

Talking Tech with Cisco



TED Talk 10-Pack: Security Lectures That Will Open Your Eyes and Mind

Posted by [Gary Pfitzer](#) in [Talking Tech with Cisco](#) on Jun 22, 2016 5:23:10 PM

With all of last week's big security news at Cisco—[Global Cybersecurity Scholarship program](#), [CCNA Cyber Ops certification](#), and [CCIE Security v5.0](#)—I'd like to provide some further security fuel for thought and motivation this week. And what better place to go for that than to TED Talks? We all love TED Talks, right?

CSO, the IDG publication providing news, analysis, and research on security and risk management topics, makes it easy by having collected all in one place "10 Security TED Talks You Can't Miss." Says CSO, "These talks tackle some of the biggest security challenges of our time, from securing medical devices to how cyberattacks can threaten world peace. ... We think you'll be better for having taken the time to listen and consider their messages."

These 10 talks are all relatively short—ranging from 9 to 19 minutes in length—so not a huge investment in return for the kind of wisdom, insight, and passion that TED Talks can provide. Many of them are galvanizing calls to action. You could start each day off with one talk for a couple weeks, or else listen to them all in one 2½-hour sitting.

Whether Sobering, Chilling, or Inspirational, the Talks Are Riveting

Here's a taste of what awaits:

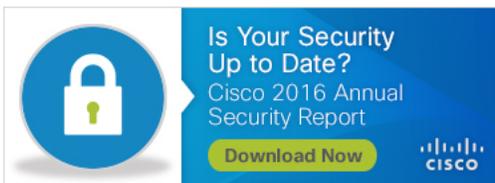
- ["Hackers: The Internet's Immune System"](#): Cybersecurity expert Keren Elazari discusses how hackers—even with the scary power they have—ultimately make the Internet a stronger, more resilient place by forcing the networked world to respond and evolve. The key, she says, is to find those hackers who are less motivated by financial gain through organized crime and more fascinated simply by the power of being able to "break things." We need to harness the latter to be our heroes, showing us the weaknesses in our systems and how to fix them.
- ["Fighting Viruses, Defending the Net"](#): In this talk, computer security expert Mikko Hyppönen provides a history of the computer virus, showing us with intriguing examples how viruses have evolved from the province of hobbyists and teenagers to that of organized criminals with increasing sophistication. More than devoting all of our energy to antivirus methods, we must undertake a concerted global effort, he advocates, to finding online criminal gangs and taking them down.
- ["Hire the Hackers!"](#): British journalist Misha Glenny paints a vivid picture of the struggle in which we are engaged for control of the Internet. We are fixated on "dazzling technological solutions" when what we should be doing, he argues, is gathering more "human intelligence" on the character and nature of hackers and, instead of imprisoning them, focus on improved socialization and better use of their extraordinary skills.
- ["All Your Devices Can Be Hacked"](#): It is not news to us that with the potential of the Internet of Things (IoT) comes the decided risk of so many connected devices being hacked. Avi Rubin, expert in systems and network security, provides chilling examples of how cars, smartphones, and medical devices can be compromised. Developers of today's technology must take security into account from the very beginning and think outside the typical threat models, Rubin stresses.
- ["How Cyberattacks Threaten Real-World Peace"](#): Author Guy-Philippe Goldstein gets us to think about how cyber weapons could be used to trigger armed conflict. The problem is complicated by the fact that one country might not even be able to determine where a cyberattack is coming from, thus creating dangerous room for confusion. Also problematical is the fact that when a country builds a cyberwar unit for defense, there can be a fine line between defensive and offensive uses of that unit.
- ["Governments Don't Understand Cyber Warfare. We Need Hackers."](#): Today's platforms for cyberwarfare can be deployed by activists, criminals, and corporations faster than governments can react, according to information security researcher Rodrigo Bijou. Governments are not adapting and learning fast enough, he says, and are using mass online surveillance that just causes more fear. Individuals and organizations need to step up because they have the power to work across borders more rapidly and effectively than governments can. The technological opportunity and cooperation should be inspiring, not fearful, he adds.



- **"What's Wrong with Your Pa\$\$w0rd?":** Computer science and engineering professor at Carnegie Mellon University, Lorrie Faith Cranor, shares with us the extensive research that she has done in the area of passwords. She gets us thinking more seriously about the passwords we create by showing us the techniques that cybercriminals can use to hack them. Her presentation contains useful tips for creating stronger passwords.
- **"The 1s and 0s Behind Cyber Warfare":** Cybersecurity researcher Chris Domas gets down to binary nitty-gritties here. In an engrossing account, he relates how he employed visual pattern recognition to translate all those 1s and 0s into images that he could then use to radically simplify and speed up the process of pinpointing vital cyber information. This approach creates "a new weapon in the evolving theatre of cyberwarfare" and allows cyber engineers to "become first responders in emergency situations," Domas says.
- **"A Vision of Crimes in the Future":** The author of the book "Future Crimes," Marc Goodman, says he is afraid of what he sees when he looks at the future of crime and terrorism. He uses the example of the 2008 Mumbai attacks to show us how we seriously underestimate what cybercriminals and terrorists, who have now proven themselves capable of building whole terrorist operations centers, can do. He talks about how new technologies such as 3D printing and IoT can be used to ill effect and how human DNA might be hacked. Goodman ends on the constructive note of suggesting approaches that we can take in the face of so much threat, notably to engage average citizens as a whole to take action.
- **"Everyday Cybercrime and What You Can Do About It":** In this final segment, James Lyne, global head of security research at the security firm Sophos, shows us some of "the cybercriminal's latest and nastiest creations." We are given a concrete look at the modern cybercriminal, infiltration techniques, and the ways in which you make yourself vulnerable. The next time we get a "shiny new toy," Lyne urges us to look at it carefully in terms of what it can expose about us and learn its best practices in terms of basic security. On a broader level, Lyne believes that we need to focus more aggressively on how we are developing our talent pool.

You can find all 10 TED Talks from CSO [here](#). Which of the talks resonates most with you? Let us know why in the Comments below!

Fired up to do something about security and cybersecurity? Be sure to investigate the Security and Cybersecurity learning and certification pathways on the ["Certifications" page](#). And don't forget to look into our new [Cybersecurity Scholarship program](#).



Is Your Security Up to Date?
Cisco 2016 Annual Security Report
[Download Now](#)

Get the latest IT industry news and exclusive Cisco learning offers. [Sign Up Now!](#)



Gary Pfitzer is a content manager at Learning@Cisco, focused on bringing various aspects of today's IT journey to light through business papers, blogging, customer success stories, and other writing.

61300 Views Tags: [cybersecurity](#), [cybercrime](#), [it security](#), [hackers](#), [security ted talks](#), [cybersecurity ted talks](#), [cyberwarfare](#)

MOST LIKED

280 Comments

1 2 3 ...



Milan Jun 22, 2016 11:24 PM

Hi Gary,

Superb collection thanks for sharing with us.

I would say "Awareness" is only the thing that could help us prevent this crime in future. So i would pick [""What's Wrong with Your Pa\\$\\$w0rd?"](#) among them.

If we are able to aware people how they can browse securely over the internet then that will be awesome.

As i read somewhere, We can't totally stop hackers, Only difficulty level can be increased. So, spreading the awareness program is one of the best things to do.

Cyber-security Scholarship Program is an awesome program initiated by Cisco for the Future.

Thank You
Milan

[Actions](#)





Gary Pfitzer Jun 23, 2016 9:59 AM (in response to Milan)

Interesting, Milan, thanks. It is true that the very helpful information in "[What's Wrong with Your Pa\\$\\$w0rd?](#)" is great basic advice that all people can put into practice right away. It was intriguing to read about how Lorrie Faith Cranor went about researching password strength at Carnegie Mellon, and the sometimes surprising results she obtained. I'm glad you found that particular segment to be valuable!

--Gary

[Actions](#)



Sheldon.Copper Jul 28, 2016 7:18 PM

Its a good thing to see Cisco taking interest in training and teaching future Security Professionals.

There is however one thing that is most important of all, and that is Internships/Co-operative training opportunities where individuals get a feel for working In IT/Network Security in real life.

I don't see any organizations or companies taking on an initiative to train people on the job, of course there are few companies/groups out there that do that.

after training you will need to test those skills in the real world.

[Actions](#)



Arsalan Dec 18, 2016 8:33 AM

Great Videos, I saw a few of them before seeing this list. My point is pretty simple.

See we try to block or contain a virus or correct an application we wrote ourselves. Well, seen technically, if the program is very well written with extra security installed in the very beginning and highly sophisticated testing phase of the program. Many and I mean thousands or even millions of these vulnerabilities would not even be there to be exploited by hackers.

If we keep going with the way we are, we might end up having billions of vulnerabilities which are too much to block for networks unless of course you block all tcp and udp connections , which will make sure you are safe, but you lose the world wide web connectivity.

[Actions](#)



Kristopher Jul 29, 2016 9:49 AM

The videos linked are a great resource into the future of the industry. Although, I have to say, that linking TED videos is like waving a steak in front of a hungry lion. Those things are addictive. I think I enjoyed [Marc Goodman: A vision of crimes in the future - YouTube](#) the most as it opens your eyes to the flip side of the tech and encourages you to look at things from the villain's perspective. Reminded me that I'm not as paranoid as my non-technical family thinks I am.

Thanks,
Kris

[Actions](#)



Gary Pfitzer Jul 29, 2016 11:20 AM (in response to Sheldon.Copper)

Thanks for the thoughtful response, Abdullah. [Cisco offers internships](#), but they tend to be for individuals who are already pursuing a college or university degree program. An internship might be something that you need to scout out or even create on your own, perhaps by offering your services for free to an organization or business that inspires you in exchange for the experience that you will get. I agree with you that it would be wonderful if internships were more widely available in the industry, for all ages. If you happen to enter the new Cisco Global Cybersecurity Scholarship program, perhaps the mentor assigned to you will have some thoughts about this.

--Gary

[Actions](#)



Gary Pfitzer Jul 29, 2016 11:49 AM (in response to Arsalan)

Arsalan, I am sorry to hear that trying to take the initiative with internships has not really panned out for you yet. It can be hit or miss. It sounds as if you are being as enterprising as you can about gaining experience. And I hope that your involvement with Cisco and with the Cisco Learning Network community will continue to keep you fitting the pieces of the career puzzle together. There is, of course, no one set course to success, and we each do our best to figure out a satisfying pathway for ourselves.

Actions



Gary Pfitzer Jul 29, 2016 12:19 PM (in response to Kristopher)

Ha, you can't be too paranoid, it seems, sad to say. Marc Goodman's talk was definitely one of the darker ones of the 10 videos, I'd say. I know what you mean about the TED Talks being addictive--glad you found them engaging, Kristopher. Have you seen [Cisco's 2016 Midyear Security Report](#) yet? I haven't had a chance to check it out yet myself, but there's more to satisfy the morbid curiosity there about ransomware, I understand. With security, you are clearly immersing yourself in a field that needs you.

Best,

Gary

Actions



Sila Jul 29, 2016 9:31 PM

That's such a great videos, I am very interested with those, I just finished a few and I will watch all to get to know more and learn new things from expert. I am glade to be here.

Thanks for sharing.

Regards,
Sila

Actions



Arsalan Dec 18, 2016 8:34 AM (in response to Gary Pfitzer)

Thank you Gary I hope it does fit the pieces together. Oh Yes, it surely has been very enterprising.

Actions



sathappan Jul 30, 2016 12:05 AM

Hi Gary,
Nice collections. But why don't you update the collections with TED videos from 2015 and 2016 if available, because in cybersecurity everyday is a new challenge?

with regards
sathappan.s

Actions



Glenn Jul 30, 2016 4:04 PM

Hello Gary!

Thanks for the videos! I am now even more excited and even much more motivated to move forward with cyber security!

Actions



Jim Jul 31, 2016 8:04 AM

Great collection of videos and perspectives from all over the globe, for me it was nothing new that the sentiment is to employ the hackers, but interesting to see so many sharing that viewpoint. I was quite keen on learning more on the Binary side of things and how to visualise through colours what is difficult to read. The vulnerability in the Internet of Things was a bit of an eye opener, I guess I was aware of it, but never considered how much computers we have around us in our daily life - It is almost as common place as water or air.

Final note, I did enjoy the tie ins to the pop cultural aspect and sometimes it is a bit impressive how the story tellers from 20 - 30 - 40 - 50 years ago could predict today's technology, from Arthur C. Clarke to Robert Heinlein to Gene Roddenberry to Rafael Moreau writing the 1995 film Hackers (albeit far too visually cool back then, the concept of security is essentially what we face today). Through out all the videos in this list, they all seem to echo what the bad guy in the film said about hackers, that they have no borders, friends or family, they are nations of their own, with only temporary allies and associates. Scary thought, but an interesting concept.

Actions



Gary Pfitzer Aug 1, 2016 11:16 AM (in response to Sila)



You are welcome, Sila. I'm glad you are finding the videos to be intriguing. They're each fascinating in their own way, so do enjoy the rest of them!

Thanks,

Gary

[Actions](#)



[Gary Pfitzer](#) Aug 1, 2016 11:27 AM (in response to sathappan)

Thanks, "sathappan"! Good point about staying on the lookout for even more TED Talks -- from 2015 and 2016. These videos are still immensely timely, but I will hope to find more of them by and by.

--Gary

[Actions](#)



[Gary Pfitzer](#) Aug 1, 2016 11:30 AM (in response to Glenn)

That's great to hear! Wishing you the best in this, Glenn.

--Gary

[Actions](#)



[Gary Pfitzer](#) Aug 1, 2016 11:37 AM (in response to Jim)

Thanks for the thoughtful comments, Jim. When you look at all of the ways that cybercrime has evolved, you could say that truth is stranger than fiction. Certainly the Internet of Things has recently added a lot more to think about when we contemplate security.

--Gary

[Actions](#)



[Ejel](#) Aug 2, 2016 6:50 PM

Have watched all but the last two so far. Was very excited and even a bit frightened by what I heard.

The most chilling was the medical devices that can be reverse engineered and then hacked. Voting machines too. And vehicles. Mr. Rubin really shared a great deal about the vulnerabilities of any system. Knowing that the accelerometer can be used to determine what someone types. All things I have suspected but now are verified.

To hear that the Drug Cartel was killing people and decapitating them. Even going so far as placing the head of someone on a computer to show that hackers best stay away. To know that some people will resort to anything to protect their wrongdoing was very sobering. But it also made me angry at the same time. To think there are people out there exploiting the computer age for their own nefarious purposes, is upsetting.

Selfishly, my love for nerding and this remarkable medium that set me free from the chains of poverty, giving me access to anything I ever wanted to learn, being taken over by those who want to use it for less than responsible things, boils my blood. It makes me want to be a part of the groups who are combating the cyber threats. Whether it be someone taking someones passwords to those using it to physically harm others, I am protective of this new world available to anyone with internet access because of what it has meant to me and to others who may have otherwise been at a disadvantage in their quest to escape difficult circumstances by learning things that will help them become more qualified to work at better paying jobs.

Each Ted Talk thus far has added a new dimension to my understanding of the new challenges we face and how they are changing. It is clear to me that there is no way to prevent hacking while the system remains 1s and 0s. Even with encryption, it is all still 1s and 0s (voltages and non-voltages). There is a built in Rosetta Stone. The answer is in the question and the question is in the answer. We are so dependent on computers in our daily lives and so many of those coming of age have never lived in a world without computers and are very dependent on them. It seems that we will always be plagued by the attacks on the systems and no place is completely safe unless they are completely an isolated system not hooked into the public infrastructure. That of course negates the purpose of transfer of information but could secure a system.

Fascinating talks. Very helpful to my learning and also thought provoking. Now on to my last two...

[Actions](#)



[JONATHAN HAMILTON](#) Aug 3, 2016 7:04 PM

Whao, from James Lynes to Prof Aviel to the force man Marc and down to the pretty Geek Keren, I will say I had a blast and whao moments with these videos. Thank you

One thing I realized is that, most hackers, started young, ready to work for fun, thus love what they are doing, intelligent, hardworking and IGNORED. If an intern (as mentioned by Gary in the above comment) can willingly work for free for the fun and experience worth, guess the intern will work all sweat out at the offer of a million dollars, so this is same to most hackers that are given better offers and sometimes made to choose between death of a family member and millions of dollars work sessions in multimillion dollars hacker's infrastructures. Guess you know the choice of the young talented who wants to save his family and live a luxury life with his skills.

As much as great organizations and forums try to reduce/prevent this act, there is much more work for the government to not ignore the hacking mind and fun act of a child, to set up bigger infrastructures for IT securities and employ hackers (well with understandable policies).

If you want THEM then be THEM.

Thank you Cisco.

[Actions](#)



[Gary Pfitzer](#) Aug 4, 2016 7:08 PM (in response to JONATHAN HAMILTON)

Thanks, Jonathan, for the food for thought. In the near-term (hopefully, by September), we'll have a post in this blog titled "Malware, Inc.," which will explore the idea of malicious hackers going to their highly organized 9-to-5 jobs in the world of cybercrime. It is a daunting reality to contemplate. I think it is Keren Elazari in the first video above who makes the point that hackers who are more motivated by the thrill or challenge, versus being driven by financial incentive, are those who could be guided to using their hacking skills for good. I'd like to think that is the case, but I'd be curious to hear what others think.

Best,

Gary

[Actions](#)



[WhiteVudoo](#) Aug 4, 2016 7:45 PM

Hey Gary, "[Fighting Viruses, Defending the Net](#)"

I think the Gov needs to do more to fight those hackers to wish to do harm. Like criminal groups that spread ransom ware and hold hospitals and patients for ransom. I finished watching the complete TEDx videos in one sitting. What I got out of all these videos is less talk and more action. This is the new cold war.

A few years ago I received a letter in the mail that my information was stolen from one of the most secure place in the Gov. So not only did the criminals have my information, but they had information about me far beyond my SSN. I immediately went online and google the security breach and confirmed my greatest fear. I felt powerless and angry at the same time. How can criminals get into a system that is suppose to be the most protected system on the planet. Since then I started to study security, networking and penetration testing. Every second of every minute from the time I wake up to the time I go to bed has been a mission to gain knowledge about the network. In order for me to be a great white hat, I had to learn and understand the network down to the binary. This is not about money this is personal.

[Actions](#)



[Gary Pfitzer](#) Aug 4, 2016 8:28 PM (in response to Ejel)

Thanks very much, Ejel, for sharing your personal experience and feelings about this. Your comments are riveting like the TED Talks, especially this one: "*Selfishly, my love for nerding and this remarkable medium that set me free from the chains of poverty, giving me access to anything I ever wanted to learn, being taken over by those who want to use it for less than responsible things, broils my blood.*" Yes ...

Though there is much to brood about in the TED Talks, I hope there is also a continuing call to action for you. It sounds like there is!

Thanks again,

Gary

[Actions](#)



[Shrijan Pradhan](#) Aug 5, 2016 12:54 AM

Hi Gary,

It is so true that now matter how we try to secure our self but somehow we let our self to vulnerability by disclosing personnel info in public and social medias.

Even though So many Antivirus software seems promising but after watching TED - "Everyday Cybercrime and What You Can Do About It", there is a Christmas Party for the Hackers Everyday.. :-(

Many thanks for the awareness collection.

Regards,
shrijan

[Actions](#)



[Mike Gannon](#) Aug 5, 2016 5:06 AM

Keren Elazari mentioned Blackhat & Defcon talks on Youtube. I started watching these as background when I'm doing the more mundane tasks at work and it really opened my eyes to whats possible with IoT, and that while innovation is great it is bringing massive challenges to network engineers.

Mikko Hyppönen is great. I've watched a lot of his talks on security, privacy and free speech.

We need an educated workforce to design, build and maintain our infrastructure. But more than that we need people with these skills to be able to sit in front of customers and educate them and guide them to the right solutions.

[Actions](#)



[AndresTX](#) Aug 5, 2016 6:56 AM

Hello Gary,

Thanks a lot for this information. I'm amazed how vulnerables we are regarding Cyber security in our world. A game changer for IT professionals and anyone who has any relation with a computer. Thanks again sir.

Best regards,

Andres L.

[Actions](#)

1 2 3 ...