

INSIDE THE MIND OF A HACKER 2023

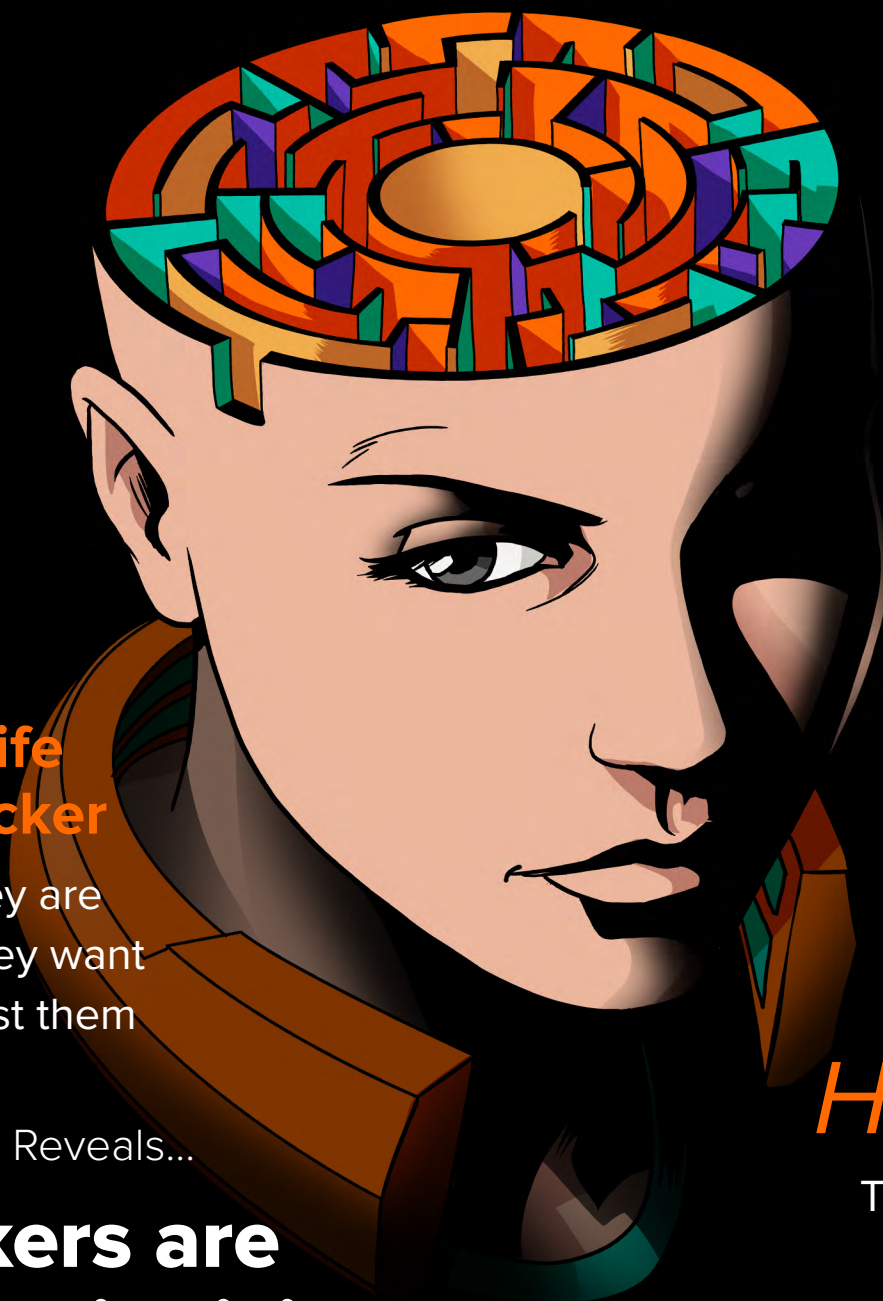
ITMOAH

**SECURITY IN THE AGE
OF GENERATIVE AI**

bugcrowd

VOLUME 7

ISSUE 1



A Day in the Life of a Hacker

- Who they are
- What they want
- Why trust them

Casey Ellis Reveals...

**‘Hackers are
Revolutionizing
the Internet's
Immune System’**

Security Red Flags

6 Signs your
organization
is vulnerable

Hackers!

They're just like us

Bombshell Interview

‘You don't want to
underestimate hackers’

Table of Contents

Letter from the Editor	3	The Anatomy of a Hacker 2023 <small>INFOGRAPHIC</small>	12	Hackers Tapped to Keep OpenAI Safe	25
Report Highlights	4	What the hack is going on with AI? <small>QUIZ</small>	13	Cybersecurity Red Flags <small>INFOGRAPHIC</small>	26
Hackers! They're just like us.	5	The Generative AI Hacking Revolution	14	The Secret Social Lives of Hackers <small>INFOGRAPHIC</small>	27
How well do you know hackers? <small>QUIZ</small>	7	The Heart of Hacking	18	The Texas Chainsaw Ransomware <small>POSTER</small>	29
A Day in the Life of a Hacker	8	Unsolved Cyber Mysteries <small>SNEAK PEEK</small>	21	CISO Spotlight: Nick McKenzie	30
I Know What You Clicked Last Summer <small>POSTER</small>	10	Hacker Spotlight: Nerdwell	22	Conclusion	32
Hacker Spotlight: OrwaGodfather	11	CISO Spotlight: David Fairman	23	Glossary	34

An introduction from our founder and CTO

Bugcrowd recently celebrated its 10-year anniversary, and I've observed a lot of changes in the cybersecurity industry over the past decade. Ten years ago, hackers were almost exclusively assumed to be criminals.

Over time, perceptions have changed. Consider, for example, the difference between burglars and locksmiths. Both parties use creative ways to try to open a locked door, but only locksmiths have good intentions. Changing perception has increased awareness of the digital locksmiths, otherwise known as ethical hackers. Now the word “hacker” conjures images of both the digital burglars and locksmiths. I'm very proud of the work Bugcrowd has done through our platform, reports like this one, and direct work in influencing standards, policy, and public perceptions to change the operating environment for those who hack in good faith.

Crowdsourced security used to be an anomaly, but now, the idea of accepting and even soliciting technical attention and security feedback from hackers has gone from an “if” question to a “when and how” question. Mature organizations have come to accept that vulnerabilities are a product of human creativity and therefore inevitable for as long as humans write code.

But what will happen to the human element with the introduction of mainstream generative AI technologies? There is a lot of speculation out there about the impact generative AI will have on security. I believe that

cybersecurity is about to become less predictable. 91% of hackers surveyed believe that generative AI will increase their effectiveness, which implies that the adversary is innovating in similar ways.

As such, tactics, techniques, and procedures are changing at a faster rate.

Cybersecurity leaders must consider what cyber defense will look like in a world where a more diverse and numerous range of threat actors will have access to more powerful tools to create impact, as with more power comes more threats. One way to ensure that leaders are mounting an adequate defense is by learning from and engaging with hackers to stay ahead of the game.

However, it's not all doom and gloom. I'm really excited about some of the findings in this report that indicate positive trends in the hacking community.

For example, I'm amazed to see the doubling of engagement from those 18

years old and younger. This cohort understands technology—and, by extension—security, in ways their older peers never will, and they'll ultimately inherit the problems the current generation is working to solve. The fact that they are showing such adaptive curiosity in the emerging technology landscape is really exciting. Another interesting example that shows trends in the early adoption of generative AI by the hacking community is the way that hackers in non-English speaking countries are leveraging ChatGPT as a language translator. This extends the accessibility of hacking, providing avenues for hackers to better understand their targets and submit reports.

Although I believe cybersecurity is becoming less predictable, I feel reassured by the ways that

hackers are revolutionizing the internet's immune system to keep organizations secure and make life harder for the bad guys.

Inside the Mind of a Hacker really spotlights that, and I hope you find it as insightful as I did.



Report Highlights

This edition of *Inside the Mind of a Hacker* analyzed 1000 survey responses from hackers on the Bugcrowd Platform, in addition to millions of proprietary data points on vulnerabilities collected across thousands of programs.

78%

of hackers believe that AI will disrupt the way they conduct penetration testing or work on bug bounty programs.

93%

of hackers are fluent in at least two languages.

84%

of hackers believe that there are more vulnerabilities now than at the start of the pandemic.

88%

of hackers believe that point-in-time security testing isn't enough to keep companies secure year round.

89%

of hackers believe that companies are increasingly viewing hackers in a more favorable light.

84%

of hackers believe that less than half of companies understand their true risk of being breached.

87%

of hackers believe that reporting a critical vulnerability is more important than trying to make money from it.

72%

of hackers do not believe AI will ever replicate their human creativity.

96%

of hackers agree that they help companies fill their cybersecurity skills gaps.

75%

of hackers identify non-financial factors as their main motivators to hack.

91%

of hackers believe that AI technologies have increased the value of ethical hacking or will increase its value in the future.

94%

of hackers plan to start using AI in the future to help them ethically hack.

HACKERS!

THEY'RE JUST LIKE US

This report does not feature a picture of a hacker doing a weekend Dunkin' run in sweats and sunglasses, but there's no doubt about it: hackers are **EVERYWHERE**. Society is slowly starting to ditch the hoodie-in-the-basement hacker stereotype and embrace the fact that like celebrities, *hackers are just like us*.

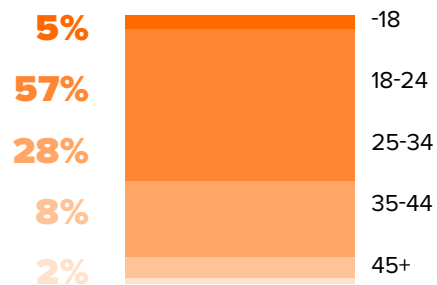
NUMBER OF LANGUAGES SPOKEN BY HACKERS

93% of hackers are fluent in at least two languages. Linguistic diversity enhances creativity and logical flexibility, equipping multilingual hackers to effortlessly switch between competing tasks and recognize changes in their environments.



AVERAGE AGE OF HACKERS

Hackers are multigenerational and younger than ever before. Millennials (born 1981–1996) represent slightly less than a third of all hackers, while 57% belong to Gen Z (born 1997–2012)—the largest and most ethnically diverse generation in history, according to the Pew Research Center (2020). Raised under the influence of the internet and other modern technologies, most hackers are highly engaged digital natives who recognize their responsibility in shaping a more secure future for everyone.



LANGUAGE TRANSLATION THROUGH AI

Hackers from non-English speaking countries are starting to use ChatGPT and other generative AI technologies as translators when hacking to better understand their targets and aid in writing and submitting reports. Although a lot of the internet is written in English, hackers find ways to leverage new technologies for increased accessibility.

TREND TO WATCH

Teenagers may be ditching traditional summer jobs like lifeguarding at the local pool. While hackers under 18 years old represent only 5% of all hackers, this number has over doubled since last year, and we expect it to keep rising. This could partly be a result of the increased accessibility of hacking. Using internet resources to learn how to hack has never been easier.

TOP 10 COUNTRIES WHERE PARTICIPATING HACKERS LIVE



India



United States



Nepal



Egypt



Brazil



Bangladesh



Pakistan



Turkey

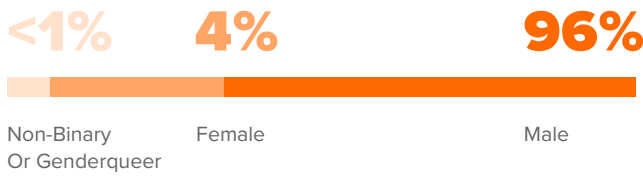


Indonesia



Vietnam

GENDER DIFFERENCES IN HACKERS



As well represented as hackers tend to be in their ages, geographic locations, and educational backgrounds, a stunning 96% are male.

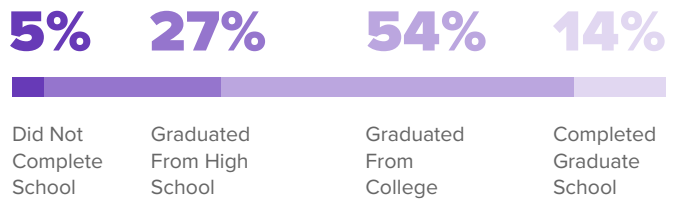
This glaring gender gap actually represents a decrease in female hackers since 2020, when 6% of hackers identified as female. One of the potential causes of this decrease could be the extra pressure the pandemic put on women. According to a study published by [UN Women](#), women did 29% more childcare per week than men during the pandemic. Given these additional responsibilities, it makes sense that there has been less time for women to dedicate themselves to professional endeavors such as hacking.

This gender gap poses a real, immediate threat to the diversity and multiplicity of perspectives that make crowdsourced security such a powerful force today.

HOW CAN I HELP?

By incentivizing women or nonbinary individuals with a broader scope of more accessible programs, organizations can empower a huge (and necessary) movement toward greater gender representation within the hacking community.

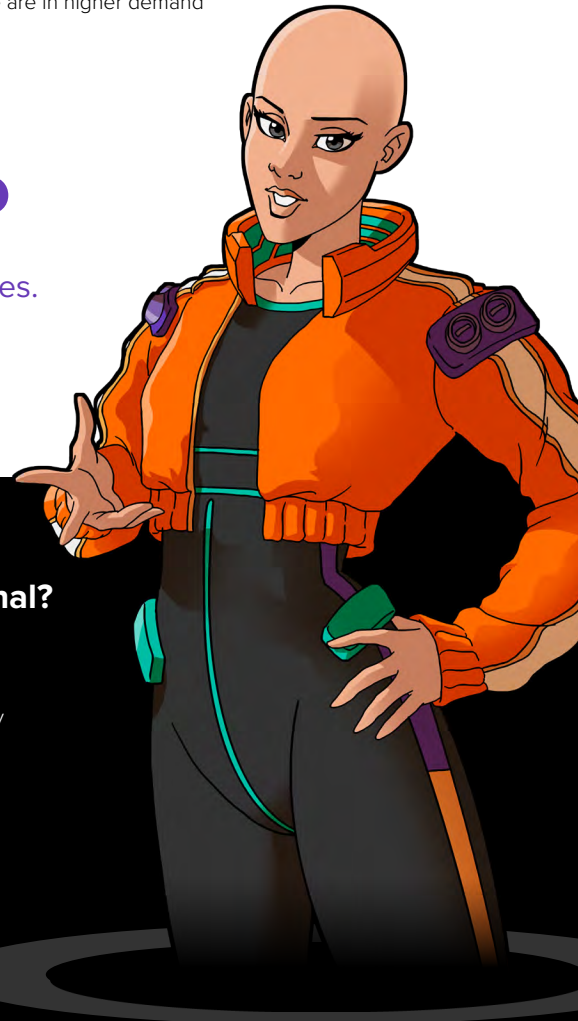
AVERAGE EDUCATION COMPLETED BY HACKERS



The stereotypes perpetuated by the media show two extremes in the hacking community—a genius working in a government control room who can hack anything in 10 seconds with a few furious keystrokes or a nerdy individual sitting in a dark room in their mom’s basement wearing a black hoodie speckled with Cheetos dust.

The hacker community is more aptly represented by a massive spectrum which can be seen in the average education completed. Hackers represent a well-educated subset of the population whose keen resourcefulness, critical thinking skills, and subject matter expertise are in higher demand now than ever before.

68%
of hackers are college graduates.



DEFINING “HACKER”

What’s the difference between a hacker and a cybercriminal?

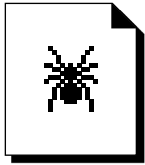
If you were to ask 10 people off the street, they’d probably all say that hackers and cybercriminals are the same. Merriam-Webster defines a “hacker” as “an expert at programming and solving problems with a computer.” While “hacker” is the dominant self-descriptor used by the cybersecurity community, this benevolent term has become synonymous with malice. The bad guys also call themselves hackers, and unfortunately, they are getting a lot of attention right now.

However, it is important to draw a line in the sand defining the difference between a hacker and a cybercriminal. An easy way to think of it is in terms of a locksmith and burglar.

LOCKSMITH — Hacker

BURGLAR — Attacker or Cybercriminal

In *Inside the Mind of a Hacker*, we refer to the good guys, aka the locksmiths, as hackers. Other terms you may have heard include ethical hackers, white hat hackers, and security researchers.



How well do you know hackers?

As hackers dive into a program, what sort of things are they looking for? What are the common challenges they face? What are their specializations?

Test your knowledge of hackers with this quiz

Yeah Nah

Nah Yeah



What percentage of hackers choose not to disclose a vulnerability because a company lacks a clear pathway for them to report it without risking legal consequences?

- A. 13%
- B. 28%
- C. 54%
- D. 72%



What percentage of hackers found a new vulnerability in the past 12 months that they had not encountered before?

- A. 9%
- B. 21%
- C. 48%
- D. 63%



70% of hackers identified what as their area of specialization?

- A. Web applications
- B. Network pen testing
- C. Recon/asset discovery
- D. Social engineering



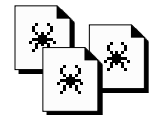
What is the top reason hackers give regarding what is stopping them from being more successful when hacking?

- A. Not enough scope
- B. Not having the physical technology needed
- C. Unresponsive program owners or brands
- D. Inadequate incentives



What is the number one reason hackers identify as to why they choose to hack on Bugcrowd's platform?

- A. To reduce the risk of breaches and reputation damage for companies
- B. To improve processes between security and engineering teams
- C. To connect with more lucrative programs and engagements
- D. To help companies accelerate their time to market securely



Answer 1: C. 54%

The threat of retaliation remains a real barrier to hackers' reporting of bugs, as does the inability to report a vulnerability securely without further compromising a company or its data. This number has decreased by 4% since last year, which indicates that more organizations are implementing VDPs. Backed by our crowd-powered SaaS platform, Bugcrowd VDP overcomes this challenge by providing organizations with a secure, monitored channel that anyone can use to report potential risks.

Answer 2: D. 63%

New vulnerabilities emerge every day, and the industry is struggling to keep up. Luckily, hackers are curious and creative by nature, dynamically finding these new bugs and always learning new skills. By working with hackers, organizations can level the playing field and proactively reduce their exposure risks.

Answer 3: A. Web applications

Throughout the years we've published this report, web applications have always been a hacker favorite. Other top specialties include network pen testing, recon/asset discovery, API assessment, and social engineering. Bugcrowd's CrowdMatch technology takes these specializations into account, dynamically matching the right trusted hackers to companies' needs and environments.

Answer 4: A. Not enough scope

A third of hackers report a lack of scope as the main roadblock to success when working with organizations. While every company's risk appetite is different, programs with a narrow scope typically stop hackers from identifying more impactful vulnerabilities. Entrusting hackers with greater latitude allows them to do their work more effectively and empowers companies to quickly reduce risk through more rigorous, holistic testing.

Answer 5: A. To reduce the risk of breaches and reputation damage for companies

Many organizations assume that hackers are only motivated by money, but most of the hacking community is driven by a desire to make the world a more secure place. Over half of hackers cited a desire to reduce the risk of breaches and reputation damage for companies.

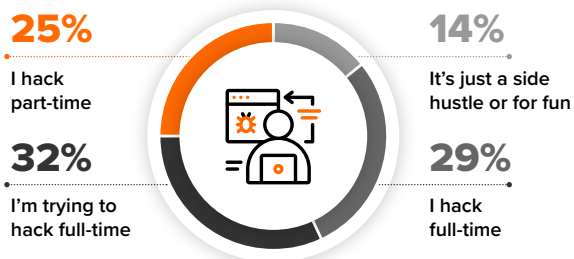
A Day in the Life of a Hacker

Although more and more companies are turning to hackers to expose critical vulnerabilities in their infrastructure, some organizations are still unsure whether they can be allies.

We get it; opening your organization up to crowdsourced security testing can be scary, especially when this means partnering with hackers, a group that is often misunderstood.

Inside the Mind of a Hacker digs deeper into who hackers are, what motivates them, and why you can trust them. What better way to get to know someone than by walking a mile in their shoes? Let's look at a day in the life of a hacker.

EMPLOYMENT STATUS OF HACKERS



When looking at a hacker's typical day, it's important to understand that many people hack full-time, while others approach it as a side hustle. Interestingly, only 29% of hackers report hacking full-time, a decrease from 42% just a year ago. However, 33% are part-time but trying to hack full-time. This number is almost double the 18% reported last year. This increasing interest indicates the attractiveness of hacking as a career and the heightened demand for crowdsourced security.

FORMULA FOR A GOOD SIDE HUSTLE

$$SH = (MN + E) \times P^F$$

SIDE HUSTLE = (Market Needs + Expertise) multiplied by Passion to the power of Flexibility

The rise of the side hustle can be attributed to many factors, including the pandemic, the rising cost of living, and an increasing desire for flexible work.

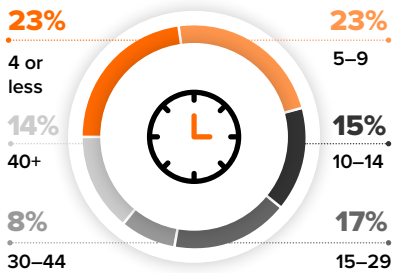
A good side hustle is characterized by several key factors. For example, a side hustle should be versatile and adaptable to changing market demands. However, perhaps more importantly, side hustles are driven by passion and expertise, allowing individuals to capitalize on their unique skills and knowledge. Side hustles also often focus on work-life balance and flexibility.

FIELDS UNRELATED TO SECURITY RESEARCH IN WHICH HACKERS HOLD OCCUPATIONS



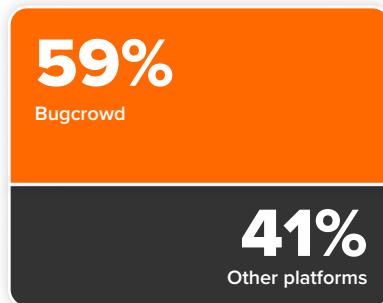
A DAY IN THE LIFE OF A HACKER

HOURS PER WEEK DEVOTED TO HACKING



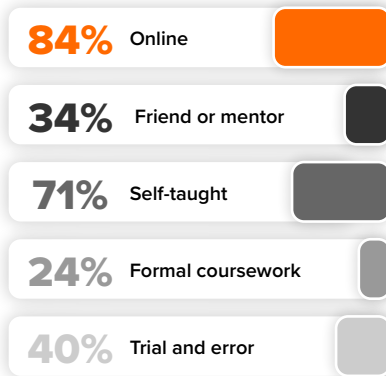
84% of hackers dedicate up to 14 hours a week to hacking. While some report working hours similar to most corporate professionals (14%), historical submission data indicate that hackers work fewer hours while earning an income similar to that of their salaried peers.

WHERE HACKERS CHOOSE TO SPEND THEIR TIME



Hackers are independent, free agents. Some choose to work across multiple platforms, while others focus primarily on one platform. The majority of hackers (59%) choose to hack with Bugcrowd, which represents a 14% increase from last year. The most cited reasons for this are Bugcrowd's superior triage services, fast response time, and supportive, collaborative community.

HOW HACKERS LEARN SKILLS



In our conversations with the hacker community, one constant that comes up every year is the fact that hackers use a diverse set of resources to increase their hacking skills. Hackers leverage a variety of online resources, work with mentors, and pursue traditional methods, such as academic or professional coursework. Many hackers also teach themselves how to hack, which often comes down to trial and error.

THE HACKING COMMUNITY

One might expect hackers who participate in bug bounty programs to be fiercely competitive, keeping their tactics secret to give them an advantage in their searches for vulnerabilities.

Although elements of competition exist, most would describe hackers as an extremely community-oriented group. From Twitter to YouTube, hackers are constantly sharing insights and tips to help their community grow their security skills. If you're a hacker looking for a place to start, we recommend checking out the free LevelUp content in [Bugcrowd University](#).

INDUSTRIES THAT HACKERS WORKED WITH ON THE BUGCROWD PLATFORM IN THE PAST 12 MONTHS

- Aerospace and defense
- Automotive
- Banking
- Civic and non-profit groups
- Chemicals
- Computer hardware
- Computer software
- Construction and building materials
- Consumer product manufacturing
- Consumer services
- Corporate services
- Electronics
- Energy and environment
- Financial services
- Food and beverage
- Government
- Hospitals and healthcare
- Holding companies
- Industrial manufacturing and services
- Insurance
- Leisure, sports, and recreation
- Media
- Pharmaceuticals and biotechnology
- Real estate
- Retail
- Schools and education
- Telecommunications
- Transportation

Hacking isn't reserved only to industries in the immediate realm of technology and computers. Hackers solve problems across every step of the global supply chain.

Security research plays a prominent—and often unnoticed—role in our everyday lives.

POSTER



Some links haunt you forever



I KNOW
WHAT YOU CLICKED
LAST SUMMER

Meet OrwaGodfather

A bug hunter and chef in Jordan

OrwaGodfather started hacking in 2020 without a security background or previous experience. He started by watching videos online and looking for leaks to quickly learn how to hunt. He got six bounties in his first month and was off to the races! Since then, Orwa has been awarded the MVP, P1 Warrior, and Top Bug Hunter: LevelUpX Champion Buggy Award.

Orwa is a chef and is passionate about helping empower others through education: “I donate 20% of every bounty I get to help people. In the past, I suffered from poverty, so I could not complete my studies and did not obtain certifications. I didn’t want to watch other people suffer from the same thing, so every year, I pay for the university fees of two people who can’t afford the fees.” In just three years of hacking, Orwa has been able to pay off his debt, travel for fun, buy his home, and continue helping others. We were inspired by Orwa’s success and story, so we sat down with him to get his thoughts on AI and the future of cybersecurity.

DO YOU THINK AI WILL REPLACE YOUR JOB AS A HACKER?

AI is great, but it will not replace me. There are some bugs and issues, just like any other technology. It can have an effect on my place in hacking, though. For example, automation has huge potential to help hackers. It can make things easier and save time. If I find a bug when performing a pen test and I don’t want to spend 30 minutes writing a report, I can start by using AI to write descriptions for me. **AI makes hacking faster.**

WHAT ADVICE DO YOU HAVE FOR COMPANIES USING OR CONSIDERING USING CROWDSOURCED SECURITY?

Many companies keep their scope too narrow, which isn’t in their best interest. Hackers are going to find those big bugs no matter what. It is best to incentivize the “good guys” to find them first.

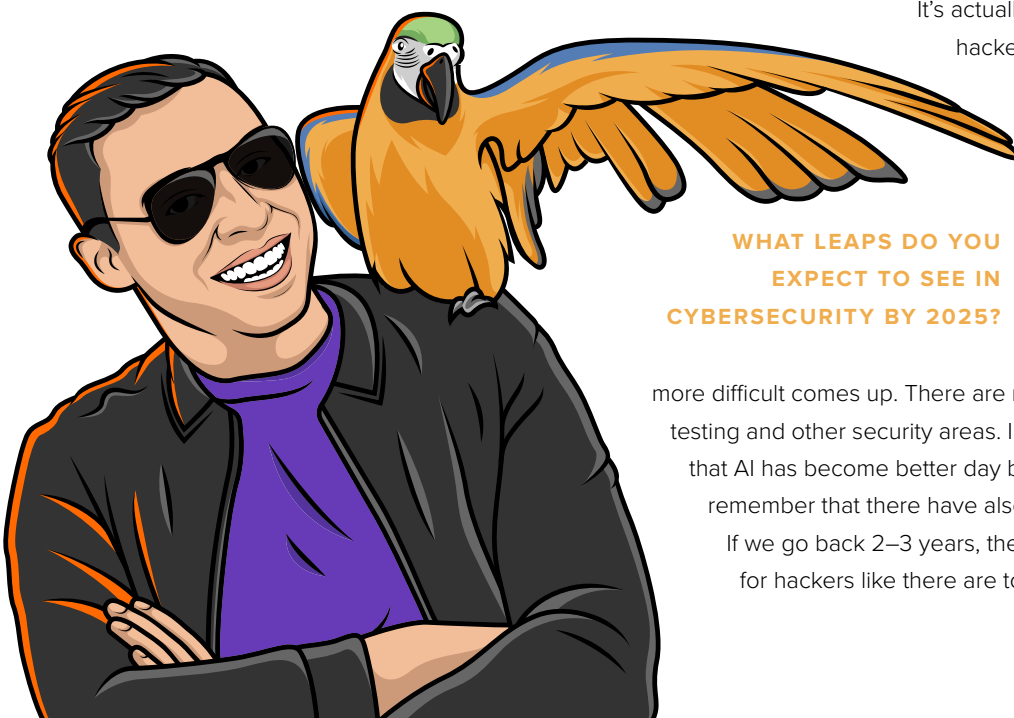
I’ve had mixed experiences submitting reports on bugs that are out of scope, but many companies still take them really seriously. They recognize the potential impact of these bugs.

HOW ARE MAINSTREAM PERCEPTIONS OF HACKERS CHANGING?

I’ve noticed changes over the past 2–3 years. I’m excited to be part of this new era. We’re not like what you see in movies, where hackers are portrayed as wearing hats or masks and just as dark characters. Hackers are normal people. It’s actually becoming very cool now to be a hacker. You can pay the bills with hacking, plus you can add these skills and accomplishments to your CV.

WHAT LEAPS DO YOU EXPECT TO SEE IN CYBERSECURITY BY 2025?

Over the last three years, I’ve seen a lot of changes in security. Every day, something new and more difficult comes up. There are many challenges, for example, in pen testing and other security areas. I expect huge leaps to come. I can see that AI has become better day by day, month by month. But we need to remember that there have also been huge leaps for patches and bugs. If we go back 2–3 years, there were no AI tools for bugs and reports for hackers like there are today.



THE ANATOMY OF A HACKER

23

75%

identify non-financial factors as their main motivators for hacking

68%

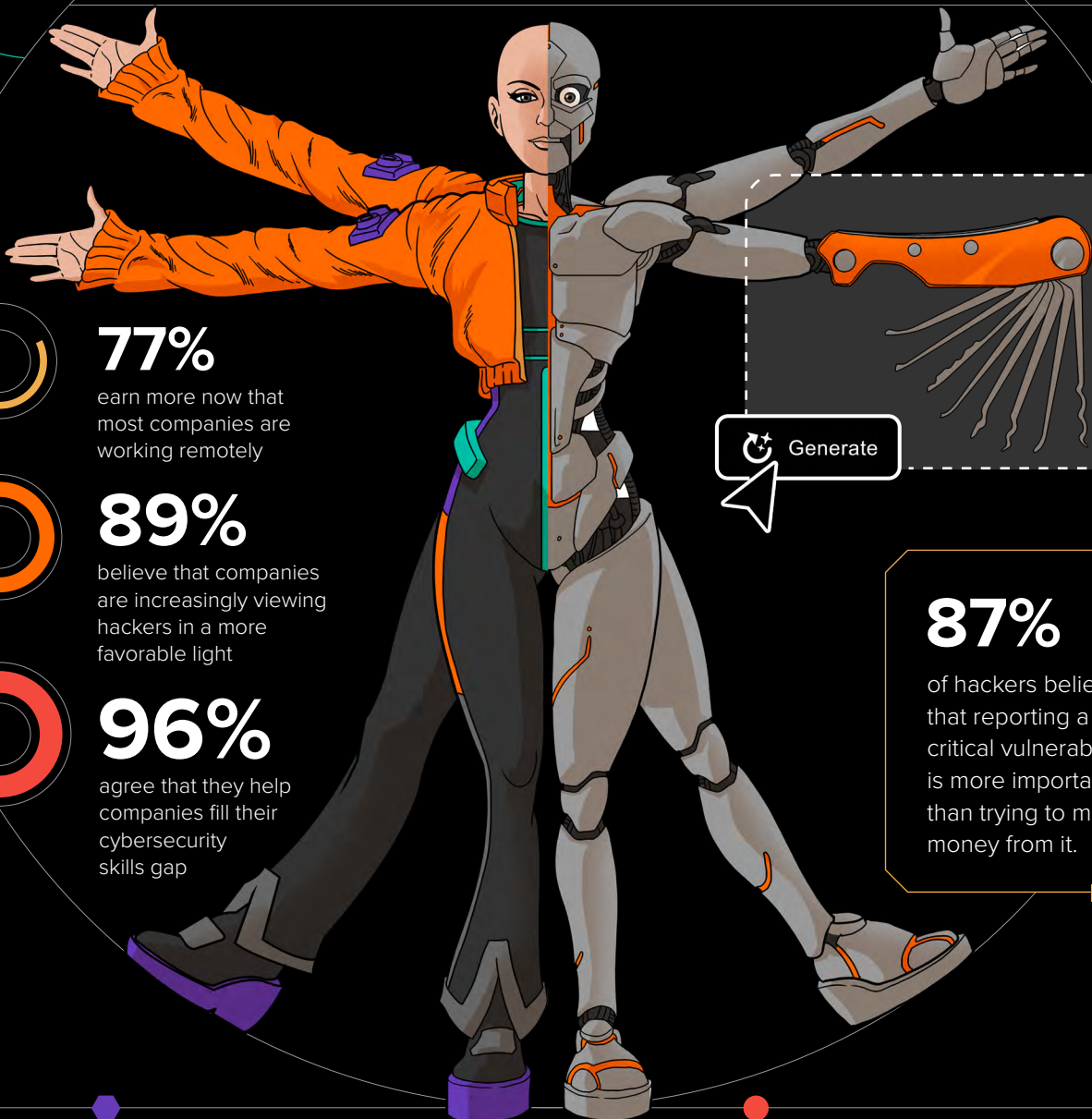
of hackers graduated from college

14%

of hackers completed graduate school

93%

of hackers are fluent in at least two languages



77%

earn more now that most companies are working remotely

89%

believe that companies are increasingly viewing hackers in a more favorable light

96%

agree that they help companies fill their cybersecurity skills gap

87%

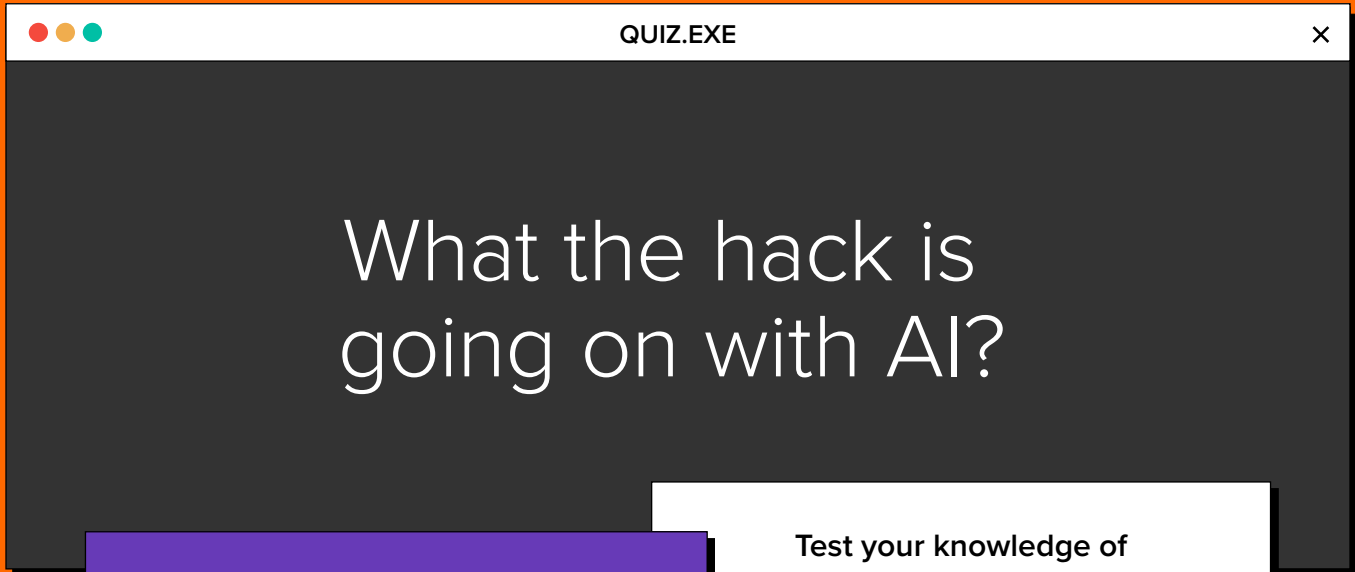
of hackers believe that reporting a critical vulnerability is more important than trying to make money from it.

50%

engage with a social or community group related to security

60%

follow news about cybersecurity and the latest breaches for tips on where to look next



How are hackers using generative AI technologies? What do hackers really think about AI?

Test your knowledge of generative AI with this quiz

Yeah Nah Nah Yeah

1 What percentage of hackers currently use generative AI in an aspect of their lives?

A. 52% B. 64% C. 79% D. 85%

2 What percentage of hackers believe that generative AI will never outperform hackers?

A. 28% B. 45% C. 57% D. 84%

3 Which AI chatbot is not among the most frequently used in hackers' security research workflows?

A. Chatsonic B. ChatGPT
C. Google Bard D. Bing Chat AI

4 What is the top use case for generative AI technologies in the hacking community?

A. Analyzing data B. Identifying vulnerabilities
C. Validating findings D. Automating tasks

- Answer 1: D. 85%
- Answer 2: B. 45%
- Answer 3: A. Chatsonic
- Answer 4: D. Automating tasks

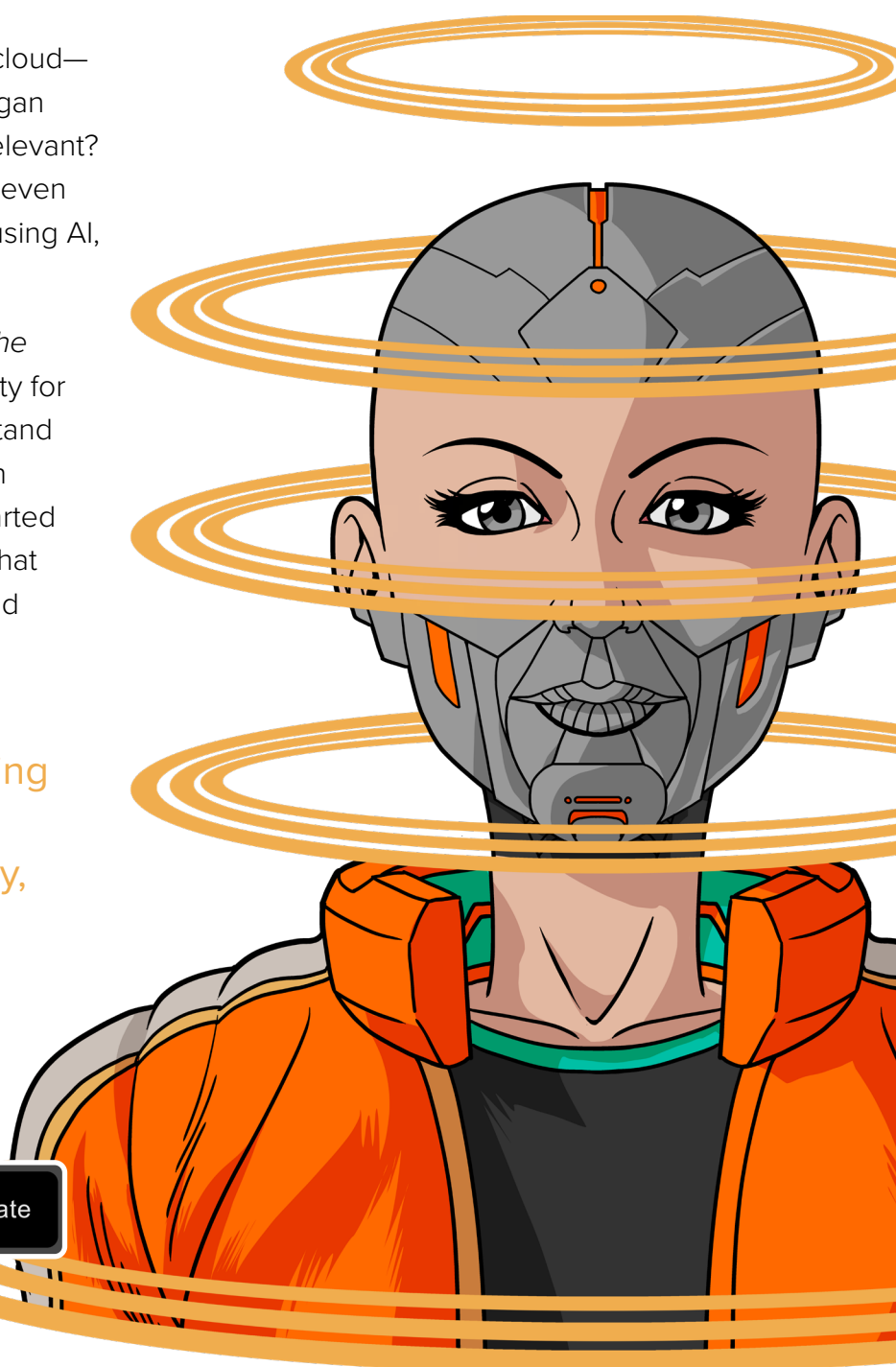
The Generative AI Hacking Revolution

How Hackers Are Using AI Technologies to Increase the Value of Their Work

For so long, AI felt like a looming storm cloud—distant yet ominous. Then, questions began surfacing. Is AI going to make my job irrelevant? How will AI make my life easier? Does it even make sense for me to use AI? If I'm not using AI, does that make me out of touch?

Every year, Bugcrowd publishes *Inside the Mind of a Hacker* to create an opportunity for the security community to better understand hackers and the crucial roles they play in the fight against cyber threats. As we started writing this edition, there was no doubt that addressing some of the questions around AI was paramount.

The internet is full of fear-mongering articles covering the terrifying consequences AI could have on cybersecurity, but what about ways hackers can use AI to make the world a safer place?

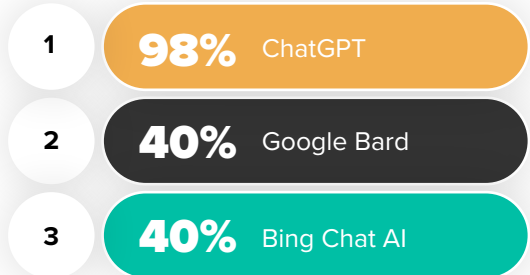


TOP AI TECHNOLOGIES USED

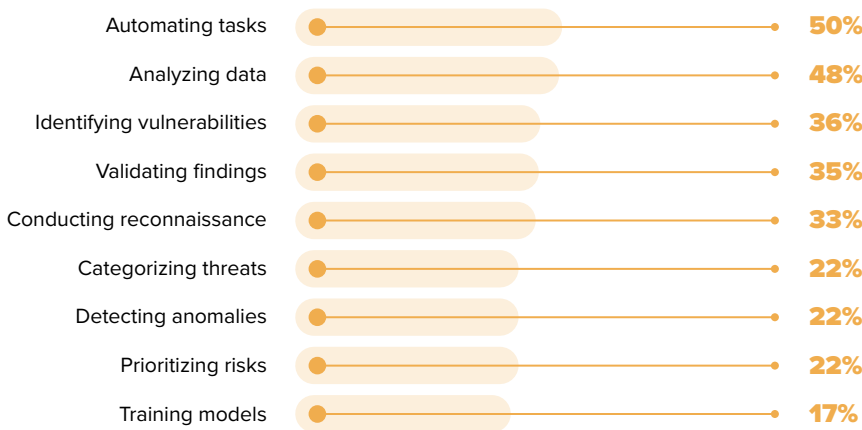
We asked both hackers who currently use AI and those who plan to start using AI which chatbots they'll use in their security research workflows. Both groups overwhelmingly answered the same thing: ChatGPT, Google Bard, and Bing Chat AI. Although AI chatbots are certainly in vogue, they aren't the only way hackers are leveraging AI.

We're seeing signs that point to hackers being early adopters of AI technologies, as they are constantly testing out different use cases to be more well-rounded and efficient at their jobs.

Top three AI chatbots used for hacking



Top use cases for AI in security research

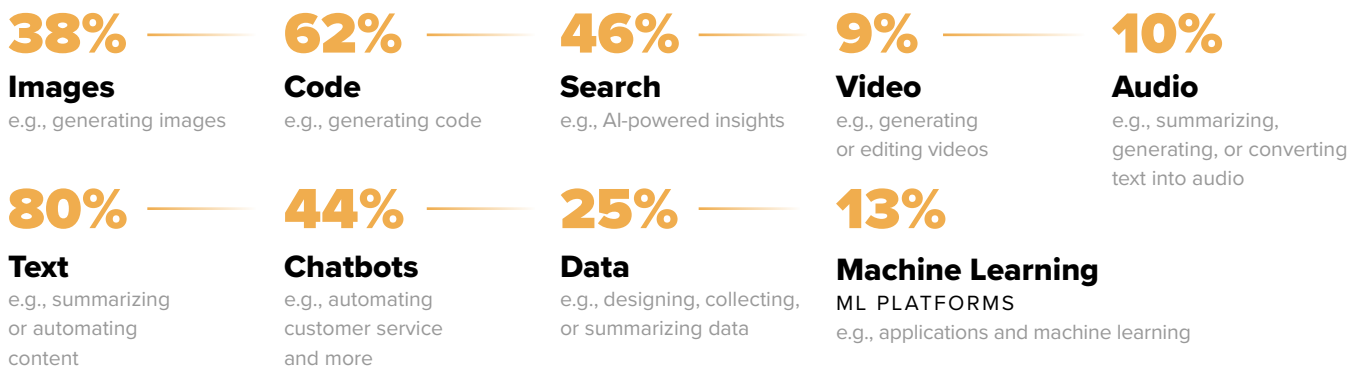


Even though we are currently in the early adoption of AI technology, it is fascinating to see the variety of ways hackers are leveraging AI. Although automating tasks and analyzing data are the top use cases for AI, hackers are using AI in increasingly new ways, including conducting reconnaissance, identifying variabilities, and validating risks.

Sincerely, AI

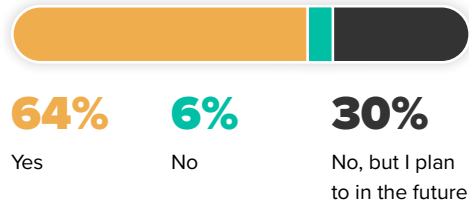
A trending use case for AI we're seeing from our survey and hacker interviews is using AI chatbots to help hackers write reports. Many find the initial text generated by AI to be a good jumping off point, especially for hackers who find writing reports cumbersome or time intensive.

Generative AI technology types used by hackers



USING AI FOR HACKING

Do hackers use generative AI technologies as part of their hacking workflow?



85% of hackers have used generative AI technologies

but so far, only 64% are using AI specifically in their security research workflow. This number is expected to increase, with 30% of hackers reporting that they plan to start using AI in the future to help them hack.

5 WAYS ATTACKERS ARE USING AI

Now that we've seen the top use cases for hackers using AI in security research, let's look at some of the top ways attackers are leveraging AI. According to the [World Economic Forum](#), the top five risks include:

BUILDING BETTER, MORE SOPHISTICATED MALWARE

In the hands of hackers, generative AI can be used to generate hard-to-detect malware strains and execute attacks. Combined with AI models, malware could mask its intention until it fulfills its ill purpose.



WRITING AI-POWERED, PERSONALIZED PHISHING EMAILS

With the help of generative AI, phishing emails no longer have the tell-tale signs of a scam—such as poor spelling, bad grammar, and lack of context. Plus, with AI like ChatGPT, threat actors can launch phishing attacks at unprecedented speed and scale.



GENERATING DEEP FAKE DATA

Since it can create convincing imitations of human activities—like writing, speech, and images—generative AI can be used in fraudulent activities such as identity theft, financial fraud, and disinformation.



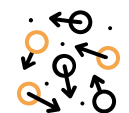
CRACKING CAPTCHAS AND PASSWORD GUESSING

Used by sites and networks to comb out bots seeking unauthorized access, CAPTCHA can now be bypassed by hackers. By utilizing ML, they can also fulfill other repetitive tasks such as password guessing and brute-force attacks.



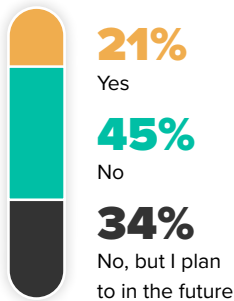
SABOTAGING ML IN CYBER THREAT DETECTION

If a security system is overwhelmed with too many false positives, a hacker can take it by surprise with a real cyberattack.



GENERATIVE AI AND HACKERS

Do generative AI technologies outperform the abilities of hackers?



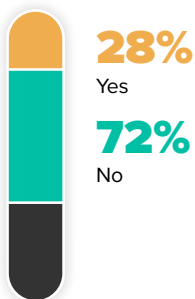
The BIG question—will AI outperform me and make my job irrelevant? Interestingly, 21% of hackers believe that AI is already outperforming them. Compare this to 45% who believe AI will never outperform hackers. A third of hackers believe that AI will outperform them in the next five years. This means that a shocking 55% of hackers believe AI technology will outperform them in the next five years, if not already.

This edition of *Inside the Mind of a Hacker* includes multiple hacker spotlights, on some of the top hackers in the industry. It's interesting to compare their qualitative responses to this question versus the survey data. **Many of the top hackers in the industry don't feel threatened by AI. Instead, they see it as a tool that can give them a competitive edge.**

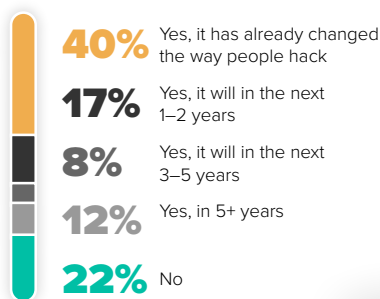
A LOOK BACK

In 2020, we asked hackers this same question, and 78% said that they believe hackers will continue outperforming AI technologies for the next 10 years. Just three years later, it's clear that the percentage is decreasing. This can partly be attributed to the massive leaps generative AI technologies have made recently, becoming increasingly commonplace in everyday life.

Will generative AI technologies eventually replicate the human creativity of hackers?



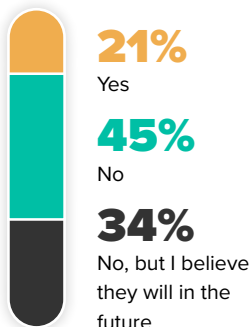
Are generative AI technologies disrupting the way hackers work on penetration testing or bug bounty programs?



A whopping 78% of hackers believe that AI will disrupt the way hackers work on penetration testing or bug bounty programs sometime in the next five years, with 40% of hackers reporting that AI has already changed the way people hack.

Hackers are trending toward embracing AI and the many changes it will have on their day-to-day lives, but most hackers still have doubts about how far AI can actually go. 72% of hackers do not believe AI will ever replicate their human creativity.

Can generative AI technologies increase the value of hacking and security research?



91% of hackers believe that AI technologies have increased the value of hacking or will increase its value in the future.

A WORD FROM THE U.S. DEPARTMENT OF DEFENSE

According to the [U.S. Department of Defense](#), "The value of harnessing AI in cybersecurity applications is becoming increasingly clear. Amongst many capabilities, AI technologies can provide automated interpretation of signals generated during attacks, effective threat incident prioritization, and adaptive responses to address the speed and scale of adversarial actions. The methods show great promise for swiftly analyzing and correlating patterns across billions of data points to track down a wide variety of cyber threats of the order of seconds. Additionally, AI can continually learn and adapt to new attack patterns—drawing insights from past observations to detect similar attacks that occur in the future."

The Heart of Hacking

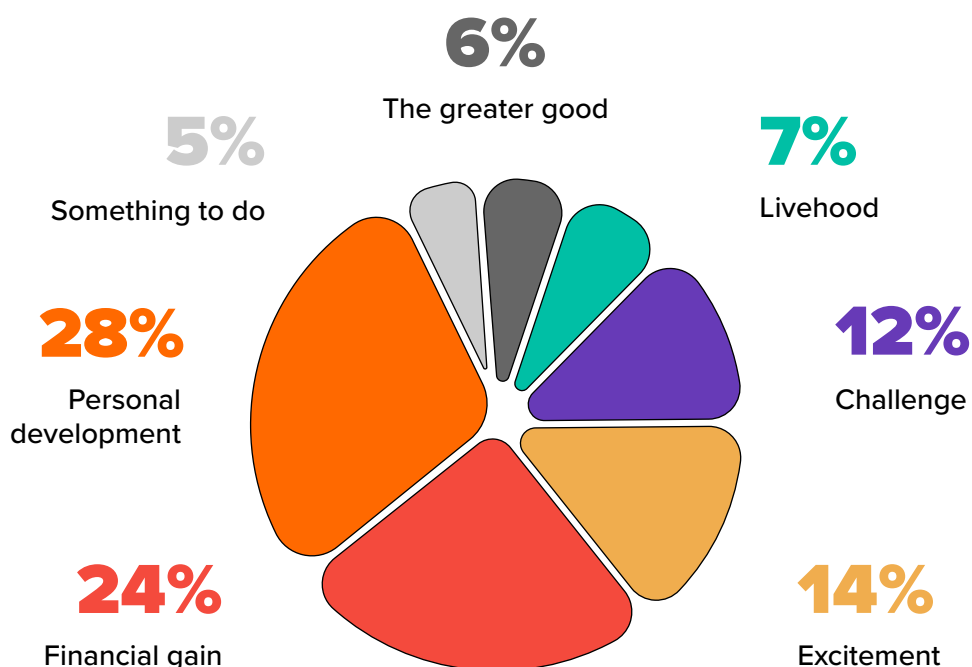
So much of *Inside the Mind of a Hacker* is focused on breaking hacker stereotypes by addressing fears rooted in dated pop culture portrayals and general misinformation. Understanding hackers' motivations can help companies embrace the talent of the Crowd.

By better understanding why hackers love their work and why they love working with Bugcrowd, we can learn how these hackers are making the world a better place. This knowledge can especially help companies that leverage or are considering leveraging crowdsourced security, as it will leave them better equipped to cultivate great future partnerships with our hackers.

WHY HACK?

While money matters to some, **75% of hackers identify non-financial factors as their main motivators to hack.**

They hack to develop personally, challenge themselves, seek excitement, and give back to the community.

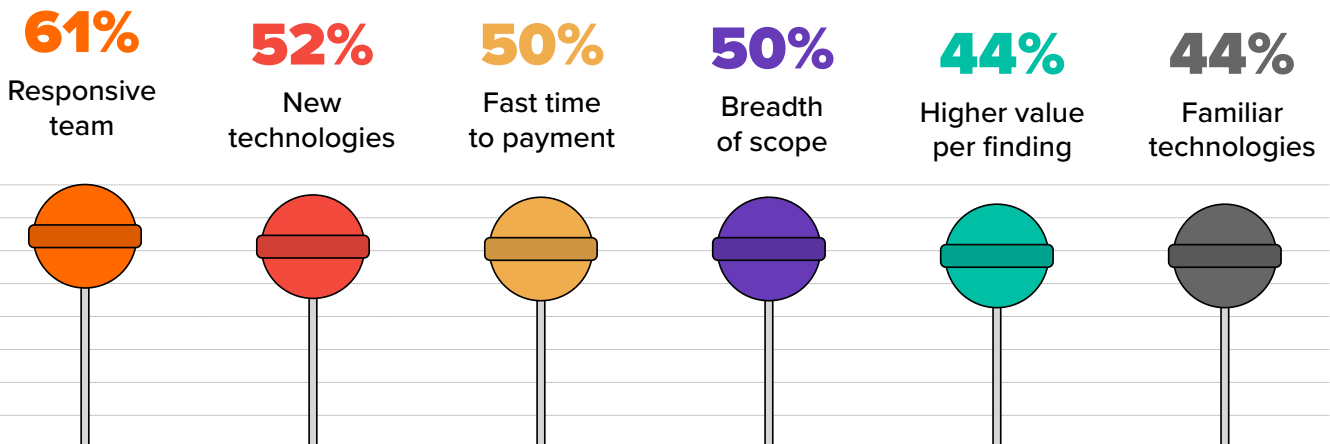


LEADING REASONS WHY HACKERS CHOOSE A PROGRAM OR ENGAGEMENT

There is a common misconception that hackers are drawn to programs that pay the most; however, our findings suggest that hackers take a much more holistic approach when assessing their professional opportunities.

Over the past two years, “working with a responsive team” has been overwhelmingly the top reason for choosing a program. Interestingly, “fast time to payment” dropped from the top three reasons last year to one of the least cited reasons this year.

This supports our finding that **hackers’ motivations are complex and multi-faceted.**

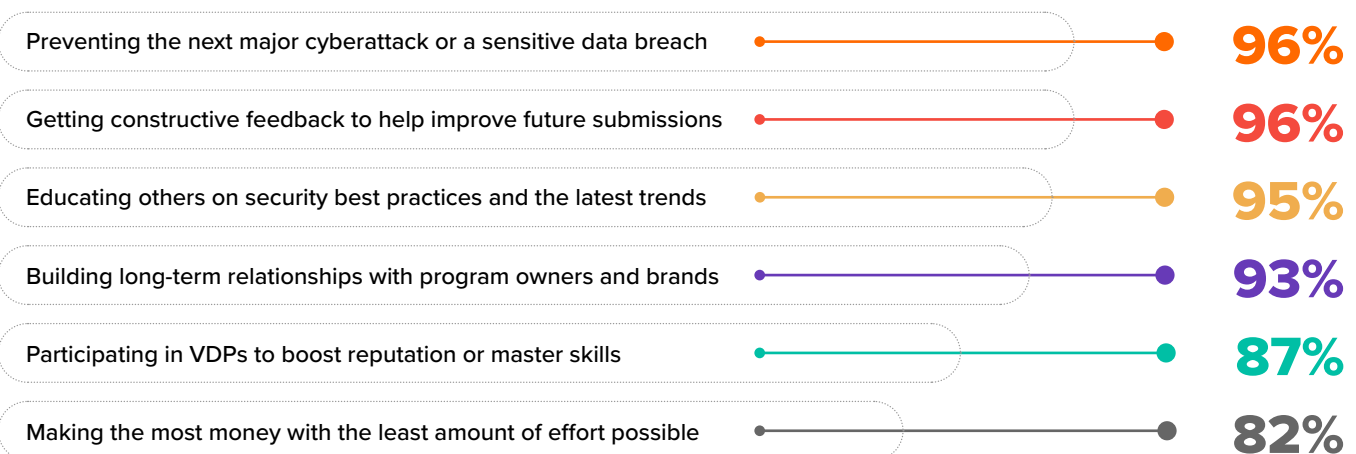


MOST IMPORTANT ISSUES WHEN HACKING ON BUGCROWD

We asked hackers to rate common reasons why people hack on a scale from very important to not important at all. The issues that hackers rate as important when hacking on Bugcrowd highlight their heightened sense of community and growth.

Ultimately, hackers care about preventing the next major cyberattack or a sensitive data breach. They hack to make the world a more secure place.

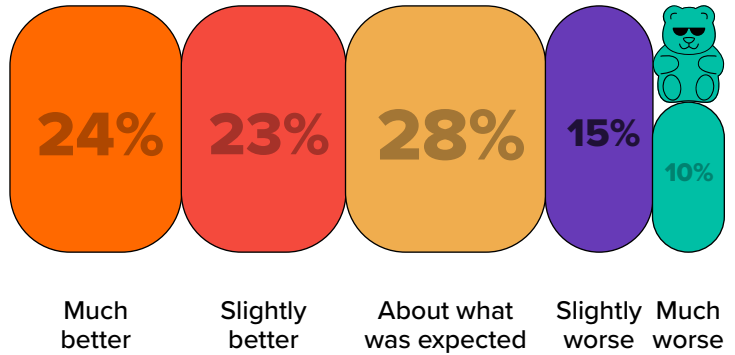
Other top reasons include professional growth and educational opportunities—as both teachers and students. Hackers care about learning to improve future submissions and educate others on security best practices.



PERCEPTIONS OF EARNINGS FROM HACKING

Although financial motivations are not the primary reasons why hackers hack, they are certainly important considerations.

The majority of hackers have a positive opinion about the income they earn from security research, with 75% reporting earning what they expected or even better. This positive trend highlights global organizations' increasing adoption of—and investment in—hacking.

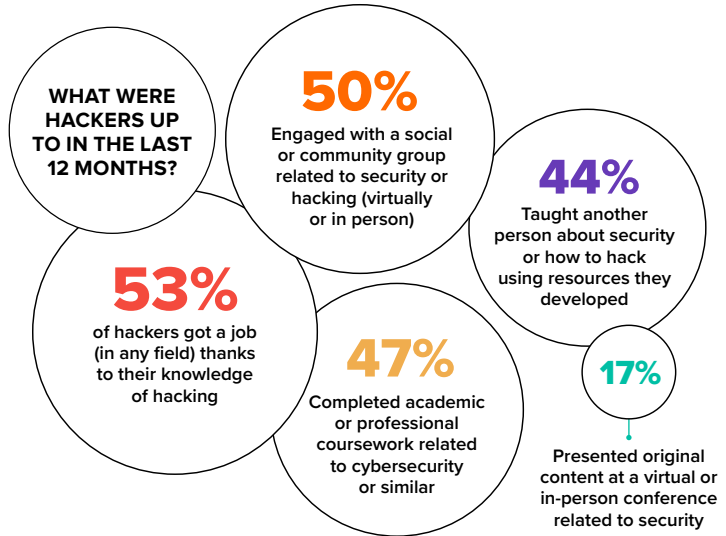


CAREER OPPORTUNITIES AND GROWTH

Hackers actively pursue their careers the same way other professionals do; they seek networking opportunities through community groups and conferences, they mentor others, and they supplement their skills with academic coursework and certifications.

Over half of all hackers use the skills they learn about hacking as a stepping stone to get a new job.

This evidence shows the increased legitimacy of hacking as a career, not just a side hustle.



TOP_FIVE_REASONS_HACKERS_CHOOSE_BUGCROWD.EXE

1

TO REDUCE
the risk of breaches and reputational damage for companies

2

TO CONNECT
with more lucrative programs and engagements

3

TO IMPROVE
processes between security and engineering teams

4

TO HELP
companies accelerate their time to market securely

5

TO IMPROVE
the performance and ROI of security in companies

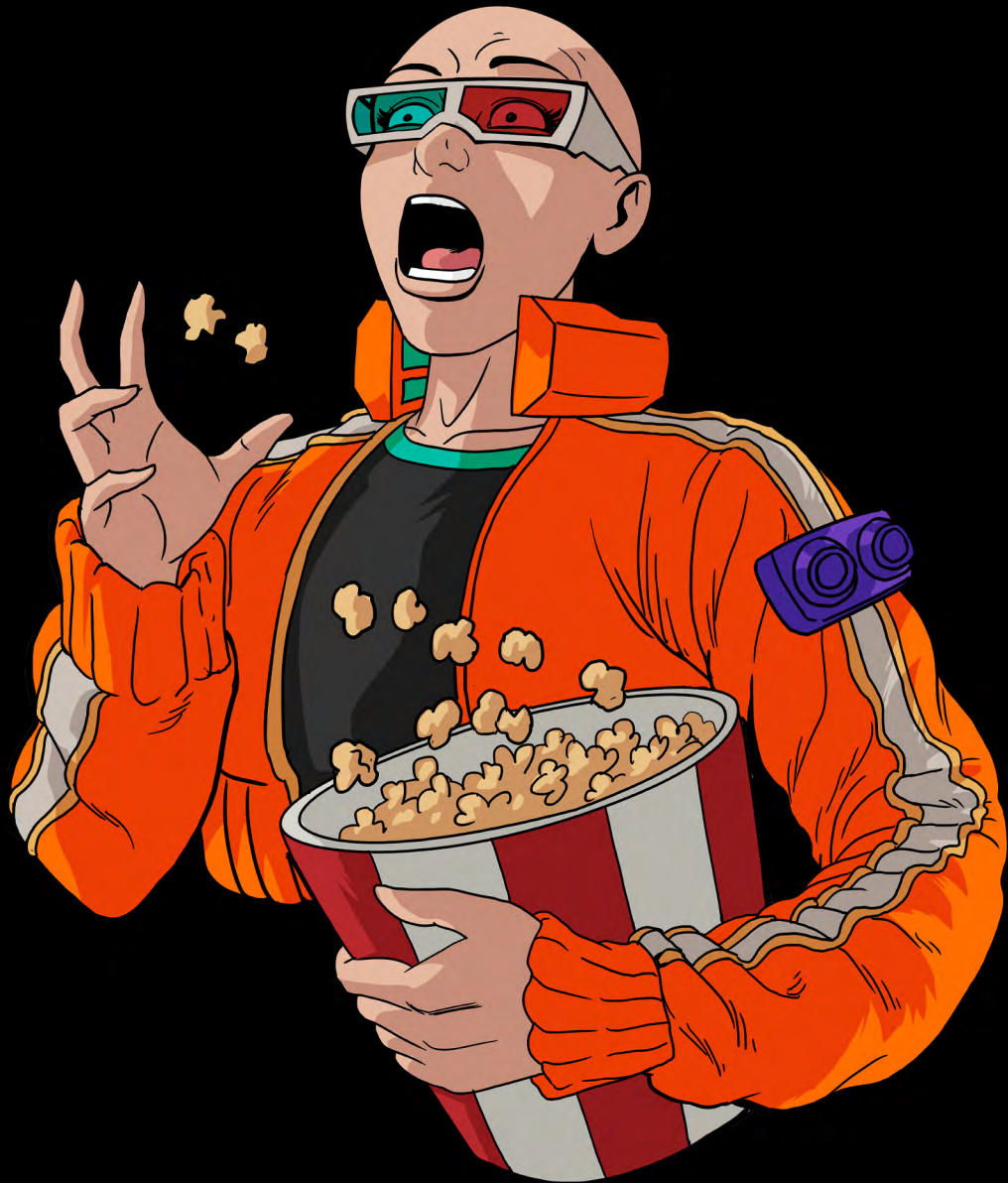
WHY_BUGCROWD.EXE

83% of hackers believe Bugcrowd offers more opportunities to be successful than other platforms

SNEAK PEEK

A BUGCROWD ORIGINAL SERIES

UNSOLVED CYBER
mysteries



COMING SOON **bugcrowd**

Meet Nerdwell

An award-winning hacker with 20 years of experience in cybersecurity

Over the Christmas holidays in 2018, Nerdwell decided to give bug bounty programs a try. He had been working in cybersecurity for over a decade, and he had watched the bug bounty industry emerge. In just five short years, he has received multiple awards from Bugcrowd, including MVP and Level 4 P1 Warrior recognition.

Nerdwell's experience makes him an integral part of the hacking community, and he enjoys networking and sharing knowledge with fellow hackers. Check out some of his thoughts on generative AI and the future of cybersecurity.

SHOULD HACKERS FEEL THREATENED BY AI?

My personal view has always been, especially in technology, that if you're

not growing, your knowledge is shrinking because everything else is changing around you. **If you're stagnant and don't grow your skills, then maybe you should be worried about AI, but if you embrace it and use it as a tool, then I believe you'll likely become even more valuable.**

WHAT CHANGES DO YOU EXPECT TO SEE IN CYBERSECURITY IN THE NEXT TWO YEARS?

I predict that the rapidly changing geopolitical

landscape will drive the biggest changes in the next few years. Industries that didn't think they were valuable targets before are finding that they actually are targets, while the ones who already knew that they were targets are seeing compromises become more impactful.

DO YOU THINK AI WILL REPLACE HACKERS?

I've done a fair amount with AI, and as impressive as it is, I don't think it will be replacing humans for quite some time, if ever. AI is very good at what it does—pattern recognition and applying well-known solutions to well-known problems. Humans are biologically designed to seek out novelty and curiosity. Our brains are literally wired to be creative and find novel solutions to novel problems.

DO COMPANIES REALLY UNDERSTAND THEIR RISK OF BEING BREACHED?

It varies a lot. Awareness has increased a lot, and breaches are in the news cycle more every day, so the mentality around security is changing.

I've worked with companies of all sizes, and from what I've seen, small businesses and startups tend to think a breach won't happen to them. Once they become medium-sized businesses, the transition toward better security programs is really difficult because now they're big enough to really be targeted, but not big enough to have the resources to dedicate to security.

A challenge from the large enterprise side is that even though you have the awareness of risk, you have all of this legacy stuff, and your attack surface is probably a lot bigger than most teams anticipate. **Basically, what I'm saying is that regardless of company size, there is always risk.**

WHAT DO YOU WISH COMPANIES UNDERSTOOD ABOUT HACKERS (BOTH ETHICAL AND MALICIOUS)?

My advice to both groups is that you don't want to underestimate hackers. I still get the impression that companies envision hackers as people in their mothers' basements who haven't seen the light of day in a month when, in reality, **hackers are a well-funded, well-organized, professional group of people, whether malicious or not.**



Meet David Fairman

CIO and CSO of Netskope

When it comes to cybersecurity expertise, look no further than David Fairman. David has over 20 years of security experience in a range of disciplines from fraud and financial crime to business continuity to operational risk. He's worked for, and consulted to, several large financial institutions and Fortune 500 companies across the globe, has been recognized as one of the top CISOs to know, is a published author, an adjunct professor, and was involved in founding several industry alliances with the aim of making it safer to do business in the digital world.

For the past three years, he's been Chief Information Officer and Chief Security Officer for the Asia Pacific region at Netskope. Netskope is a global SASE leader helping organizations apply zero trust principles to protect data and modernize their security and network infrastructure. Netskope has been a Bugcrowd customer for over a year.

We chatted with David about the potential cybersecurity risks of generative AI and evolving roles of security professionals.

HOW ARE GENERATIVE AI APPLICATIONS REVOLUTIONIZING THE WAY ORGANIZATIONS OPERATE, AND WHAT ARE THE POTENTIAL CYBERSECURITY RISKS ASSOCIATED WITH THEIR USE?

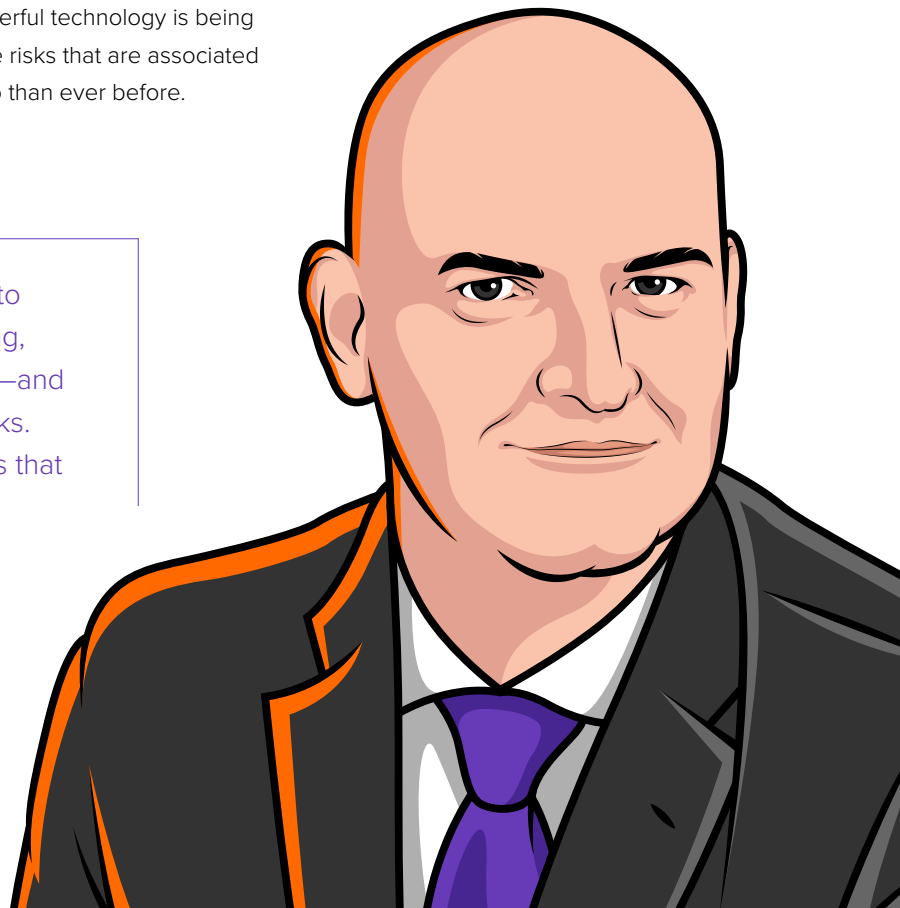


AI has been around for many years, so there are a number of risks associated with AI. AI is transforming business through hyper-automation, identifying new business models and trends, speeding up decision

making, and increasing customer satisfaction. Prior to late 2022, AI required specialized skill sets and vast amounts of training data; consequently, it was not used in the mainstream. The launch of ChatGPT made generative AI accessible to the masses. The barrier to entry has lowered, which means the adoption and use of this powerful technology is being taken up at a rapid pace. This means the risks that are associated with AI can have a large impact, more so than ever before.



There are a number of risks that need to be considered, including data poisoning, prompt injection, and model inference—and these are just a few of the technical risks. There are also responsible AI elements that need to be considered, such as bias and fairness, security and privacy, robustness and traceability.



WHAT ARE THE POSSIBLE WAYS SENSITIVE DATA CAN BE INADVERTENTLY EXPOSED THROUGH GENERATIVE AI APPLICATIONS, AND HOW CAN ORGANIZATIONS MITIGATE THESE RISKS?

Generative AI uses prompts to take inputs from a user and produce an output based on its logic and learning. Users

can input sensitive data, such as personal information and proprietary source code into the large language model (LLM). This information could then be accessed or produced as output for other uses of the LLM. Users should be cognizant of the fact that any data they input into an LLM will be treated as public data.

Many organizations are asking—should we permit our employees to use generative AI applications like ChatGPT or Bard? The answer is yes, but only with the right modern data protection controls in place.

WHAT IMPACT DOES THE USE OF GENERATIVE AI HAVE ON THREAT ATTRIBUTION, AND COULD IT BLUR THE LINES BETWEEN ADVERSARIES, MAKING IT CHALLENGING FOR ORGANIZATIONS OR GOVERNMENTS TO RESPOND EFFECTIVELY?

There are two sides to this question. On one hand, defenders will be able to use AI to perform threat attribution (and threat intelligence more broadly) to speed up the process, better defend their organizations, and respond more effectively than ever before. Conversely, threat actors will be using this to their advantage to increase their capability to attack—at a scale and velocity never seen before.

We, the defenders, need to lean into how we can leverage this to transform our defensive capabilities.

COULD GENERATIVE AI APPLICATIONS LEAD TO THE DEVELOPMENT OF “SELF-HEALING SYSTEMS,” AND IF SO, HOW MIGHT THIS CHANGE THE WAY ORGANIZATIONS APPROACH CYBERSECURITY?

I think this has to be the case. I've said this for a long time—we need to find ways to operate at machine speed. When we talk about 'mean time-to-detect' and 'mean time-to-contain,' we're reliant on human beings in the process, which

can slow it down significantly. We know that time is critical when it comes to defending an organization—the faster, more efficiently we do this, the better we will protect our companies and customers. Self-healing systems will be one piece in this jigsaw puzzle.

AS GENERATIVE AI BECOMES MORE PREVALENT IN CYBERSECURITY, HOW DO YOU THINK THE ROLE OF SECURITY PROFESSIONALS WILL EVOLVE, AND WHAT IMPLICATIONS DOES A FUTURE WITH MORE HUMAN-MACHINE COLLABORATION HAVE FOR INFORMED DECISION MAKING IN CYBERSECURITY?

I think cyber practitioners increasingly become the 'trainers' of AI—using their cyber expertise to train models to perform cyber analysis at pace and at scale. There

will always be a need to have a human in the loop in some respect, whether that be in the training of the model, the monitoring and supervision of the model (to ensure that it is behaving the way it is expected and is not being manipulated), or in the generation of new models.

Hackers Tapped to Keep AI Safe

OpenAI says working with ethical hackers helps it keep users and systems secure

A whopping 98% of hackers who use AI have used ChatGPT. When narrowing the results to hackers who have used AI specifically in their hacking or security research workflow, 85% have used ChatGPT. ChatGPT is by far the most commonly used generative AI chatbot in the hacking community.

This edition of *Inside the Mind of a Hacker* looks extensively into how the hacking community is using AI to augment security research workflows, but let's explore how one of the most forward-thinking AI platforms is harnessing the power of the hacking community.

In April 2023, OpenAI launched a bug bounty program on the Bugcrowd platform. OpenAI is the research and deployment company pioneering the common adoption of generative AI, and is widely known for its AI services, including ChatGPT. Its mission is to shape the future of humanity by building safe and beneficial artificial general intelligence.

OpenAI announced its bug bounty program as an initiative essential to its commitment to developing safe and advanced AI. Furthermore, it aims to demonstrate this commitment to security in a public and transparent way.

Therefore, it turned to the power of the Crowd to allow it create technology and services that are secure, reliable, and trustworthy, all while developing and releasing features at a remarkable rate, and introducing the concept of AI to the market. According to the OpenAI website,

“We recognize the critical importance of security and view it as a collaborative effort.”

The program recognizes and rewards the valuable insights of hackers who submit bugs, knowing that their contributions, diversity of skill, and ability to scale are key to securing their groundbreaking technologies. At the time of the launch, OpenAI was offering cash rewards based on the severity and impact of the reported issues, ranging from \$200 for low-severity findings to up to \$20,000 for exceptional discoveries.



In the first two months of the program's implementation, roughly 50 vulnerabilities were rewarded, with an average payout of \$600. The OpenAI bug bounty launch attracted the most interest of any program launch or internet event in Bugcrowd's decade-long history, garnering more submissions from interested hackers in the first three days than Log4J did in three months.

In speaking to the hacking community, OpenAI said,

“We believe that transparency and collaboration are crucial to addressing this reality.”

That's why we are inviting the global community of security researchers, ethical hackers, and technology enthusiasts to help us identify and address vulnerabilities in our systems. Your expertise and vigilance will have a direct impact on keeping our systems and users secure.”

Cybersecurity Red Flags

As Told by Hackers

▶ **RED FLAG 1**

Security Breach Potential

84% of hackers believe that less than half of all companies understand their true risk of being breached.

Only 2.5% of hackers believe that 75–100% of companies understand their true risk of being breached.

▶ **RED FLAG 3**

Point-In-Time Testing

88% of hackers believe that point-in-time security testing isn't enough to keep companies secure year round.

▶ **RED FLAG 5**

Lack Of A VDP

Over half of all hackers have not disclosed a vulnerability because a company lacked a clear pathway for reporting it without risking legal consequences.

▶ **RED FLAG 2**

Increased Vulnerabilities And Complexity

84% of hackers believe that there are more vulnerabilities now than at the start of the pandemic.

75% of hackers believe it's becoming more difficult to find vulnerabilities in critical assets.

▶ **RED FLAG 4**

Privacy Vs. Cost Savings

Over one-third of hackers believe that at least half of all companies are willing to sacrifice their customers' long-term privacy and/or security to save money in the short-term.

▶ **RED FLAG 6**

Not Enough Scope

One-third of hackers report that programs without an adequate scope stop them from being successful.

Cybersecurity red flags are practices, attitudes, and trends in the security market that hackers are flagging as areas of concern. Count up your red flags, and get your results below!



0-1 RED FLAGS

You've achieved Cyber Expert Status!

Congratulations! Your security program is mature and ahead of many organizations, but note that security is an ongoing journey.

2-4 RED FLAGS

Not bad, but needs improvement.

You're already doing a lot in terms of your cybersecurity, but all it takes is one critical vulnerability for disastrous results to occur. Consider using crowdsourced security to strengthen your efforts.

5-6 RED FLAGS

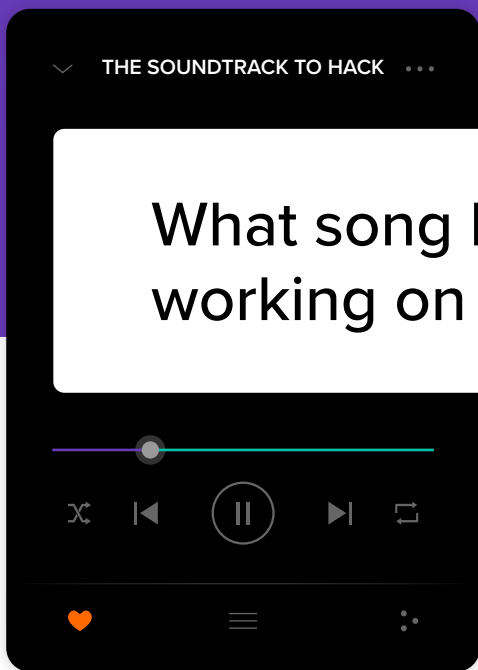
Time to break up with your security provider.

Don't worry—between the cybersecurity skills gap and the rapidly changing landscape, it's hard to keep up. Consider using crowdsourced security to strengthen your efforts.

The Secret Social Lives of Hackers

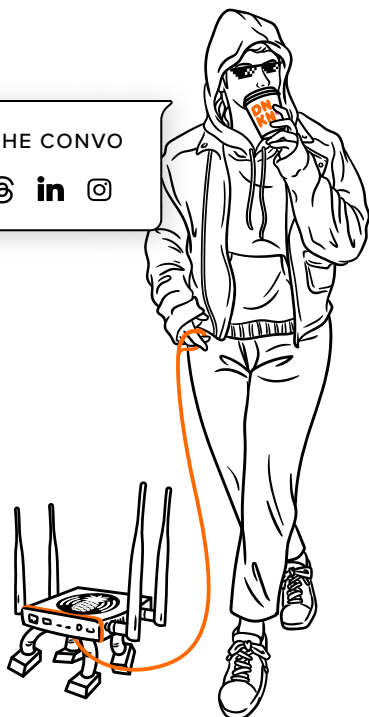
Bugcrowd's Twitter is a hub where organizations, hackers, and security professionals alike come to find up-to-date cybersecurity news, vent about common challenges, and crack a joke or two.


We love the community you've helped us build!





What song helps motivate you when working on a difficult program? 🎧


JOIN THE CONVO
🐦 @ @ in 📷




- 

Hall of Fame
By The Script
Areeb Tanzeem
@areeb_tanzeem
- 

Never gonna give you up
By Rick Astley
seko9m
@seko9m
- 

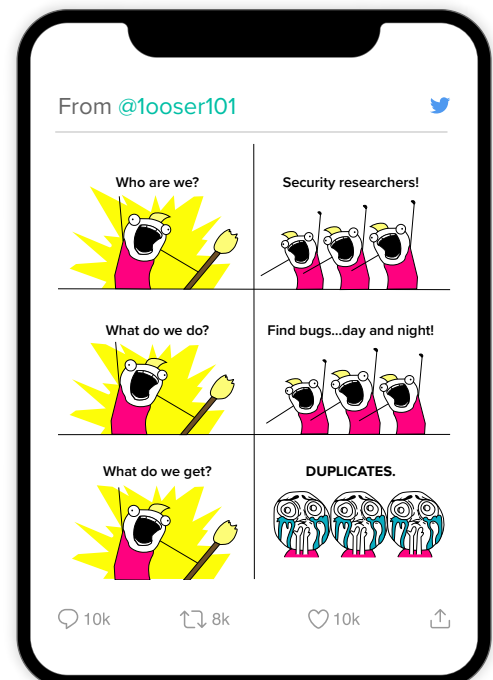
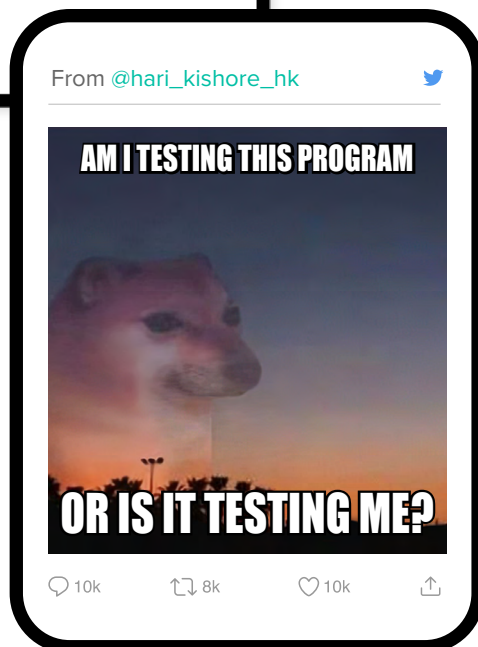
Big Things Poppin' (Do It)
By T.I.
voidimmoral
voidimmoral
- 

Unstoppable
By Sia
Aniket Akhade
@_Aniket_Akhade_
- 

Gangster Paradise
By Coolio and L.V.
Nittonull
@nittonull

Mememes that Made our Day

Check out some recent posts that highlight the varying interests and killer personalities of the amazing security experts who hack with us to keep you safe.



POSTER

b

Which companies will survive and
what will be left of them?



THE TEXAS CHAINSAW RANSOMWARE

Meet Nick McKenzie

CISO with 25 years of security experience

Nick McKenzie, CISO at Bugcrowd, has seen a shocking amount of change in his almost 25 years in the cybersecurity industry. Before Bugcrowd, Nick served as executive general manager and CSO at National Australia Bank (NAB), one of Australia's four largest financial institutions. At NAB, he was responsible for overseeing the enterprise security portfolio, which included cyber, physical security, investigations, and operational fraud capabilities to protect customers and employees, support business growth, and enable an operationally resilient bank.

Nick currently serves as an advisory board member for Google, Amazon Web Services, Netskope, and Digital Shadows. We wanted to tap into Nick's breadth of experience and get his expert CISO opinion on some of the biggest challenges and the way AI is changing security.

WHAT ARE THE MOST DEMANDING CHALLENGES THAT CISOs ARE CURRENTLY FACING IN THEIR ROLES?

CISOs juggle multiple responsibilities, including maintaining a secure foundation and protecting against ever-evolving threats while trying to attract top talent in a highly competitive environment. CISOs must strike a balance between enabling business agility and providing robust protection—all while navigating the intricacies of country-specific technologies and cyber regulations.



HOW SHOULD CISOs APPROACH WORKING WITH HACKERS AND IMPLEMENTING CROWDSOURCED SECURITY?

By leveraging a select number of curated hackers with small-scope proof of value (POV), CISOs can safely and effectively mitigate the perceived risk of crowdsourced security. Running this POV gives a CISO's team familiarity with the platform, triage services, and customer success capabilities. As CISOs become more accustomed to the crowdsourced model, they are likely to go wider and deeper—sometimes straight to a public program to glean the ultimate benefits from a bigger, more diverse community of hackers.

In my personal view, the adoption of crowdsourced security does not increase operational risk; instead, it only decreases risk, as it enables the earlier identification of vulnerabilities harvested by experts in the security community before attackers can discover and exploit them.



IN THE AGE OF AI, COULD GENERATIVE TECHNOLOGIES OUTPACE AN ORGANIZATION'S ABILITY TO ESTABLISH EFFECTIVE CYBERSECURITY MEASURES?

AI has progressed to the point where it is being used to both weaponize and circumvent traditional controls in organizations' defenses. For example, more advanced malware, phishing campaigns, deep fakes, and voice cloning are continually being developed. As AI advances, CISOs must adapt existing security measures—or introduce new ones—to counter the increasingly sophisticated threats posed by generative technologies.

GIVEN THE POTENTIAL MISUSE OF GENERATIVE AI BY CYBERCRIMINALS, SHOULD THERE BE STRICTER REGULATIONS ON ITS DEVELOPMENT AND USE BY HACKERS, OR WOULD THAT HINDER INNOVATION?

Imposing restrictions on the use of generative AI for the hacking community would hinder creativity and create the opposite intended effect. Regulations should be put in place across industries and organizations; rather than restricted to hackers.

HOW CAN CISOs STRIKE A BALANCE BETWEEN ENJOYING THE BENEFITS OF GENERATIVE AI AND ENSURING THEY DON'T INADVERTENTLY CONTRIBUTE TO THE RISE OF MORE SOPHISTICATED CYBERATTACKS?

CISOs must be aware of the duality of generative AI to both benefit from it and prevent its misuse by attackers or employers. Ultimately, it's a tug of war between threat actors and defenders, who are constantly trying to evolve with the use of AI to outsmart each other.

COULD AN INCREASED RELIANCE ON GENERATIVE AI DISPLACE HUMAN INTELLIGENCE AND DIMINISH THE VALUE OF HACKERS?

Generative AI will certainly help with speed and accuracy in vulnerability analysis, but it cannot replace the creativity and diverse perspectives of human hackers.

Hackers spend long, arduous hours deconstructing a complex problem or unveiling an abstract vulnerability; presently, this is something that modern AI systems struggle with.

CONSIDERING RECENT ECONOMIC HEADWINDS, WHAT SUGGESTIONS CAN YOU GIVE TO FELLOW CISOs WHO WANT TO INCREASE THE ROI FROM SECURITY PROGRAMS WITHOUT SIGNIFICANTLY INCREASING THEIR BUDGETS?

CISOs should consider investing in newer frameworks and products such as bug bounty programs or penetration testing as a service, which improve time-to-remediation (TTR), digitize the experience end to end, and deliver continuous outcomes across an evolving attack surface.

WHAT DO YOU PREDICT THE NEXT TWO YEARS OF CROWDSOURCED SECURITY WILL LOOK LIKE, AND HOW IS BUGCROWD PLANNING TO GIVE HACKERS AND CUSTOMERS THE BEST EXPERIENCE?

In the next two years, crowdsourced security will become the preferred model for continuous assurance, incorporating generative AI to improve customer experiences—through things like improved triage and increased integration capabilities—and eventually expand the usage of hacker data.

Conclusion

That's a wrap on this year's edition of *Inside the Mind of a Hacker*. At the beginning of this report, Bugcrowd's founder, CTO, and Chairman, Casey Ellis, predicted that cybersecurity is about to become a lot less predictable.

The first reason for this is the impact of generative AI becoming mainstream. Aspects of hacking are being automated, creating a swath of new techniques, threats, vulnerabilities, and opportunities for impact. The adversary is innovating in similar ways to hackers, and threat actors now have access to more powerful tools to create a bigger impact faster.

The second reason comes down to motivation—something we've examined closely in this report. In "The Heart of Hacking," we looked at data and interview responses to understand why hackers do what they do. But what do we know about the motivations of the bad guys—the attackers?

Before now, it's been fairly easy to predict the motivations of attackers. For the past eight years or more, cybersecurity has focused mostly on symmetric, rational actors—cybercriminals who want to make money or nation-states who want to advance their nation's interest.

But that is changing. Threat actors are undergoing significant evolution, and organizations need to keep up. The LAPSU\$ Group's attacks showed that truly chaotic threat actors with asymmetric intentions can have tremendous impact. Security leaders need to actively consider an accelerating chaotic threat in their models.

With this in mind, it's important to remember how far these three fundamentals will get you.



Do the simple things well.

The simple things are vital for a reason. Do them well and ensure that your organization is capable of "outrunning the other guy" before it attempts to "outrun the bear." This includes, at minimum, having an established and well-run VDP.



Hackers are crucial partners.

Hackers are creative, multi-faceted professionals who represent an army of brilliant, diverse minds. When organizations partner with hackers, they multiply their security posture tenfold.



Now is the right time.

When it comes to cybersecurity, good timing and easy solutions are rare. But with the right crowdsourced security platform, you'll have top-tier hackers at your fingertips just when you need them most. Don't play the odds against cyberattacks—beat them with Bugcrowd.

[Request a Demo](#)

We must look ahead to innovation. With a whopping 94% of hackers planning to bring generative AI into their future workflows, and 78% of hackers believing AI will disrupt traditional penetration testing and bug bounty programs, there is no denying that change is coming.

Has generative AI hitting the mainstream created opportunities for attackers? Yes. Will security become less predictable in the wake of these technologies? Probably. Does this mean organizations and hackers are fighting a losing battle? No way.

For as long as humans write code and deploy the systems that power the internet—and for as long as humans have a reason to maliciously attack these systems—crowdsourced security will play a fundamental role in delivering an army of allies who can outsmart the adversaries.

More hearty hacker stories

DATA SHEET

CrowdMatch

The Right Crowd at the Right Time

EBOOK

Introduction to the Bugcrowd Platform

Defend Against Cyber Attacks with Data, Technology, and Human Intelligence

DATA SHEET

Researcher Trust

How We Build the Right Trusted Team for Your Program

GUIDE

What's a Vulnerability Worth?

Building a Rewards Model for Your Bug Bounty Program

[Request a Demo](#)

Glossary

a

ADVERSARY: An individual, group, or organization that actively seeks to compromise the security of a system or network.

AI BIAS: Systematic errors in the output of an AI system resulting from underlying biases in the training data or algorithm design.

ALLY: A person or entity that supports and cooperates with another to protect the security of a system or network.

API: An application programming interface is a way for two or more computer programs to communicate with each other. It is a type of software interface, offering a service to other pieces of software.

ARTIFICIAL INTELLIGENCE: The simulation of human intelligence processes by machines, particularly computer systems, to execute tasks akin to learning and decision-making found in humans. Subsets of AI include expert systems, neural networks, deep learning, natural language processing, speech recognition, and machine vision. In cybersecurity, AI applications include attack surface management, automated detection and response, and intelligent authentication and fraud prevention.

ASSET: Any data, device, or environmental component that supports information-related activities. Assets generally include hardware, software, and confidential information.

ASYMMETRIC INTENT: Cyberwarfare that seeks to inflict a proportionally large amount of damage compared to the resources used by targeting the victim's most vulnerable security measure.

ATTACK SURFACE: The sum of the different points in a software environment where an unauthorized user can enter or extract data. Minimizing the attack surface is a basic security measure.

ATTACKER: An individual or group who performs malicious activities to destroy, expose, alter, disable, steal, or gain unauthorized access to or make unauthorized use of an asset.

b

BAD ACTOR: Also called a malicious actor or threat actor, an entity that is partially or wholly responsible for an incident that impacts or has the potential to impact an organization's security.

BLACK HAT: Bad actors that operate alone or in groups and may be sponsored by nation-states or organized crime rings who break into otherwise secure networks and assets with the primary purpose of stealing, destroying, or modifying data, extorting or stealing funds, or making the networks and information systems unusable.

BOUNTY: Monetary rewards offered in exchange for a vulnerability finding, discovery, or report.

BOUNTY HUNTER: A highly skilled hacker who receives recognition and compensation in exchange for reporting bugs, especially those pertaining to security exploits and vulnerabilities.

BREACH: A cyberattack in which sensitive, confidential, or otherwise protected data have been accessed or disclosed in an unauthorized manner.

BUG: A software defect that can be exploited to gain unauthorized access or privileges on a computer system.

BUG BOUNTY: Bug bounty programs allow independent security researchers to report bugs to an organization and receive rewards or compensation.

BUGGY AWARD: An award that recognizes organizations for championing internet safety, supporting the hacker community, and excelling through crowdsourced security. This commendation celebrates transparent, committed, and generous collaboration with ethical hackers on the Bugcrowd platform.

BURGLAR: A person who unlawfully enters a building with the intent of stealing or committing a crime.

c

CHIEF INFORMATION SECURITY OFFICER (CISO): The senior-level executive within an organization responsible for establishing and maintaining the enterprise vision, strategy, and program to ensure assets and technologies are adequately protected.

CONTINUOUS ASSURANCE: The process of continuously monitoring and validating the security controls and procedures in a system or organization to ensure ongoing compliance and effectiveness.

CREDENTIALS: The verification of identity or tools for authentication. These may be part of a certificate or other authentication process that helps confirm a user's identity in relation to a network address or system ID.

CROWDSOURCED SECURITY: An organized security approach wherein ethical hackers are incentivized to search for and report vulnerabilities in the assets of a given organization. The power of crowdsourced security is derived from the proportion of active testers per asset/ecosystem versus more traditional testing methods.

CUSTOMER: Organizations that leverage the Bugcrowd platform or its associated services.

CYBERCRIMINAL: An individual or group that commits malicious activities on a system or network with the intention of stealing sensitive information or personal data to generate profit.

d

DATA POISONING: A form of adversarial attack involving the intentional manipulation of training data in machine learning systems to produce incorrect or biased outcomes.

DIGITAL NATIVE: An individual who grew up under the ubiquitous influence of the internet and other modern information technologies.

DIGITAL TRANSFORMATION: The process of fundamentally changing an organization with technology and culture to improve/replace what existed before.

DISCLOSURE: The practice of reporting security flaws in computer software or hardware.

DUNKIN': A popular American multinational coffee and donut chain known for its variety of donuts and beverages.

e

ENGAGEMENT: Measurable indicators of the level of interest, involvement, and influence that a crowdsourced security program generates among ethical hackers or custom-designed penetration testing solutions tailored to an organization's unique needs.

ETHICAL HACKER: A person who hacks into a computer network to test/evaluate its security, rather than to carry out an act of malice.

ETHICAL HACKING: An authorized attempt to gain unauthorized access to a computer system, application, or data.

EXPOSURE: All vulnerabilities and risks associated with an organization's networks, systems, applications, and data. It encompasses the potential weaknesses and threats cybercriminals may exploit, resulting in security breaches, data loss, or other adverse consequences for an organization.

GENERATIVE AI: Generative AI is a type of artificial intelligence technology that can produce various types of content, including text, imagery, audio and synthetic data in response to prompts. Generative AI models learn the patterns and structures of their input training data, and then generate new data that have similar characteristics.

GEN X: A demographic cohort born between the mid-1960s and early 1980s, known for being resourceful, independent, and keen on maintaining work-life balance. Gen X has fewer members than the generations that precede or follow it. This cohort is also known as the MTV Generation.

GEN Z: A demographic cohort born between the mid-1990s and early 2010s; known for a strong affinity for technology, ubiquitous access to the internet, and progressive views on issues such as diversity, equality, and climate change. Gen Z is the largest generation in American history, constituting 27% of the country's population. Members of this cohort are also known as Zoomers.

h

HACKER: Someone who uses technical knowledge to achieve a goal or overcome an obstacle within a computer system by non-standard means.

HUMAN ELEMENT: The role people play in the design, implementation, and operation of technology systems, as well as their potential to introduce vulnerabilities or mitigate risks.

HUMAN-IN-THE-LOOP: A system design that integrates human input and decision-making within an automated process to improve accuracy, reliability, and ethical considerations.

i

INTERNET OF THINGS (IOT): Any device (often called a smart or connected device) that connects to and exchanges information over the internet.

INCIDENT RESPONSE: A term used to describe the process by which an organization handles a data breach or cyberattack, including the way the organization attempts to manage the consequences of the incident so that damage, recovery time, and costs are limited and collateral damage, such as brand reputation, is kept to a minimum.

j

JAVASCRIPT: A scripting or programming language that allows the implementation of complex features on web pages.

L

LARGE LANGUAGE MODEL (LLM):

An AI algorithm that uses deep learning to understand language from vast datasets. LLMs can summarize, translate, predict, and generate human-like text, making them powerful tools for natural language processing tasks, such as machine translation, question answering, and creating contextually relevant content.

LEVELUP: A series of technical and educational resources designed to support ethical hackers in improving their skills. Launched in 2016 as a virtual security conference, LevelUp has since evolved into an on-demand library of resources encompassing peer-led discussions on innovative security techniques, testing methods, hunting strategies, short and long-form talks, in-depth blogs, reporting guidelines, and templates.

LOCKSMITH: A professional who specializes in the installation, repair, and manipulation of locks and security devices.

M

MALICIOUS HACKER: Someone who is actively working to disable security systems with the intent of either taking down a system or stealing information.

MILLENNIALS: A group born between the early 1980s and mid-1990s, known for their tech-savviness, adaptability, and focus on meaningful motivations. Millennials appreciate creativity, teamwork, and positive workplace interactions. They question traditional hierarchies, prioritize tasks, and welcome feedback. Millennials lived through the rise of the internet while still having cable television and landline phones. This generation is also known as Gen Y.

MODEL: A program that analyzes mathematical representations of relationships between variables to make predictions or decisions in artificial intelligence systems.

MODEL INFERENCE: The process of using a trained AI model to make predictions or classifications based on new input data.

N

NATION-STATE: Individuals or groups sponsored by a sovereign government, engaging in cybercrime to advance national interests, often targeting critical infrastructure in an attempt to disrupt or compromise another country's economic, military, or political sectors.

NON-BINARY: A term describing gender identities that do not fit within the traditional binary classification of women and men.

P

PAYOUT: The money paid to a researcher once their vulnerability submission has been validated.

P1: Critical: Vulnerabilities that cause a privilege escalation from unprivileged to admin or allow for remote code execution, financial theft, etc.

P1 WARRIOR: An incentive program that rewards hackers for submitting multiple valid P1 vulnerabilities in a specific period. To be eligible, an ethical hacker must have a notable number of submissions accepted, assigned a P1 severity rating, and marked as "Unresolved," "Resolved," or "Informational" by the Program Owner.

P2—HIGH: Vulnerabilities that affect the security of the software and the processes it supports.

PENETRATION TESTER / PENTESTER: Someone who professionally attacks computer systems to find security weaknesses that can then be fixed.

PENETRATION TESTING / PENTESTING:

A simulated cyberattack done by authorized hackers who test and evaluate the security vulnerabilities of the target organization's computer systems, networks, and application infrastructure.

PLATFORM / SAAS PLATFORM:

Bugcrowd is an all-in-one SaaS platform that combines actionable, contextual intelligence with the skill and experience of the world's most elite hackers to help leading organizations solve security challenges, protect customers, and make the digitally connected world a safer place.

POINT-IN-TIME ASSESSMENT /

SECURITY TESTING: A point-in-time review of a company's technology, people, and processes to identify problems. Such assessments can find vulnerabilities at a single moment, but fail to monitor activity between assessments.

PROGRAM: A program—which can be public or private—permits independent researchers to discover and report security issues that affect the confidentiality, integrity, or availability of customer or company information and rewards them for being the first to discover a bug.

PROGRAM BRIEF: A single-page researcher-facing document that contains all relevant information regarding a bounty program (what is in/out of scope, rewards, how submissions will be rated, instructions for accessing or testing the application, etc.). This is drafted with the Bugcrowd team after the initial kickoff call.

PROMPT INJECTION: The malicious act of inserting unauthorized commands or data into a user's interactions with a system, often to gain unauthorized access or control.

R

RANSOMWARE: A type of malware designed to extort money from its victims, who are blocked or prevented from accessing data on their systems.

RISK: The potential for loss, damage, or negative consequences resulting from threats to the confidentiality, integrity, or availability of information or systems.

SCOPE: Outlines the rules of engagement for a bounty program. This includes a clearly defined testing parameter to inform researchers what they can and cannot test, as well as the payout range for accepted vulnerabilities.

S

SECURITY LANDSCAPE: The entirety of potential and identified cyber risks affecting a particular sector, group of users, time period, etc.

SECURITY RESEARCH: The study of technology, algorithms, and systems that protect the security and integrity of computer systems, the information they store, and the people who use them.

SECURITY RESEARCHER: Refers to the diverse group of skilled participants who hunt for vulnerabilities using the Bugcrowd platform. These trusted experts are sometimes referred to as white hats or ethical hackers.

SIDE HUSTLE: A secondary job or project pursued outside of one's primary employment, often for additional income or personal fulfillment.

SOFTWARE DEVELOPMENT LIFECYCLE (SDLC): A structured process that enables the production of high-quality, low-cost software in the shortest possible time.

SUBMISSION: The report a researcher submits to Bugcrowd describing the vulnerability or bug they found.

SWEATS: A casual and comfortable style of clothing, including garments like sweatpants, sweatshirts, and hoodies, designed for lounging, athletic activities, or informal occasions. The term "sweats" was derived from their original purpose as attire for perspiration-inducing physical exercise, but they have since become a popular choice for everyday wear.

T

TARGET: A web or mobile application, hardware, or API that the Crowd tests for vulnerabilities.

THE CROWD: The global community of white hat hackers on the Bugcrowd platform who compete to find vulnerabilities in bug bounty programs.

THREAT ACTOR: An individual, group, or organization that poses a potential risk to the security of information or systems through malicious activities.

TIME-TO-CONTAIN: The duration between the initial detection of a cybersecurity incident and the implementation of measures to limit its spread or impact within a system or network.

TIME-TO-DETECT: The period between a cybersecurity event, such as a breach or intrusion, and its discovery by security personnel or systems.

TIME-TO-REMEDiation: The interval between identifying a vulnerability, threat, or security incident and successfully implementing corrective actions to address the root cause or mitigate potential risks.

TRAINING: The process of teaching an artificial intelligence model to recognize patterns and make predictions by feeding it large amounts of labeled data.

TRIAGE: The process of validating a vulnerability submission from raw submission to a valid, easily digestible report.

V

VALID: The state of a vulnerability that has been tested and confirmed as real.

VULNERABILITY RATING TAXONOMY (VRT):

The official standard used by Bugcrowd for assessing, prioritizing, and benchmarking the severity of security vulnerabilities.

VULNERABILITY: A security flaw or weakness found in software or in an operating system that can lead to security concerns.

VULNERABILITY DISCLOSURE

PROGRAM (VDP): Clear guidelines for researchers to submit security vulnerabilities to organizations while also helping organizations mitigate risk by supporting and enabling the disclosure and remediation of vulnerabilities before they are exploited. VDPs usually contain a program scope, safe harbor clause, and method of remediation.

W

WHITE HAT HACKER: A computer security expert who uses penetration testing skills to help secure an organization's networks and information system assets. A white hat hacker is also known as an ethical hacker. White hat hackers work with information technology and network operations teams to fix vulnerabilities before black hat hackers discover them. White hat hackers operate with the permission of the organization and within the set boundaries.

INSIDE THE MIND OF A HACKER 2023

NOT ALL
HACKERS
WEAR HOODS

bugcrowd