NABIL NEZZAR

# Think like a hacker

Cyber-lawyer **Scott Shapiro** believes there is more to beating hackers than getting better at programming. He tells David Adam why online security is as much about humans as technology and how understanding both can keep us safer online

Scott Shapiro wants to teach the world how to hack. An expert on legal philosophy and the founding director of Yale University's Cybersecurity Lab, his day job is to provide cutting-edge teaching for Yale law students on how the online world works and how to keep it secure.

He believes that we can only effectively tackle cybercrime if we understand not only how people hack, but why. In his new book *Fancy Bear Goes Phishing* he explores true stories from the front line of cybercrime, from the hacker known as Dark Avenger who wrote the first mutating computer virus, to the teenage boy who hacked Paris Hilton's phone because he wanted to be famous. The book's title derives from the exploits of Fancy Bear, a group working for Russian military intelligence that hacked the governing body of the US Democratic Party during the 2016 presidential campaign.

Shapiro talks to *New Scientist* about what we can learn from hackers, why he wants to teach the world to hack in a free online course and just how close he came to committing cybercrime himself.

**David Adam: You teach people to hack. Why?**
Scott Shapiro: I think it's very hard for people to understand how hacking works when it is described abstractly. It's a bit like explaining how to do carpentry through a description – you can read the words, but you don't really ›

understand what's happening. If you teach people how to hack, they can understand in a much more intuitive way not only how it works, but also how to protect themselves against hackers.

**Is it difficult to learn how to hack?**
It's upsettingly easy to learn to hack. My teaching partner and I put together an online course with 12 videos, each an hour long, plus assignments and explanations on how to hack. So, that's 12 hours of videos with some homework. That's open to anybody and if you do it, you'll learn not just how to hack, but more importantly you'll learn why it works. I want to teach people how to understand how information is stored, manipulated, transferred and, ultimately, exploited.

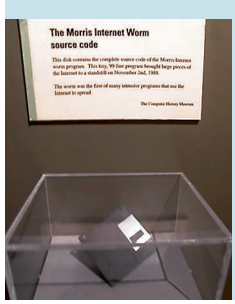
**Your book says there is no technical way to stop hacking. Why is that?**
There are many technical solutions to improve cybersecurity, such as protecting accounts with passwords, providing easy-to-use encryption on the internet and sophisticated firewalls. But there's no technical way to achieve perfect cybersecurity.

Even if we just want to improve cybersecurity, as opposed to perfecting it, it is a mistake to think that the way to do that is through technical means. It's primarily a human problem. We need to try to fix the political, social and psychological vulnerabilities that generate vulnerable code. If people just try to fix vulnerable code, in some sense they have already lost the game.

**What changes are required to tackle these vulnerabilities?**
We need to focus on what I call "upcode" – the social, legal, economic and psychological factors that drive, encourage and permit the anti-social, disruptive and illegal behaviours of hackers.

The UK has been very forward-leaning in this respect. The National Crime Agency published a report on "pathways into cybercrime" to understand how young people start engaging in low-level deviant behaviour online. There have been attempts to try to have law enforcement meet with these people to try to divert them away from criminality. We know that mentorship can do that. In the US, new types of competitions have been created to divert people who might ordinarily commit crimes on the internet into projects where people engage in activities that are safe.

> "Cybersecurity is primarily a human problem that requires human solutions"




**Now in a museum, the floppy disk with the code that hacker Robert Morris (left) used to crash the internet in 1988**

LOWER: GO CARD USA/CC BY-SA 2.0; UPPER: INTEL FREE PRESS

**While we work out how to tackle hacking, is it really a good idea to teach large numbers of people how to do it?**
Somebody needs to teach people what's happening. The idea is to provide this information for interested people, presented in a responsible way, so that they can learn it and understand the news and what's happening around them. And to make them more secure.

When we teach the course, we repeat – over and over again – the absolute importance of not hacking other people without their consent. Some people who do our Yale Law School course go on to learn more about cybersecurity and become experts. Others go to work for the US Department of Justice, or they go into private cyberlaw practice, and they are newly empowered to understand things that almost nobody understands.

**In your book, you describe various high-profile hacks. Do you have a favourite?**
I'm partial to the Robert Morris hack. Morris was a graduate student at Cornell University [in New York] in 1988 and he wanted to do an experiment to see if he could infect lots of computers on the internet. He figured out multiple ways of getting a worm to spread over the internet. He didn't intend to cause any harm, though it ended up crashing the internet and he was ultimately convicted for doing so.

I like it a lot because it was technically very interesting, how he was able to allow his worm to spread. But it also raised novel legal questions about the desire to hold people responsible for intentionally releasing viruses and worms onto the internet if they didn't intend to create any damage, but nevertheless did so.

At the time, Morris's dad was chief scientist for cybersecurity at the US National Security Agency (NSA). A lot of the things he did, he learned from his father. I feel a kindred spirit with Morris. We're the same age, we used to


STEPHEN J. COHEN/WIREIMAGE/GETTY IMAGES

**State-funded Russian hackers were accused of disrupting the 2016 US election campaign**

both go with our dads to their work at Bell Labs, (where Morris senior worked prior to his move to the NSA). We never met, but I know we were both really interested in the UNIX operating system and we both read all the manuals.

**It seems that you have more sympathy for some of the hackers than for the big tech companies like Microsoft. Why is that?**
Well, partly because it's adults versus children. And because I want to hold Bill Gates to account for, in my opinion, wanting to crush the free and open internet and not prioritising security. Also, the hackers I'm talking about are often young boys who are trying to win the respect and esteem of their peers, which is something I think we all can relate to. They often get sucked into a cycle of escalating transgressions, which is a very well known behaviour pattern in human psychology. And they tend not to be, you know, billionaires.

**What have we learned from the hacks you write about that could help tackle cybercrime?**
One of the things that has been said many times is that it's a cat-and-mouse game. Somebody does something, you fix it. Somebody does something else and, again, you fix that. They respond and so on. Cybersecurity is so much better than it used to be, but the attacks are so much better than they used to be too. I feel this cat-and-mouse game will keep going forever.

The question is, can we win the game more than we are right now? I think the answer is yes if we start to view cybersecurity as primarily a human problem that requires human solutions. We need to develop rules and norms and principles to regulate how computer code is written, deployed, tested and, ultimately, used. It's always going to be a whack-a-mole situation, but we can make it so that it's not so frustrating.

**In the movies, a hacker who is caught is always offered a job with the government. Does that happen in real life?**
Yes, that's what happened in the last hack in the book. The three hackers released malware called Mirai that targeted and took control of devices connected to the internet of things, like security cameras and smart toasters. Instead of being incarcerated, they were given five years of community service, during which time they worked for the FBI and helped stop a nation-state hacking group. They were mentored by the FBI agent who caught them. The special agent diverted them into a socially productive activity instead of a socially wasteful activity like putting them in jail.

**What would you say to *New Scientist* readers who want to make sure their own computing is as secure as it can be?**
Don't freak out. Ordinary people aren't high value targets. Cybercriminals don't want to hack you, they want to make money. That means they don't want to spend time on people who take even minimal precautions. I think the most minimal precaution you could take is never clicking on a link or opening an attachment in an email from somebody you don't know.

**Has artificial intelligence changed hacking?**
Yes. Cybercriminals tend to be non-native English speakers who target the English-speaking world, and this provides a natural barrier to the effectiveness of their phishing emails. They need to write English not only with correctly spelled words, but also to write idiomatically. This has been very difficult. But ChatGPT allows everyone to write a good hacking email, a good phish, so it's going to become even more important not to click links in emails from people you don't know.

**Have you ever hacked a computer that you shouldn't have?**
Well, I got up to the edge. It was the Yale law library website. I did what was called a cross-site scripting attack, which injects malicious script, and it generated a link that I could have used to send an email, let's say to the dean, to say "hey, look at this new book that the library is ordering" and have her click on it and then gain access to her machine.

Of course, I would never do that, but I was proud of myself for being able to get to the line. I didn't gain unauthorised access, but I was tempted. I feel like I'm a responsible person, but you just get caught up in it. This is the problem, which I repeat over and over and over in my classes. You will want to use this. Do not use this. ▮

David Adam is a science journalist based in Hertford, UK, and author of *The Man Who Couldn't Stop*