

Bruce Schneier

Security Technologist & Guru

Securing Society by Hacking Society. A hacker mindset is essential to understanding the security of complex technological systems. This way of thinking applies much more broadly: not only to socio-technical systems but to purely social systems as well. Tax loopholes, for example, can be understood as hacks of the tax code. Disinformation campaigns can be understood as hacks of the democratic election process. This talk extends the core language of hacking to the broad systems that underlie our society. Bruce Schneier will talk about what it means to hack the law, to hack the market economy, and to hack the democratic process. Others have written about how social-engineering hacks trust and authority, and how social-media sites hack attention. He will generalize this further, discussing how our cognitive systems are hacked. Finally, he will extend these notions to discuss artificial intelligence and robotics; these systems will hack what it means to be human, and also how we react to things we react to as human. In the 21st century, everything is a socio-technical system, and everything is vulnerable to hacking. Our experience and expertise are necessary to secure these systems. Schneier's goal is to explain how we can do that.

Securing a World of Physically Capable Computers. Computer security is no longer about data; it's about life and property. This change makes an enormous difference, and will shake up our industry in many ways. First, data authentication and integrity will become more important than confidentiality. And second, our largely regulation-free Internet will become a thing of the past. Soon we will no longer have a choice between government regulation and no government regulation. Our choice is between smart government regulation and not-so-smart government regulation. Given this future, it's vital that we look back at what we've learned from past attempts to secure these systems, and forward at what technologies, laws, regulations, economic incentives, and social norms we need to secure them in the future.

Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. Much of surveillance is voluntary: we cooperate with corporate surveillance because it promises us convenience, and we submit to government surveillance because it promises us protection. The result is a mass surveillance society of our own making. But have we given up more than we've gained? In this speech, security expert Bruce Schneier offers another path, one that values both security and privacy. He shows audiences what they can do to reform our government surveillance programs and shake up surveillance-based business models, while also providing tips to protect their privacy every day. Your attendees will never look at their phone, their computer, their credit cards, or even their car in the same way again.

Security Technology in the Public Interest. Computer security is now a public policy issue. Election security, blockchain, "going dark," the vulnerabilities equities debate, IoT safety, data privacy, algorithmic security and fairness, critical infrastructure: these are all important public policy issues with a strong Internet security component. But while an understanding of the technology involved is fundamental to crafting good policy, there is little involvement of technologists in policy discussions. This is not sustainable. We need public-interest technologists: people from our fields helping craft policy and working to provide security to agencies and groups working in the broader public interest. We need these people in government, at NGOs, teaching at universities, as part of the press, and inside private companies. This is increasingly critical to both public safety and overall social welfare. This talk both describes the current state of public-interest technology, and offers a way forward for us individually and collectively for our field. The defining policy question of the Internet age is this: How much of our lives should be governed by technology, and under what terms? We need to be involved in that debate.

Liars and Outliers: Enabling the Trust that Society Needs to Thrive. Human society runs on trust. We all trust millions of people, organizations, and systems every day -- and we do it so easily that we barely notice. But in any system of trust, there is an alternative, parasitic, strategy that involves abusing that trust. Making sure those defectors don't destroy the cooperative systems they're abusing is an age-old problem, one that we've solved through morals and ethics, laws, and all sort of security technologies. Understanding how these all work -- and fail -- is essential to understanding the problems we face in today's increasingly technological and interconnected world. In this talk, Bruce Schneier, world-renowned for his level-headed thinking on security and technology, tackles this complex subject head-on. Weaving together ideas from across the social and biological sciences to explain how society induces trust, he shows audiences how trust works and fails in social settings, communities, organizations, countries, and the world.