Think about hackers.

The term probably brings to mind hooded figures operating in the dark,

probably in a basement, definitely in secret.

They're exploiting vulnerabilities, stealing our money or our personal

information, and costing companies millions.

In fact, cybercrime costs the world an estimated $600 billion dollars per

year. But the past decade has seen a rise in a new type of hacker called

an ethical hacker, or a white hat hacker.

These men and women want to use their hacking know-how for good, and a

legal market for their skills has rapidly emerged.

There's this creativity, there's this curiosity and there's this kind of

almost mischief in how you think.

But then that's coupled with a strong moral framework and ethical

framework to actually use that for good.

These hackers help companies protect themselves by finding **vulnerabilities**(уязвимости)

before the criminal hackers do.

When an ethical hacker finds a bug, they disclose the security issue in

exchange for cash or other rewards, in what's known as a bug bounty

program. So, we're like a neighborhood watch.

We come to your house, we look for ways to break in, and if we can break

in, we tell you.

We don't break in, we tell you how we could have done it.

Companies like HackerOne, Bugcrowd and Synack have **sprung up**(выпригиватьы) to connect

freelance hackers with corporations that offer bug bounty programs.

This has led to the creation of a geographically dispersed network of

cybersecurity experts, a.k.a. ackers, who are integral to the safety of corporations in every industry

from tech to finance to national defense.

We work with MasterCard, we work with Fiat Chrysler in the automotive

space, we work with Cisco in the engineering I.T.

technology space, you know Department of Defense, Pinterest.

These days, hackers can make a lot of money identifying security flaws for

companies like these.

The payout for finding a single, highly critical vulnerability can be tens

of thousands of dollars, and some companies have paid out millions

overall. I know Verizon Digital Media actually just passed $7 million

dollars in bounties paid.

Uber has paid out over $2 million dollars.

Hacking for good is gaining traction and there's big money at stake.

So, it may be time for the public to rethink its conception of what being a

hacker really means.

Ever since computers have existed, people have been trying to break into

them. Back when these machines were clunky novelties(неуклюжие новинки) found only in

universities and large corporations, hackers were commonly seen as

tinkerers, technology enthusiasts who liked exploring and altering

existing computer programs.

They made improvements that helped move the industry forward.

But with the emergence of the personal computer in the 1980s, cybercrimes

became much more common.

From the comfort of their living rooms, self-taught programmers learned

how to break into and manipulate important systems, pirate software and

spread viruses.

I broke into mostly websites belonging to corporations, governments,

military agencies and just defaced them.

I changed them. A lot of people went to jail.

Like a lot of people got nasty letters.

A lot of people got knocks on the door.

And that's really the history of hacking that actually precedes this

season that we're in now.

Ended up getting arrested several times by the federal government for

that. And they sent me to prison for 27 months, 10 months and 14 months.

Three separate occasions.

Ellis began hacking in the 1990s, and DeVoss in the early 2000s.

By then, the hacker stereotype was already well established, thanks to

media like the popular 1983 movie WarGames, which revolved around a

disaffected but intelligent teen accidentally hacking into a top secret

military supercomputer nearly starting World War 3.

Even though the young protagonist wasn't malicious, the idea that computer

whizzes could gain access to systems like this terrified the public.

After Ronald Reagan watched the film, he proposed a number of anti-hacking

bills resulting in the Computer Fraud and Abuse Act, which prohibits

anyone from intentionally accessing a computer without authorization.

And it hasn't really been changed since.

So, it is legal in the sense that if there is authorization, then at that

point they have safe harbor.

But outside of that, it is basically illegal.

Because the law doesn't really define what "authorization" means, it isn't

exactly clear how it relates to our new reality, where cybersecurity is

increasingly outsourced.

Security used to be something you fix internally.

It's very secretive, it's not transparent, it's not open.

And we're seeing a shift towards security becoming more and more

collaborative and enlisting outside help.

For a company, enlisting this outside help often means starting a bug

bounty program, in which corporations pay hackers who report bugs or

vulnerabilities in their software.

What's believed to be the first of these programs came about in 1983, when

a Silicon Valley startup called Hunter & Ready offered a free Volkswagen

Beetle to anyone who identified a bug in its operating system.

Over a decade later, in 1995, Netscape began offering more straightforward

financial incentives for finding flaws in its popular browser, Netscape

Navigator. The idea took a while to catch on, but by the mid-2000s,

security companies iDefense and TippingPoint, as well as the Mozilla

Foundation, offered similar programs.

Other tech giants eventually followed suit, giving rise to a new crop of

startups like Bugcrowd, HackerOne and Synack, which connect ethical

hackers with companies offering bug bounty programs.

When starting one of these programs, a company simply describes what type

of vulnerabilities they want to be notified of, what parts of their site

hackers can test, and what types of testing are allowed.

They also determine how much each bug is worth.

Then the bug bounty platforms verify the legitimacy of the

vulnerabilities, coordinate payouts to hackers and work with the companies

to ensure that bugs are properly fixed, greatly reducing the burden on a

company's in-house security team.

On average, you get about a thousand dollars per find, and the highest

bounty we've paid is $100 thousand dollars for a single vulnerability.

Companies pay a fee to use bug bounty platforms like HackerOne, but for

the hackers themselves, these sites are free and easy to join.

You fill out your Twitter handle, your LinkedIn I.D.,

your GitHub I.D.,

you know, that's really the starting point of how we figure out how to

connect you with the right programs going forward.

Every time when you file a vulnerability report to a company, you get

scored by how good it was and how serious it was.

And then you are collecting points, we call them reputation points.

And then we can see in all these metrics how good they are, what their

special skills are, and that's how we can pick the right talent for every

job. For hackers who were previously operating illegally, the fact that

you could now make good money this way seemed difficult to believe at

first. I was introduced to bug bounties in 2014, but I didn't actually

participate because it still seemed like it was too good to be true.

Because if I get in trouble for hacking illegally again, it's life in

prison. And I wasn't willing to take that risk on something that was so

new. Eventually though, hackers like DeVoss realized these platforms were

for real, and their networks have been growing rapidly worldwide.

We have half a million hackers in our network.

Half of them are 24 years or younger.

Some of them are as young as 15 or 16.

They can be all over the world.

They have **endless curiosity**(бесконечное любопытство).

They like to outsmart systems.

And they figure out how to break in, before the criminals can do that.

Today, over 1,400 organizations use HackerOne and over 1,200 use Bugcrowd.

Even though many of these organizations have their own internal security

teams, the complexity of software these days pretty much guarantees

they'll still have some weak spots.

I don't think there's ever been a company that's come onto the platform

that has had just zero vulnerabilities in it, no matter how mature it is.

There's always something, because humans make mistakes.

And in recent years, these mistakes have led to some high profile

disasters. Equifax paid a $700 million dollar settlement to consumers for

its 2017 data breach.

And in 2019, Yahoo!

agreed to pay an $117.5

million-dollar settlement for a series of hacks that exposed the personal

information of up to three billion accounts.

If you have a data breach, the average cost to you is $7 million dollars,

and many have had breaches that have cost them $100 million or more.

We help averting the breaches by fixing the vulnerabilities ahead of time.

And the price you pay for that is a fraction of a fraction of the cost of

a breach. Research and advisory firm Gartner estimated that globally,

cybersecurity spending would reach $124 billion in 2019.

Overall, the high cost of preventing and mitigating cybersecurity threats

has spurred a wide range of companies from United Airlines to the

Department of Defense to Goldman Sachs to adopt bug bounty programs over

the past five years.

Probably the turning point in adoption for what we're doing was when the

Department of Defense launched the Hack The Pentagon project, which we're

now very much a part of.

So, there you have the world's largest organization, with the most powerful

weapons in the world, unlimited budgets, and they've concluded that to be

truly secure, they need the help of hackers.

And we've found already over 12 thousand vulnerabilities for the

Department of Defense.

That's like the greatest part of it, is being able to hack like the U.S.

government and military, and not worry that your door is going to get

kicked in by a SWAT team anymore.

Because that's happened four times to me.

These days, rather than getting arrested, DeVoss's hacking obsession has

made him wealthier than he'd ever imagined.

In total, he's netted well over $1 million dollars over the course of his

ethical hacking career.

I'm at $840 thousand dollars just on HackerOne for 2019.

If you add in the other platforms, then I'm a little over $900 thousand

for the year. Only a select few have matched his success.

But their backgrounds provide an interesting glance into a diverse

network. We have six hackers today who have made more than a million, and

the first one to get to a million was 19 year old Santiago Lopez in Buenos

Aires. So, no university education, no background in a tech center in the

world. Just endless curiosity, a good sense of computers and mathematics

and hard work. And he earned a million.

CNBC got Lopez on the phone to talk about his accomplishments.

At the beginning, when I started hacking, I didn't knew that I was going

to make a million. It was like impossible for me.

So, it was a very good surprise.

But despite the incentives for hackers and organizations alike, the grand

majority of companies still don't offer bug bounties.

Actually, most don't even offer any sort of vulnerability disclosure

program, which would allow hackers to report bugs without fear of

punishment. A vulnerability disclosure program is extremely similar to a

bug bounty program. You're still allowed to hack into the system as long

as you report it to them.

The only difference is you don't get paid for your vulnerabilities.

While this may seem like an easy win for organizations, the most recent

HackerOne security report revealed that 93 percent of companies on the

Forbes Global 2000 list don't have any vulnerability disclosure policies.

Without a proper channel to report security issues.

HackerOne says nearly 1 in 4 ethical hackers have failed to disclose a

vulnerability that they've found.

Luckily, the industry is showing some trends in the right direction.

At the end of 2019, the Cybersecurity and Infrastructure Security Agency

issued a draft of a mandatory directive that would require all government

agencies to adopt vulnerability disclosure policies.

HackerOne and Bugcrowd hope this means that more companies will follow

suit. And to ensure that the talent pool is able to meet the growing

demand, both even offer their own free educational initiatives to teach

newbies the basics of hacking.

The Internet is a pretty, pretty gnarly place these days.

And really what it comes down to is that you can't control what an

attacker is going to do, but you can control where your defenses are up to

when they arrive. As for the individuals on these platforms, they just

want people to know that despite what you may have heard about "hackers",

in the world we live in today, they're often on our side.

They always see the hacker like the bad guy, but he's the good guy now.

We're here to help. We're not just some sketchy people in their mom's

basement who are out there to cause damage.

We're professionals who work in the industry who actually wanna make the

companies better.