Keren Elazari

Hackers: The Internet's Immune System

5 Four years ago, a security researcher, or, as most people would call it, a hacker, found a way to literally make ATMs throw money at him. His name was Barnaby Jack, and this technique was 10 later called "jackpotting" in his honor.

0:33

I'm here today because I think we actually 15 need hackers. Barnaby Jack could have easily turned into a career criminal or James Bond villain with his knowledge, but he chose to show the world his research instead. He believed that sometimes you 20 have to demo a threat to spark a solution. And I feel the same way. That's why I'm here today.

1:03

25 We are often terrified and fascinated by the power hackers now have. They scare us. But the choices they make have dramatic outcomes that influence us all. So I am here today because I think we 30 need hackers, and in fact, they just might be the immune system for the information age. Sometimes they make us sick, but they also find those hidden threats in our 35 world, and they make us fix it.

1:40

I knew that I might get hacked for giving 40 this talk, so let me save you the effort. In true TED fashion, here is my most embarrassing picture. But it would be difficult for you to find me in it, because I'm the one who looks like a boy standing to 45 the side. I was such a nerd back then that even the boys on the Dungeons and Dragons team wouldn't let me join. This is who I was, but this is who I wanted to be: Angelina Jolie. She portrayed Acid Burn in 50 the '95 film "Hackers." She was pretty and she could rollerblade, but being a hacker, that made her powerful. And I wanted to be just like her, so I started spending a lot of time on hacker chat rooms and online 55 forums. I remember one late night I found a bit of PHP code. I didn't really know what it did, but I copy-pasted it and used it anyway to get into a password-protected site like that. Open Sesame. It was a

60 simple trick, and I was just a script kiddie back then, but to me, that trick, it felt like this, like I had discovered limitless potential at my fingertips. This is the rush of power that hackers feel. It's geeks just 65 like me discovering they have access to superpower, one that requires the skill and tenacity of their intellect, but thankfully no radioactive spiders.

70 ### 3:20

But with great power comes great responsibility, and you all like to think that if we had such powers, we would only use 75 them for good. But what if you could read your ex's emails, or add a couple zeros to your bank account. What would you do then? Indeed, many hackers do not resist those temptations, and so they are 80 responsible in one way or another to billions of dollars lost each year to fraud, malware or plain old identity theft, which is a serious issue. But there are other hackers, hackers who just like to break 85 things, and it is precisely those hackers that can find the weaker elements in our world and make us fix it.

4:06

90 This is what happened last year when another security researcher called Kyle Lovett discovered a gaping hole in the design of certain wireless routers like you 95 might have in your home or office. He learned that anyone could remotely connect to these devices over the Internet and download documents from hard drives attached to those routers, no 100 password needed. He reported it to the company, of course, but they ignored his report. Perhaps they thought universal access was a feature, not a bug, until two months ago when a group of hackers used 105 it to get into people's files. But they didn't steal anything. They left a note: Your router and your documents can be accessed by anyone in the world. Here's what you should do to fix it. We hope we 110 helped. By getting into people's files like that, yeah, they broke the law, but they also forced that company to fix their product.

115 ### 5:07

Making vulnerabilities known to the public is a practice called full disclosure in the hacker community, and it is

controversial, but it does make me think of how hackers have an evolving effect on technologies we use every day. This is what Khalil did. Khalil is a Palestinian hacker from the West Bank, and he found a serious privacy flaw on Facebook which he attempted to report through the company's bug bounty program. These are usually great arrangements for companies to reward hackers disclosing vulnerabilities they find in their code. Unfortunately, due to some miscommunications, his report was not acknowledged. Frustrated with the exchange, he took to use his own discovery to post on Mark Zuckerberg's wall. This got their attention, all right, and they fixed the bug, but because he hadn't reported it properly, he was denied the bounty usually paid out for such discoveries. Thankfully for Khalil, a group of hackers were watching out for him. In fact, they raised more than 13,000 dollars to reward him for this discovery, raising a vital discussion in the technology industry about how we come up with incentives for hackers to do the right thing. But I think there's a greater story here still. Even companies founded by hackers, like Facebook was, still have a complicated relationship when it comes to hackers. And so for more conservative organizations, it is going to take time and adapting in order to embrace hacker culture and the creative chaos that it brings with it. But I think it's worth the effort, because the alternative, to blindly fight all hackers, is to go against the power you cannot control at the cost of stifling innovation and regulating knowledge. These are things that will come back and bite you.

7:17

It is even more true if we go after hackers that are willing to risk their own freedom for ideals like the freedom of the web, especially in times like this, like today even, as governments and corporates fight to control the Internet. I find it astounding that someone from the shadowy corners of cyberspace can become its voice of opposition, its last line of defense even, perhaps someone like Anonymous, the leading brand of global hacktivism. This universal hacker movement needs no introduction today, but six years ago they were not much more than an Internet

subculture dedicated to sharing silly pictures of funny cats and Internet trolling campaigns. Their moment of transformation was in early 2008 when the Church of Scientology attempted to remove certain leaked videos from appearing on certain websites. This is when Anonymous was forged out of the seemingly random collection of Internet dwellers. It turns out, the Internet doesn't like it when you try to remove things from it, and it will react with cyber attacks and elaborate pranks and with a series of organized protests all around the world, from my hometown of Tel Aviv to Adelaide, Australia. This proved that Anonymous and this idea can rally the masses from the keyboards to the streets, and it laid the foundations for dozens of future operations against perceived injustices to their online and offline world. Since then, they've gone after many targets. They've uncovered corruption, abuse. They've hacked popes and politicians, and I think their effect is larger than simple denial of service attacks that take down websites or even leak sensitive documents. I think that, like Robin Hood, they are in the business of redistribution, but what they are after isn't your money. It's not your documents. It's your attention. They grab the spotlight for causes they support, forcing us to take note, acting as a global magnifying glass for issues that we are not as aware of but perhaps we should be. They have been called many names from criminals to terrorists, and I cannot justify their illegal means, but the ideas they fight for are ones that matter to us all. The reality is, hackers can do a lot more than break things. They can bring people together.

10:14

And if the Internet doesn't like it when you try to remove things from it, just watch what happens when you try to shut the Internet down. This took place in Egypt in January 2011, and as President Hosni Mubarak attempted a desperate move to quash the rising revolution on the streets of Cairo, he sent his personal troops down to Egypt's Internet service providers and had them physically kill the switch on the country's connection to the world overnight. For a government to do a thing like that was unprecedented, and for hackers, it made it personal. Hackers like the Telecomix group were already active

on the ground, helping Egyptians bypass censorship using clever workarounds like Morse code and ham radio. It was high season for low tech, which the government couldn't block, but when the Net went completely down, Telecomix brought in the big guns. They found European service providers that still had 20-year-old analog dial-up access infrastructure. They opened up 300 of those lines for Egyptians to use, serving slow but sweet Internet connection for Egyptians. This worked. It worked so well, in fact, one guy even used it to download an episode of "How I Met Your Mother." But while Egypt's future is still uncertain, when the same thing happened in Syria just one year later, Telecomix were prepared with those Internet lines, and Anonymous, they were perhaps the first international group to officially denounce the actions of the Syrian military by defacing their website.

12:06

But with this sort of power, it really depends on where you stand, because one man's hero can be another's villain, and so the Syrian Electronic Army is a pro-Assad group of hackers who support his contentious regime. They've taken down multiple high-profile targets in the past few years, including the Associated Press's Twitter account, in which they posted a message about an attack on the White House injuring President Obama. This tweet was fake, of course, but the resulting drop in the Dow Jones index that day was most certainly not, and a lot of people lost a lot of money.

12:53

This sort of thing is happening all over the world right now. In conflicts from the Crimean Peninsula to Latin America, from Europe to the United States, hackers are a force for social, political and military influence. As individuals or in groups, volunteers or military conflicts, there are hackers everywhere. They come from all walks of life, ethnicities, ideologies and genders, I might add. They are now shaping the world's stage. Hackers represent an exceptional force for change in the 21st century. This is because access to information is a critical currency of power, one which governments would like to control, a thing they attempt to do by setting up all-you-can-eat surveillance programs, a thing they need hackers for, by the way. And so the establishment has long had a love-hate relationship when it comes to hackers, because the same people who demonize hacking also utilize it at large.

14:06

Two years ago, I saw General Keith Alexander. He's the NSA director and U.S. cyber commander, but instead of his four star general uniform, he was wearing jeans and a t-shirt. This was at DEF CON, the world's largest hacker conference. Perhaps like me, General Alexander didn't see 12,000 criminals that day in Vegas. I think he saw untapped potential. In fact, he was there to give a hiring pitch. "In this room right here," he said, "is the talent our nation needs." Well, hackers in the back row replied, "Then stop arresting us." (Applause)

14:52

Indeed, for years, hackers have been on the wrong side of the fence, but in light of what we know now, who is more watchful of our online world? The rules of the game are not that clear anymore, but hackers are perhaps the only ones still capable of challenging overreaching governments and data-hoarding corporates on their own playing field. To me, that represents hope.

15:22

For the past three decades, hackers have done a lot of things, but they have also impacted civil liberties, innovation and Internet freedom, so I think it's time we take a good look at how we choose to portray them, because if we keep expecting them to be the bad guys, how can they be the heroes too? My years in the hacker world have made me realize both the problem and the beauty about hackers: They just can't see something broken in the world and leave it be. They are compelled to either exploit it or try and change it, and so they find the vulnerable aspects in our rapidly changing world. They make us, they force us to fix things or demand something better, and I think we need them to do just that, because after all, it is not information that wants to be free, it's us.