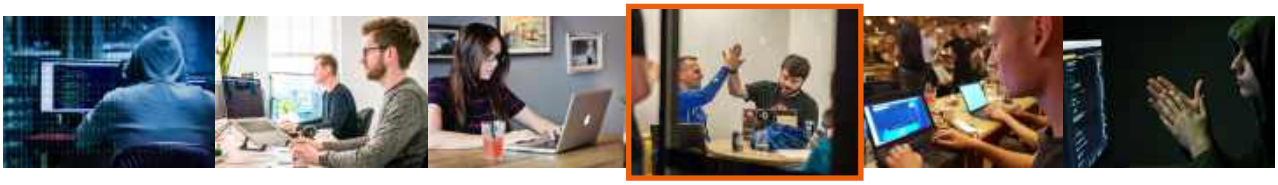
WHAT OTHER PEOPLE THINK HACKERS LOOK LIKE



71% 2% 17% 5% 4% 2%

When asked to describe how other people view them by selecting one of six images depicting people in varied technology contexts, 88% of security researchers chose a hooded character working in a dark, futuristic environment. These findings indicate the ubiquity of oversimplified ideas concerning a hacker's appearance, providing new grounds for speculation as to whether security researchers regulate themselves to minimize association with traditional assumptions. Interestingly, some ethical hackers have even started satirically adopting these false stereotypes as part of their online identities.

WHAT HACKERS THINK THEY LOOK LIKE



6% 13% 12% **40%** 21% 8%

When asked to describe how they view themselves in the same manner, only 14% of security researchers selected images that feature stereotypical representations of hackers. Most chose pictures of everyday people in a variety of informal settings that include technology. Interestingly, 40% of security researchers chose an image of two people high-fiving over a computer. This selection hints at the inextricable link between an ethical hacker's self-identity and the collective success of those with whom they collaborate. Furthermore, it indicates that security researchers generally look less like formidable hooded characters and more like someone you might see at the mall.

WHY THEY HACK ON BUGCROWD

10% 4% 24% 12% 20% **30%**

When asked why they hack on Bugcrowd, the majority of security researchers selected images representing learning (30%), followed by money (24%) and problem-solving (20%). These findings suggest ethical hackers prioritize their ongoing self-development over discrete monetary gains. Remarkably, photographs depicting material success like a job offer (10%) or public recognition (4%) were less likely to be selected than those representing scenes abstracted from income.

Take Hacktion

Hacking is more than a career—it's a ***movement.***

Inside the Mind of a Hacker 2020 casts new light on the next generation of hackers, who are scaling human ingenuity to solve the greatest cybersecurity problems of our time. It also presents a timely review of security researchers amid a growing digital crisis, highlighting how they're working together to help organizations defend their attack surface in a pandemic. While this report doesn't speak for every hacker, it provides compelling evidence that those working on the Bugcrowd platform are trustworthy, drive innovation, and excel in their craft. By providing access to this incredibly talented pool of researchers, Bugcrowd helps organizations tackle the security issues of today and tomorrow with confidence.

FORECAST

In the next six months, cybercriminals will increasingly target latent attack surfaces, and organizations will demand enhanced outward visibility.

The global transition to remote work has forced many organizations to spin up new infrastructure rapidly, and haste is the natural enemy of cybersecurity. Similar to the first wave of digital transformation in the late 1990s, internal teams are overwhelmed with managing unique exposures. At the same time, their existing footprint remains massively underestimated or unknown due to public-facing legacy assets. **Up to 40%** of these assets are unknown after having been lost, forgotten, or de-prioritized over time! Preventable in most cases, these blind spots are driving more cybercriminals to target vulnerable infrastructure through expanded reconnaissance and asset discovery.

Security decision makers know it's only a matter of time until the next major breach occurs and they are scrambling to provide meaningful answers for questions like "What is our exposure?" and "How are we managing it?" Consequently, as internal teams reprioritize attack surface visibility, Bugcrowd forecasts that they will progressively engage more security researchers to minimize risks that existing tooling might otherwise miss. While it's almost impossible to predict the next 0day, hackers on the Bugcrowd platform allow organizations to identify unknown assets, manage vulnerabilities, and verify that their critical assets meet the latest security standards.

In the next 12 months, leading organizations will leverage hackers in never-before-seen ways to harden critical infrastructure.

The long-term value of hackers lies in their flexibility to innovate and to level the defensive playing field as technology and attackers evolve. Bugcrowd enables organizations to incorporate hackers at every stage of the software development lifecycle and build defensive strategies ahead of new technology trends, even when the risk is not yet fully clear. Today, hackers empower organizations to secure everything from web applications to self-driving cars and wireless toasters. But it's not just *what* hackers test on the Bugcrowd platform that makes them extraordinary, but rather *how* they test.

Human ingenuity and creativity remain the most powerful tools in cybersecurity. While artificial intelligence and machine learning serve as useful levers, they will not replace humans for a long, long time to come. This gap between automation and human adversarial creativity suggests organizations will increasingly seek to augment their human expertise in securing their assets via crowdsourcing, the most efficient and practical approach to finding available talent.

The only limits for how organizations can leverage hackers are the limits of their imagination. COVID-19 has demystified many of the perceived differences between employees working remotely and security researchers on the Bugcrowd platform, highlighting how these teams inherently complement each other. Accordingly, Bugcrowd predicts that organizations will leverage hackers in never-before-seen ways in the year ahead.

In the next five years, hackers on the Bugcrowd platform will prevent more than $55.5 billion in cybercrime for organizations worldwide.

In 2020, the *why* of knowledge transfer has become unequivocally more important than the *how* and *where*. The rapid transition to remote work has resulted in a global shift in mindset, and with it, a greater focus on crowdsourced security. Remarkably, the number of critical P1 findings submitted on the Bugcrowd platform, those which are most meaningful to our customers, grew 65% year over year, with monthly submission averages increasing from 190 in 2019 to 315 a year later.

As organizations observe step-function changes to their risk models related to COVID-19, the prospect of remote-only cybersecurity testing is no longer a dealbreaker. Internal teams have long been overextended by bolt-on security cycles that leave little time or budget to identify and eliminate risk proactively. But today, the Bugcrowd platform is unburdening them with flexible and streamlined access to on-demand security researchers that help to secure assets before attackers exploit them.

In line with these trends, and based on conservative estimates, Bugcrowd projects that hackers working on our platform will prevent more than $55 billion in cybercrime by 2025 for organizations worldwide†.

†Three-year trailing average of 236 valid P1 submissions per month x 5 years = 14,160 P1s x $3.9M, the **average** cost of a breach in 2019 = $55.2B in cybercrime prevented over the next five years. This calculation does not take into account the expected increase in Bugcrowd's customer base, the expansion of the available attack surface, and other factors that could result in an even higher number.

About Bugcrowd

Bugcrowd is a pay-for-results security platform that plugs on-demand expertise into your team so they know what to fix first and how to get it done fast.

Our award-winning platform combines contextual intelligence with actionable skills from the world's best security researchers to help organizations identify and fix critical vulnerabilities before attackers exploit them.

Based in San Francisco, Bugcrowd is the #1 crowdsourced security company and is trusted by Fortune 500 organizations to make the digitally connected world a safer place.

sales@bugcrowd.com

press@bugcrowd.com

+1 (888) 361 9734

INSIDE THE MIND OF A HACKER

2020

#TAKEHACKTION

bugcrowd