The Hacker Culture Manual

////A celebration of hacking

For hackers=====.==========

==========By hackers.

hack the planet

Contributors

CASEY ELLIS
ERICA AZAD
SANTERRA HOLLER
ALISTAIR G.
AOS DAWSON
P3T3R_R166IT
SW33TLie
ERIK deJONG
ALX
BSYSOP
ZWINK
LUKE
VINAMRATA SINGAL
TATIANA KALIST (TATI)
DANIA DURNAS
ICEMAN
SYNTAX
CAMI MACCA

MESS WITH THE BEST. DIE LIKE THE REST.

Compiled and designed by
bugcrowd

*The Hacker Culture Manual is entirely human-made.
No AI was used in the writing or design.

Own3d

Hacker culture at a crossroads

By Erica Azad

Preserving what matters

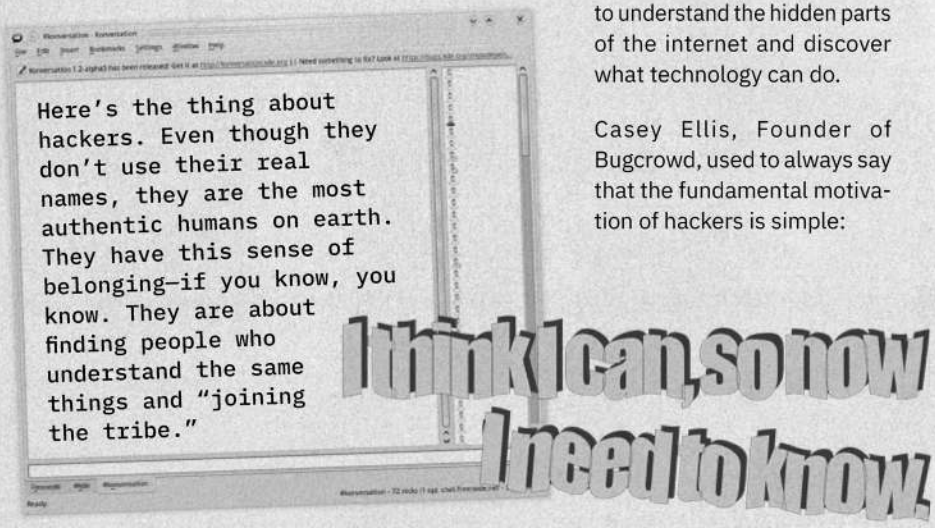
In my six years of being in Bugcrowd's orbit, I've interviewed thousands of hackers, wrote hundreds of assets, and published 378 blogs (yes, I counted). My goal was quite literally to get inside the mind of a hacker. At first, it was just a job. But now, it's a passion.

I wrote the Hacker Culture Manual to celebrate the hackers I've been quietly admiring for years and to share the stories of the people who helped Bugcrowd get where we are today.

Even though hackers are incredibly cool and often elusive, I quickly realized the exclusivity wasn't about keeping people out. Sure, they have handles and hidden spaces, but anyone curious and willing to learn belonged. They have a "you can sit with us" vibe for anyone who didn't quite fit in elsewhere, and that's just as important as the underground mystique.

Each year when I survey hackers about their motivations, it always comes back to curiosity. Hackers have a drive to understand the hidden parts of the internet and discover what technology can do.

Casey Ellis, Founder of Bugcrowd, used to always say that the fundamental motivation of hackers is simple:



Plus, hacking is just fun. Casey used to tell a story about how in the early 2000s, he'd drive around scanning for open WiFi networks. Everyone had gotten wireless internet and deployed it everywhere without thinking about security, which is a technology anti-pattern that we still see today. He'd drive around, connect to open wireless networks, find a printer on the inside, and print out a little note:

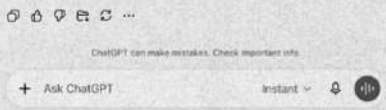
"Hey, your WiFi is open. You should probably close it."

That is objectively hilarious. I love the mental image of someone walking into their office and discovering a mysterious note on their printer. But jokes aside, it also helps people.

How hacking changed

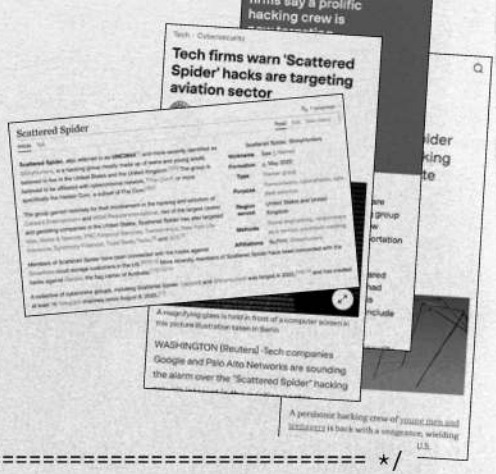
Fast forward to today, the hacking world looks quite different. The trend from my hacker interviews points to COVID really being what accelerated the change. That makes sense, considering everyone was suddenly indoors on their computers. Jobs felt unstable. We were all just trying to figure out our futures while the internet changed at a million miles an hour. The hacking scene became more serious and anxious as young people started to face career pressure.

Sound familiar? Yep, 2026 is feeling the same way with the arrival and commoditization of AI.



The playful curiosity that defined early hacker culture has been replaced by survival-mode thinking. The field's professionalization has brought about real benefits—it's diverting people away from crime and creating legitimate career paths. But it has also poisoned some of the purity, and in many ways, the actual core of hacking. The generations coming in now are really serious about everything, and while that's fine, we're losing the simple joy of exploration.

Attackers have changed as well. In the past, attacker motivations were relatively clear and predictable, including hacktivism, financially motivated cybercrimes, and nation-state activities.



Today, we have groups like Scattered Spider and Lapsus, which are essentially random threat actors driven by anger and a sense of rebellion. They hack destructively rather than curiously, which makes them both unpredictable and harder to defend against.

```
/* ========================================================== */
/*  A golden rule of hacking used to be that                  */
/*  curiosity always outweighs destruction.                   */
/*                                                            */
/*    __ _  _ _ _(_)___ __(_) |_ _  _                         */
/*   / _| || | '_| / _ (_-< |  _| || |                        */
/*   \__|\_,_|_| |_\___/__/_|\__|\_, |                        */
/*                               |__/                         */
/*    __ _| |_ __ ____ _ _  _ ___                             */
/*   / _` | \ V  V / _` | || (_-<                             */
/*   \__,_|_|\_/\_/\__,_|\_, /__/    _                        */
/*    ___ _  _| |___ __ _|__/(_)__ _| |_  ___                 */
/*   / _ \ || |  _\ V  V / -_) / _` | ' \(_-<                 */
/*   \___/\_,_|\__|\_/\_/\___|_\__, |_||_/__/                 */
/*        _          _           |___/  _                     */
/*     __| |___ __| |_ _ _ _  _ __| |_(_)___ _ _              */
/*    / _` / -_|_-<  _| '_| || / _|  _| / _ \ ' \ _           */
/*    \__,_\___/__/\__|_|  \_,_\__|\__|_\___/_||_(_)          */
/*                                                            */
/*  But when you remove curiosity from hacking, all           */
/*  you're left with are dopamine hits—you eliminate          */
/*  the art from the form. This isn't just my opinion,        */
/*  by the way. The majority of hackers, 95% of them,         */
/*  view their work as an art form.                           */
/* ========================================================== */
```

Looking ahead, as the world plunges further into instability, these changes will intensify. We're heading toward a reality where active disruption and offensive countermeasures become the norm. There's legislation moving through Congress to create frameworks for privateering against cyber threat actors, and other countries are following suit. At the same time, the internet will likely continue to balkanize as nations prioritize sovereignty over the principles of open connectivity that defined the early internet.

Passing on the knowledge

We went from networking to personal computing—to web, mobile, and now chat and AI—and everything will keep accelerating. Each generation grows up native to different technologies, which means they often skip past the foundational principles that previous generations took for granted. When Docker first became popular, there was a glut of publicly exposed and vulnerable systems on the internet. That was because newer developers did not understand basic networking concepts; they had learned in an era of containerization and cloud services. The abstraction layers keep piling up, letting people accomplish more while understanding less about what's actually happening underneath.

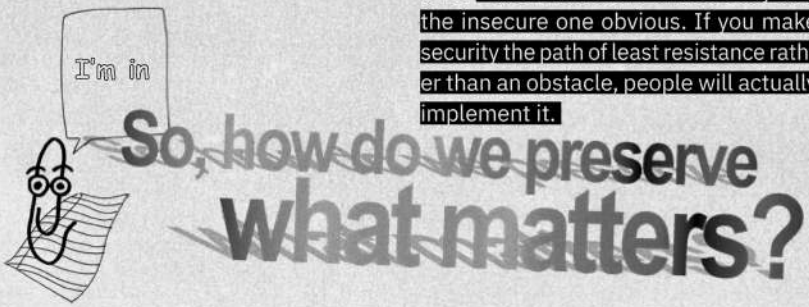
Something I've found really special is the intergenerational sharing that happens in hacking. A hacker in their 50s in Sweden is making memes with a 19-year-old hacker in Mexico. They have completely different life experiences, tooling, and perspectives on hacking. But they still come together, listen to each other, and learn. That ability is pretty powerful in today's landscape. I think the rest of the world could learn a lot from this.

At B-Sides Las Vegas last year, Casey shared a presentation about how a recent health scare taught him that our opportunity to share what we've learned isn't evergreen. There is an ever-growing list of legends and pioneers in security thinking who have passed away over the past 10 years.

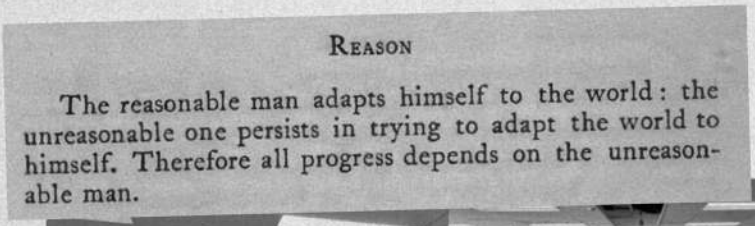
Ultimately, the newer generations are inheriting a world of challenges, and I believe older generations must create space for younger generations to understand the culture of the past in order to shape it into what they want and need.

On the other side of the coin, there are core principles in security that new generations must relearn. I keep watching people rediscover that security fundamentals always resurface. For example, most organizations don't actually prioritize security because it's expensive, inconvenient, and not their core business model. Most people entering security assume that everyone will understand its importance and implement it properly. Then, economic reality sets in. Security is, for the better part, a cost center.

Another thing Casey used to say that I love: Make the secure choice easy and the insecure one obvious. If you make security the path of least resistance rather than an obstacle, people will actually implement it.



What I hope won't change



REASON

The reasonable man adapts himself to the world: the unreasonable one persists in trying to adapt the world to himself. Therefore all progress depends on the unreasonable man.

George Bernard Shaw, Man and Superman (1803)

Researchers at Bugcrowd's recent live hacking event

In many of the hacker interviews I've conducted, I've noticed three traits that form a common thread through the different generations and seasons.

Here's the thing about hacking and the hacker community: hacking (and hackers) predates its (their) corporatization. It even predates its own legality. While there have been huge leaps and bounds in the acceptance, adoption, and embrace of "opposite thinking" by those who can benefit from it, the relationship between hackers and corporations is fragile in both directions.

It's worth calling out what the fundamentals are and what needs to be protected going forward.

The first is that childish curiosity.

337

The generations coming up now are incredibly serious and focused, which serves them well in the current climate and given all of the different problems they'll eventually inherit. Among the hacker community, there's still the irreplaceable, simple joy of exploring the digital world and getting technology to do things it was never meant to do. There's so much excitement and thrill in that discovery. I hope this aspect continues to be a hallmark of hacker culture and the foundation for incoming generations facing the difficult task of balancing pragmatism, idealism, and optimism.

The second is the antiestablishment questioning

2

...that has, in many ways, defined the hacker. Hackers question authority by default, not to cause trouble but to honor the ethos that "all progress relies on the unreasonable person." Just because you are given an explanation of how something works doesn't mean that you are going to accept that as the only answer. Hackers' immediate instinct with the assumptions they're handed is to turn them upside down and see what falls out.

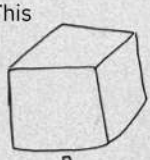
This isn't just a personality quirk or rebellious posturing. It's a core part of why hackers are strategically valuable to the broader technology ecosystem. If no one is questioning how systems fundamentally work and challenging their assumptions, then no one will uncover the vulnerabilities and systemic weaknesses that need to be addressed. Hackers are different, and that difference is what makes you irreplaceable.

The third is tenacity.

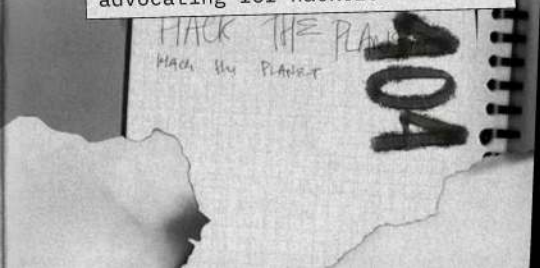
3

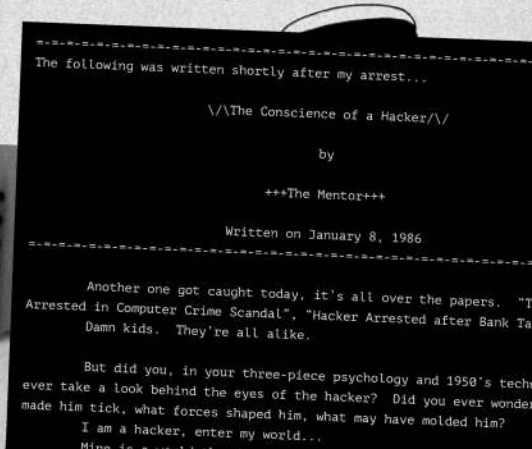
This is a throwback to The Mentor's "The Hacker Manifesto," and it still applies today. When a hacker is presented with a difficult problem, it becomes a splinter in our brain; we either need to solve it or conclude that we cannot. This stands in sharp contrast to the march toward greater and greater convenience—and all the technological and social consequences that accompany it.

Hacker culture has always attracted smart, square pegs trying to fit into round holes. Even as we've become normalized over the past 10 years, we're still very much a refuge and a tribe for the weird and the unconventional. This community aspect matters deeply. I don't see this core principle ever changing, and I hope it never does.



///// Thank you to Casey Ellis for his major contributions to this article and for always advocating for hackers.





The following was written shortly after my arrest...

\/\The Conscience of a Hacker/\/

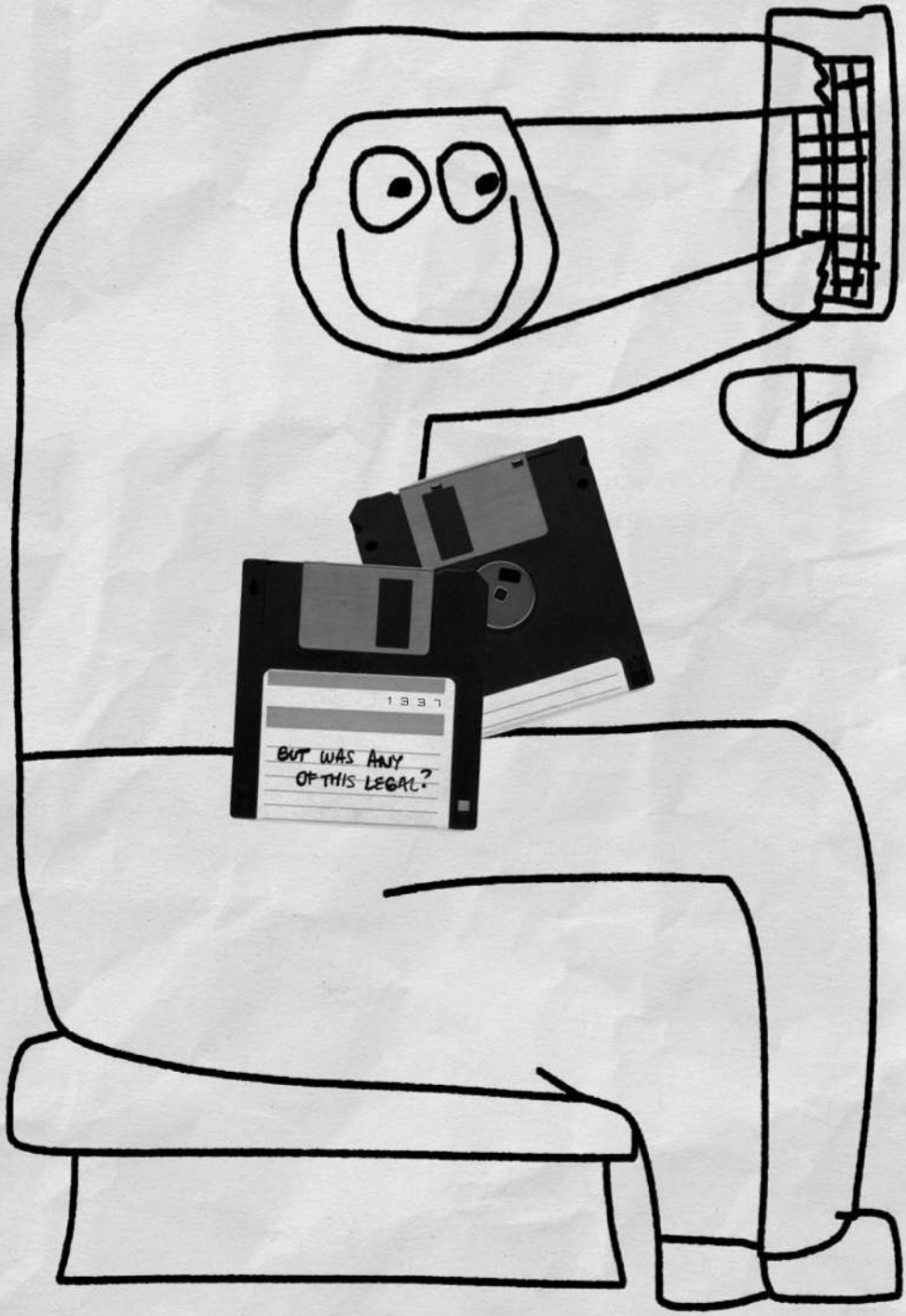
by

+++The Mentor+++

Written on January 8, 1986

Another one got caught today, it's all over the papers. "T
Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Ta
Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's techn
ever take a look behind the eyes of the hacker? Did you ever wonder
made him tick, what forces shaped him, what may have molded him?
I am a hacker, enter my world...


1337
BUT WAS ANY OF THIS LEGAL?

The unwritten rules of hacking

1. Snitches get stitches

In the realm of hacking, confidentiality is key. If you have to do something a little less-than-legal in good-faith, hackers agree to look the other way.

OK

2. Share knowledge, don't hoard it

Transparency is woven deeply into the fabric of hacker culture. If you did something cool, show how it worked.

OK

1337. Experience matters more than titles and certificates

You could spend thousands of dollars on certificate courses, but ultimately, what you can do and your experience is the most meaningful.

OK

4. PCAPs or it didn't happen

If you flex, you've got to back it up. Record logs of network traffic, provide technical proof, and keep the receipts. Yes, script kiddies, I'm looking at you…

OK

5. Curiosity outweighs destruction

When you remove the curiosity, all that is left is the occasional dopamine hit of a vulnerability finding. Hacking is about heart.

OK

6. Be gay, do crime

This rule doesn't necessarily speak about literal homosexuality, but instead, the intersection between hackers and queer counterculture spaces. It's about nonconformity, rejection of mainstream social norms, hacktivism, and breaking unjust laws.

OK

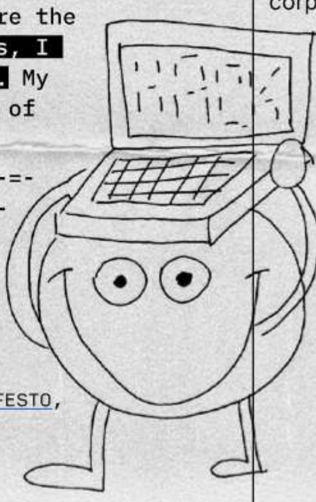
There are 25 “1337s” hidden in this manual. Are you leet enough to find them all?

The crime of curiosity

50 years of hacker culture

"We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals. Yes, I am a criminal. My crime is that of curiosity."

THE HACKER MANIFESTO, 1986.



It wasn't too long ago when hackers were viewed as everything from sophisticated criminals to societal menaces. The Hacker Manifesto set the record straight about what really drives hackers: their curiosity and desire to make the world a better place.

These words couldn't be truer today, as a small group of corporations controls how we live. To protect everyday citizens, hackers use technology and information to keep these corporations in check and, ultimately, push for a kinder, more equal society. Even if the methods have changed, this spirit of curiosity-driven rebellion has shaped decades of hacker culture.

Let's take a walk down memory lane and see how the art of hacking has evolved across the decades—even as its heart has remained the same.

'70s IT'S GIVING... PHREAK

OVERALL VIBES The 70s marked the beginning of hacking, known as phreaking. It's a combination of "phone" and "breaking," aptly capturing broader society's view of hackers at the time.

THE BIRTH OF PHREAKING

It all started with the random discovery that a **Cap'n Crunch cereal toy whistle** could generate the precise 2600 Hz tone needed to manipulate AT&T's phone system (we have Joe Joybubbles to thank for that).

The discovery ushered in the era of phreaking: manipulating phone systems to do whatever you wanted, such as getting free long-distance calls. Phreakers would often use tools like **blue boxes,** which had buttons that, when pressed, emitted sounds that could result in free long-distance calls.

Phreaking quickly became cool because it was an easy way to throw the middle finger at the man. After all, phreakers cracked the secrets of some of the biggest companies at the time—like **Blue Bell**—and shared them with the world. In fact, in 1971, ***Esquire Magazine*** even published a glowing profile on the creator of the blue box.

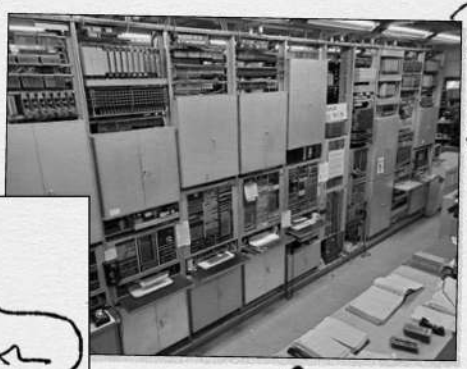
Even Steve Jobs and Steve Wozniak started as phreakers, making and selling blue boxes before building Apple. So, I guess Apple is a #phreak too!

THE MANY FACES OF PHREAKING

Phreak operations can take many forms, like:

- **Wardialing:** Dialing random numbers in hopes of connecting to a computer.
- **Trashing:** Raiding corporate trash for phone manuals and documentation.
- **Social engineering:** Calling phone company employees and pretending to be co-workers to get passwords or system information.

technically speaking the word HACKER was coined at MIT's Tech Model Railroad Club in 1995 to describe a clever shortcut for solving a technical problem ♥



after all the phone was the biggest network at the time!

Story time

ANATOMY OF A WAR DIAL

High schooler Paul Steero wardialed his way into New York Telephone's main switching system. Here's how:

1. He found his target by dialing numbers ending in 9999 (reserved by the telephone company for computers).
2. He made contact with his computer by blowing hot air into his modem.
3. He tried different commands (like "login" and "show users") to understand the system.
4. He left his mark by finding his friend's service record and giving him free three-way calling.

9999 - today's pass words of 1234.

BUT WAS ANY OF THIS LEGAL?

The short answer: kind of, but it was heavily frowned upon.

Case in point: *Ramparts*, an upstart magazine in San Francisco, published a detailed how-to guide on making mute boxes (similar to blue boxes). We're talking parts list, a detailed how-to, and troubleshooting instructions.

In the end, police raided their offices and forced the Ramparts team to recall all printed issues, resulting in severe legal, financial, and reputational damage—and the magazine went under.

get your phreak on

Get your phreak on.

"The practice [of phreaking] obviously spanned multiple decades afterward, producing notorious legends like Kevin Mitnick and inspiring an entire generation of hackers who specialized in manipulating telecommunications systems"

Hacker P3T3r_R4bb1t shares

'80s The era of transition

OVERALL VIBES The 80s had a lot going for it—Jazzercise, MTV, and the birth of the personal computer. That last one proved transformational for hackers, as it gave way to the rise of the bulletin board system (BBS), a space where they could share knowledge and trade software.

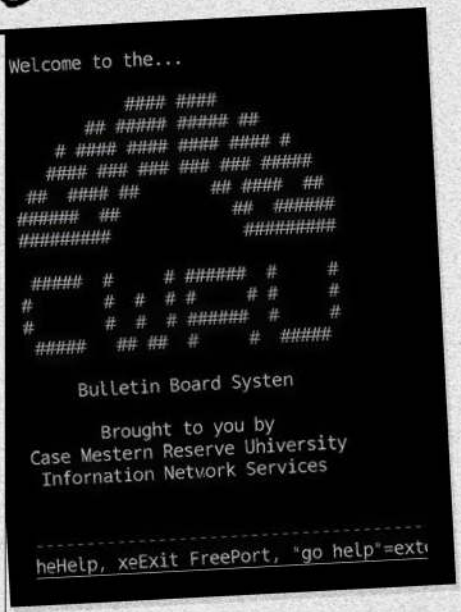
talking to people, so old school

BUT HOW DID ONE FIND A BBS?

Google didn't exist, so if you wanted to find the latest or hottest BBSs, you actually had to talk to people and ask for their phone numbers. Even if you had the correct number, you might have had to wait if the line was busy.

Once you got in, it was like entering The Matrix: a whole new world at your fingertips. It was decentralized by design, resulting in a more organic and free-form exploration experience. Soon, the BBS gave way to Internet Relay Chat (IRC), which allowed hackers to create real-time chat rooms.

the precursor to AIM (lyke yk)



But not all BBSs were good. After police started cracking down on hackers, the police created sting boards: what looked like a hacker BBS but was actually operated by cops.

1982 MY DIARY

Tuesday Date 6-8

Attend the Computer Chaos Club (C
meeting to trade notes with other ha

Wednesday Date 7-8

New issue of Phrack magazine comes out on BBS.

Thursday Date 8-8

Friday Date 9-8

Subscribe to 2600 magazine.

LOD IS BORN

In 1984, nine hackers formed The Legion of Doom (LOD), often considered the first "traditional" organized hacking group.

Phiber Optic, one of the OG members, explains their purpose: "[We took] information, primarily that was found trashing at telco central offices, and typed it in and made it available in what were known as LOD tech journals." This effort earned them a lot of street cred, making people want to join them.

But the more notorious they became, the more the police wanted to catch and punish the members, especially as LOD's anarchist rhetoric escalated. Eventually, the investigation grew so large that the Secret Service led a sting operation against them in 1988, which (fortunately) ended in a bust.

HACKING BECOMES CRIMINALIZED

In 1984, Congress passed the Comprehensive Crime Control Act (CCCA), the first computer crime law. The police began using this law to catch and punish hackers, prompting extensive raids by the FBI, the Secret Service, and local police.

In 1986, the government added an amendment to the CCCA, called the Computer Fraud and Abuse Act (CFAA). This law banned individuals from exceeding authorized access when using a computer, thereby making much of hacking illegal.

"How to Pick Master Locks"
"Acetylene Balloon Bomb"
"School and University Numbers"
READ

YES, same from DC comics!

HACK

Some of the best articles from Phrack's first issue in 1985:

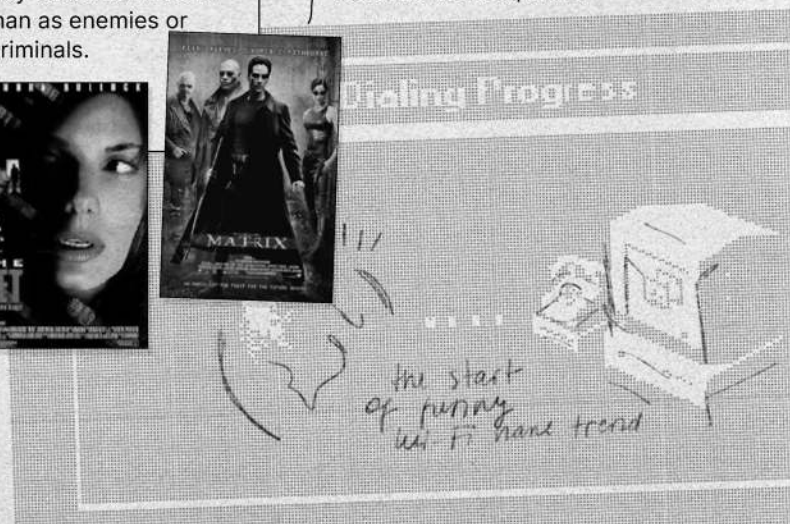
'90s The internet is born

OVERALL VIBES The 90s gave way to much of the technology we take for granted today. P3T3r_R4bb1t recounts, "Linux was born, along with the first commercial internet service providers, IRC channels, and early websites." And with all of this great power came a lot of legal troubles.

HACKING GOES HOLLYWOOD

During the 90s, Hollywood brought hacker culture to the big screen with *Hackers*, *The Net*, and *The Matrix*. These films portrayed hackers as intelligent, outsider, counterculture rebels who fought for what they believed in rather than as enemies or criminals.

"These movies created a very romanticized vision of the hacking culture: leather jackets, neon and fluorescent color everywhere, and completely unrealistic shell interfaces," P3T3r_R4bb1t explains.



CRACKDOWN ON HACKERS

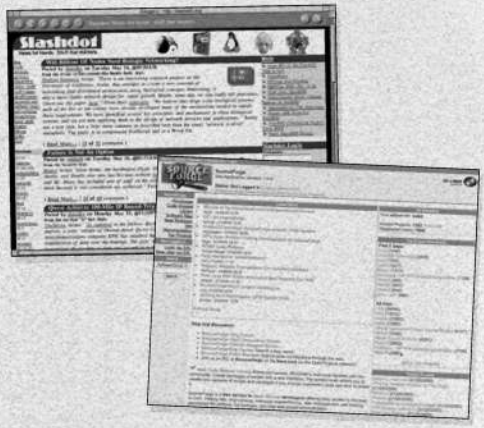
The 90s also saw an increase in legal crackdowns on hackers, and many cases became big headlines. "Governments and political systems declared war on hackers and accidentally made them folk heroes," explains Alistair G, Bugcrowd's Director of Red Teaming Operations.

Among the most notorious arrests was Kevin Mitnick, who was prosecuted twice by the U.S. Department of Justice for stealing proprietary software, accessing computers without authorization, and using illegally cloned phones. During his second conviction, the hacker community launched the "Free Kevin" campaign, but he ultimately accepted a plea deal and served five years in prison.

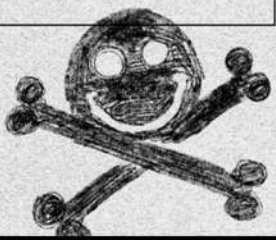
nothing boosts popularity like a government takedown!

- 1979: Mitnick conducted his first hack at age 16.
- 1988: Mitnick was convicted of hacking into Digital Equipment Corporation's (DEC) computer and copying their software.
- 1989: Mitnick served 12 months in prison for hacking DEC, where he also ended up hacking Pacific Bell's voicemail computers.
- 1993: A second warrant was issued for Mitnick's arrest, and he went on the run for 2.5 years.
- 1995: The FBI found and arrested Mitnick.
- 1997–1998: The hacker community (including 2600 magazine) launched a "Free Kevin" campaign.
- 1999: Mitnick accepted a plea deal to lesser charges and served five years in prison.
- 2000: Mitnick was released from prison.

THE OPEN-SOURCE MOVEMENT BEGINS



Hackers' push to democratize knowledge extended to the software space as well, resulting in the rise of the open-source movement. Groups such as Linux User Groups, SourceForge, and Slashdot all advocated for open-source software and knowledge sharing with the broader community.



Another major development for the hacker community was the birth of DEF CON in 1993 by hacker Jeff Moss. What started as a going-away party for a friend has become one of the biggest gatherings in the hacking community worldwide.

Read our DEF CON article for a deeper dive into the backstory.

Story time

HACKER SYNTAX REMINISCES ON HIS EARLY HACKING DAYS

A friend and I were driving around the little town where I grew up while I searched for WiFi networks on my laptop. Many of these networks were open, and I'd often join them out of curiosity... and more times than not, I could!

One day, I found an open network by an energy company that shall not be named. So obviously, I connected and dug in to see what I could find. To my surprise, this network had all kinds of private data openly available. We're talking bank records, pictures, and customer and employee data.

So, I did what any hacker would do. I logged in to the WiFi admin console and changed the network name to "(redacted) was here!" My intent was not to harm the company, but I did want to spook them a bit to encourage greater care with their customer data.

I loved this so much that I spent the rest of the summer changing all the open access points to "Hacked by ___" or "I was here." Looking back, I guess we were just a bunch of teenagers goofing around with a new internet, following our curiosity (which still remains today!)

I WAS HERE

2000s The golden age of hacking

OVERALL VIBES The 2000s were a decade of significant evolution, bringing technological progress (hello, smartphones), digital privacy movements, the corporatization of hackers, and greater security awareness.

DIGITAL PIRATES TO HACKTIVISM

In the new millennium, hackers pushed the envelope on copy protection and digital rights, which had been codified into law with the passage of the Digital Millennium Copyright Act (DMCA) in 1998. "The decade became the age of digital piracy as platforms like Napster, Kazaa, and BitTorrent revolutionized how people shared music and movies," P3T3r_R4bb1t explains.

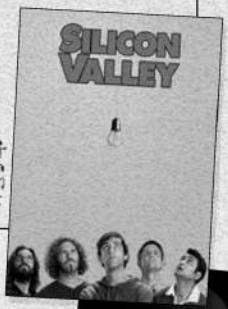
Eventually, as digital piracy was curbed, many hackers turned their passion toward hacktivism, hacking corporations when they felt that companies had overstepped their responsibilities.

Hall of Fame for the most well-known hacktivists of this era.

CORPORATIZATION OF HACKING

Many tech entrepreneurs were students of the hacker movement, leading to a blending of hacker and Silicon Valley cultures. The most famous example: Meta's (fka Facebook) headquarters are located on 1 Hacker Way. Hackers were suddenly in demand for their expertise, partnering with companies to beef up the latter's security programs—leading to the birth of crowdsourced security as we know it today.

But this corporatization was starting to give rise to something more sinister....



In the 2000s, hackers went from rebel outsiders to mainstream protagonists. Shows like Chuck and *Silicon Valley* captured how much hacker culture had permeated West Coast tech culture, while *Mr. Robot* showed the corporate side of hacking without losing sight of its gritty counterculture origins.

As Gavin Belson famously said, "I don't want to live in a world where someone else makes the world a better place better than we do."

yes, hackers actually became spies.

MILITARY-HACKING INDUSTRIAL COMPLEX

Governments and defense contractors worldwide recognized the value of hackers in advancing their national security objectives. So they began recruiting hackers, often encouraging them to work abroad while sharing what they learned with their home country.

This diaspora created a cycle of knowledge transfer that permeated across nation-states and corporations. For instance, in the U.S., most intelligence and military agencies are staffed by civilian contractors, and they are often paid very little. Therefore, when they move to higher-paying jobs (such as security consulting), they'll take the knowledge they gained from their agency days with them, leading to broader cultural and knowledge transfer.

contractors, clearances, oh my!

THE SPREAD OF SAFE HARBOR LAWS

As governments and corporations saw how hackers could help them, they pushed to create exceptions to the CFAA and DMCA to encourage hackers to report vulnerabilities. This movement gave rise to the idea of "responsible disclosure" policies, where companies include "safe harbor" language and pledge not to take legal action against researchers who report vulnerabilities in their systems.

Soon, through the work of companies like Bugcrowd and HackerOne, major tech companies began adopting these policies in their vulnerability disclosure programs. Eventually, governments followed suit. The U.S. passed the HIPAA Safe Harbor Law in 2021 to prioritize security for healthcare organizations.

Safe harbor laws have entered the chat.

Story time

P3TEr_R4bb1t SHARES WHAT IT WAS LIKE DURING THE GOOD OL' DAYS

You could change a single letter in a binary file, which was enough to bypass antivirus software. Plus, "Password1" worked every time, and logs and SOC teams were practically nonexistent.

I have countless personal and professional memories from that period, like exploiting a 2002 CVE to gain my first domain admin privileges without any payload encryption or evasion techniques whatsoever.

EXPLOITS on EASY MODE

HACKING NOW

Hackers are now a celebrated part of security programs, working hand in hand with corporations and governments to keep everyone safe. It's a far cry from the days when the Secret Service or the FBI persecuted hackers for simply finding and reporting a vulnerability.

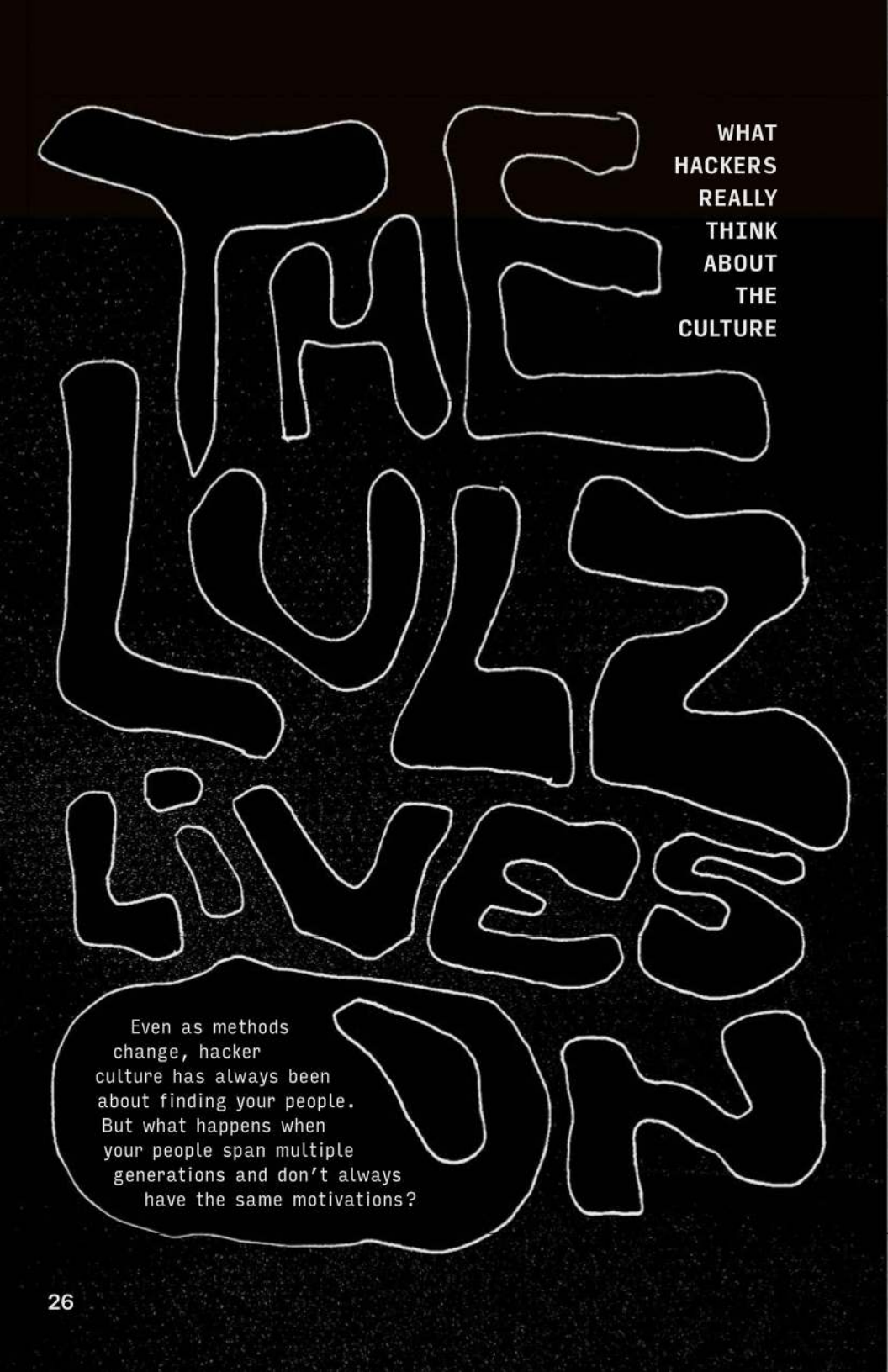
However, AI is reshaping everything, evolving faster than hackers can keep up. While this shift presents new challenges, if there's anything we've learned from history, it's that hackers are incredibly resilient, with a clear north star: protecting people's rights and freedoms against overreach. Regardless of what happens, hackers will always be there to fight against the overreach of power, even if it means using a slightly different toolkit.

"I AM A HACKER, AND THIS IS MY MANIFESTO. YOU MAY STOP THIS INDIVIDUAL, BUT YOU CAN'T STOP US ALL... AFTER ALL, WE'RE ALL ALIKE."

To quote the infamous "Hacker Manifesto">>>

Give the podcast a listen if you want to dive deeper.

Huge thanks to P3T3r_R4bb1t and the Darknet Diaries podcast for their excellent documentation about the early hacker era.

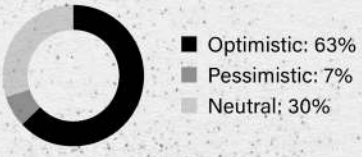

WHAT HACKERS REALLY THINK ABOUT THE CULTURE
THE LIFE CYCLE OF A HACKER
Even as methods change, hacker culture has always been about finding your people. But what happens when your people span multiple generations and don't always have the same motivations?

VIBE CHECK

Overall, the vibes are fairly strong, which isn't surprising—the need for hackers and related tools and technologies has increased exponentially in the past few years. That being said, there's still a significant group that feels ambivalent about where things are headed, which makes sense as we unpack the sentiment further.

Many hackers feel that the original ethos of hacking—curiosity and fun—has become less important. Instead, money and geopolitical motivation have taken precedence, which has many hackers (rightfully) concerned.

Overall, how do you feel about the direction hacker culture is going?



Hacking is increasingly becoming about geopolitics rather than curiosity/fun.

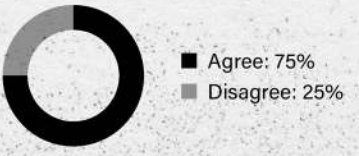
Alx, a hacker, explains it ↴

"With hacking now, things have gotten so ***commercialized*** that people often hoard their discoveries instead of sharing them. This goes against everything that made hacking culture worth joining in the first place."

But there's a silver lining. Almost all hackers still believe in the artistic side of hacking, which might be exactly what the community needs to resist full corporatization. Many are looking to their community to preserve the original spirit of hacking. Speaking of which...

Hacking is an art form.

Hacking is increasingly becoming about money rather than curiosity/fun.



As hacking becomes more mainstream, it's becoming less fun.

1337

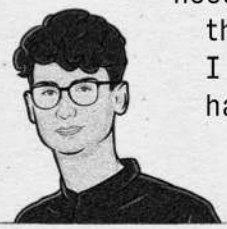
Finding Your People

The hacker community, despite increasing commercialization, is still going strong. As hacker Erik de Jong puts it, "Making money is good, but making friends is even better." This sentiment reflects a community that still values human connection over pure profit.

Where do you connect with other hackers?

- **Discord: 73%**
- **X/Twitter: 71%**
- Signal or Telegram: 33%
- In-person events: 30%
- Reddit: 25%
- Slack: 9%
- Bluesky: 3%

Sw33tLie, another hacker, shares this optimism:



"As hacking becomes more corporate, we really need to keep the community strong. I think we're doing a good job at that. I constantly see hackers helping other hackers by sharing resources, and I don't think that's going to stop any time soon."

However, how hackers find each other has changed. Gone are the old ways, such as IRC and bulletin boards. Today's hackers use apps like Discord, Twitter/X, Signal, and Telegram. But what's interesting is that in-person interactions remain key to fostering real bonds with hackers, with over a third meeting up in person.

Many of my friends are hackers.

I prefer hacking as a team rather than individually.

Even if older and younger hackers don't always agree on the same things, they still care about respecting the traditions and keeping the old ways alive. Some traditions bridge generations, like hacking "for the lulz," where people tinker with something just for the joy of it. This part of the culture has stayed alive largely thanks to individuals who serve as unofficial "keepers of the lore," sharing stories and knowledge with younger generations through blogs, forums, and mentorship.

Do you feel knowledgeable in hacker culture and lore?

- Very knowledgeable: 37%
- Somewhat knowledgeable: 54%
- Not knowledgeable: 7%

Language is another way hackers preserve their culture. When we asked hackers to list their favorite words, many of the most popular were slang from the 90s and early 2000s. For example, pwned (the most popular word) originated among hackers chatting on BBSs or gamers playing games like Warcraft. However, leet (also spelled l33t or 1337) was popular in the late 80s/early 90s to describe "elite" hackers. It's great to see these cultural elements still relevant among the hackers of today.

When hacking, have you ever done something purely for the"lulz"/laughs?

- Agree: 62%
- Disagree: 38%

What's your favorite hacker word or slang?

1. pwned
2. 33t leet 1337
3. hack THE PLANET
4. ZERO-day
5. NO SYSTEM SAFE

THE HACKER'S ETHICAL DILEMMA

As much as hackers believe in the value of their work, that doesn't mean it's always clear cut.

"There's always this tension in hacking—you know you're probably breaking some law, but when the end result is stronger security and a safer internet for everyone, it feels like the right thing to do."

Iceman explains ↳

This sentiment also appears in our survey, which shows that nearly half of the surveyed hackers have struggled with the ethical implications of their work.

However, there has been a shift—younger generations are less scared and more empowered in the moral importance of their work. Hacker Zwink explains, "I think the newer generation is less paranoid than us old-timers. We grew up in a time when any kind of hacking could land you in federal prison, so we learned to be extremely cautious. The newer generation seems less worried about that stuff—maybe rightfully so."

But even when laws aren't on their side, hackers recognize the importance of their work and remain motivated to report critical issues that help secure the internet, even if it means earning less money. This deep feeling of purpose gives them a sense of pride in their work.

I have struggled with the ethical implications of my work.

■ Agree: 47% ■ Disagree: 53%

Reporting a critical vulnerability is more important than making money from it.

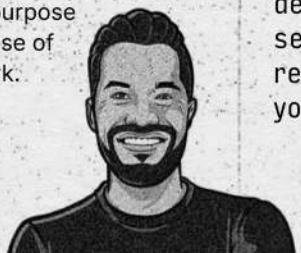
■ Agree: 85% ■ Disagree: 15%

I am proud of the work I do as a hacker.

□ Agree: 98%
■ Disagree: 2%

↳ bsysop explains

"You'll find these massive, widespread vulnerabilities and think that if someone malicious got their hands on this, it would be devastating. When that sense of responsibility really kicks in, you know you have to report it."



THE AI-LEPHANT IN THE ROOM

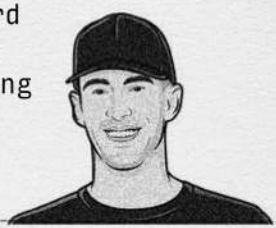
AI has quickly become a go-to tool for hackers, turning hours of manual coding and testing into minutes of automated work. But as AI use increases, it raises some real questions about the future of hacking culture. How can hacking remain fundamentally human if AI takes over more of the work? And what does it mean for community bonds when hackers turn to AI for answers instead of each other?

The community is actively wrestling with these questions, and many believe the answer lies in what AI can't replicate.

Have you used AI as part of your hacking workflow?

- Yes: 82%
- No: 7%
- No, but I plan to in the future: 12%

"Real hacking requires creativity and exploration across multiple targets, finding weird connections and combining disparate pieces."



Zwink explains

"AI isn't there yet, and even when it gets closer, it'll need to be specifically trained on each target with massive amounts of input data to be truly useful. That's why human creativity will always be needed."

TERMINALS to theaters

The rise of the hacker archetype

Long before hoodies and green terminals became hacker symbols, Hollywood had mythologized hackers as god-like experts. Movies like Wargames (1983) portrayed a kid who almost triggered World War III with a modem.

Another film, Hackers (1995), turned dial-up into a rebellion sign, further glorifying the hacker archetype. It mixed code with graffiti, portraying skateboarding as a side hobby for rebels.

Hacking evolved beyond technical skills into a cultural vibe. It felt punk, like skating through firewalls while giving authority the middle finger. This underground style flaunted that hackers didn't need permission; they needed payloads and bragging rights. Masks, manifestos, and the belief that code could spark protests blurred the lines between chaos and purpose, giving birth to **hacktivism**—when hacking meets activism, using code to challenge power and fight for causes.

HACKING BECAME AN IDENTITY, A CULTURE AND A MOVEMENT

marking the first moment in which many found themselves amid the noise.

The strategic PIVOT and why this was no sellout

The chaotic BBS couldn't last forever. As the internet grew, the innocent fun of phreaking and early hacking turned into security risks and breaking the law. Governments and corporations realized they couldn't just jail hackers; they needed to hire them. In 1998, tensions peaked when L0pht was called to testify before the U.S. Senate. Picture social misfits, once in the shadows, now in suits, telling powerful politicians, "We could take down the entire internet in 30 minutes."

This moment showed that only rebels understood how to save the system.

This led to the strategic pivot. **Peiter Zatko** (or Mudge), a L0pht member, testified and didn't just leave with a consulting gig; he became a changemaker from within. He worked for the **Defense Advanced Research Projects Agency** (DARPA) developing defense systems and later became Twitter's (now X) Head of Security.

"We could take down the entire internet in 30 minutes."

Why they were summoned

L0pht showed up in front of the Senate in 1998 because the U.S. government needed a serious reality check about computer security. L0pht's testimony made it clear—people across the country were starting to worry about these issues. However, neither the vendors nor anyone in Washington seemed to understand the extent of the vulnerabilities caused by insecure system designs. L0pht's work over the years had highlighted two main problems:

1. **Systemic insecurity**

   The basic structures supporting the internet (and, by extension, the government) were insecure by design.

2. **Vendor indifference**

   Major software companies showed little interest in fixing the flaws L0pht had responsibly disclosed.

The group aimed to use the prestige of a Senate hearing to pressure these companies into taking action. And by testifying, they had achieved a few remarkable goals:

1. **Public and political wake-up call**

   The obvious achievement was the shock factor that forced the government and public to take digital threat seriously.

3. **The legitimization of hackers**

   They had transformed the hacker stereotype of basement-dwelling criminals into valuable assets.

3. **Influencing policies and standards**

   Their testimony shifted government focus to digital security, leading to greater funding and development of federal standards and guidelines (like those from NIST).

7. **Accelerated security fixes**

   It also applied pressure that ended the "patch and pray" culture, forcing companies to take responsibility for their insecure products.

The greatest hack ever: INFILTRATING the system to save it

This transition wasn't a sellout. By joining corporations, L0pht could see digital weaknesses up close. Real change requires authority. The biggest hack isn't infiltrating a system; it's being given the formal authority to rewrite the rules and secure the infrastructure hackers had helped build. Once inside, the transition to an attacker-centric way of thinking did more than just patch a few government servers. It helped establish procedures that are currently accepted as industry norms. Among the noteworthy guidelines and ideas put into practice are the following:

The career pipeline—Mudge's employment laid the foundation for a well-defined and esteemed career path as an ethical hacker. This led to the creation of contemporary positions such as penetration testers and chief security officers (CSOs).

Responsible disclosures—The practice of security researchers giving vendors a set period of time (e.g., 60–90 days) to address vulnerabilities they found before making them public was formalized by hackers such as Mudge. This placed the responsibility of resolving flaws on the vendor rather than the community.

Security-by-design advocacy—Within businesses, L0pht promoted the idea that security should be a fundamental necessity rather than an afterthought.

By transforming the philosophy of chaos and disruption into a legally binding policy, L0pht established rules for integrating security into development processes. They created internal procedures for resolving issues rather than merely pointing them out from the outside. With their new role, they demanded that flaws be fixed prior to product shipment while promoting the integration of security into development life cycles.

However, operating within "the system" risked dulling the hacker spirit. If rebellious energy were channeled into corporate meetings and compliance forms, what would happen to curiosity and chaos? A paradox exists in corporate "white-hat hackers"—the corporate life of compliance, budgets, and endless auditing stifles the spontaneous exploration that develops a hacker's skills and street cred. The thrill of finding the next zero-day vulnerability can easily be replaced by the comfort of a high-paying and routine hacker life, which feels rewarding but lacks the excitement of spontaneous exploration. This threatens the preservation of the creative, but destructive, skill set necessary to stay ahead of the next generation of attackers.

The Bug Bounty revelation: The bridge that HONORS the ethics

The shift to corporate security, while necessary for global protection, also risks draining the rebellious ethos. It replaces freedom and curiosity with dull corporate mediocrity. If hackers become the very authority they challenge, the punk aesthetic and playful mischief naturally wither. That's where bug bounties come in. It's not just a way to make money; it creates a legal space for chaos that rewards the joy of discovery. This allows the rebellious DNA of hacker culture to flourish within the very systems it once sought to disrupt.

Bug bounties offer hackers real systems to explore, free from legal repercussions. This system acknowledges that outsider curiosity is vital for digital defense. By finding and reporting vulnerabilities, hackers maintain their independence while protecting the world's integrity. It's the ultimate evolution: **hack the planet and get paid for saving it.**

Hack the system, heal the culture

Where does this leave today's digital rebels? History shows that OG hackers weren't criminals or corporate pawns. They were explorers who saw the system as a puzzle. Their mission was to preserve the integrity of information and the excitement of exploration, not make money. OG hackers like Mudge didn't sell out by testifying to Congress or taking corporate roles. They executed the smartest hack possible—"infiltrating" the system they once disrupted. They gained influence to help protect and trigger change from within, showing that real change needs authority.

Today, the spirit of OG hacker groups lives on through every bug bounty program. These programs offer a safe space for rebellious curiosity to thrive, merging the punk-rock spirit with real-world impact. So, what's the takeaway?

HONOR THE ROOTS

Hack for curiosity, not just for the paycheck.

EMBRACE THE EVOLUTION

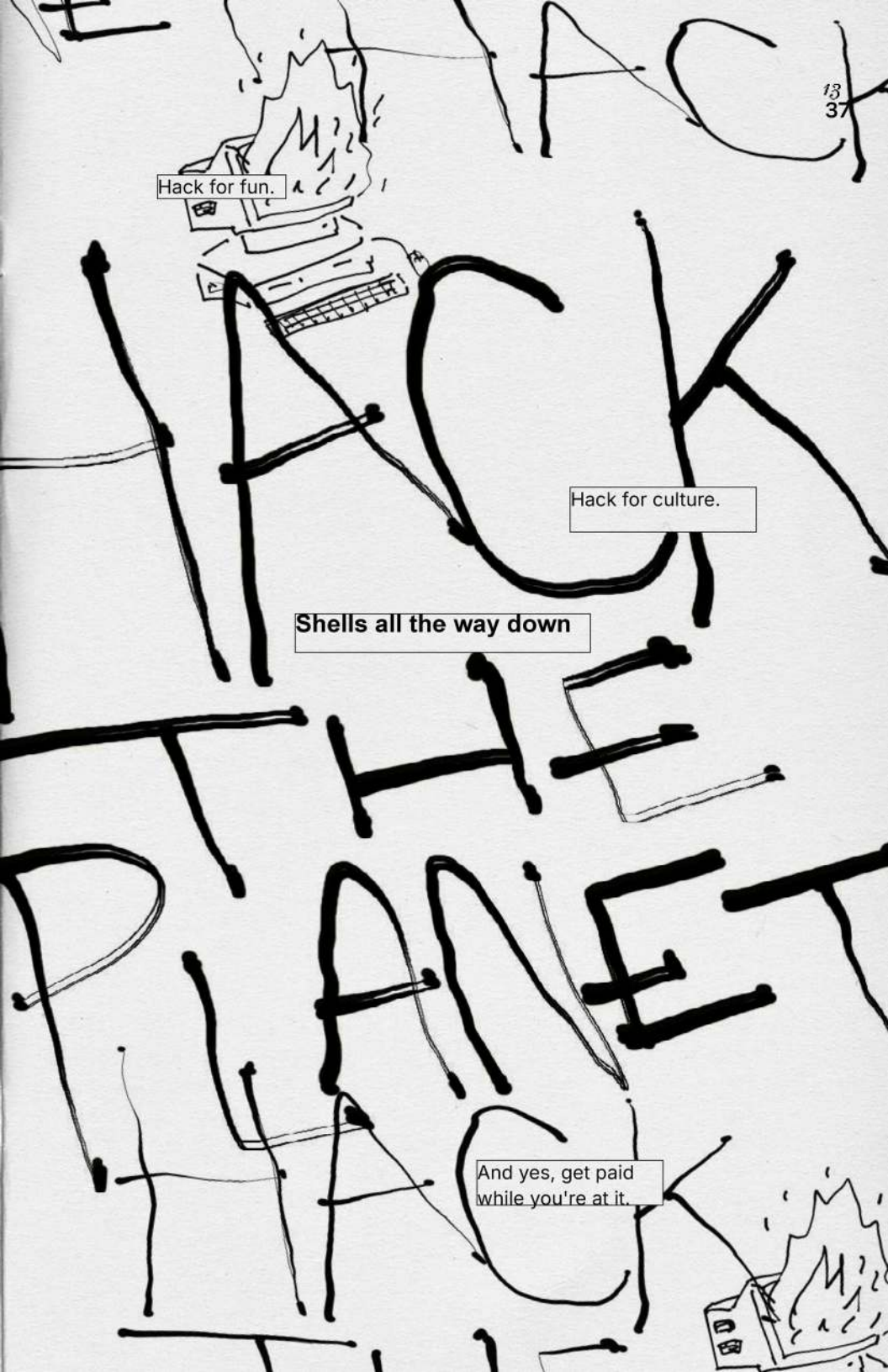
Use your skills to influence systems, not just break them.

STAY REBELLIOUS

Bring your unique voice, creativity, and chaos to the table

DRIVE CHANGE FROM WITHIN

Sometimes the smartest hack is rewriting the rules from the inside.


Hack for fun.
Hack for culture.
Shells all the way down
And yes, get paid while you're at it.

THE RISE OF LIVE HACKING

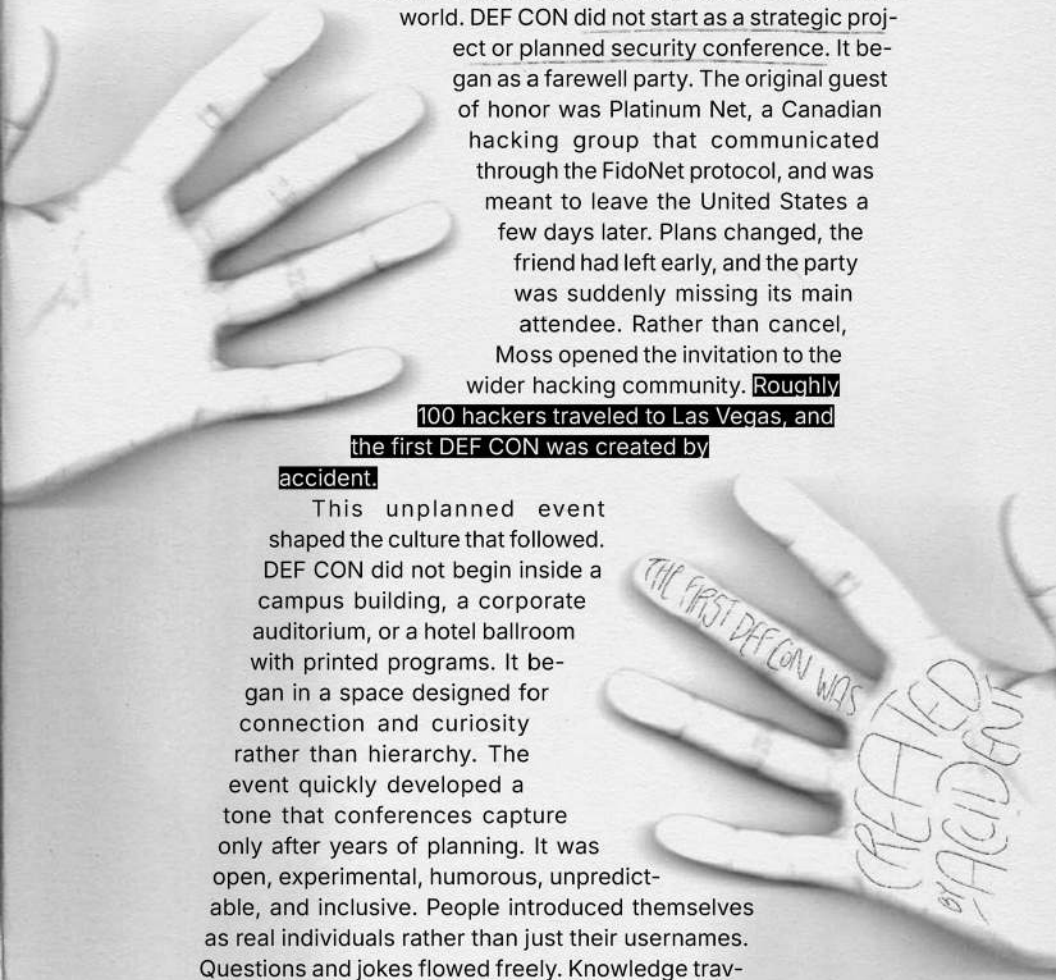
Long before modern social platforms, hackers found each other in remote corners of the internet using message boards, BBSs, IRC channels, and text files passed quietly between strangers who shared the same curiosities. Skill development happened across borders, time zones, and entire continents without anyone ever needing to meet in person. The hacking world proved early on that knowledge, discovery, and collaboration can travel at lightspeed when untethered from physical constraints.

Yet, even within a field built for remote interaction, something unique continues to happen when hackers meet face to face. Live hacking events create a type of energy that online channels cannot fully recreate. These gatherings feel part research lab, part social club, part puzzle-solving arena, and part cultural festival. Ideas spark faster, conversations flow more naturally, and trust forms at a pace that chat logs cannot match.

IDEAS SPARK FASTER

The DEF CON legacy

The strongest example of this can be traced back to 1993 in Las Vegas, when teenager Jeff Moss, known as Dark Tangent, created what is now recognized as one of the most influential hacker events in the world. DEF CON did not start as a strategic project or planned security conference. It began as a farewell party. The original guest of honor was Platinum Net, a Canadian hacking group that communicated through the FidoNet protocol, and was meant to leave the United States a few days later. Plans changed, the friend had left early, and the party was suddenly missing its main attendee. Rather than cancel, Moss opened the invitation to the wider hacking community. Roughly 100 hackers traveled to Las Vegas, and the first DEF CON was created by accident.



This unplanned event shaped the culture that followed. DEF CON did not begin inside a campus building, a corporate auditorium, or a hotel ballroom with printed programs. It began in a space designed for connection and curiosity rather than hierarchy. The event quickly developed a tone that conferences capture only after years of planning. It was open, experimental, humorous, unpredictable, and inclusive. People introduced themselves as real individuals rather than just their usernames. Questions and jokes flowed freely. Knowledge traveled by conversation, not protocol.

DEF CON evolved into a cultural anchor rather than a technical seminar. New friendships, rivalries, inventions, ideas, and learning rituals emerged naturally. The event became a place where hacker identity formed in public view.

Spot the Fed, a tradition that acknowledged federal attendance, demonstrated that even tense relationships could be addressed through dialogue. The Wall of Sheep showed the community how unencrypted traffic placed credentials at risk by displaying real examples, turning security into something visual and memorable. Capture the Flag competitions became a new format for measuring practical offensive skill and eventually matured into a respected global benchmark for both education and recruitment.

DEF CON also became the launchpad for several influential research moments. One of the most well-known involved the release of Back Orifice by members of the Cult of the Dead Cow, which sparked broader conversations about security accountability in widely deployed software. Later years saw hands-on investigation into election equipment, medical technology, vehicles, and even satellite systems. These demonstrations helped influence media narratives, policy focus, and industry investment around safety and resilience.

Even in a world where communication tools allow instant global collaboration, communities continue to seek opportunities to learn in the same physical space. The history of DEF CON reinforces the central idea behind today's live hacking events.

Hacker culture grows faster and stronger when people gather in person, *share ideas freely, and learn through lived experience rather than written instruction alone.*

In-person knowledge transfer is critical

Online knowledge sharing plays a crucial role in vulnerability research. Payloads, scripts, notes, and tools can be exchanged faster than ever before through documentation, repositories, and tutorial videos. These resources provide the technical building blocks. However, hacking skill is not limited to technical output. The most valuable insights often come from observing how another researcher thinks. This includes pattern recognition, hypothesis testing, debugging habits, risk-taking, creativity, and persistence after repeated failure. These elements are difficult to learn purely through text.

INVISIBLE → VISIBLE

→ In-person environments make this invisible layer visible. When hackers work side by side, it becomes possible to watch how someone approaches a challenge, how quickly they pivot after reaching a dead end, how they choose which function to test next, or how they decide whether to brute force, fuzz, or switch vectors. Conversations happen live rather than in delayed messages. Clarifying questions are quick rather than rewritten several times. The entire research process becomes a shared experience rather than an isolated one.

1337

The learning that happens in person also tends to be remembered more vividly. Seeing someone solve a problem while verbalizing their thinking leaves a deeper impression than receiving the same information written out after the fact. These environments also allow people to overhear conversations, notice unfamiliar tools, or witness a completely new style of methodology that would never have appeared on a forum post or recorded stream. Live hacking events transform knowledge from something transactional to something embodied and interactive.

Live hacking events remain irreplaceable because learning, trust, and culture develop faster in person than online.

Trust grows faster face to face

In remote environments, hackers often recognize each other by usernames, ranking scores, avatars, or submission history. Although these provide valuable information about skill, they do not reveal personality, intent, or values. Trust can be difficult to build when communication is limited to text and profile statistics. People may hesitate to share details about experimental findings or partially formed ideas in case they are misunderstood or taken out of context.

Face-to-face interaction changes this dynamic. Tone, humor, patience, curiosity, and collaboration habits become clearer. People can read expressions, hear excitement, recognize sincerity, and detect shared motivation. These signals help establish trust in a way that text cannot match. Once trust forms, hackers become more comfortable sharing unpolished insights. They begin to talk about tools that are still private, research paths that might go nowhere, and errors that led to unexpected discoveries. Collaboration becomes less about protecting credit and more about combining strengths.

Trust also reinforces fairness. When people work together in person, it becomes easier to recognize effort, acknowledge contributions, and agree on shared outcomes. This prevents misunderstandings and supports a healthy research culture. The trust formed at live events often continues long after an event ends, leading to future collaborations, mentorship, and joint research publication.

Hacking culture, history, *and the future*

Modern live hacking events carry the same cultural DNA that shaped early DEF CON gatherings while offering far greater diversity, domain expertise, and global participation. The original spirit of curiosity and experimentation remains central, even as the technological landscape expands into areas such as vehicles, hospitals, financial systems, satellites, and industrial infrastructure. Conversations that happen in these physical environments influence not only technical work but also ethical thinking and long-term community responsibility.

Live hacking is likely to evolve further as technology and collaboration methods change. Hybrid formats may combine virtual preparation with in-person discovery. AI-supported tooling may enhance research efficiency without reducing creativity. Specialist hacking villages may continue to expand across new industries. Regardless of the direction, the value of learning together in real time will remain unparalleled.

Hacking began online, but hacking culture became real when people met in person. The accidental party that created DEF CON proves that hackers thrive when curiosity meets community. Modern live hacking events continue that legacy by accelerating knowledge exchange, strengthening trust formation, and developing future leaders through shared experience.

Live hacking events will never be replaced; our culture thrives where learning and trust begin — in person.

A love letter to the hacker community

By Tatiana (Tati) Uklist, Technical Program Manager at Bugcrowd and unofficial "Hacker Mom"

> To wrap up our first Hacker Culture Manual, I wanted to write a love letter to the community that has come to accept me as one of their own, even when I was (and still am) hesitant to see myself as one of its own. But to understand why that matters, you have to go back to 2020.

How we got here

Opening Scene: The year is 2020. I was working for a nonprofit in upstate New York. On a good day when classes were in session, the town had 30,000 people, but the community feeling was incredibly low. Then COVID hit and a majority of the town disappeared. That's when I decided I needed something new. I wanted something that would challenge and continuously push me. After facing numerous rejections for "not having enough experience," my friend sent me a job posting for a company (and industry) I had never heard of.

Enter stage left: Bugcrowd. At the time, I genuinely had no desire to join a cybersecurity company. Honestly, I just saw this as a way to get more experience to eventually go off to a more traditional corporate career path. It seemed more predictable and I *thought* that's what I was craving. But life had other plans.

Those plans came in the form of a question: Can you help out with our upcoming Bug Bash before DEFCON? At the time, that sentence was gibberish. Bug Bash? DEFCON? But sure, I was eager to prove myself and had a background in logistics, so it was easy to pick up.

Little did I know that that ask would change how I view my job and what security means in general. One of the core memories that I have from that year was walking into a room full of security researchers and hackers and just feeling the energy.

Fast forward five years later, and I'm still here. I've had the privilege of meeting hundreds of hackers over so many DEFCONs, Bug Bashes, and industry events. I've earned the nickname of "Hacker Mom" and I'm proud to call so many of you my friends.

Why hackers are truly 1337

What I love the most about hackers is the curiosity that drives them. As someone with lifelong imposter syndrome, seeing folks that generally seem allergic to feelings of inadequacy and just operate based on pure curiosity was something I've never experienced before. The curiosity about the technology they were testing was eye opening, but the curiosity about the people around them was on another level. The non-transactional desire to help and collaborate with each other to get a greater impact bled over from submissions to the conversations that happened at the happy hours or over meals.

At Bug Bashes, it's not uncommon for me to step outside at dinners or during testing to take a beat for myself. Within two minutes, I usually have hackers coming up to me asking if I need anything and coming back with my favorite soda or a RedBull without me even needing to ask. These small moments are usually what stick with me the most, because at a moment where I'm supposed to be looking out for them, they're doing the same for me. These friendships last far outside the walls of events. They've followed me in so many ways. They give me a place to spend my free time when I'm travelling. They are the built-in crowd when I announce I'm speaking at a DEFCON village. They're the random check-ins on how I'm doing, just because.

Ultimately, they're what makes me feel like I'm the the luckiest person in the world for getting to do what I do.

Ultimately, they're what makes me feel like I'm the luckiest person in the world for getting to do what I do.

B I U S

A final word to the best humans around

AI has become more of a talking point and let's be honest—it has left a lot of uncertainty for the industry as a whole. The security in security feels like it's dissipating.

This isn't another thought piece that's even attempting to answer the existential questions about the future of security research. There is a time and a place for those conversations, but I want to make sure we're not skimming over the decades of hacking the planet that got us here. This Hacker Culture Manual attempted to spotlight just a fraction of the incredible humans who broke shit, pushed boundaries, and never stopped asking questions. I've met many of you and am constantly inspired by the lore you're contributing to daily.

> **Without you all, the internet would be a far less safe place, and the world would be significantly less interesting. So I wanted to take an opportunity to say thank you.**

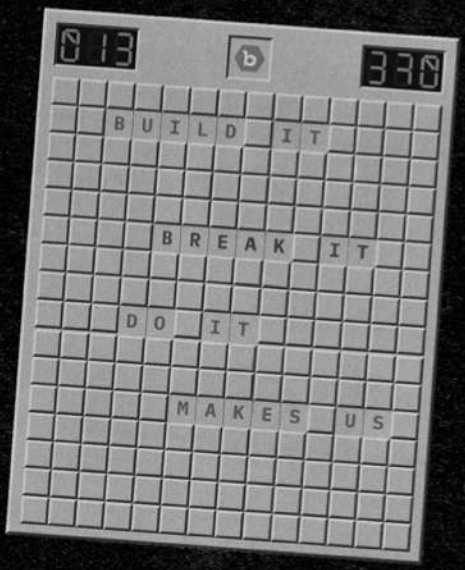
Thank you for being human in a world where being human is increasingly rare. Y'all haven't strayed from that.

Bugcrowds Hacker... PDF
Bugcrowds Hacker... File

Shift + Return to add a new line


ZERO
DAYS
SINCE LAST
INCIDENT
THERE'S NO RIGHT AND WRONG. ONLY FUN
AND BORING.

THE QUIETER
YOU BECOME



THE MORE
YOU HEAR