THE 2020 HACKER REPORT

The survey and statistics of the ethical hacker community.

Miguel | @fisher

hackerone

HACK'ER

/'ha–ker/

noun

One who enjoys the intellectual challenge of creatively overcoming limitations.

INTRODUCTION

No industry or profession has experienced an evolution quite like hacking. It started in the darkest underbelly of the internet, where hackers roamed the online world in search of vulnerabilities.

It later grew into a respectable hobby, something that talented people could do on the side. Now it's a professional calling: hackers, pentesters, and security researchers are trusted and respected, and they provide a valuable service for us all.

But it's much more than that. Hacking is a global movement. The international community of hackers, who delight in taking things apart to see what makes them tick, is building something the world hasn't seen before. Hacking is a philosophy, a mindset, and a way of life.

Hackers face a monumental task. We live in an era of massive data breaches, stunning security failures, and breakneck innovation. Bad actors can now easily obtain the tools they need to steal our most precious resource: our information. Health records, financial data, private communication between friends and family... The stakes could not be higher. Security is everyone's responsibility.

Enter the hackers. Hackers are here for good, to bring their intelligence and their grit to bear against our connected society's toughest challenges. We are at the forefront of a tectonic shift: rather than putting our collective safety in the hands of the few, the burden of our security is now shared by many.

But who *are* hackers? What inspires them? And what's next in their journey?

EXECUTIVE SUMMARY

This fourth annual Hacker Report shares stories from the global hacking community and celebrates their impact.

This report details the efforts and motivations of more than 600,000 individuals who represent our hacker community. Every day, these hackers work to secure the technologies of more than 1,700 customer programs. The report highlights where hackers live, their favorite hacking targets and tools, why they collaborate, and much more.

In 2019, hackers earned nearly $40 million in bounties, almost equal to the entire amount awarded in all prior years combined. And while the most successful hackers find their efforts very lucrative — 6 hackers surpassed $1 million in lifetime earnings this past year — most do it for more than the money. Hackers want to make an impact. They seek out opportunities to enhance their careers, with companies hiring from within the hacker community at a faster clip than ever before. Companies are utilizing bug bounty reports and hacker engagement as an enhanced resume of proven skills that will impact security efforts from day one.

The concept of hacking as a viable career has become a reality. Not only are more hackers earning most or all of their income from hacking, they're making a good living doing it. Besides the seven hackers passing the $1 million earnings milestone, thirteen more hit $500,000 in lifetime earnings and 146 hackers earned $100,000, up from 50 last year. That puts the potential earnings power of a hacking career well above today's global average IT salary of $89,732.

But not all organizations are using this talent pool to its full potential. Nearly two-thirds of hackers say they've found bugs and chosen not to report them to the organization. 38% of hackers said this was due to "threatening legal language" posted on the organization's website regarding the discovery of potential vulnerabilities. In other cases, 21% said the companies didn't have an obvious channel through which to report findings, and another 15% said that the company was unresponsive to previous bug reports. That's thousands of bugs that have gone unreported, and a significant amount of untapped potential.

As hacking grows in popularity, learning continues to be a focus. Hundreds of hackers are registering to join the ranks every day — nearly 850 on average. As such, training modules such as Hacker101 capture the flag challenges are in high demand.

Hackers represent a global force for good, coming together to help address the growing security needs of our increasingly interconnected society. The community welcomes all who enjoy the intellectual challenge to creatively overcome limitations. Their reasons for hacking may vary, but the results are consistently impressing the growing ranks of organizations embracing hackers through crowdsourced security — leaving us all a lot safer than before.

600K+
TOTAL REGISTERED HACKERS

150K+
TOTAL VALID VULNERABILITIES SUBMITTED

$80M+
TOTAL BOUNTIES PAID

As of February 2020

TABLE OF CONTENTS

IMPORTANT TERMS

Hacker: One who enjoys the intellectual challenge of creatively overcoming limitations.

Hacker-Powered Security: Any goal-oriented hacking technique that utilizes the external hacker community to find unknown security vulnerabilities and reduce cyber risk. Common examples include private bug bounty programs, public bug bounty programs, time-bound bug bounty programs, hacker-powered penetration testing for compliance, and vulnerability disclosure policies. With hacker-powered security testing, organizations can identify high-value bugs faster with help from the results-driven ethical hacker community.

Hacker-Powered Pentest: A limited access program where select hackers apply a structured testing methodology and are rewarded for completing security checks.

Hacktivity: Hacker activity published on the HackerOne platform.

Public Bug Bounty Program: An open program any hacker can participate in for a chance at a bounty reward.

Private Bug Bounty Program: A limited access program that select hackers are invited to participate in for a chance at a bounty reward.

Time-Bound Bug Bounty Challenge: A limited access program with a pre-determined time frame where select hackers have a chance at earning a bounty award.

Vulnerability: Weakness of software, hardware or online service that can be exploited.

Vulnerability Disclosure Policy (VDP): An organization's formalized method for receiving vulnerability submissions from the outside world, sometimes referred to as "Responsible Disclosure". This often takes the form of a "security@" email address. The practice is outlined in the Department of Justice (DoJ) Framework for a Vulnerability Disclosure Program for Online Systems and defined in ISO standard 29147.

KEY FINDINGS

Global growth of bug bounty programs is being followed by the **globalization of the hacker community**. Hackers from Switzerland and Austria earned a combined over 950% more than in the previous year, and hackers from Singapore, China, and other countries in APAC earned over 250% more than in 2018.

Hacking provides valuable professional experience, with 78% of hackers using their hacking experience to help them find or better compete for a career opportunity.

Hacking is becoming a popular income supplement or career choice. Nearly 40% of hackers devote 20 hours or more per week to their search for vulnerabilities. And 18% of our survey respondents describe themselves as full-time hackers.

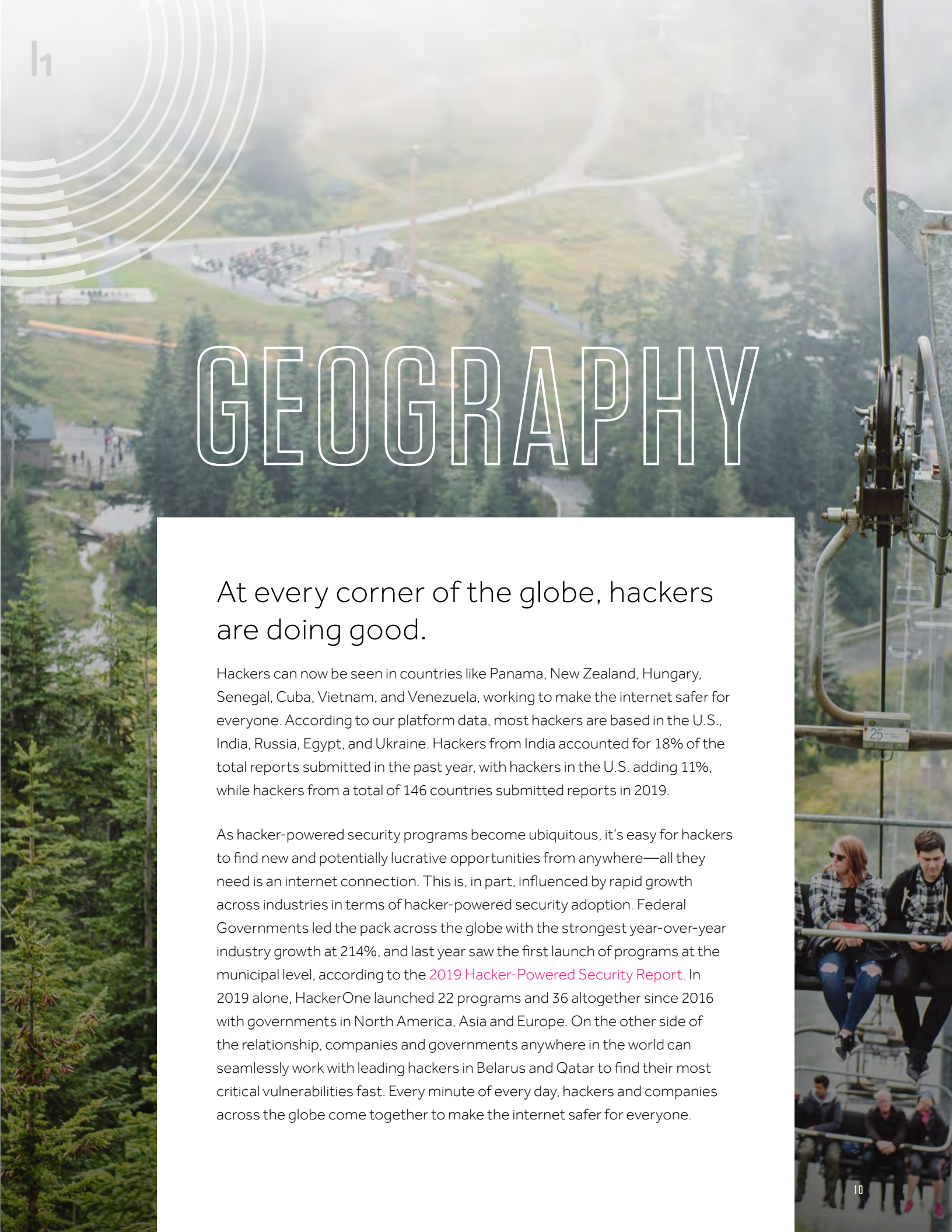
Hackers earned nearly $40 million in bounties in 2019, which is nearly equal to the bounty totals for all preceding years combined. At the end of this past year, hackers had cumulatively earned more than $82 million for valid vulnerability reports.

KEY FINDINGS

The hacker community continues to grow at a robust pace, **nearly doubling in the past year to more than 600,000** registered.

Hackers in the U.S. earned 19% of all bounties last year, with India (10%), Russia (8%), China (7%), and Germany (4%) rounding out the top 5 highest-earning countries.

Hacker training continues to take place outside of the traditional classroom, as **84% say they learned their craft through online resources and self-directed educational materials** like Hacker101 and publicly disclosed reports. Just 16% have completed a formal class or certification on hacking.



GEOGRAPHY

At every corner of the globe, hackers are doing good.

Hackers can now be seen in countries like Panama, New Zealand, Hungary, Senegal, Cuba, Vietnam, and Venezuela, working to make the internet safer for everyone. According to our platform data, most hackers are based in the U.S., India, Russia, Egypt, and Ukraine. Hackers from India accounted for 18% of the total reports submitted in the past year, with hackers in the U.S. adding 11%, while hackers from a total of 146 countries submitted reports in 2019.

As hacker-powered security programs become ubiquitous, it's easy for hackers to find new and potentially lucrative opportunities from anywhere—all they need is an internet connection. This is, in part, influenced by rapid growth across industries in terms of hacker-powered security adoption. Federal Governments led the pack across the globe with the strongest year-over-year industry growth at 214%, and last year saw the first launch of programs at the municipal level, according to the 2019 Hacker-Powered Security Report. In 2019 alone, HackerOne launched 22 programs and 36 altogether since 2016 with governments in North America, Asia and Europe. On the other side of the relationship, companies and governments anywhere in the world can seamlessly work with leading hackers in Belarus and Qatar to find their most critical vulnerabilities fast. Every minute of every day, hackers and companies across the globe come together to make the internet safer for everyone.

WHERE HACKERS ARE LOCATED IN THE WORLD

Figure 1: Geographic representation of where hackers are located in the world.

THE INTERNATIONAL FLOW OF BUG BOUNTY CASH

While today hackers are located in 170 countries, the most prolific paying organizations and highest earning hackers hail from just a few countries.

Those in the U.S. and Canada paid the bulk of bounties, followed by the U.K., Germany, Singapore, and Russia all contributing significant bounty awards.

The chart below shows the outflow and inflow of bug bounty cash from organizations to hackers on the HackerOne platform as reported in the Hacker-Powered Security Report 2019.

GEOGRAPHIC MONEY FLOW

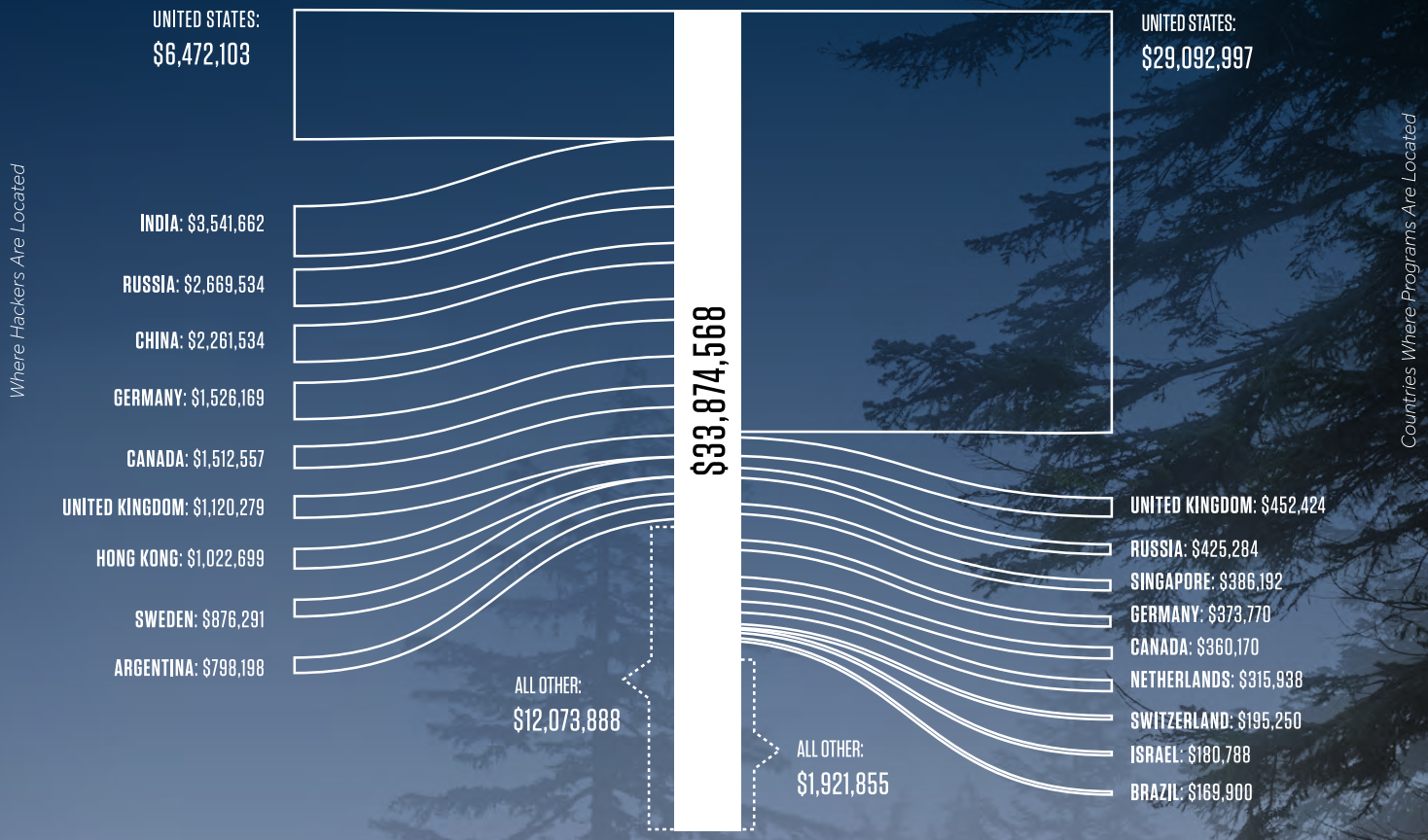


Figure 2: Visualization of the Bounties by Geography showing on the right where the organizations paying bounties are located and on the left where hackers receiving bounties are located.

ACROSS THE GLOBE, HACKERS ARE MAKING MILLIONS

Just one month into 2020, HackerOne witnessed an exciting milestone: Cosmin — better known as @inhibitor181 — became our seventh hacker to reach $1 million in bounties! The thirty-year-old was born and raised in Romania and currently lives in Germany. While working as a developer, he took a practical hacking seminar in Hamburg, where he learned about bug bounty programs and fell in love with ethical hacking. Now, he's been hacking full-time for 2 years.

> "I really love spending my time hacking, and I enjoy trying to break other people's work to make it better for everybody."

While most hackers are still concentrated in the U.S., the million-dollar hackers are emblematic of the truly global scale of the community. Cosmin and the other six million-dollar hackers are each from different countries. Hacking is democratizing online safety and making it possible for people around the world to make a living.

Data was collected from the HackerOne Platform, survey data, and Harris poll data.

HACKING AS A PROFESSION

Hacking for good is more than just a past-time. It's a career.

Hacker-powered security is creating opportunities across the entire globe. Whether you're a trained professional looking for a side hustle, in search of an intellectual challenge, or pursuing hacking as a full time endeavor, there is no shortage of opportunity to earn and learn. Leading organizations including the U.S. Department of Defense, Goldman Sachs, Shopify, Facebook, have recognized hackers' enormous potential to do good. Dozens of companies in the past year have hired from within the community, utilizing submitted bug reports, personal interactions and public HackerOne profile activity as a bellwether for hiring decisions — a practice encouraged and championed within HackerOne.

But hacking itself has become an increasingly promising career opportunity. More than 50 hackers earned over $100,000 in 2019.

As hacking becomes a critical component of security for more, larger, and more risk averse organizations, business leaders view hackers as just another consultant, contractor, or otherwise outsourced area of domain expertise. Add in an extreme shortage of security professionals and their high salaries, and outsourced security is becoming a necessity, not a luxury. As more high-profile organizations adopt and promote hacker-powered security, like the U.S. Department of Defense, Starbucks, General Motors, HBO, the European Commission, and others, it has moved from the fringes of corporate infosec and into a decidedly mainstream occupation.

The bulk of hackers make less than $20,000 per year from bug bounties as a hobby. But 85% of hackers spend less than 40 hours per week hacking. That means they're earning a competitive wage while working part-time, leaving more time to spend with family, experience other interests, or even work another job.

WHAT PERCENTAGE OF YOUR INCOME COMES FROM HACKING?

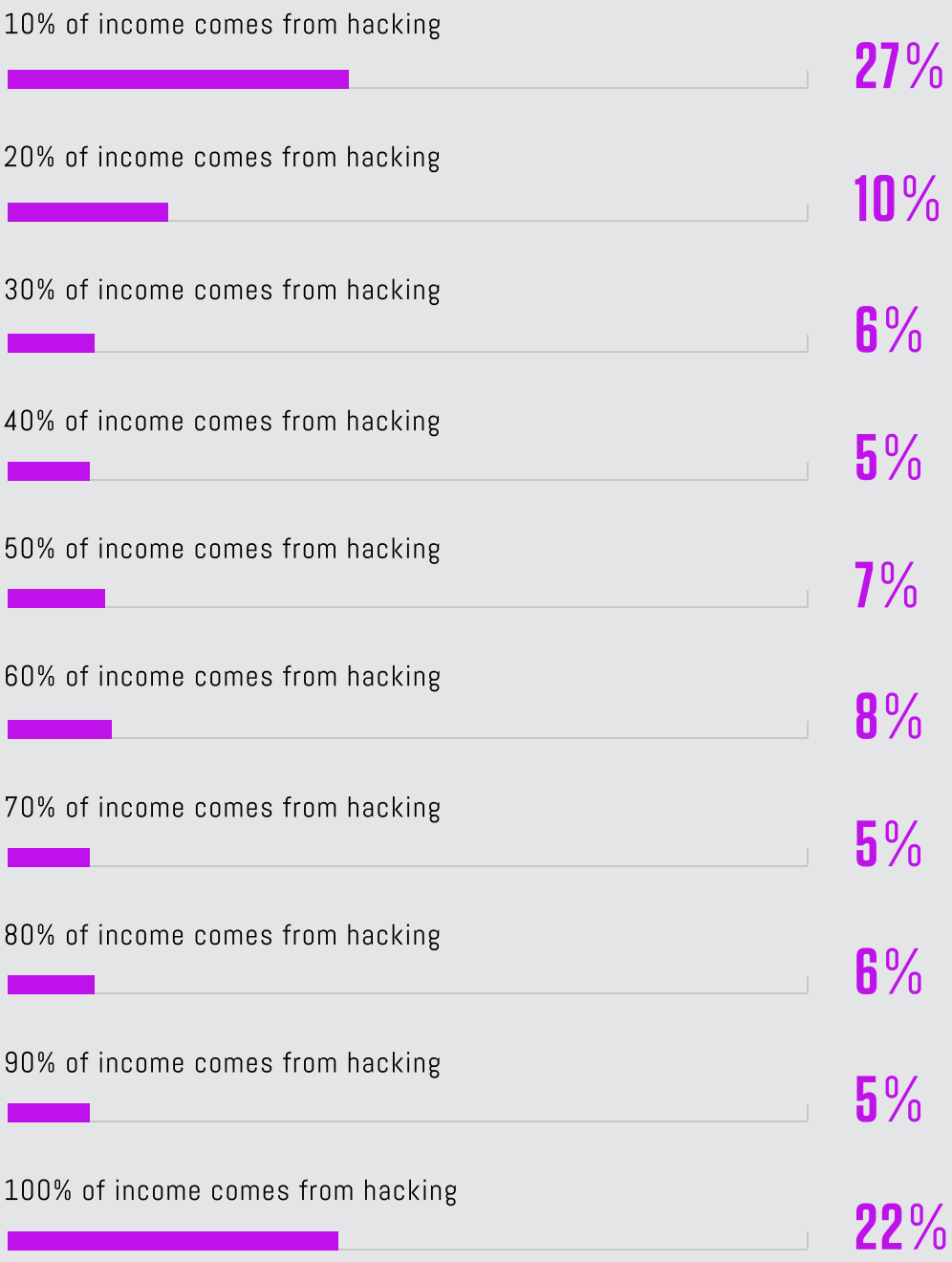


Figure 3: Hacking percentage of income

HACKER SPOTLIGHT

EUGENE

@SPACERACCOON

"I am motivated by the thrill of finding a bug and learning something new. Every time I read an article on new exploitations or discovery techniques, I'm itching to try it out. I love thinking of clever ways to bypass a defense or apply a novel attack."

CALLOUT

HACKERS HELP BRIDGE THE CYBERSECURITY WORKFORCE GAP

The unemployment rate for trained cybersecurity personnel has been infamously pegged at 0%. The acute demand for workers in this profession, and the lack of supply, have helped push security engineer salaries over $225,000. It's only going to get worse, however, as experts predict a global shortage of 1.8 million cybersecurity workers by 2022.

But hackers are helping to relieve some of this pressure as they work to fill that gap for many organizations. The decision to work with hackers through methodical crowdsourced security efforts makes good financial sense for both the individual hacker as well as the organization. Hackers get the opportunity to be well-rewarded for their efforts, and CISO's can expand their security talent almost instantaneously with a results-driven compensation model.

Hacking also helps train those future cybersecurity workers. Since most hackers consider themselves self-taught, and since formalized cybersecurity engineering educations have yet to become common, bug bounty programs and public VDPs give promising hackers the ability to quickly learn, grow, and contribute to everyone's increased security. In fact, 78% of hackers say that they've used or plan to use their hacking experience to help them land a job.

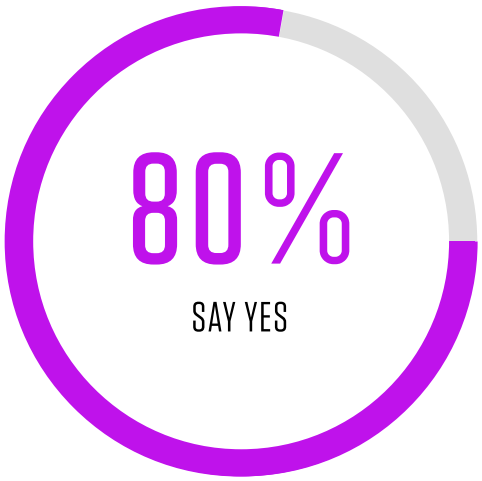


Figure 4: Has hacking helped you land a job or do you plan to use it as you job hunt?

DEMOGRAPHICS

Millennials and Generation Z. Energetic, creative, and educated.

That's the profile of the average hacker in the HackerOne community. More than 87% of hackers are age 34 or younger, yet they're nearly all self-taught. Nearly nine out of 10 hackers are under 35, nine out of 10 are self-taught, and more than half have been at it for over 3 years.

WHAT'S YOUR AGE?

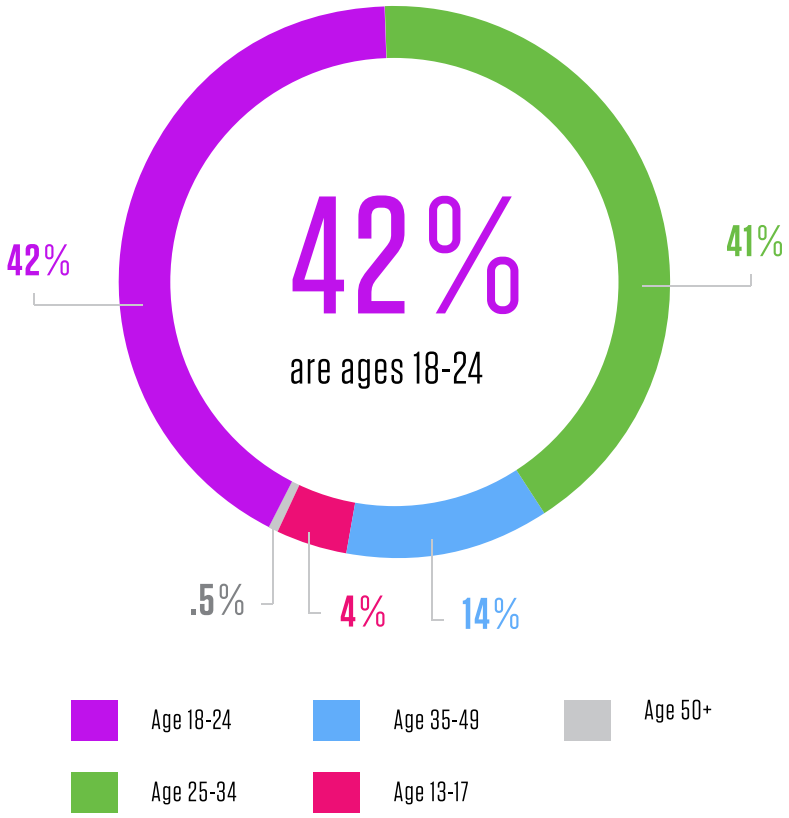


Figure 5: What's your age?

Most of the hackers on HackerOne are under the age of 35, with a big, 5% increase in participation from those 25-34. Older folks are getting more involved, however, with 12% in the 35-49 age group, up from last year's 9% representation. The number of hackers between the ages of 18 and 24 dropped from 48% to 42%. The story here is clear: our hackers have a wide range of professional histories, from development backgrounds to lifetime infosec professionals to self-taught part-timers who are picking up some money on the side.

Gender: While the vast majority of hackers identify as male, the number of female and non-binary individuals in this community is increasing. 10% of the community identifies as female or non-binary. While this is a slight increase from last year, it shows there's still work to be done.

CALLOUT

IS A "HACKER" GOOD OR BAD?

IT'S NO LONGER A QUESTION

HackerOne commissioned a survey of over 2,000 U.S. adults to gauge their perception of hackers. The survey found that 82% of Americans believe hackers can help expose system weaknesses to improve security in future versions. However, a nearly identical share said they believe hacking to be an illegal activity.

But this is rapidly changing. Now that everyone from the Department of Defense to Goldman Sachs recommends hacker-powered security as a best practice, it has become clear that there is no turning back. For most organizations, the question of whether hackers are good or bad is moot. Instead, they are asking how quickly and effectively they can incorporate hackers into their security infrastructure.

DO YOU THINK PERCEPTIONS OF HACKERS ARE CHANGING FOR THE BETTER?

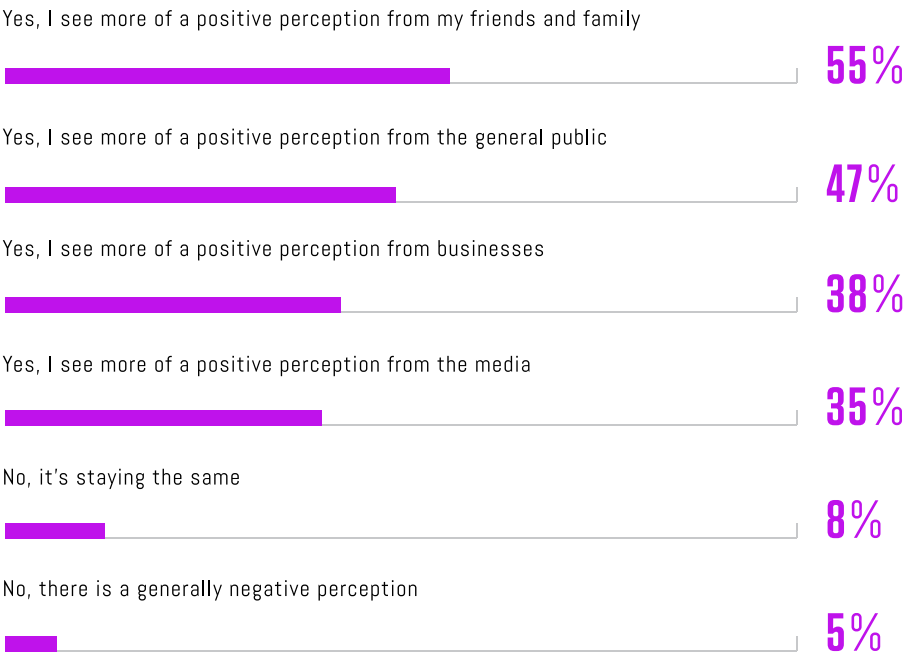


Figure 6: Perceptions of a Hacker

MORE HACKERS HAVE A FORMAL COMPUTER SCIENCE EDUCATION

Hackers are becoming more educated via formal channels, from school programs through advanced degrees. Those who studied programming or computer science in high school increased from 23% last year to over 26% this year. Those who've gone on to study in undergraduate or advanced degrees also increased from 53% last year to 75% this year. Even those taking continuing education courses increased slightly, leaving "none of the above" as the only shrinking segment.

WHAT BEST DESCRIBES YOUR EDUCATION SPECIFICALLY RELATED TO COMPUTER SCIENCE AND/OR PROGRAMMING?

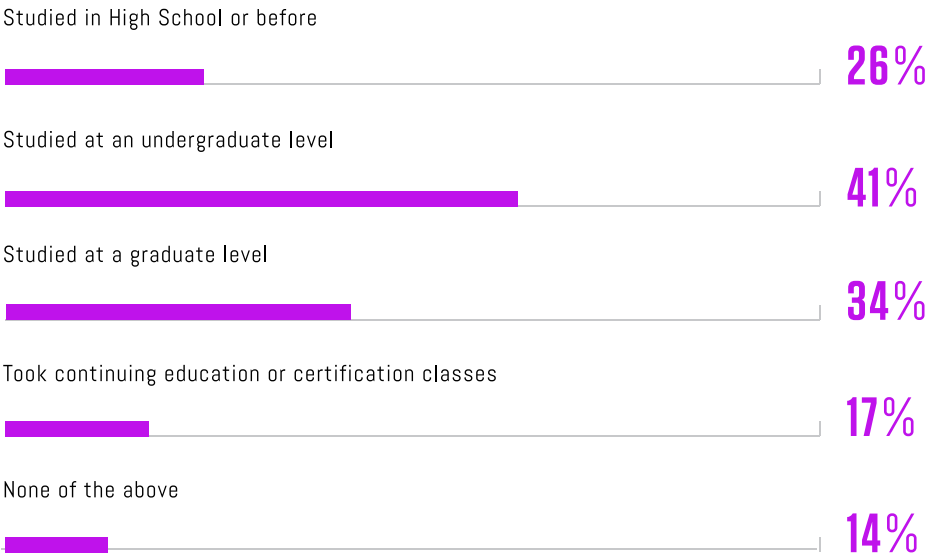


Figure 7: What best describes your education specifically related to computer science and/or programming?

HACKERONE HELPS HACKERS LEARN HOW TO HACK FOR GOOD

hacker101

Hackers are hungry for knowledge. Many top hackers do what they do because they're passionate about learning. Since our inception, HackerOne has provided free online resources for any hacker who wants to learn how to hack for good. Hacker101 teaches you the hacking basics, while Hacker101 CTF (capture the flag) lets learners find bugs in a simulated environment. From webinars to hands-on lessons, HackerOne is thrilled to offer the tools hackers need to hone their skills and win bounties.

WHAT BEST DESCRIBES YOU?

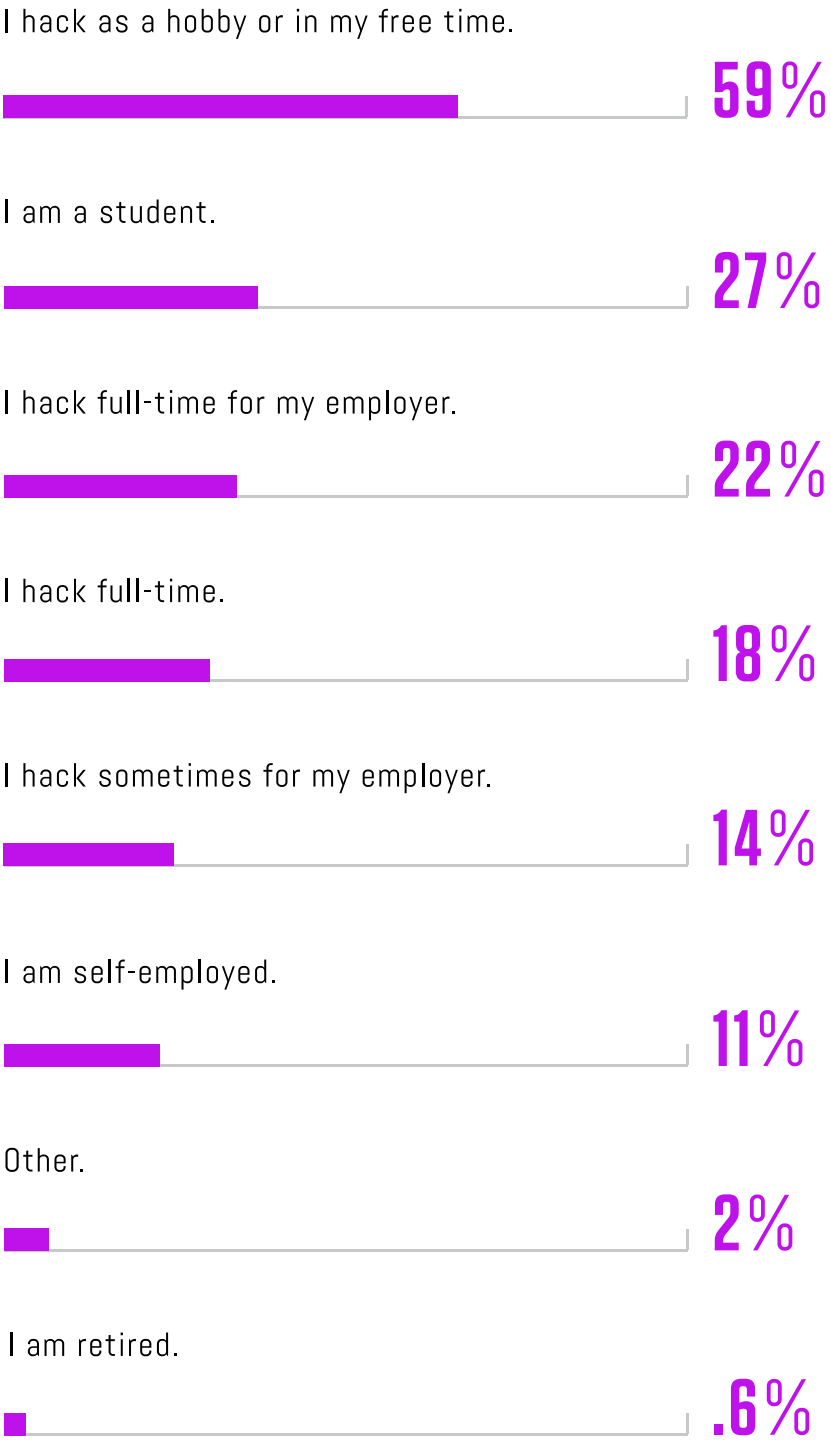


Figure 8: What best describes you?

Hacking can be a lucrative hobby or, a full-time pursuit. A majority of the community fits in the first category, spending most of their days working a full time job or as students with a full class load. Over one-quarter are students, and another 35% have a security-related job.

ON AVERAGE, APPROXIMATELY HOW MANY HOURS PER WEEK DO YOU SPEND HACKING? (NOT JUST TIME RELATED TO H1)

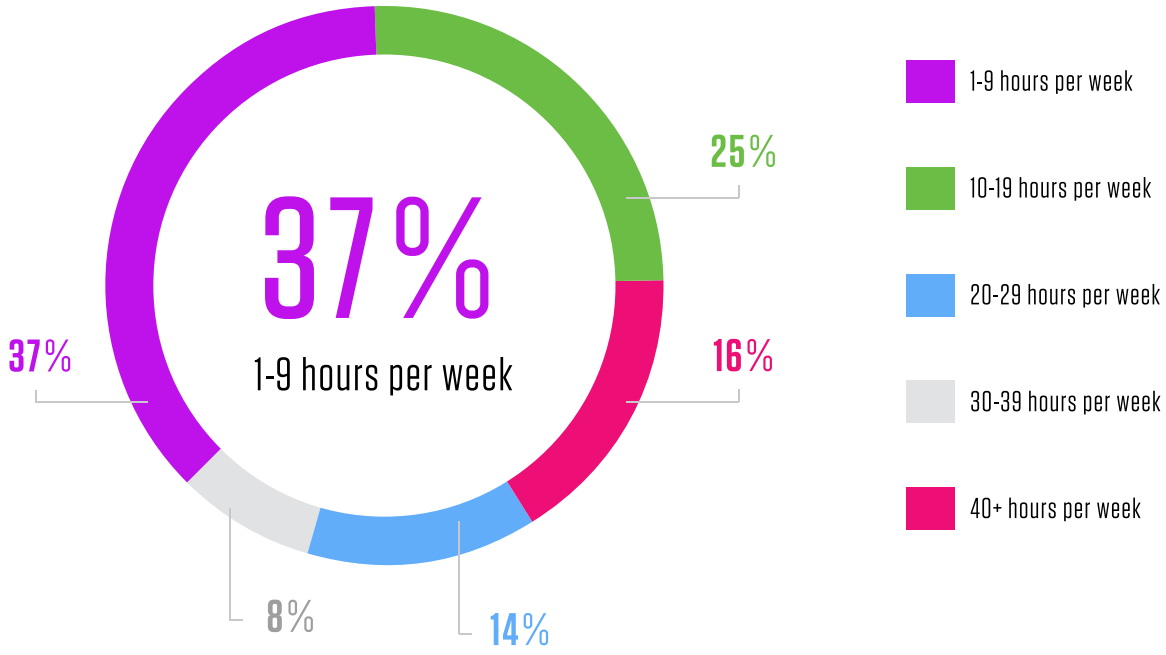


Figure 9: On average, approximately how many hours per week do you spend hacking?

HACKER SPOTLIGHT

TOM

@TOMNOMNOM

"It's a lifelong obsession with how things work. There's this great Richard Feinman quote, which is: *'What I cannot create, I do not understand.'* And I think, for software, you've got to apply an additional layer of '*What I cannot break, I do not understand.*'"

EXPERIENCE

Hacking and bug hunting continue to attract young and eager digital natives.

Online training tools have lowered the barriers for entry. That easy (and free!) access to education has attracted many new hackers over the past year, doubling the hacker community. Today, 76% of hackers have 5 or less years of experience. While some professions might lag from a younger workforce, hacking is decidedly different: creativity, exploration, and failed attempts often lead to novel and unexpected discoveries.

Anecdotal and statistical evidence also point to proof that age doesn't accurately reflect experience, skills, nor education levels. Community members with less slated experience are making meaningful contributions to the collective security of our connected society. Some great reading is CSM's 15 under 15, rising stars in cybersecurity, check it out to learn more about Paul, Mira, Reuben and 12 other incredible young people.

HOW MANY YEARS HAVE YOU BEEN HACKING?

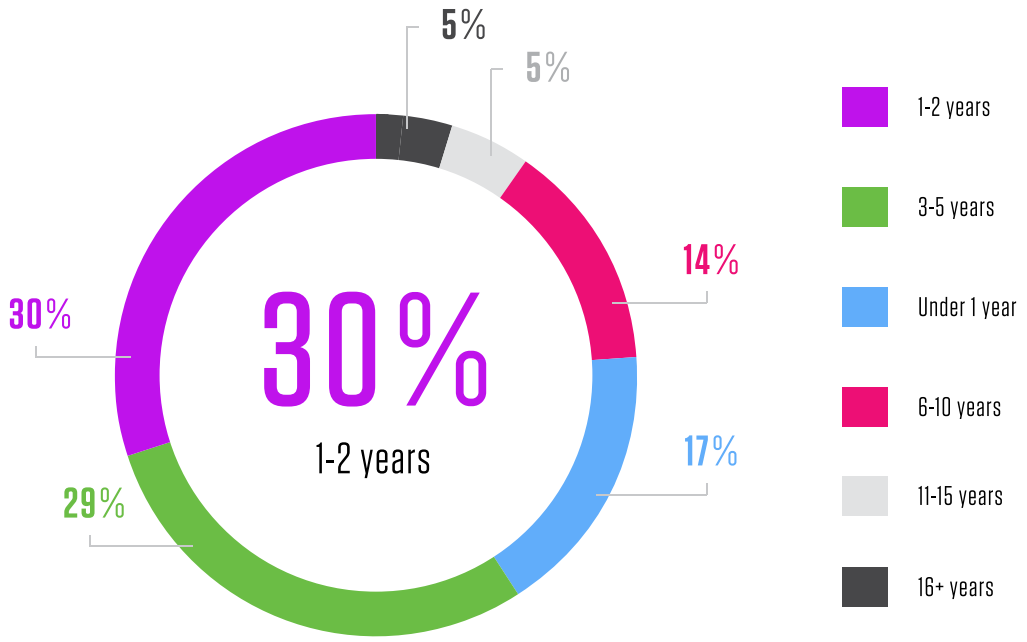


Figure 10: Approximately how many years have you been hacking?

WHAT IS THE PRIMARY WAY YOU LEARNED TO HACK?

Insight: most are self-taught, underscoring the importance of community and online resources. Hacker101 is 5%, so given massive size of community, that could be significant? Hacker101 videos have been viewed more than half-a-million times!

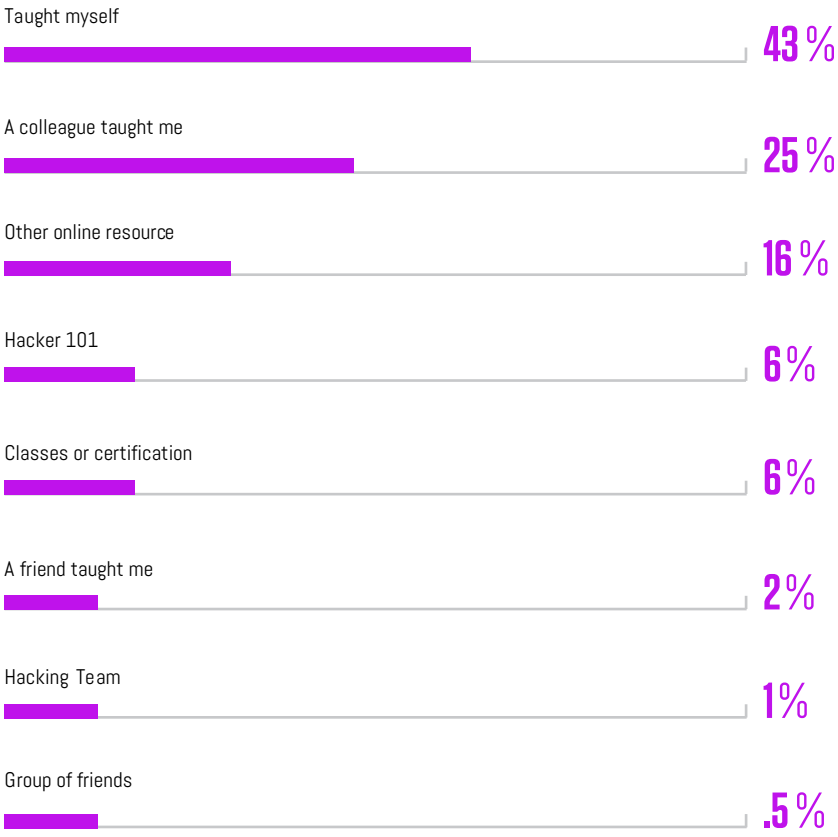


Figure 11: Primary way to learn to hack

HACKER SPOTLIGHT

KATIE

@ INSIDER_PHD

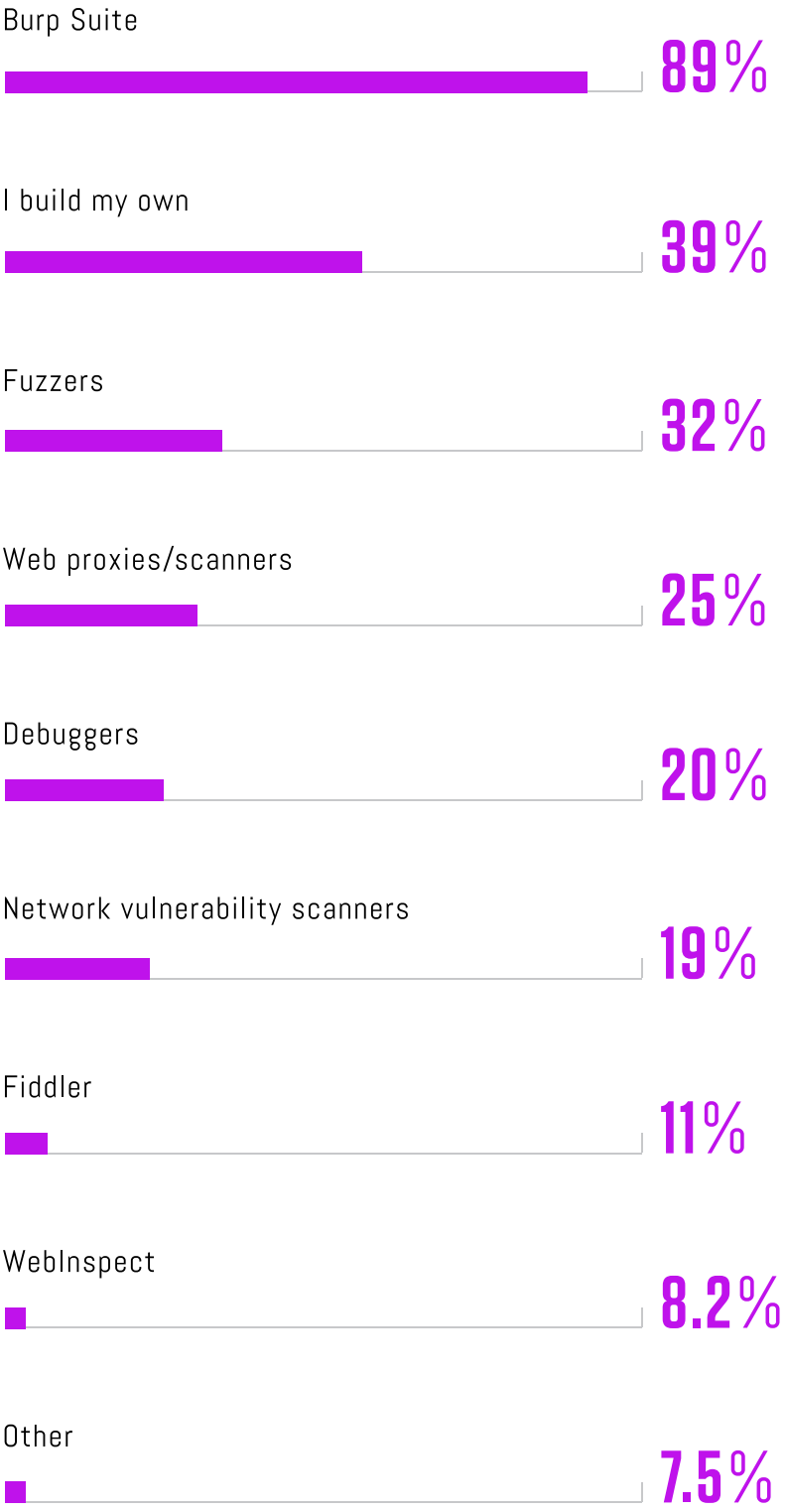
"The community is super encouraging. The community is super willing to help out. It's, as far as I'm concerned, my home."

TARGETS & TOOLS

How do hackers decide which programs to hack?

What are their tools of choice? What attack surfaces do they prefer? These questions matter because they help organizations build bug bounty programs that attract top talent. Hackers wrote in to describe the wide variety of tools in their arsenal. Some use commercially available software and hardware, while others prefer to build their own.

WHAT SOFTWARE, HARDWARE, OR TOOLS HELP YOU MOST WHEN YOU'RE HACKING?



The popularity of Burp Suite jumped significantly this year, with more than 88% of hackers using the tool versus just 33% last year. But, also the number building their own tools jumped from under 10% to more than 38% this year, pointing to the resourcefulness and creativity of hackers.

Figure 12: What software. hardware, or tools help you most when you're hacking

WHAT IS YOUR FAVORITE KIND OF PLATFORM OR PRODUCT TO HACK?

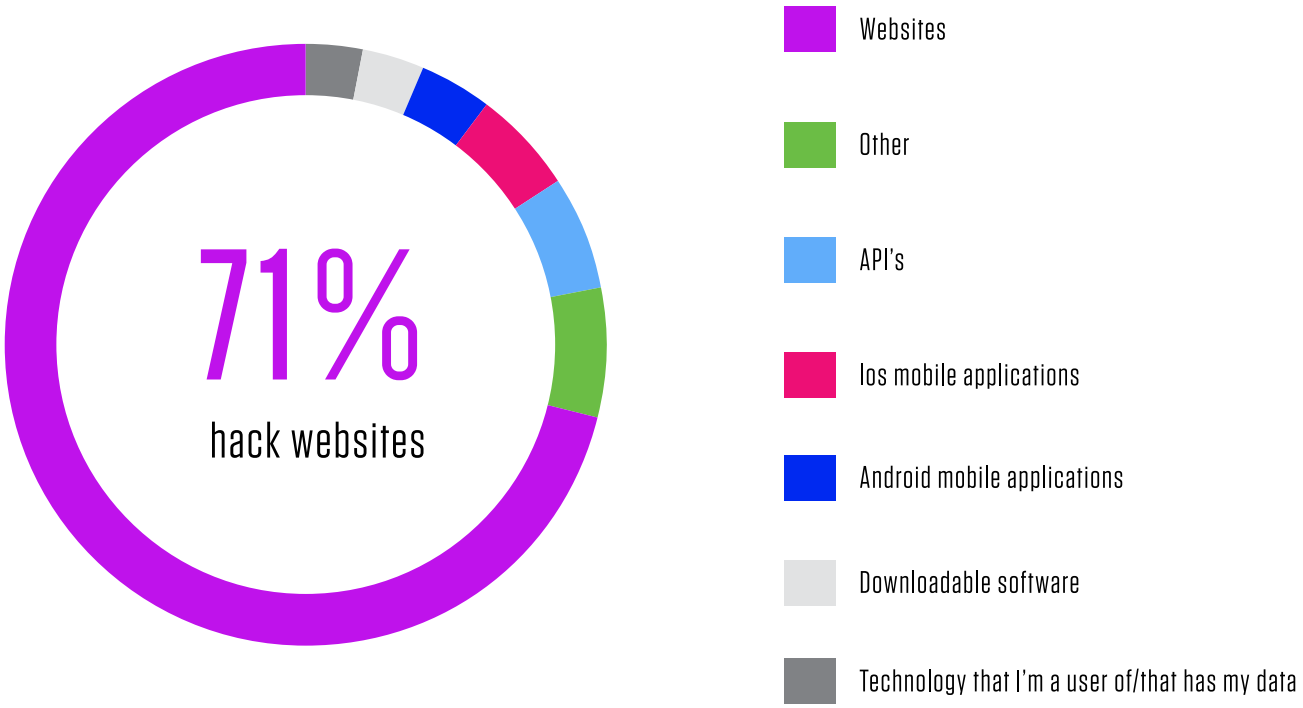


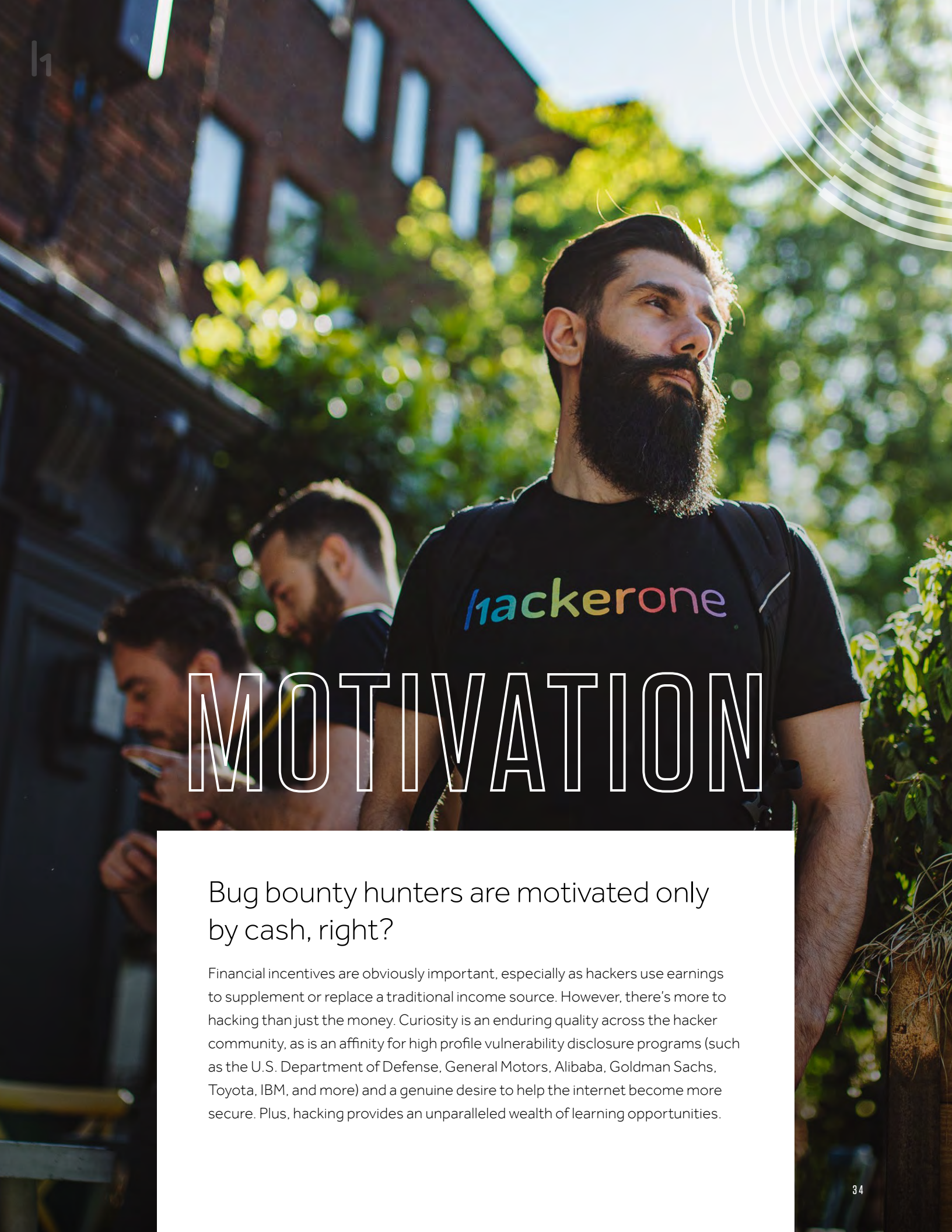
Figure 13: What is your favorite kind of platform or product to hack?

HACKER SPOTLIGHT

CORBEN

@CDL

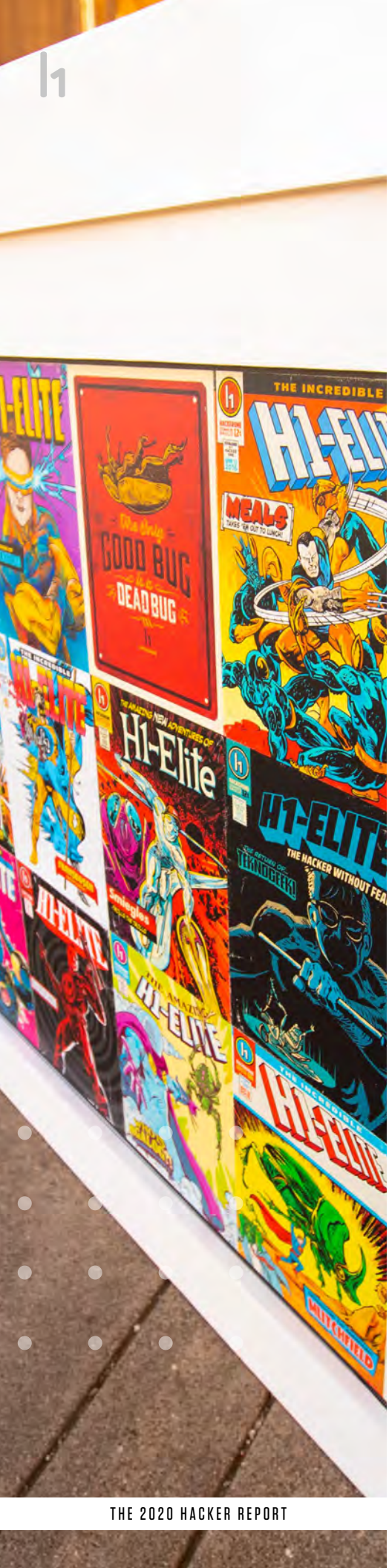
"Being part of the hacker community means the world to me. I've met a ton of people. I've made a ton of friends through it. It's really become a big part of my identity. Everyone who is a part of the community is bringing something important."



MOTIVATION

Bug bounty hunters are motivated only by cash, right?

Financial incentives are obviously important, especially as hackers use earnings to supplement or replace a traditional income source. However, there's more to hacking than just the money. Curiosity is an enduring quality across the hacker community, as is an affinity for high profile vulnerability disclosure programs (such as the U.S. Department of Defense, General Motors, Alibaba, Goldman Sachs, Toyota, IBM, and more) and a genuine desire to help the internet become more secure. Plus, hacking provides an unparalleled wealth of learning opportunities.



THE CHALLENGE IS THE BIGGEST DRIVER

So what motivates hackers if it's not just money? More than two-thirds of hackers do so to be challenged, while half also do it to learn and contribute to their own growth. Unsurprisingly, nearly as many hack just "to have fun" as those who do it for the money. The generosity and altruism of hackers also shines through, with more than one-quarter hacking to protect, help others, and simply to do good in the world. The professional benefits shine through as well, with 44% saying they do it to help advance their own careers.

WHY DO YOU HACK?

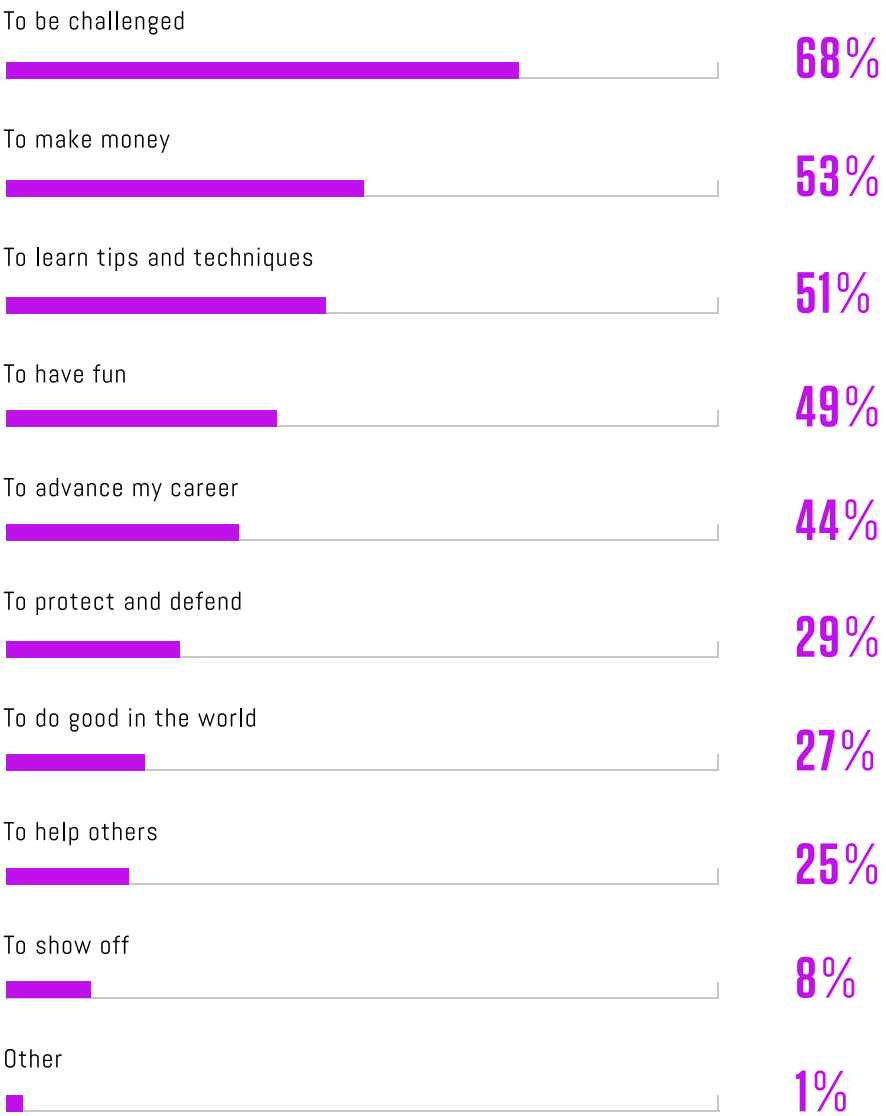
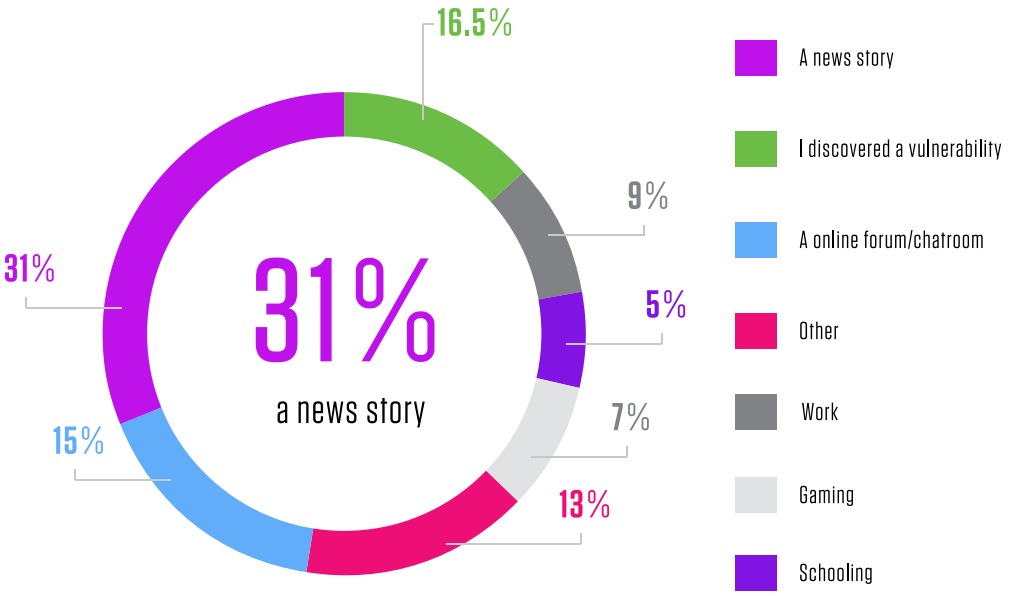


Figure 14: Why do you hack?

HOW DO YOU GET INTERESTED IN ETHICAL HACKING TO BEGIN WITH?



Reflecting the altruistic side of hackers, nearly one-third were motivated by a related news story. Another 16% actually discovered a vulnerability and turned it into a hobby, and, surprisingly, 6% were driven to hacking via gaming.

Figure 15: How did you get interested in hacking?

HAVE YOU EVER USED BOUNTIES TO PAY FOR THE FOLLOWING?

It's not just for the money, but the money does help. Relating to hacking as a career choice, hackers tend to use their earnings for typical expenses, such as homes, cars, and education. Paying for a home (27%), education (22%), and transportation (8%) were popular ways to use bounty earnings. But hackers are also using their winnings for good: 27% donated at least part of their earnings to charity.

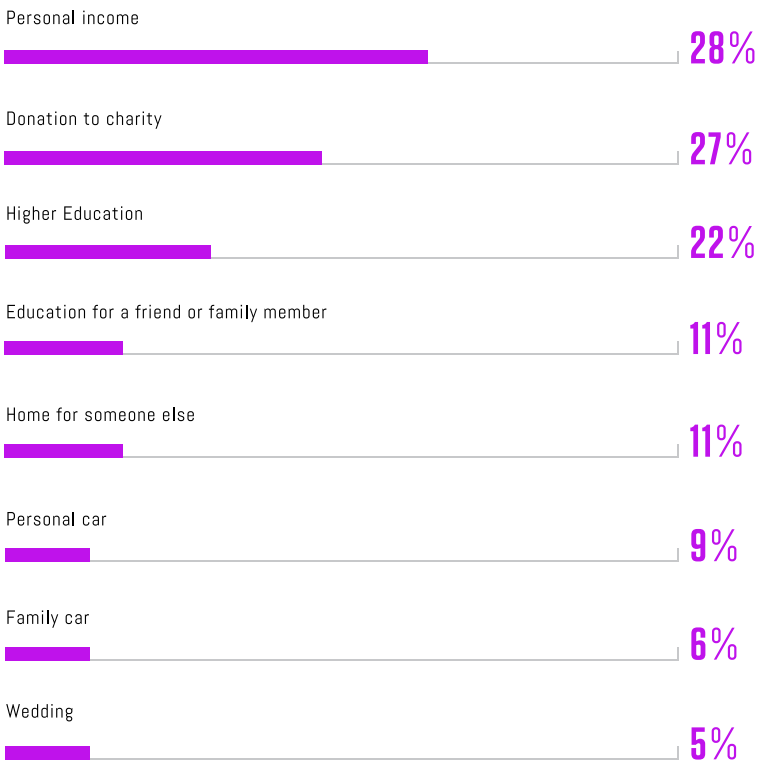


Figure 16: How do you spend your hacker earnings?

GOVERNMENTS LEAD THE WAY IN HACKER-POWERED SECURITY

"Governments lead the way" isn't a phrase you often hear, especially in technology. But in the realm of hacker-powered security, governments and government agencies are decidedly progressive on their use and promotion of this proven approach to cybersecurity.

The U.S. Department of Defense has partnered with HackerOne for several years, running pioneering programs such as Hack the Pentagon and Hack the Army to great success. In late 2018, they announced the results of their seventh bug bounty program, which was their third Hack the Air Force event, and which resulted in hackers from across the globe submitting 120 valid vulnerabilities and earning over $130,000 in just one month. This past year the U.S. General Services Administration became the country's first civilian agency to launch a public multi-year bug bounty program, awarding HackerOne its second contract with GSA.

Governments in other regions are also embracing hacker-powered security. The European Commission partners with HackerOne as part of a framework created by the EU-Free and Open Source Software Auditing (EU-FOSSA) project, which aims to help EU institutions better protect their critical software. FOSSA plans to launch more than two dozen additional bounty programs in 2019.

In Singapore, building on the success of the bounty program run by their Ministry of Defense (MINDEF), the Government Technology Agency of Singapore (GovTech) and the Cyber Security Agency of Singapore (CSA), are working with HackerOne to launch a government bug bounty initiative designed to protect Singapore's citizens and help secure public-facing government systems.

Governments continue to lead the way with their successful hacker-powered programs. This is further proven by the legislation recently proposed and passed in favor of hacker-powered programs, such as the Cyber Intelligence Sharing and Protection Act (CISPA) and the Cybersecurity Information Sharing Act (CISA) in the U.S. and new budget in Singapore. More and more, organizations across a spectrum of sectors realize the value these white-hat hackers add to their security apparatus.

WHAT ATTRACTS HACKERS TO A PARTICULAR PROGRAM?

THE CHALLENGE, THE BRAND, AND, YES, THE MONEY.

Hackers are motivated in a number of ways, as has been detailed above. Money still matters, however not money earned but rather money offered for bounties. Programs paying higher bounties not only attract more hackers, they attract the best hackers. Obviously, not every hacker earns a bounty, but higher awards convey a respect and appreciation of the hackers' work as well as the challenge involved in finding a unique vulnerability. Responsiveness to hackers was also mentioned by many as a reason for hacking, in addition to working with brands they personally like and use.

WHY DO YOU CHOOSE THE COMPANIES THAT YOU HACK?

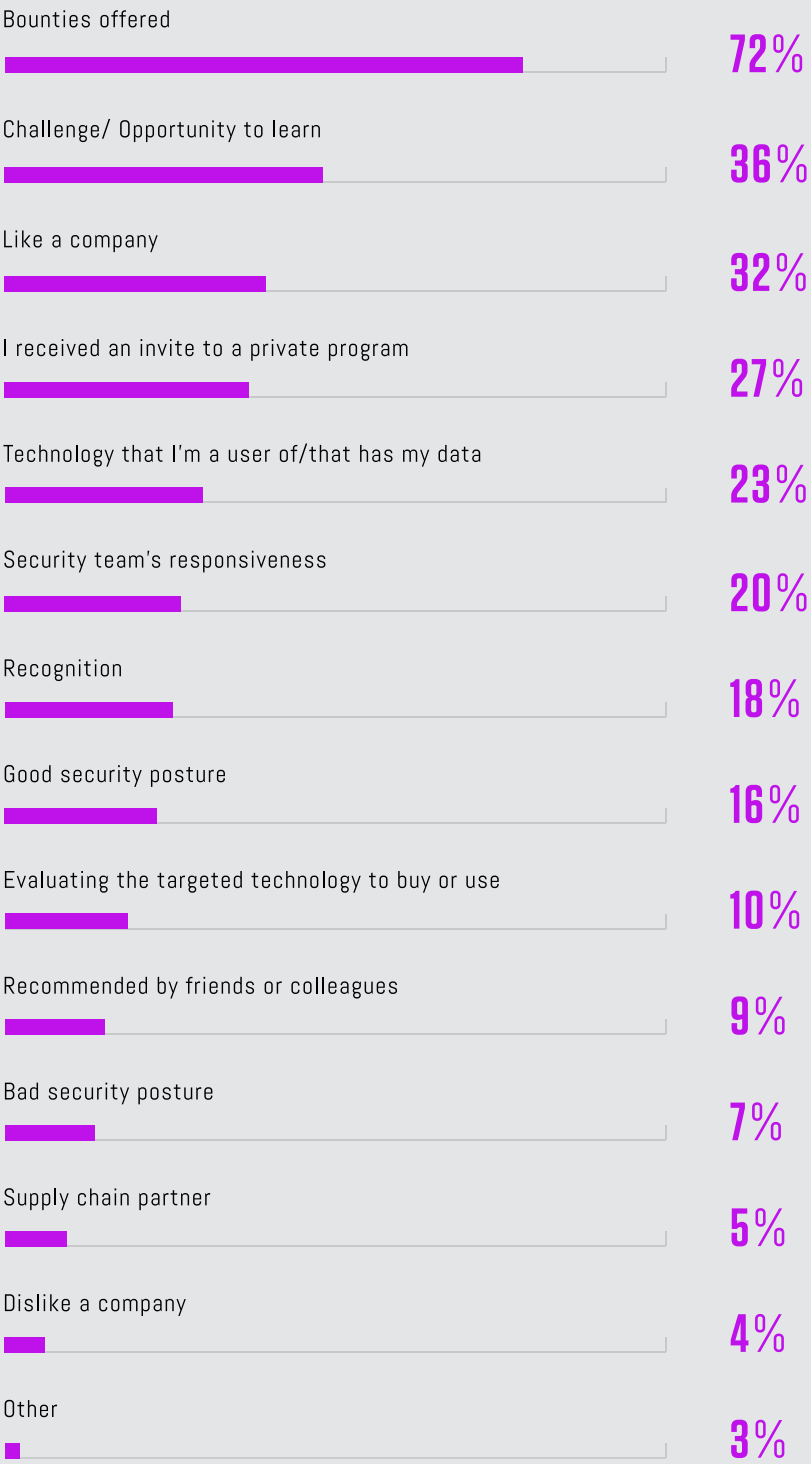


Figure 17: Why do you choose the companies that you hack?

HACKER SPOTLIGHT

ALYSSA

@ALYSSA_HERRERA

"What motivates me is wanting to help out security companies protect against breaches and improve their general security. Another motivation is being a role model for other women who also might want to get into this field of work"

INTERLUDE

BRINGING THE COMMUNITY TOGETHER FOR GLOBAL LIVE HACKING EVENTS

Since HackerOne's Live Hacking Events program launched with our first event in Las Vegas in 2016, we have hosted 20 events in 12 different cities with 14 different customers. As of our final event of 2019, HackerOne has paid out over $7M in bounties and had over 5,000 reports submitted at live hacking events to date.

Live Hacking Events in 2019 smashed records left and right: we had the highest ever single-day bounties (h1-702 with over $1 million paid by Verizon Media alone), the most paid out at a single live event ever (h1-702 with almost $2 million in bounties paid across 3 days), and the first woman to make the leaderboard top 3 (@randomdeduction at h1-702). Nearly $3.8 million in bounties was paid in 2019 alone, with over 2,400 unique report submissions across 8 days in 6 cities. The images seen here are the logos for each event adorned with a local icon and the event name — the area code of the live hacking location.

BUILDING THE COMMUNITY

Our hashtag, *#TogetherWeHitHarder*, reflects the fact that impact is infinitely greater when a community rallies around a common cause.

Hackers are making the internet safer, and HackerOne is helping to connect organizations with hackers who have the skills and energy to protect them.

HACKERS FREQUENTLY WORK ALONE BUT LIKE LEARNING FROM OTHERS

As hackers look to their community to learn and grow, they're also forming relationships that translate into knowledge sharing and direct collaboration. Many hackers choose to work alone, but half still rely on blogs and reports from other hackers to learn. Teaming up with other hackers is becoming more popular, with 22% working at least sometimes with other hackers and 14% doing so regularly, both up from last year's responses.

HOW DO YOU TYPICALLY WORK WITH OTHER MEMBERS OF THE COMMUNITY?

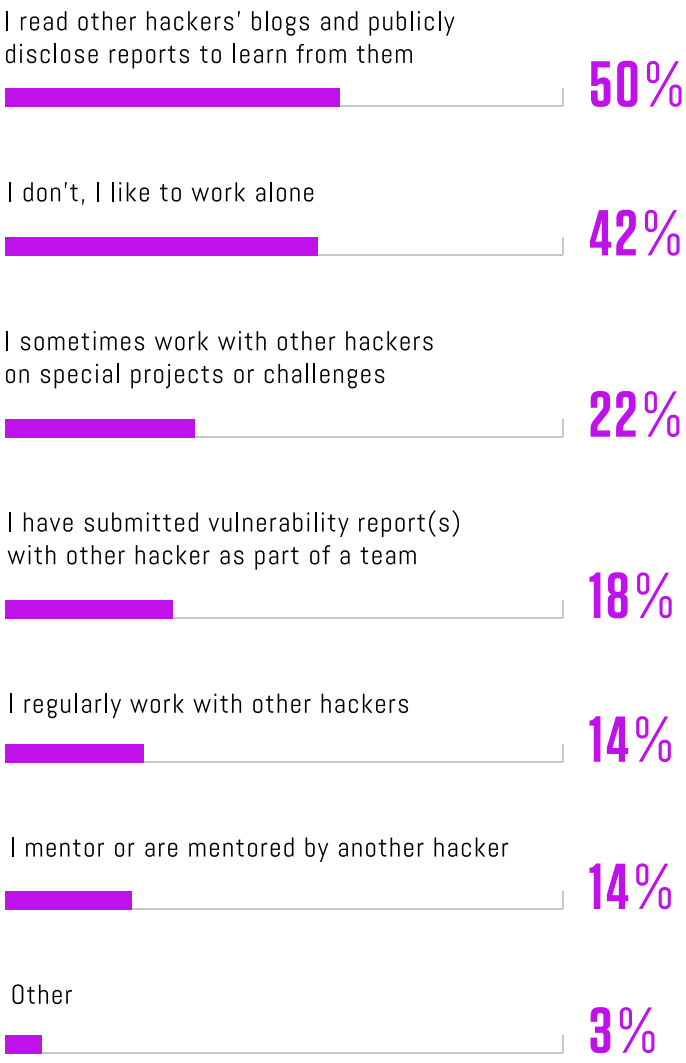


Figure 18: How do you typically work with other members of the hacker community?

HACKING FOR GOOD— AND COMMUNITY

They regularly contribute their time, talents, and treasures to support cybersecurity initiatives. These are just a few of the organizations that our community wrote in that they actively engage with.

Slack, Discord, other channels	26%
OWASP	20%
BSides	12%
Nullcon	11%
Hacker education group	8%
Local DefCon groups	8%
Chaos Computer Club	2%

Figure 19: Do you actively participate in any hacker oriented community-based organizations?
Source: Hacker Report 2020 Survey Data

HACKER SPOTLIGHT

ALEX

@AJXCHAPMAN

"I like the challenge. I like the variety that hacking gives and the opportunity for continued learning. It's a really good way of proving yourself and extending your knowledge every day."

HACKERS WANT TO HELP, SO WHY DON'T ORGANIZATIONS LET THEM?

It's critical for every organization to enable a pathway for the reporting of potential security gaps. It's even more imperative with technology, since the consequences can cripple an organization but also because even the most capable security and development teams know that no technology is ever 100% secure.

When a customer, product user, or other visitor encounters a potential security issue, it should be easy for them to report it. Think of a non-technology example: if a busy restaurant employee accidentally left the cash drawer open, a friendly patron could quickly mention it to a passing server. But in the online world, there's no one around to notify. A knowledgeable bug finder could search for a "security@" email address or look in the code for a reporting mechanism. But that takes time and effort. Diligent finders could go so far as to seek a customer service email address or even reach out to a social media account, but that gets the report far away from the security team that needs it.

With today's ubiquitous and ever-more-complex technologies, there are a near-infinite number of ways a clever criminal can break, modify, bypass, hijack, or otherwise find a way to access your valuable data. So much so that no organization can possibly consider or find them all, especially by themselves. Coincidentally, friendly hackers are coming across security issues every day, not least of which because they know where to look and what to look for.

But what remains shocking is that, according to The 2019 Hacker-Powered Security Report, 93% of the Forbes 2000 still don't have an easy means for finders to report potential security issues. It's as if most companies still turn a blind eye to outside help on cybersecurity issues, better known as "security through obscurity." By ignoring any mention of potential cybersecurity risks, companies assume no one will find them.

It's not surprising to discover that nearly two-thirds of hackers say they've found bugs and chose not to report them to the organization. When asked why, 21% said the companies didn't have an obvious channel through which to report findings and 15% said the company was unresponsive to previous bug reports. But the most hackers, 38%, said it was due to "threatening legal language" posted on a website regarding the discovery of potential vulnerabilities. Since so many organizations are taking an adversarial approach to all hackers, even friendly ones, it leaves thousands of potentially catastrophic security gaps in place, unknown to security and development teams, and open for criminals to exploit.

HAVE YOU EVER FOUND A BUG BUT LEFT IT UNREPORTED?

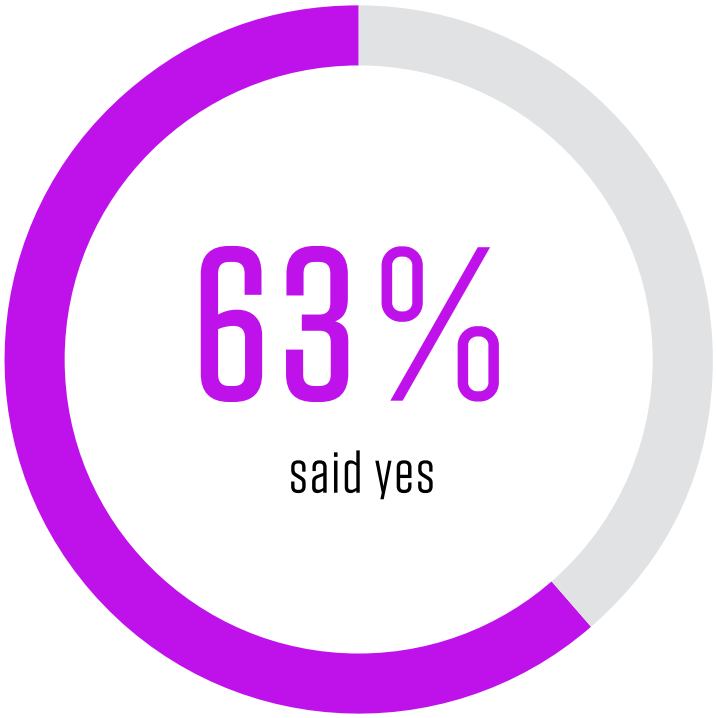
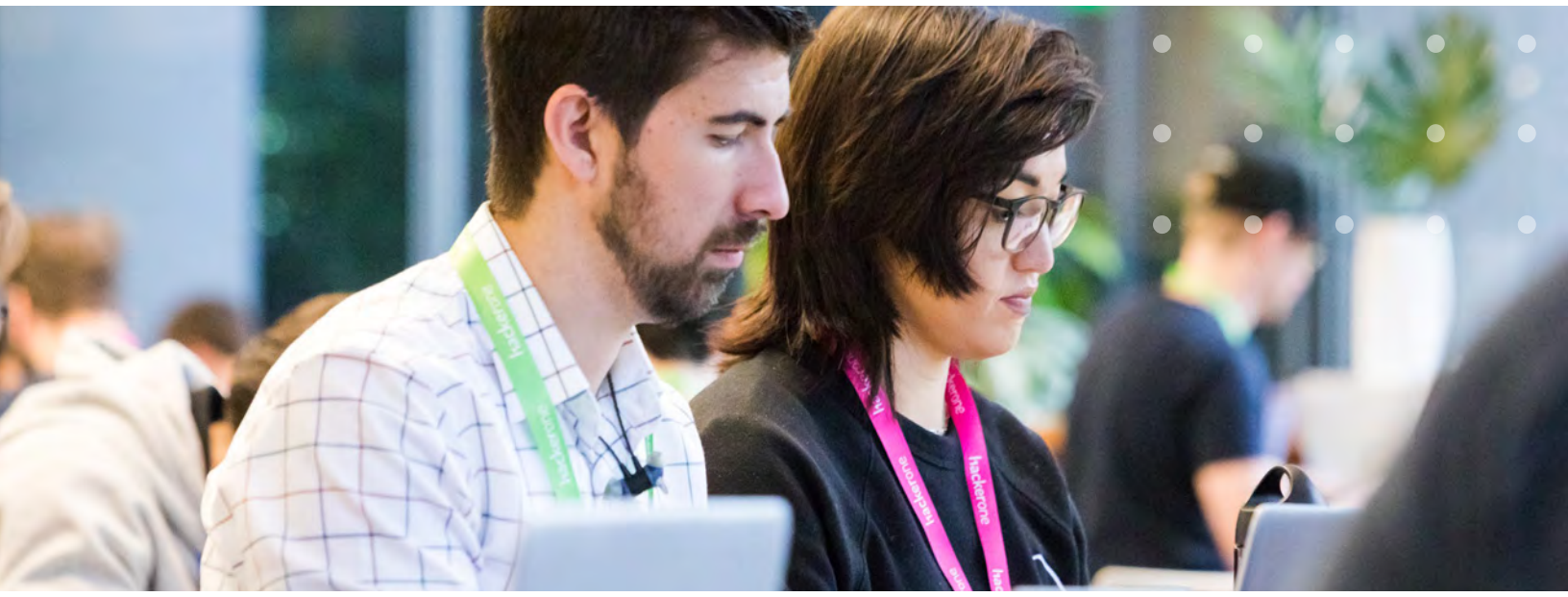


Figure 20: Have you ever found a bug but left it unreported?

A Vulnerability Disclosure Policy (VDP) offers a free, simple, and effective means to encourage the reporting of potential vulnerabilities while protecting those who take the time to do so. It's the digital equivalent of "if you see something, say something" and is intended to give anyone who stumbles across something amiss clear guidelines for reporting it to the proper person or team responsible. It also eliminates the hacker community's #1 reason for not reporting a bug by creating a "safe harbor" to assure finders who report in good faith that they won't be penalized for doing so.

Developing a simple yet effective VDP is an easy first step towards reducing risk by giving hackers an obvious means for reporting any potential vulnerabilities. Many VDP templates and guides exist so putting one together for yourself can be done in as little as a few hours. HackerOne Response also serves as a completely turnkey, ISO 29147-compliant solution, giving hackers an easy and familiar way to submit vulnerabilities to you and your team while reducing risk. It also offers optional report assessments, triaging, and communication with the outside hackers to reduce the burden on your internal teams.



HACKER SPOTLIGHT

BEN

@NAHAMSEC

"The one skill hackers must inherently have is the ability to problem solve and a strong sense of curiosity around how technology works and how it could possibly fail us."

CONCLUSION

Hackers are here for good.

Around the world, the hacking community— pentesters, security researchers, breakers, finders— are using their talent and grit to keep us safe. Organizations like the Department of Defense, Goldman Sachs, Facebook, and Google have embraced hacking as part of a mature security infrastructure. But it's more than that: it's a lifestyle, a mindset, a philosophy, and a global movement. HackerOne is proud to partner with our global community of hackers to continue to do good.

"Everything is a game of speed. All software has some degree of bugs. The quicker we can find and fix them is an approach that is intuitive and obvious to everyone."

PHIL VENABLES, SENIOR ADVISOR AND BOARD DIRECTOR AT GOLDMAN SACHS, TO HACKERONE BOARD MEMBER AND GENERAL PARTNER AT BENCHMARK, BILL GURLEY, DURING **SECURITY@**

METHODOLOGY

Data was collected from a proprietary HackerOne survey in December 2019 and January 2020, totalling over 3,150 respondents from over 120 countries and territories. The surveyed individuals have all successfully reported one or more valid security vulnerabilities on HackerOne, as indicated by the organization that received the vulnerability report. Additional findings were collected from the HackerOne platform using HackerOne's proprietary data based on over 1,700 collective bug bounty and vulnerability disclosure programs.

ABOUT HACKERONE

HackerOne is the #1 hacker-powered pentest & bug bounty platform, helping organizations find and fix critical vulnerabilities before they can be exploited. More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative. With more than 1,700 customer programs, including The U.S. Department of Defense, General Motors, Google, Goldman Sachs, PayPal, Hyatt, Twitter, GitHub, Nintendo, Lufthansa, Microsoft, MINDEF Singapore, Panasonic Avionics, Qualcomm, Starbucks, Dropbox, Intel, HackerOne has helped to find over 150,000 vulnerabilities and award more than $82M in bug bounties to a growing community of over 600,000 hackers. HackerOne is headquartered in San Francisco with offices in London, New York, the Netherlands, France and Singapore.

TRUSTED BY

More Fortune 500 and Forbes Global 1000 companies trust HackerOne than any other hacker-powered security alternative.






MAKE THE INTERNET SAFER

WWW.HACKERONE.COM / SALES@HACKERONE.COM / +1 (415) 891-0777

hackerone