INSIDE THE MIND OF A HACKER 2024

ITMOAH

bugcrowd

VOLUME 8

THE RISE OF HARDWARE HACKING

Defining “Hacker”

If you were to ask 10 people off the street whether they could distinguish between hackers and cybercriminals, they’d likely be unable to do so.

Merriam-Webster defines a “hacker” as “an expert at programming and solving problems with a computer.” While “hacker” is the predominant self-descriptor used by the cybersecurity community (with even some CISOs we know adopting the moniker), this benevolent term has sadly become synonymous with malice. The bad guys also call themselves hackers, and unfortunately, they get most of the attention.

Here at Bugcrowd (and in this report), we refer to the good guys as hackers. Other terms you may have heard include “ethical hackers,” “white hat hackers,” and “security researchers.”

Table of Contents

Report Highlights

This edition of *Inside the Mind of a Hacker* analyzed almost 1300 survey responses from hackers on the Bugcrowd Platform, in addition to hacker interviews.

An introduction from our CEO David Gerry

Celebrating hackers is at the core of what we do at Bugcrowd. I've witnessed so much change over the past decade when it comes to perceptions of the hacking community.

Years ago, hackers were almost exclusively assumed to be criminals. Now, most security professionals not only understand the difference between threat actors and hackers, but they actually have personal experience with ethical hacking.

This is the eighth year in a row that we've published Inside the Mind of a Hacker, and we've covered some really compelling subjects over the years. From neurodiversity in the hacking community to the rise of hacking influencer platforms, we've examined a broad spectrum of important topics.

Originally, we published *Inside the Mind of a Hacker* with the goal of breaking through dated hacker stereotypes. As perceptions changed, this report seized the opportunity to do something different; it now focuses on highlighting what's next for the hacking community. What trends are we seeing? What unique directions are hackers taking in their security research? How can Bugcrowd customers and the greater cybersecurity community benefit from these shifts?

In the last edition, Bugcrowd provided an exclusive first look into how the hacking community is leveraging generative AI as a tool. Owing to its widespread adoption, generative AI was suddenly a topic of conversation everywhere. But we noticed something interesting this year when analyzing the data provided by almost 1300 hacker survey respondents. There is no denying that AI is still top of mind for many, but a surprising trend surfaced: the increasing prominence of hardware hacking.

At first glance, nothing might seem further from the abstract world of AI than the concrete world of hardware hacking. However, consider the infrastructure needed to support the growing demands of AI and complex applications.

In our distributed computing world, it's easy to forget that the cloud is made of iron.

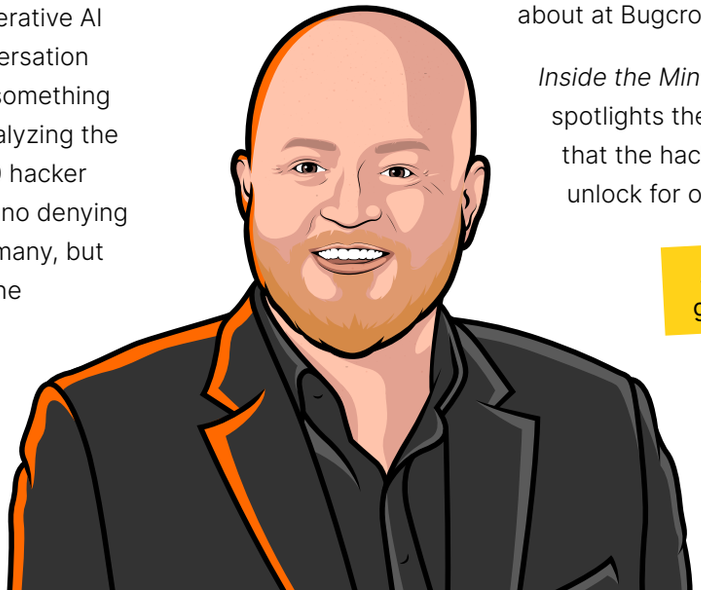
Internet of Things (IoT) devices are in our homes. Autonomous vehicles are on the streets. Technology is in our pockets and wearable on our wrists. Hardware powers everything, and that hardware needs to be secure.

Beyond the tie-ins between hardware hacking and AI as a target, AI is also seen as a tool. Hardware hackers can use AI for educational purposes, such as when deciding what frequency to try for a fault injection on a device.

I've personally had the privilege of attending several Bug Bashes, where I've witnessed firsthand expert hardware hackers combining technology with the hands-on ingenuity of humans. They're taking machines apart, turning them upside down, and breaking them down, all while running automation programs, pulling apart code, and testing gaps in technology. It's truly the perfect union between innovative technology and human ingenuity, which is something we're really passionate about at Bugcrowd.

Inside the Mind of a Hacker spotlights the immense power that the hacker community can unlock for our customers.

And we're just getting started!



THE ANATOMY OF A HACKER 24

61% say that hacking helped them get a job

64% hack part-time

Personal development is the main hacking motivator for **28%**

58% are 24 years old or younger

83% are confident in hacking AI-powered hardware and software

77% use AI technologies to hack

90% are Gen-Z or millennials

92% speak two or more languages

2/3 encountered a vulnerability type they hadn't seen before in the past year

72% have a college degree

87% believe that reporting a critical vulnerability is more important than trying to make money from it

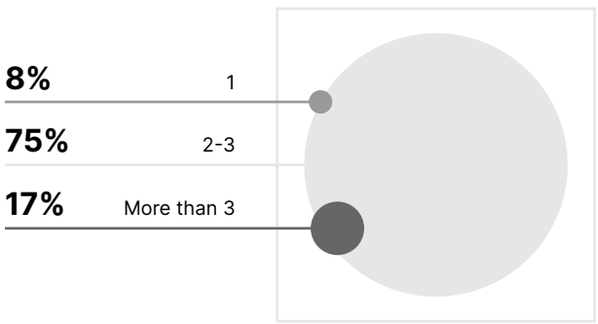
A Day in the Life of a Hacker

The world of hacking is as diverse as it is dynamic. Far from being a monolithic group, hackers of today represent a broad spectrum of backgrounds, experiences, and approaches to cybersecurity. From dedicated professionals who've turned their passion into a full-time career to weekend warriors balancing day jobs and bug hunting, these individuals are united by their drive to uncover vulnerabilities and strengthen digital defenses.

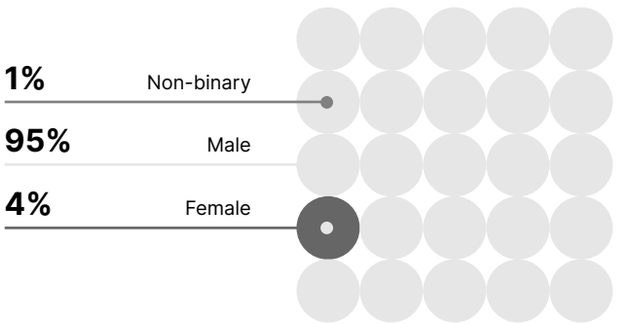
In this section, we'll explore the demographics of the hacking community, shedding light on their work habits, educational backgrounds, and the various paths that led them to this field. By understanding who hackers are and how they operate, we gain valuable insights into the human element of cybersecurity—an aspect that's just as crucial as the technology itself.

The Basics

Languages Spoken



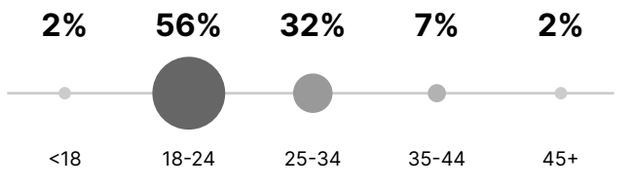
Gender Differences



Top 10 Countries Where Participating Hackers Live

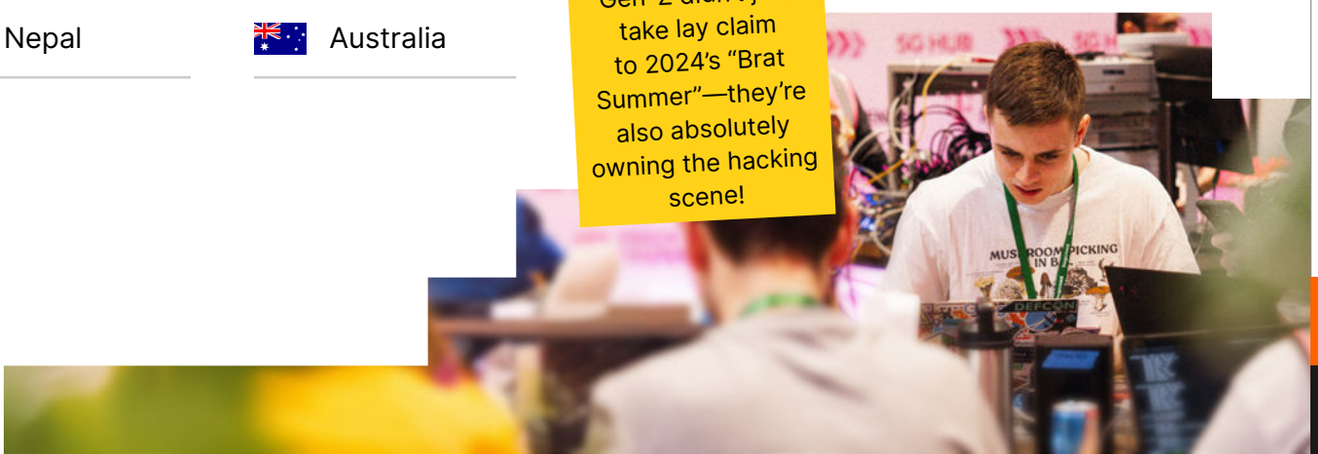
- India
- Egypt
- Bangladesh
- Nigeria
- USA
- UK
- Pakistan
- Vietnam
- Nepal
- Australia

Average Age

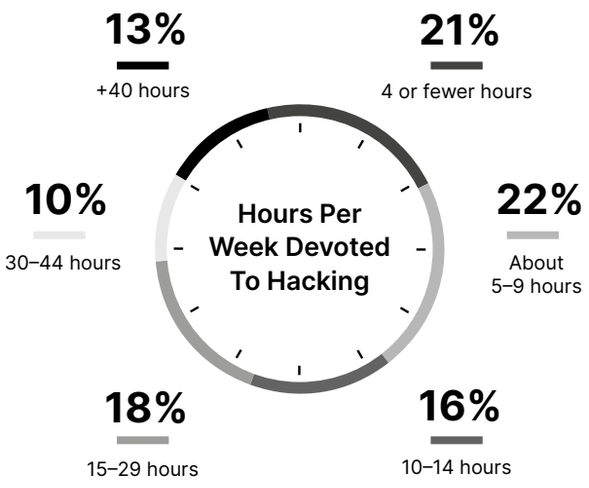


90% of hackers are Gen-Z or millennials—so demure, so mindful.

Gen-Z didn't just take lay claim to 2024's "Brat Summer"—they're also absolutely owning the hacking scene!



Hack Around the Clock



Nearly half of the hackers in our sample spend **less than 14 hours a week hacking,** with over 40% dedicating less than 10 hours to their craft.

This approach to hacking—more marathon than sprint—allows hackers to keep doing what they love without burning out. It's a reminder that hackers are not obsessive recluses but balanced individuals who approach their craft with the same degree of professionalism as in any other career.

95% of hackers believe they help fill the cybersecurity skills gap. Hackers are crucial in today's digital defense.

The Dual Lives of Hackers

Top 10 Industries Hackers Work In

01	Hacking and security research
02	Information and web application security
03	Architecture and engineering
04	Education, training, and libraries management
05	Business and financial operations
06	Installation, maintenance, and repairs
07	Office and administrative support
08	Sales or business development
09	Arts, design, entertainment, sports, and media
10	Healthcare practitioners and technicians

While 84% of hackers identify hacking and security research or information and web application security as their primary occupations, a diverse range of professionals moonlight as hackers.

From educators and engineers to healthcare workers and even a few food service workers, these individuals bring a wealth of real-world experience to their hacking endeavors.

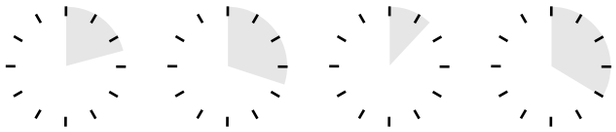
It's not rocket science...but some hackers can do that too!

Plot twist!

Only 37% hack full-time. The rest? They're your coworkers, neighbors, and maybe even your barista!

Hack How You Want

Employment Status of Hackers



21% I hack part-time

30% I'm trying to hack full-time

12% It's just a side hustle or for fun

37% I hack full-time

Who says you can't make a living finding bugs?

Over 75% of hackers prefer probing for software vulnerabilities in their homes, while others prefer hacking in a coffee shop or at a tech meetup.

More than a third of hackers have turned their passion into a full-time gig, while another third are aspiring to make hacking their full-time career, showcasing the growing appeal of this field. Whether it's a career, a side hustle, or just for kicks, it seems everyone's got a bit of hacker in them.

Teach Me How to Hack

Hackers have a striking preference for self-directed learning, with 87% of hackers crediting online resources for their skills. This digital-first approach to education reflects the rapidly evolving nature of cybersecurity, where the latest techniques and vulnerabilities are often shared online long before they make it into formal curricula.

But the learning doesn't stop at online tutorials. A remarkable 78% of hackers proudly wear the badge of **being self-taught,** showcasing a DIY spirit that's deeply ingrained in hacker culture. This self-starter mentality is complemented by peer-to-peer learning, with 35% of hackers citing friends or mentors as key to their educational journeys.

But don't discount formal education. Almost a third of hackers learned how to hack in school. In general, hackers are a well-educated group. Almost three-quarters boast college degrees or higher, reflecting a level of academic achievement rivaling many traditional professional fields. It's a strong reminder that today's hackers aren't just self-taught techies but often highly educated individuals who blend their academic foundations with practical self-directed learning. Going beyond being a technical skill set, hacking is a field that benefits from diverse knowledge, from both higher education and a scrappy self-directed education.

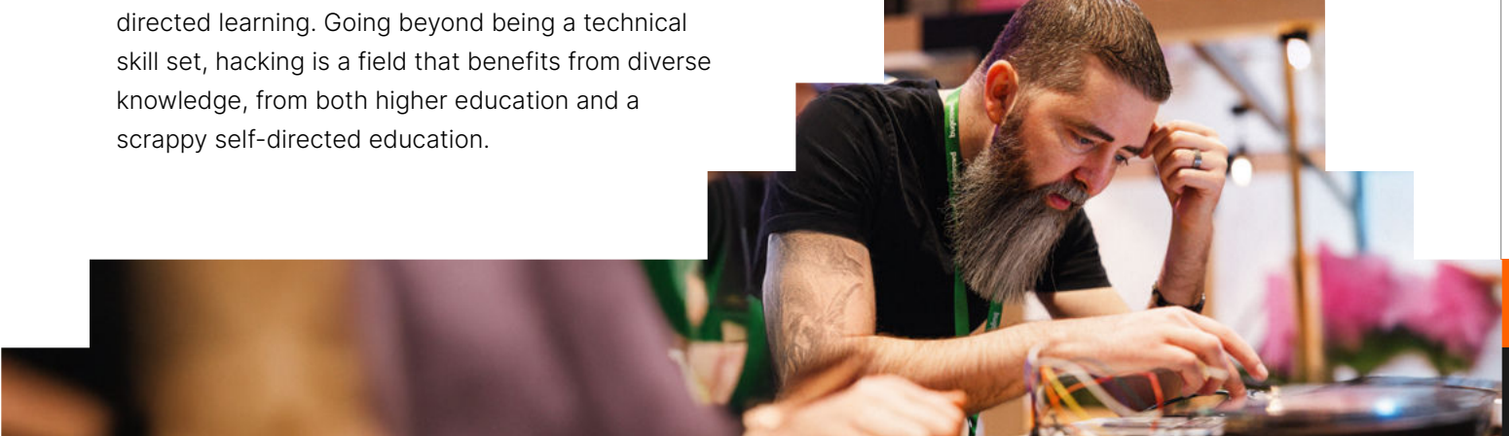
Average Education Completed by Hackers

Did not complete high school	**3%**
Graduated from high school	**24%**
Graduated from college	**56%**
Completed graduate school	**17%**

How Hackers Learn Skills

Online resources	**87%**
Friends or mentors	**35%**
Self-study	**78%**
Academic or professional coursework	**29%**
Trial and error	**43%**

69% of hackers stay up to date on the latest breaches



Meet Ads Dawson

Security Engineer, AI Red Teamer, and Hacker

At Bugcrowd, we talk a lot about the societal misconception that hackers and security professionals are two separate groups when in reality, they are one and the same. Full-time security professionals often hack on the side.

There is no better example of this than Ads Dawson, who has been both a Bugcrowd customer and a hacker on the Bugcrowd Platform. Ads has achieved some amazing accomplishments in his career, including most recently contributing to the Bugcrowd VRT update on AI application vulnerabilities. Read on to learn more about Ads!

A Journey into Building and Breaking

Ads started in the security space with an apprenticeship at an MSP. He did not have an educational background in computer science. Nevertheless, from there, he progressed along the path toward networking and security, network pen testing, application security, and eventually LLM applications and AI security. Ultimately, he has a passion for dissecting concepts down to the essence, which is extremely relevant in hacking and the security space. “I figured that if I already know how to build, manage, and deploy hybrid cloud networks, why not learn how to break them?” Ads says.

Ads has been hacking for about six years, and he’s loving it so far. He’s a self-described “meticulous dude” who cites a dedication to curiosity in every aspect of his life to be a main driver of his hacking success. “I have always challenged and motivated myself to fully comprehend a solution or function at a very detailed level,” Ads shares.

“This has kept me constantly driven to adapt, learn new concepts or technologies, and improve my skills.”

VIEW PROFILE

Ads is a self-described "networking nerd at heart," although he applies a well-oriented full-stack approach to hacking. He is also heavily involved in AI red teaming, which is a particularly new space. He is extremely motivated to constantly improve his machine learning (ML) adversarial capabilities.

"Another cool aspect of hacking that I love is developing and building tools or a script that helps me fix common hacking problems."

"It is really effective to spend time on enhancing your offensive arsenal for investing in the long run," Ads says.

Advice for Security Teams

For teams hoping to get more out of their bug bounty programs, Ads shared valuable insights from the hacker perspective. It starts with fostering better relationships with the hacking community.

"Challenge the hacker and always motivate them to dig deeper! If you are denying a submission, it's important to elaborate why and always be open to the possibility of a decision change. Another thing that goes a long way is spending some time on a cadence to update your program with new features or even notifications about behavior changes," Ads says.

He also recommends that teams put themselves in a hacker's shoes. Ask yourself if your scope is clear and concise while providing a clear and valid reporting chain with achievable acceptance criteria. By reviewing your program details from a different lens, you can catch areas where you're potentially pigeonholing your program.

To wrap up, we asked Ads what he wished security leaders understood about hackers. "Hackers spend a lot of time out of their personal lives working within reasonable disclosures and constraints to secure companies' attack surfaces. Come to the table with a cooperative spirit and a willingness to achieve mutually fair reasoning," Ads says. "Embrace the fact that every hacker has unique insights, perspectives, and capabilities to offer. Having a dedicated and motivated hacker finding holes in your ecosystem is incredibly valuable, especially compared to traditional methods of security testing in resource-constrained environments."

"Embrace the fact that every hacker has unique insights, perspectives, and capabilities to offer."

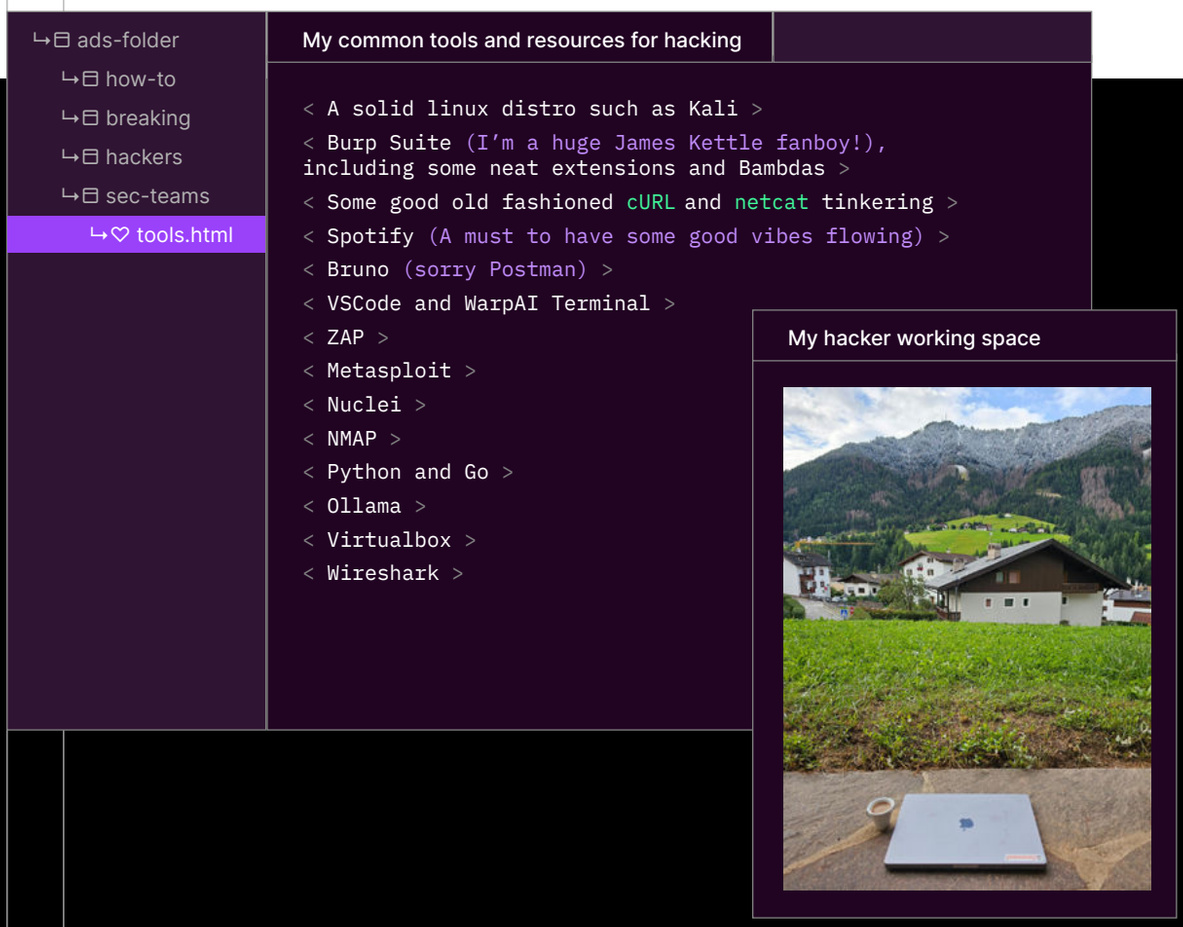
Advice for Hackers

Ads has been on both sides of a bug bounty program. Therefore, his perspective is valuable for hackers looking to improve their skills and earn greater recognition. When it comes to advice for hackers who are engaging with security teams, Ads suggests a well-rounded approach.

"Consider every angle, leave no stone unturned, and always parse information thoroughly. It's always incredibly easy to skim information, especially when you're running on fumes. Prioritize yourself when you're feeling burnt out—taking a walk or going to the gym does magic for your productivity. Lastly, don't become hard-set on your favorite toolset or setup—always take the opportunity to step outside of your comfort zone," Ads advises.

Ads also views stepping outside their comfort zones as a great way for hackers to earn more invites to hack on private programs. By involving themselves in the community and ongoing CTF events, hackers can increase their visibility. One way Ads does this is through his involvement in an OWASP chapter, which keeps him in the loop and regularly allows him to challenge himself.

Ads also suggests that hackers document their work (such as writeups) as a great way to show off their experience.



The Heart of Hacking

Hackers are driven by a mix of personal and altruistic motivations that go far beyond the stereotype of the lone coder seeking a payday. Earning money is certainly a benefit, but hackers love making a difference in the digital world, protecting both individuals and organizations from threats.

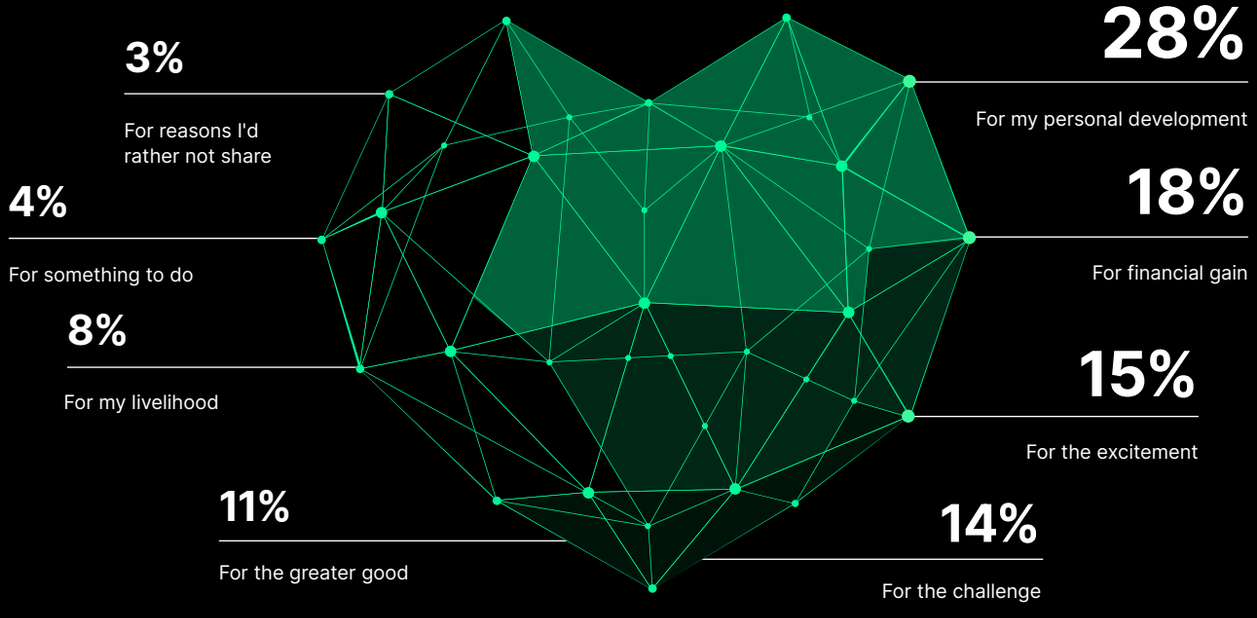
The rush of outsmarting cybercriminals? Exhilarating. The satisfaction that comes with strengthening digital defenses? Unmatched. And the real magic happens when individual triumphs become collective victories. In this world, every bug squashed and every vulnerability patched is a win for the entire community.

So while the challenging puzzles and cutting-edge tech are cool, the best part about being a hacker is the opportunity to make the digital world a safer place while getting to do so alongside an awesome community. It's a reminder that in the world of cybersecurity, the whole is greater than the sum of its parts—and that's what makes hacking so cool.

More Than Just a Paycheck

Why do you hack?

While hackers still consider making money important, they are increasingly being driven by other factors.



What stands out is the mix of motivations—today's hackers aren't one-dimensional. They're professionals who want to earn a living, sure, but they're also passionate about learning, solving problems, and making the internet safer.

Hacking isn't just about the money

It's about personal and professional fulfillment.

Unleash the Hacker

Top Hacking Roadblocks

Not enough private program invites	45%
Not enough scope	26%
Not enough programs that match my interest	25%
Not having the physical technology needed	20%
Unresponsive program owners or brands	19%
Inadequate incentives	11%
No safe harbor	6%
None of the above	15%
Other	13%

Level up!

91% of hackers say they are now armed with more powerful tools than before.

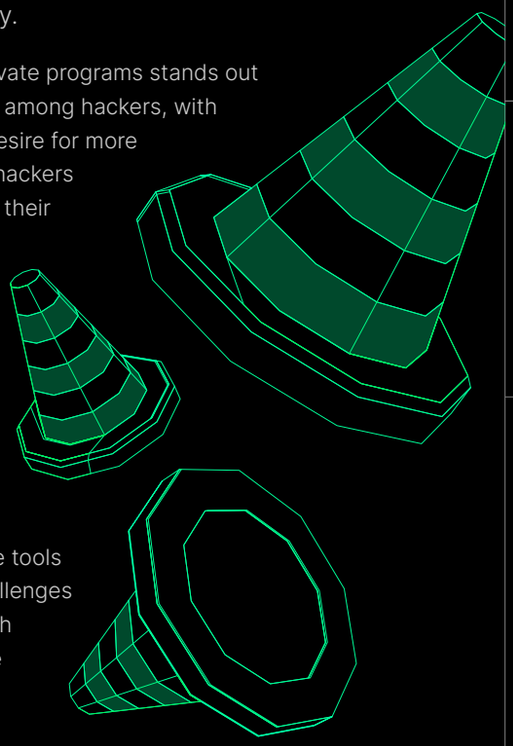
87% of hackers agree

Point-in-time security testing isn't enough. Companies need ongoing, continuous security measures to stay protected in today's dynamic digital world.

The hacker community is full of untapped potential waiting to be unleashed. While hackers are eager to dive deeper into their work, they are held back by narrow scopes, mismatched interests, and a lack of required technology.

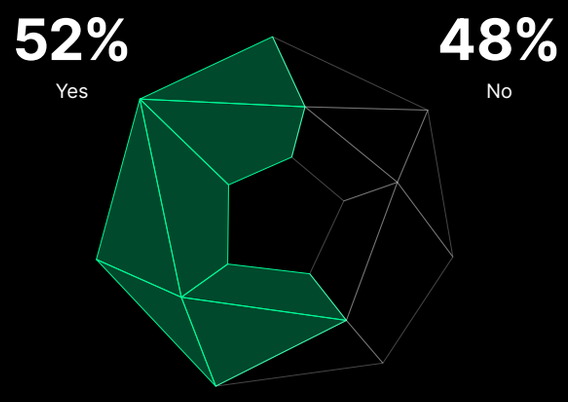
Limited access to private programs stands out as the top frustration among hackers, with almost half citing a desire for more opportunities. While hackers can continue to build their reputations, companies have the chance to expand their programs or explore new approaches.

The message is clear: Give hackers the room to roam, the tools to tinker, and the challenges to conquer, and watch as they transform the cybersecurity world.



The Disclosure Dilemma

Have you avoided disclosing a vulnerability because a company lacked a clear pathway for you to report it without risking legal consequences?

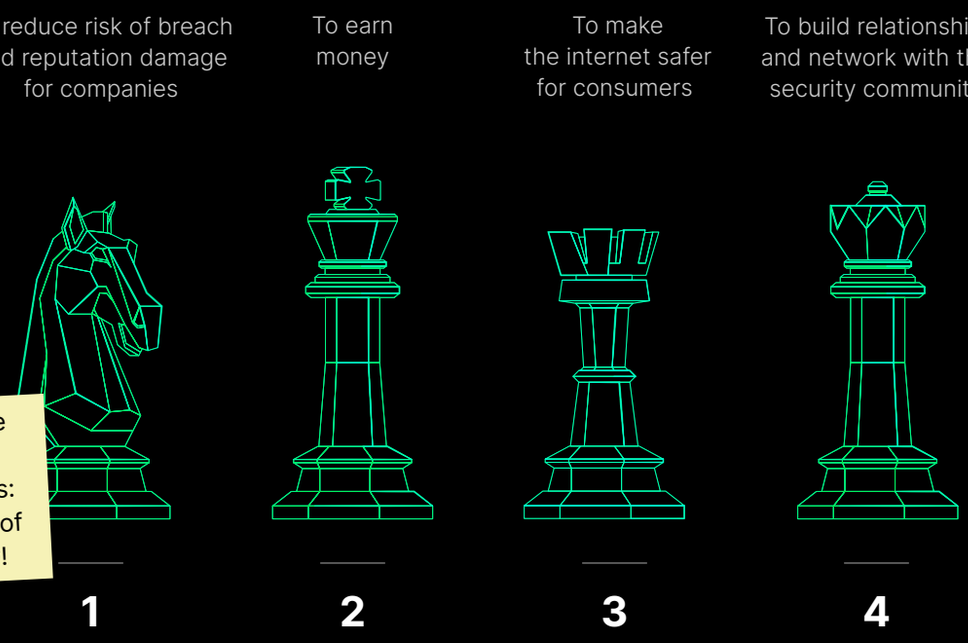


The legal aspect of vulnerability disclosure represents another challenge for hackers. More than half of hackers have held back on reporting disclosures due to unclear reporting pathways. Without a safe harbor, hackers tread a fine line between well-intentioned probes and unauthorized access, turning their exploration into legal trouble.

There's certainly a path forward. Organizations can potentially double their influx of valuable security information if they can implement clear, hacker-friendly policies.

73% of hackers observed more vulnerabilities than last year. It's dangerous out there!

Top Four Reasons to Be a Hacker



The tides are changing!

89% of hackers believe companies appreciate hackers more than ever before.

58% hack to reduce breach risks for companies. Hackers: The unsung heroes of corporate security!

Hacking Together

How Important Are These?

Hacking is evolving beyond solo missions. Today's hackers are active community members working toward the common good. A significant 82% are committed to building lasting relationships with companies and bug bounty program owners, creating a sustained defense.

Knowledge sharing is at the heart of this community, with 85% of hackers dedicated to educating others This "rising tide lifts all boats" mentality strengthens our collective digital safety.

The spirit of mentorship is strong too. Instead of gatekeeping, hackers are inviting others in, with 81% involved in guiding and working with peers. This commitment to growth extends to their own skills, as 89% actively seek constructive feedback.

Hackers are team players!

82% are in it for the long haul, building solid relationships with program owners.

Today's hackers are building more than just secure systems—they're creating a dynamic, collaborative community that's redefining cybersecurity. This allows individual expertise to combine with collective effort to create a safer digital landscape.

Meet Specters

From Experiencing Homelessness to Being a Hardware Hacking Specialist

Meet Neiko—also known as Specters—a skateboarder by day, a punk music enthusiast by night, a full-time skilled hacker in between, and a truly selfless individual who prioritizes giving back to his community on top of it all.

Born in Chicago, Specters stumbled upon hacking during a tumultuous time in his life—when he found himself homeless and searching for a way out.

Hacking to Change Your Life

Specters was experiencing homelessness when he started hacking. "I figured hacking would be good to learn because it seemed like 'computer people' made some money," Specters says.

He was first inspired by old-school phreaks like Mark Abene. He got started in car hacking and malware analysis.

"My first bug bounty was used to pay for my first apartment and quite literally saved me from homelessness."

As he journeyed into the hacking world, Specters had to learn that not all bugs have an impact. He would remind himself of the importance of stepping back when he didn't get the result he wanted.

"Bugcrowd truly gave me a shot to prove myself. I had zero credentials or achievements when I started," Specters shares.

I was homeless, I had just started car hacking, I was literally a nobody. Bugcrowd gave me a chance to change that.

VIEW PROFILE

Getting Started with Hardware Hacking

Specters started with car hacking, but he also loved malware analysis. Now, he is passionate about everything related to hardware hacking.

"Hardware hacking is experiencing a huge resurgence right now. To be honest, I think it's kind of due. There are a ton of embedded devices that are not secure, and a lot of people are realizing that again," Specters says.

For hackers looking to get into hardware hacking, Specters recommends starting with different Arduino kits. These will help aspiring hackers learn many aspects of hardware hacking. Specters personally bought an IoT clock Arduino kit that had many different protocols and circuits that he had to set up, which he recommends as well. He advises aspiring hackers to analyze hardware using different tools and to seek out resources from the security community to get started.

Finally, whether you're passionate about hardware or other specializations, Specters' advice for new hackers is, "hack for fun, not for profit."

Paying It Forward

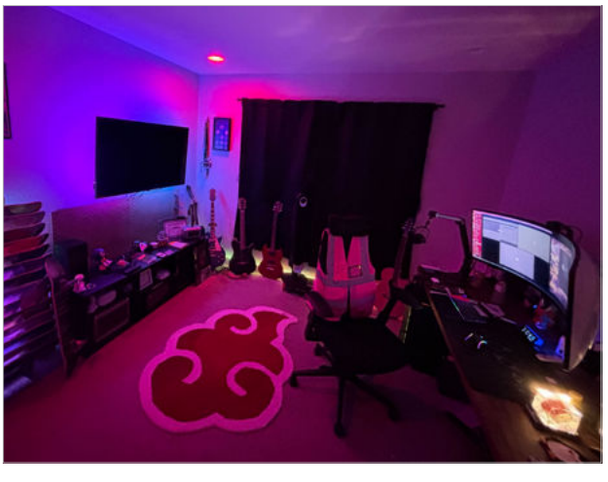
Specters is extremely passionate about paying his success forward and expanding diversity in the hacking community. "I think something that bothers me is the lack of Hispanic representation in hacking," Specters says.

Specters does presentations for Latinx groups, introducing them to computers and hacking. He also mentors people who are seeking guidance, providing them with instruction and materials to get them started.

He recommends supporting Hack the Hood and Boards 4 Bros, which are two organizations that are very personal to him.

"Their efforts go toward neighborhoods like the one I grew up in, and they help kids like me."

"Identity has always been a difficult issue for me. I am talking to so many different communities now and so many people who had similar experiences, and just making friends has really helped me, so I want to pay that forward."

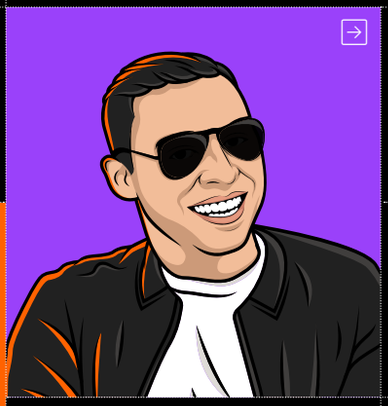


Specters' hacking space

HACKER HALL OF FAME

We asked 1300 hackers who inspired them most as security professionals.

Here are some of the most popular responses. These hackers inspired a generation, and they all happen to be part of the Bugcrowd Crowd!



OrwaGodfather

#1 top Bugcrowd hacker

Top 3 P1 hacker on Bugcrowd

Two-time LevelUpX champion

BusesCanFly

Self-taught hardware hacker

100% accuracy on Bugcrowd

8x Bug Bash competitor

Nagli

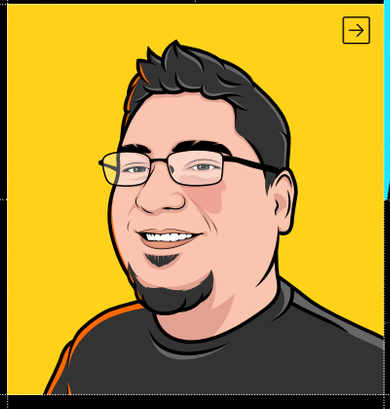
Earned over $1 million in bug bounties

Winner of Indeed's 2022 Bug Bash

InsiderPhD

Has 80k subscribers on Youtube

Has a PhD in Defense and Security



Jhaddix

Multiple time DEF CON and BlackHat speaker

Pioneered a world-renowned recon methodology

Iceman

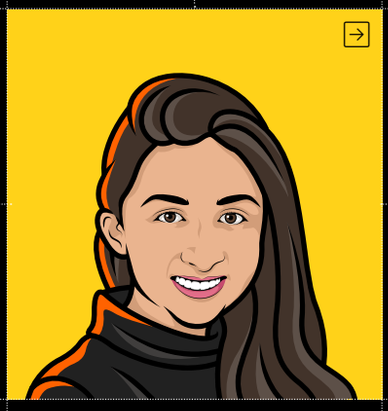
Knows more than 8 programming languages

Created Proxmark3 RDV4 with RRG

Codingo

Previous top 10 hacker on Bugcrowd

Co-founder of Subfinder



Farah Hawa

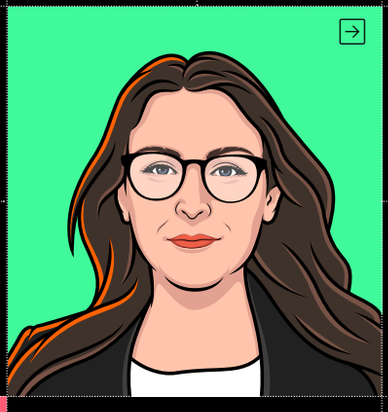
Cybersecurity content creator and influencer

Bug triage professional

TodayIsNew

Almost a decade hacking

1st place in total points from Bugcrowd Bug Bounty Engagements



Rachel Tobac

3x DEF CON 2nd place winner in the Social Engineering Competition

CEO of SocialProof Security

Zwink

Bugcrowd all-time top 10 hacker for P1/P2 vulnerabilities

Hunts broken access control vulnerabilities

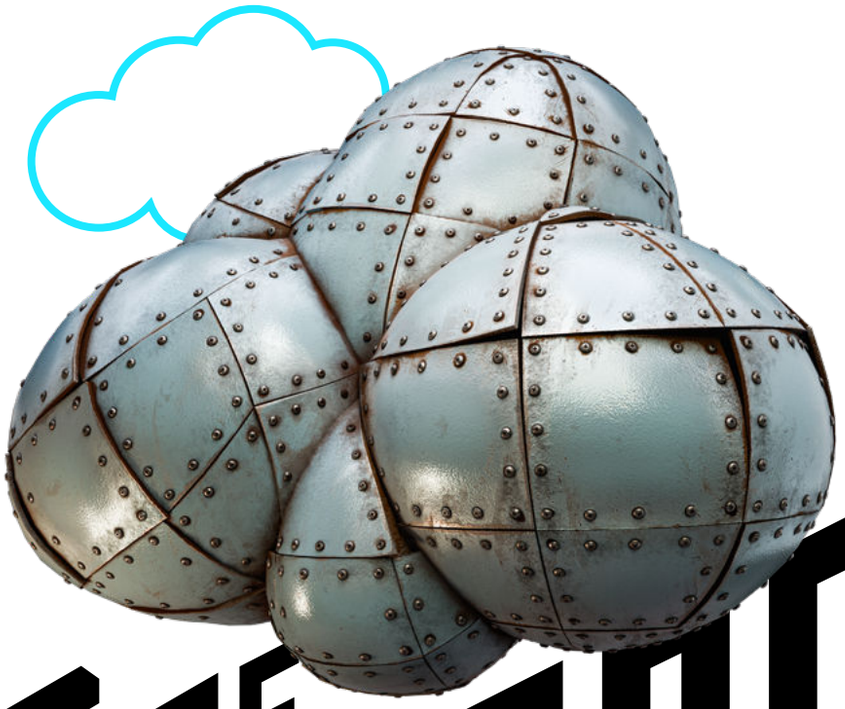
rez0

One of Yahoo's top 10 bug bounty program hackers

Speaker at the AI Village at DEF CON

HACKER HALL OF FAME

Hardware hacking was once considered a niche pursuit. Today, it's experiencing a dramatic acceleration.



THE RISE OF HARDWARE HACKING

Given the increase in cheaply made and often unnecessarily complex smart devices on the market and the advancements in tools for hacking, the conditions are ripe for hardware hacking. Unfortunately, this also means that the conditions are perfect for threat actors who target hardware, threatening consumers, companies, and governments.

There's a tendency to oversimplify hardware hacking—people assume that physical access makes hacking easy or, conversely, that remote attacks are impossible. Hardware hacking is far more complex than both these scenarios, and these misconceptions are harmful because threat actors will exploit every hardware vulnerability they can find.

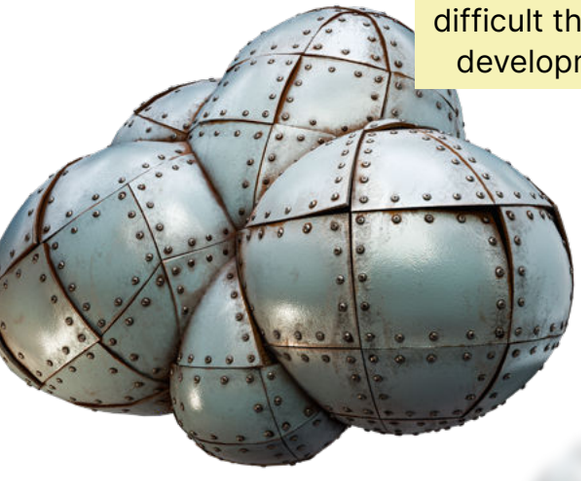
Hardware Hacking 101

At its core, hardware hacking exploits vulnerabilities in the physical components of electronic devices rather than just in their software.

It involves the unauthorized manipulation or modification of a device's hardware to bypass security measures, gain unauthorized access, or alter a device's intended functionality. The goal of hardware hacking is often to circumvent protections, steal data, or gain control of a device in ways its designers didn't intend. Software security, no matter how sophisticated, is practically useless if attackers find ways to exploit the physical hardware.

A number of common techniques are used to break into hardware. In side-channel attacks, for example, a threat actor observes a system and monitors it to catch unintentional information leakage, like power consumption or electromagnetic emissions, to recover cryptographic keys or other secret data. Firmware manipulation is a technique to change a device's core programming, opening doors to unauthorized access. Fault injection is a common hardware hacking technique that deliberately introduces errors into a device's operations. By causing precise, temporary malfunctions through means like voltage glitches or clock signal manipulation, threat actors can bypass security measures, skip important instructions, or gain access.

"It's a myth that hardware hacking requires expensive tools or is more difficult than web development."



Democratization of Hacking Tools

Many believe that hardware hacking is a prohibitively expensive pursuit that requires specialized equipment or that it's too complex for anyone but advanced technical experts to engage in. These notions are becoming increasingly outdated, as tools are becoming more affordable and resources more accessible. Consider, for example, side-channel attacks. These are becoming increasingly common, as measuring equipment has become more precise and affordable. With these tools, hackers can now capture detailed operational data from live systems. While some extremely expensive tools can certainly make things easier, they're rarely necessary. Like with all forms of hacking, creativity and problem-solving go a long way.

Fault injection attacks are also on the rise, also in part because of the accessibility of low-cost gadgets. An impressive example of this is when security researcher Lennert Wouters hacked a Starlink satellite dish using a custom-built modchip costing just $25. By physically attaching this device to a stripped-down dish, they launched a fault injection attack that temporarily shorted the system. This anomaly allowed them to effectively bypass Starlink's security measures, granting access to previously locked areas of the system's software.

Not-So-Smart Devices

As our world becomes increasingly interconnected and as more smart devices are connected to the internet, security risks will multiply exponentially as a result. Devices connected to the internet are part of the large global network, and unfortunately, this means they are exposed to potential dangers. Today, the market is flooded with these "smart" devices, from "smart" microwaves to "smart" flip-flops, and many of these prioritize features over security, creating numerous entry points for cyberattacks. A smart device getting hacked can have immediate real-world impact.

For instance, a vulnerability in a smart oven could allow a threat actor to remotely activate the appliance, creating a significant safety risk. This scenario isn't hypothetical; a security flaw in LG's smart home app once made such a smart oven exploit possible.

Hardware security flaws are found beyond kitchen appliances, and the consequences of these vulnerabilities in other smart devices can be even more severe. The medical field is an industry where hardware hacks of smart devices can be extremely dangerous. In 2017, the FDA confirmed serious security flaws in St. Jude Medical's cardiac devices. It revealed that hackers could potentially manipulate pacemakers and defibrillators through their remote monitoring systems, not only compromising patient data but potentially endangering lives. For such industries, the stakes extend far beyond data protection to matters of life and death.

The Power of AI

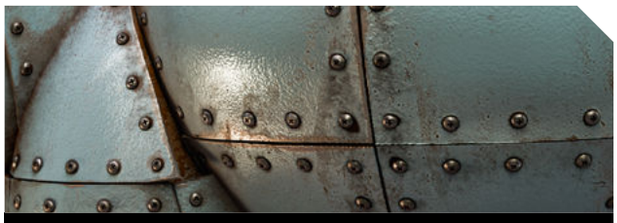
AI is changing the security industry, and hardware is no exception. First, it's making tools more powerful. AI significantly enhances the effectiveness of side-channel attacks.

For example, AI algorithms can perform complex analyses, discovering minute variations in power consumption, electromagnetic emissions, or timing data from a device. Additionally, they can identify behavioral patterns that humans might miss. Moreover, AI's ability to quickly process and adapt to complex patterns makes it particularly suited for tackling the intricate timing issues often associated with fault injection techniques. AI can help determine the correct frequency, timing, and intensity of induced faults.

AI can also extend the reach and speed at which a hacker accesses systems—the ability to automate and parallelize attacks enables simultaneous breaches across multiple devices. For instance, an AI can digitally analyze webcams and access vision data that would normally take one person hours to process.

Using AI, a threat actor can tap multiple webcams and create reconnaissance targets and large, powerful intelligence networks. In the not-so-distant future, devices may be so interconnected that an AI could hack all sorts of devices with just an internet connection.

AI could also pose a threat to physical security. It could analyze vast amounts of data to create convincing fake identities, complete with realistic credentials and background information. These might create digital IDs or RFID badges, potentially granting access to restricted areas like server rooms or data centers. Once inside, an attacker could compromise systems or install backdoors, leading to data breaches, espionage, or service disruptions.



What Happens Next

Looking to the future of hardware security, we can expect several key developments as AI continues to evolve. AI-driven defense mechanisms will likely emerge, resulting in automated systems for detecting and responding to hardware vulnerabilities. We'll see an increased focus on securing the intersection of hardware and software, recognizing that vulnerabilities often lie in their integration.

While the threat of hardware hacks is significant, this is not a cause for panic but a call for action. The growing community of hardware security experts, now more open to newcomers than ever, stands ready to protect the vast array of devices that our world depends upon.

The security of any system is only as strong as its weakest link. Let's ensure that hardware doesn't become that weak link.

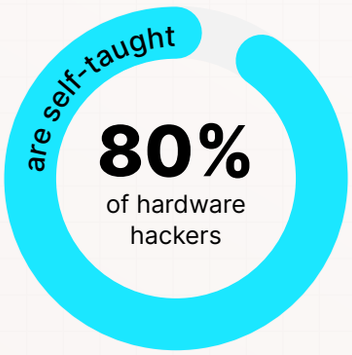
Hardware Hacking Quantified

It's hard to buy anything these days without some form of an interconnected functionality.

Hardware hacking specialist Brandon Reynolds said it best: "IoT has taken the world by storm and has become the true Wild West of our constantly evolving world. Unfortunately, not many understand what is happening underneath the shiny exterior of their new toy. It could be running around all day shouting your WIFI password, and you wouldn't have a clue unless you knew what to look for!"

Whether we're talking about cars or medical devices, the idea of hardware vulnerabilities being exploited is a scary prospect. Luckily, the Bugcrowd Platform partners with hardware hacking specialists, some of whom are spotlighted in this report, to help support organizations' attempts to secure their hardware and firmware.

Get to Know Hardware Hackers



Many hackers start with tools such as microcontrollers, breadboards, voltmeters, logic analyzers, and packet sniffers.

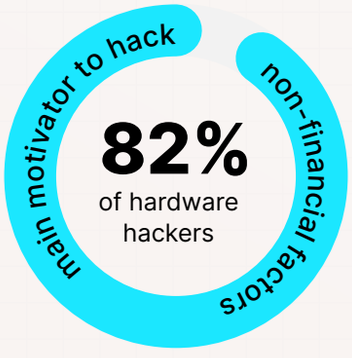
Ask a Hacker

Is hardware hacking too expensive to break into?

BusesCanFly "I think there have been some big advancements and steps to make hardware hacking much more accessible, like less costly tools and plentiful guides and information. While there are absolutely some crazy pricey tools that can make things easier, they're very rarely necessary. Like with all hacking, creativity and problem-solving go a long way."

83%
of hardware hackers are confident in hacking AI-powered hardware and software.

1/3
of hackers believe hardware hacking is one of the most valuable specialties.



Only 18% of hardware hackers hack for the money. In contrast, 31% hack for personal development, 18% hack for excitement, and 11% hack for the challenge

The State of Vulnerable Hardware

81%
of hardware hackers encountered a new vulnerability they had never seen before in the past 12 months.

64%
of hardware hackers believe there are more vulnerabilities now than there were a year ago.


Ask a Hacker

What kind of hardware or firmware are most vulnerable to attacks?

Top Five Types of Hardware and Firmware Most Vulnerable to AI Attacks

According to Hardware Hackers

1. IoT devices
2. Autonomous vehicles
3. Smartphones
4. Medical devices
5. Industrial control systems

Lennert → "Devices that were not designed with security in mind are the most vulnerable to attacks. Other vulnerable hardware includes unnecessarily complex devices and cheap consumer hardware."

Topy → "Anything IoT/cloud/network-enabled is most vulnerable to attack. The attack surface explodes when it's network-connected. Very often you'll find that one device holds the keys to the kingdom and can attack all other devices through some kind of cloud infrastructure."

Partnering with Hardware Hackers

Ask a Hacker

How important is it to work with hardware hackers?

Brandon Reynolds → "There are some great minds out there who truly understand the potential vulnerabilities that can be found in hardware. But based on my experiences going out into the real world and speaking with the companies developing hardware devices, I find that often, they don't understand unless someone can handhold them through the process. There are exceptions, but I fear the average internal hardware team is going to be of a much lower caliber than your average hardware-tinkering hacker out there on the Bugcrowd Platform."

You'll get to know more through the next article.

Because there was no clear pathway to do so.

57%
of hardware hackers say a responsive team is the most important factor when considering their next engagement.

Meet Brandon Reynolds

A Hardware and Embedded/IoT Specialist

Brandon Reynolds is a hardware expert and IoT specialist. He's been a key participant in multiple Bugcrowd Bug Bashes, and his supportive nature, friendly attitude, and excellent work ethic leave a lasting impression on everyone he meets.

Read on to learn more about how Brandon balances hacking, a security career, and a family in this hacker spotlight!

Brandon's "Hacking Origin Story"

Brandon grew up in Central Illinois surrounded by cornfields, cornfields, and more cornfields. While this meant that there wasn't much to do, it did mean that he had a lot of time to dedicate to programming and security.

When he was roughly 14 years old, Brandon wanted to understand how his game consoles and other electronics worked at their most basic levels. Learning to dis-assemble video games, PC applications, and other software or firmware led him to software development, and eventually, to a full-time focus on cybersecurity.

"If I hadn't been so interested in how everything worked as a child, I likely wouldn't have developed the early knowledge required to do all of the unique things I can today."

When he was around 16 years old, he wrote video game software that was sold at stores like Walmart.

The World of Hardware Hacking

Brandon started hacking in 2020, roughly when the COVID-19 pandemic started. He hacks part-time, mostly late in the evening. He also works as a principal security architect and a CSO.

"In general, finding security bugs was always a big puzzle to me. If it's built by humans, there's always mistakes."

He specializes in embedded development and IoT/hardware hacking. However, to take on these technologies, you also have to have a solid understanding of various other areas (mobile, cloud, etc.), which Brandon has.

"I don't have a specific methodology I incorporate. I tend to focus on many different pieces of hardware at once. If I get stuck on a particular problem or hurdle, I switch to a separate device altogether," Brandon says. "This strategy has both pros and cons; it makes it easy to let a project sit for too long or to take much longer than I had hoped when I switch back and remember everything involved in where I had left off."

In the hardware world, there are so many tools that are not only necessities but also derivatives of one another (like serial/UART adapters). His favorite tool is his Saleae Logic Analyzer.

Hacking Impact

In the three years that Brandon has been hacking, he's already earned life-changing rewards. The bug bounties he has received paid for nearly his entire wedding and a new car (all from a single program)! "I'll always be thankful for the rewards I've received for helping companies secure their products," Brandon says.

When asked why he hunts with Bugcrowd, Brandon says, "I've gotten to know so many people (both hackers and Bugcrowd employees). They've all treated me with respect."

Looking forward, Brandon hopes to continue building his own security company with a hardware focus.

"Getting to work with others who are certainly more skilled is humbling and provides the chance to learn a great deal about certain areas I have potentially overlooked or could optimize."

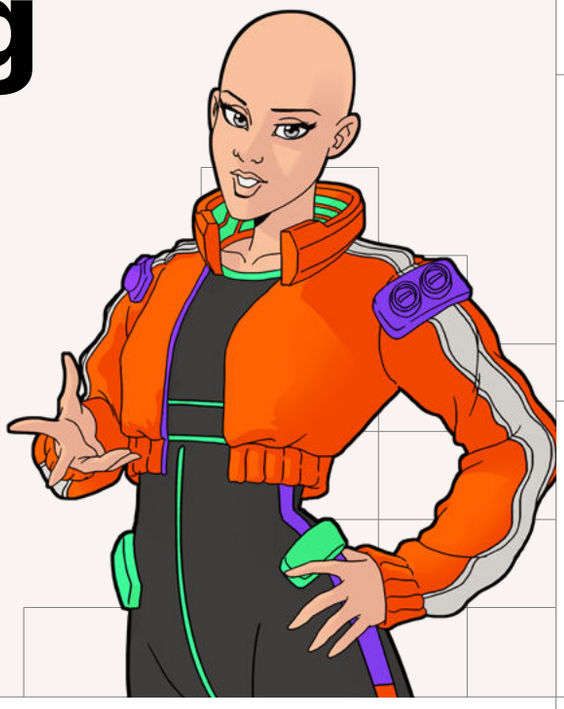
VIEW PROFILE

12 MONTHS OF AI INNOVATION

We asked hackers these five questions about their generative AI usage and beliefs in early 2023, and we asked them the same questions a year later. Check out how their responses changed in only 12 months!

	2023	2024	
Hackers who believe AI technologies increase the value of hacking	21%	**71%**	Whoa! In just a year, AI dramatically proved its value to hackers.
Hackers using generative AI for hacking	64%	**77%**	More hackers are adopting generative AI technologies in their security research workflows!
Hackers who believe AI technologies outperform the abilities of hackers	21%	**22%**	Beliefs around AI outperforming or replacing hackers have relatively stayed the same.
Hackers who believe AI technologies will eventually replicate the human creativity of hackers	28%	**30%**	
Top use case for generative AI in hacking	Automating tasks	**Analyzing data**	From automation to report writing to improved accuracy of hacking tools to analyzing data, hackers are finding new ways to leverage AI.

The Three T's of AI Hacking



A lot happened in AI last year. The release of GPT-4, Claude 3, and numerous open-source models, as well as the introduction of vision and voice models, have electrified, and concerned, the security industry. Some hackers are wondering, "How can I use AI to become a better hacker?" while others are concerned AI might fully replace them. Meanwhile, everyone agrees that companies using AI have a new class of vulnerabilities to worry about now. At Bugcrowd, we frame this as the three Ts of AI: AI as a tool, a target, and a threat.

We wrote an eBook on the top Generative AI vulnerabilities earlier this year.

Check it out here to read up on the vulnerabilities, the systems most at risk, and ways to mitigate the damage.

AI as a tool

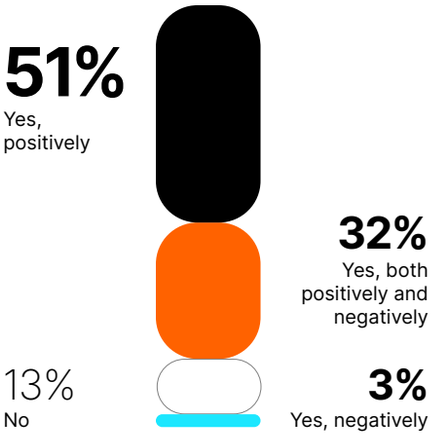
Both sides of the cybersecurity game will use AI to increase the scale and sophistication of their tactics. For example, threat actors can create convincing spear phishing attacks at scale and defenders can use AI models to detect intrusions within milliseconds.

86% of hackers say AI has fundamentally changed their approach to hacking, for better or worse.

Top five ways AI technologies make hacking more fun, profitable, or interesting (according to hackers)

- Automating repetitive tasks to free up time for more complex ones.
- Enhancing data analysis, allowing for deeper insights.
- Simulating reconnaissance and attacks to predict weaknesses.
- Developing and training AI copilots to support workflows.
- Uncovering new patterns and trends in data.

Has AI fundamentally changed your approach to hacking?



Top 3 Ways Hackers Use AI

I, Robot is not quite here yet. AI is not, by itself, automatically detecting vulnerabilities.

Despite how advanced AI seems, most hackers are using it for basic tasks like running queries on data and creating reports.

In most cases, AI takes away the tedious hacking tasks so hackers can reserve their brainpower for the hardest parts: identifying and exploiting vulnerabilities.

Analyzing data

62%

Automating tasks

61%

Identifying vulnerabilities

38%

Ask a Hacker

That's not to say that AI can't offer valuable help.

Anonymous "AI is great for helping to understand error conditions in binary protocols that I'm not as familiar with."

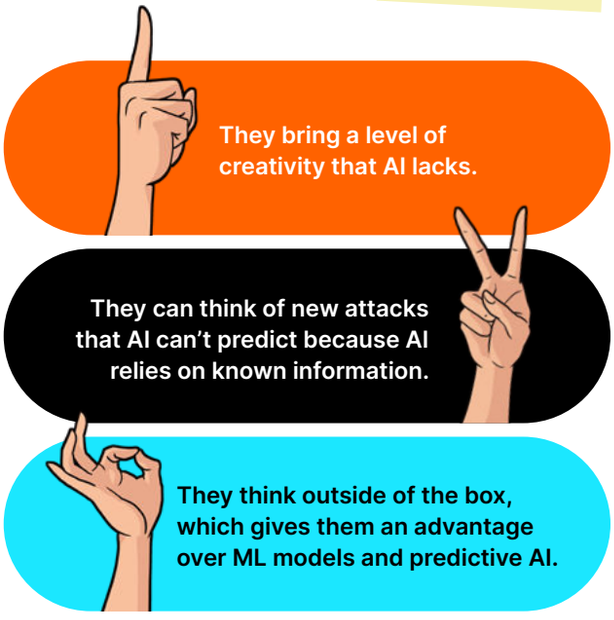
A task that could have taken hours to digest could take just a few minutes.

Top three ways hackers believe they provide more value than AI in cybersecurity

The reasons revolve around creativity and adaptability. Most hackers believe that AI cannot match human creativity, such as the ability to try out crazy-sounding attack vectors and find they actually work.

AI reasons based only on past knowledge while hackers can venture outside the box to find exploits. Additionally, hackers can easily uplevel themselves while finetuning a model takes quite a bit of effort and data.

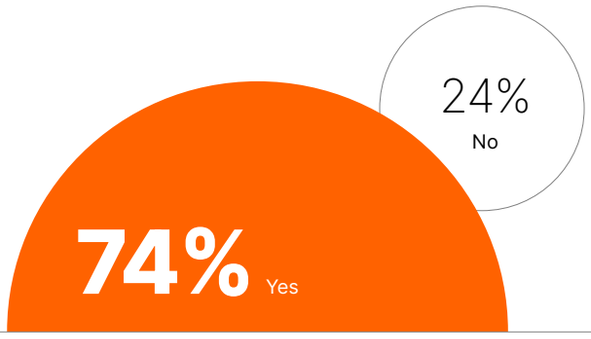
Almost half of the hackers believe that AI will never beat them in value or effectiveness.



Has AI made hacking more accessible?

AI makes learning a lot more digestible. ChatGPT and Claude have helped new hackers advance their understanding of hacking methods.

Hackers can also use these tools to explain tricky code or why certain exploits work and others don't. (That is, of course, if hackers can detect and ignore the hallucinations.)



Ask a Hacker

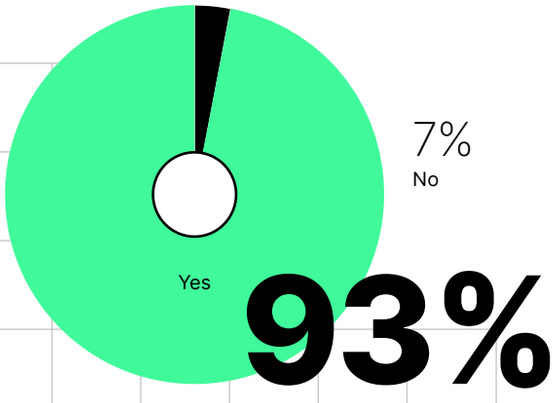
How AI has impacted the accuracy and reliability of their hacking tools, such as scanners and scripts

Anonymous "AI has significantly improved the accuracy and reliability of hacking tools by enhancing detection capabilities, automating large-scale data analysis, and continuously adapting to new threats. It excels at recognizing patterns and anomalies, enabling quicker and more precise identification of vulnerabilities. Additionally, AI's predictive capabilities and customization options make these tools more effective at handling complex cybersecurity challenges."

AI as a target

AI systems will be a new attack vector. Many new AI systems have access to company data and resources, and unmitigated vulnerabilities (such as prompt injection) will give threat actors a new way into these resources.

Have companies using AI tools introduced a new attack vector for threat actors to exploit?



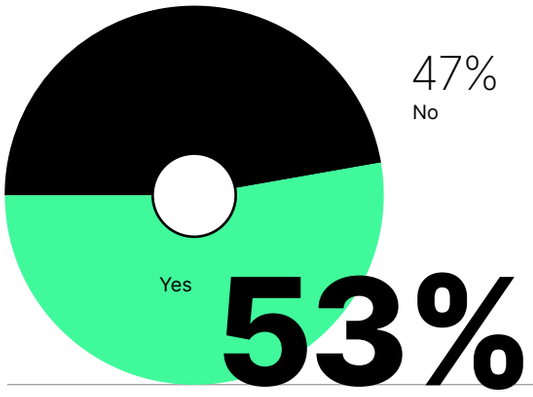
Ask a Hacker

Here is one hacker's example of discovering a new vector:

Anonymous "I achieved a remote code execution (RCE) accidentally while chatting with an AI bot that was misconfigured and had the ability to execute OS commands on the system where it was hosted. It provided me with the command output."

Hackers *overwhelmingly* believe AI is ripe for exploitation. Even using AI on the backend creates new flaws in the attack surface of the product.

Do existing security solutions meet the needs and risks of AI?



Vendors are racing to provide security solutions that actually secure the AI attack surface. Hackers are split down the middle as to whether these solutions are actually effective.

Luckily, the crowdsourcing model of security testing will always stay on top of emerging threats.

Human ingenuity wins again!

As expected, hackers don't have much confidence in companies securing their AI systems. It's also not surprising to see that CISOs are more confident in their security abilities. What is surprising, though, is the sheer difference in confidence levels. More than two times as many hackers think that the vast majority of companies will be blindsided by AI security issues.

The devil is in the details, and hackers see AI exploits every day, which explains this discrepancy.

Hackers and CISOs both agree that *most* companies are not prepared for AI, period.

How many organizations are adequately prepared to tackle AI security?

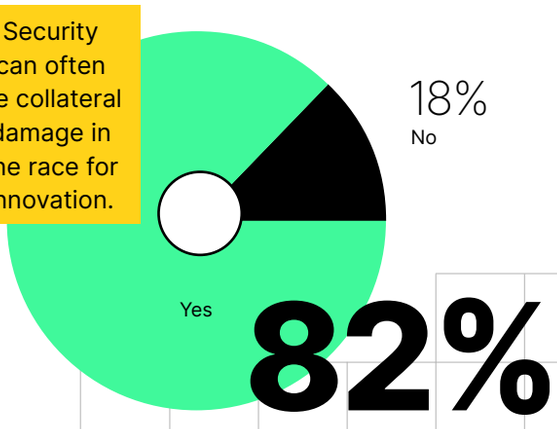
Hackers		CISOs
41%	Less than 10%	**17%**
33%	10–25%	**31%**
20%	26–50%	**34%**
5%	51–75%	**15%**
1%	76–100%	**3%**

Are you confident in your abilities as a hacker to uncover vulnerabilities in AI-powered apps?

Even though AI-powered apps are relatively new, three-quarters of hackers already feel confident in their abilities to bug hunt on this new attack surface.

Is the AI threat landscape evolving too rapidly to adequately secure?

Security can often be collateral damage in the race for innovation.



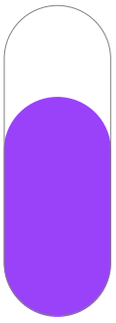
AI as a Threat

AI systems can cause harm to users. This harm could range from realistic (saying biased things) to speculative (future models could be used to create weapons).

Can organizations broadly trust AI-informed decisions and workflows?

To a point, but organizations must balance AI's power with human creativity to reduce risks	**37%**
AI is fine for low-stakes tasks, but we should tread carefully in critical applications	**45%**
Yes, but only with the safety net of human oversight to ensure accountability	**7%**
Yes, as long as AI models are transparent and regularly audited	**6%**
No, there's still too much uncertainty and potential bias in AI systems	**2%**

Do the risks associated with AI outweigh its potential?



No
28%

Yes
72%

As you can see, AI offers many benefits when hackers use it as a tool.

However, hackers overwhelmingly believe that the risks associated with AI outweigh the benefits.

Top five ways AI technologies can be misused to weaken an organization's cybersecurity or GRC measures (according to hackers)

1. Creating fake data and identities that are hard to detect
2. Manipulating systems to carry out nefarious tasks
3. Developing tools and methods for large-scale attacks
4. Poisoning data inputs to influence predictive models
5. Exploiting errors and biases that affect risk decisions

Conclusion

That's a wrap on this year's edition of *Inside the Mind of a Hacker!* This year, we explored how quickly hacker attitudes regarding AI (as a tool, a target, and a threat) are changing. We also explored the unexpected path into the world of hardware hacking.

Here are three major takeaways from the research:

Hacking is a viable income source.

The majority (90%) of hackers are Gen-Z or millennials. Younger generations are flocking to hacking and reaping the benefits. 61% cited that hacking helped them find a job. 59% are hacking fewer than 14 hours per week, making hacking the flexible income source that is so desirable right now, especially considering it can be done at home (or anywhere else in the world, for that matter).

Hardware hacking is on the rise.

Hardware is everywhere, and even more is being created to support the infrastructure needs of AI. Hardware vulnerabilities are on the rise, and they have major implications. 81% of hardware hackers encountered a vulnerability type they had never seen before in the past 12 months. Hackers are up for the challenge, partially due to the increased accessibility of hardware hacking tools and educational materials.

AI is the new normal.

AI is making hackers faster and more accurate and is overall making hacking more fun. It's also making hacking more accessible. 77% of hackers use AI to hack and 86% say it has fundamentally changed their approach to hacking. But AI isn't just a tool—it's a target. AI is a new attack vector that 82% of hackers believe is evolving too rapidly to adequately secure.

The hackers surveyed and spotlighted in this report are security experts on the cutting edge of an ever-evolving threat landscape. They aren't just breaking our applications, network infrastructure, and hardware, they're building it back up too. With each flaw that is exposed, security teams' defenses strengthen.

For as long as humans write code and deploy the systems that power the internet—and for as long as humans have reason to maliciously attack these systems—crowdsourced security will play a fundamental role in helping organizations tap into the creativity, technical expertise, and ingenuity of hackers.

Pair this badass hacker community with an AI-powered platform, skill-matching technologies, and a fast-moving triage team?

Your security team will be unstoppable. But you know who won't be unstoppable? The threat actors waiting at your perimeters. Let's keep them out, shall we?

Content Gallery

Chow down on more hearty stories from Bugcrowd below

REPORT

Inside The Mind Of A CISO

Gain a Better Understanding of the Evolving, Nuanced Role of the CISO

GUIDE

The Ultimate Guide To AI Security

The Basics of AI Security + Ways to Prevent Attacks Against AI Systems

DATA SHEET

Engineered Hacker Trust

How We Build the Right Team of Trusted Hackers for your Program

DATA SHEET

Discover CrowdMatch

The Technology that Brings You the Right Crowd at the Right Time

Glossary

This year's edition of Inside the Mind of a Hacker has 9,594 words! That's a lot of foundational security terms, emerging AI lingo, hidden pop culture references so our Gen-Z social media manager thinks we're still relevant, and even the occasional buzzword (we're only human).

We've defined a few here, but check out the Bugcrowd Glossary for an extensive list of definitions and additional resources.

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

AI Red Teaming: A technique used to test the security of machine learning models. It involves simulating attacks on the model to identify vulnerabilities and weaknesses.

Autonomous Vehicles: A vehicle capable of sensing its environment and operating without human involvement.

Brat Summer: A social media trend during the summer of 2024, originated from the themes of Charli XCX's album, Brat.

Bug Bash: In-person, 1-2 day events that bring hackers and customers together in a high-intensity, highly collaborative, bug bounty-style program managed by Bugcrowd.

CTF Events: A Bugcrowd Capture the Flag (CTF) event is a collaborative hacking challenge where hackers can win swag bundles, earn private invites, and network with other hackers.

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

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

Fault Injection: A technique used to evaluate a system's dependability by intentionally introducing faults to observe how it reacts.

Firmware: A form of microcode or program embedded into hardware devices to help them operate effectively.

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.

Hardware Hacking: The process of manipulating or modifying physical devices in order to gain access to their functions or data.

I, Robot: A 2004 science fiction action movie where highly intelligent robots fill public service positions throughout the world.

Internet of Things (IoT): Any device (often called a smart or connected device) that connects to and exchanges information over the internet.

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.

OWASP: The Open Web Application Security Project (OWASP) is a non-profit organization that works to improve the security of web applications.

Phreak: A subculture of hacking that started in the 1970s. These hackers focused on manipulating and exploiting telephone networks.

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.

Safe Harbor: A provision from an organization that hackers engaged in good faith security research and ethical disclosure are authorized to conduct such activity and will not be subject to legal action from that organization.

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.

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

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

Vulnerability Rating Taxonomy (VRT): The official standard used by Bugcrowd for assessing, prioritizing, and benchmarking the severity of security vulnerabilities.

INSIDE THE MIND OF A HACKER 2024

bugcrowd