CYBERPHOBIA : IDENTITY, TRUST, SECURITY AND THE INTERNET PDF, EPUB, EBOOK

Edward Lucas | 306 pages | 17 Nov 2015 | Bloomsbury USA | 9781632862259 | English | New York

Cyberphobia: Identity, Trust, Security and the Internet: Edward Lucas: Bloomsbury USA

My daughter fell for this on her tenth birthday. However, the top entry which came up on Google directed her not to the openoffice. This was Mindspark, produced by a legitimate company, but the subject of some controversy because of the way it operates. There is nothing illegal in that

— but it was not something that either my daughter or I had consented to. The book is giving; if anything it gave too much as it felt at times overwhelming. This reviewer is quite familiar with computer security and related matters and it managed to keep his interest; in the hands of an interested generalist one can imagine it could be liquid gold. It might encourage them to be a little more alert with their online usage. Of course, even the more experienced of us can get hit; whether by our own laziness, lack of attention or a new, hidden attack vector.

We should always be on the alert. Yet the book delivered what it promised and then some. One would rather there was not a need for a book like this, but there is, so there is no use crying about it. Acting to reduce the threat is the action word of the day. Get to it. Get the book and work on your defensive strategy. Cyberphobia, written by Edward Lucas and published by Bloomsbury. ISBN Feb 28, Jon Stonecash rated it it was ok. This review has been hidden because it contains spoilers. To view it, click here. I confess that I quit reading about half way through. There may be some solid ideas in the second half of the book, but the simplistic and sometimes sensation tone of the first half just put me off. Part of my problem is that I have worked in this field and read fairly deeply in this area.

This book was just too oriented to a general reader. View 1 comment. Sep 20, Dusan Tatransky rated it liked it. This book was easy to diggest, short, comprehensible, with good examples. But in some parts I was confused about the target audience, is the book meant for the laic individuals and small company owners, or is it for somebody interested in geopolitics. Nevertheless, I would highlight 3 strong features of the book: First, the made-up couple Chip and Pin Hakhetts, the author uses to show the cybersecurity needs and dangers in common life, the most readers can easily relate to.

Secondly, I enjoyed t This book was easy to diggest, short, comprehensible, with good examples. Secondly, I enjoyed the part about the Estonian e-governance, it was very interesting, since Mr. Lucas had first-hand insights into the system, being the first honorary digital citizen outside Estonia. And lastly, I find the notes at the end of the book invaluable, if you are as deeply interested and hungry for resources in cybersecurity as I am, you will find many great sources there. Attackers need to be get lucky only once. Defenders need to be lucky all the time Author is correct We are not yet came to Zero Day. We need to protect ourselves. How hard to trace Malware codes.. MS-DOS 4, lines. Lightweight Content with Heavy Book But can get few Good quotes.

Dec 07, Keith rated it liked it Shelves: sci-tech-misc-nonf. Kind of scarey overview of the dangers of the Internet. It was designed to be free and open, not particularly secure. It was based on trust. It has become so essential and huge that defending against cyber attacks, etc. Vital reading for anyone concerned with security and online use. Jun 30, Jonathan Cantor rated it liked it. The topic is interesting and the book is filled with relevant information. That said the book is structured poorly and jumps from topic to topic haphazardly. But if you need a good overview of cyber security it is a quick and easy read. Jul 25, Paul W rated it really liked it Shelves: technology , cyber-security , internet.

Computers, and computing are broker. If you do not take elementary precautions … you are a menace not just to yourself, but to others. You will benefit more from the right to identify yourself to others, than from being anonymous. But nothing of the kind exists to keep it safe and reliable. George Tenet, Director of the CIA, has said that "We are staking our future on a resource that we have not yet learned to protect". The internet of things is growing rapidly: there were 1. We focus very hard on two rights: to be anonymous and to be private. And, there are some editing errors eg p 73, p87 - sadly increasingly common in books published today.

Paranoia is the second. Jun 27, Florin Pitea rated it really liked it Shelves: until , non-fiction. Interesting and informative. Nov 28, Timo rated it really liked it. Riding a bicycle at night, we use lights. Driving a car, we wear seatbelts. So why is our attitude towards online security so relaxed? In this lecture journalist, author and LSE alumnus Edward Lucas talks about his new book Cyberphobia: Identity, Trust, Security and the Internet , which reveals the ways in which cyberspace is not the secure or private zone we may hope, how passwords provide no significant obstacle to anyone intent on getting past them, and how anonymity is easily accessible to anyone — malign or benign— willing to take a little time covering their tracks. The internet was designed by a small group of computer scientists looking for a way to share information quickly. In the last twenty years it has expanded rapidly to become a global information superhighway, available to all comers, but also wide open to those seeking invisibility.

This potential for anonymity means neither privacy nor secrecy are really possible for law-abiding corporations or citizens. As identities can be faked so easily the very foundations on which our political, legal and economic systems are based are vulnerable. Please check your email to confirm your email address. Your School account is not valid for the United States site. You have been logged out of your account. Sarah J. Susanna Clarke. Carol Anderson. Miriam Toews. Brigid Kemmerer. Mark Kurlansky. Samantha Shannon.

Sign in Create an account. Sub-total excluding delivery. Shop in. Books Authors Discover Connect. Featured authors View all authors. About Us Overview. Missions and Values. Environmental Policy. Investor Relations. Contact Us Customer Service. Trade Contacts. Working at Bloomsbury Current Opportunities. Working at Bloomsbury. Maas Sarah J. Maas Books. Downloadable Free Activities. Bloomsbury Digital Resources Products. Librarian Resources. Contact Information. BDR Global Catalog. Bloomsbury Academic. Item added to basket. Checkout Continue Shopping.

Add to basket. Description Cybercrime is increasingly in the news on both an individual and national level--from the stolen identities and personal information of millions of Americans to the infiltration of our national security networks allowing access to both economic and trade secrets. Close Preview.

Security by the Book - Cyberphobia: Identity, Trust, Security and the Internet | Hoover Institution

Please update your billing information. The subscription details associated with this account need to be updated. Please update your billing details here to continue enjoying your subscription. Your subscription will end shortly. Please update your billing details here to continue enjoying your access to the most informative and considered journalism in the UK. Accessibility Links Skip to content. Menu Close. Log in Subscribe. Hugo Rifkind. For folks who aren't familiar with the topic and are interested, I'd highly recommend the book. View all 3 comments. Esimene pool raamatust on hea sissejuhatamaks tavalist uudishimulikku lugejat arvutiturbe maailma. Nii nagu meie Eestis harjunud oleme. Nov 01, Darren rated it

it was amazing. Even if you erect a mini Faraday cage around your house, your life is still going to be impacted by acts of cybercrime and cyberterror.

Maybe mankind will learn, possibly this is going to be an accelerated form of evolution as society has seen such massive technological leaps in a relatively short period of time. The author seeks to dampen down fear and possible hysteria whilst taking a sensitive look at the risks that cybercrime can create. We can all play our part in reducing its growing footprint, no matter if we are mere users or high-up executives who should know better. What about messing about with power stations and other sensitive infrastructure; best not to think too much about that. Lots of fun and games await, with potentially deadly, costly consequences. It is written in an open, accessible and demanding format, pulling the reader in without needing to add structures to scare them: the potential cold reality can do that for itself. Many of the crimes undertaken are quite ingenious or simple on a theoretical level — such as breaking into a bank computer, grabbing debit card numbers and changing their access rights to make them limitless, before the details were sent to gangs in 27 countries who went, armed with copies of the cards, around emptying the accounts in a short time.

One enterprising gang visited two thousand cashpoints in New York City alone. Some of the attack vectors are simpler and rely on people not knowing better or assuming things. My daughter fell for this on her tenth birthday. However, the top entry which came up on Google directed her not to the openoffice. This was Mindspark, produced by a legitimate company, but the subject of some controversy because of the way it operates. There is nothing illegal in that — but it was not something that either my daughter or I had consented to.

The book is giving; if anything it gave too much as it felt at times overwhelming. This reviewer is quite familiar with computer security and related matters and it managed to keep his interest; in the hands of an interested generalist one can imagine it could be liquid gold. It might encourage them to be a little more alert with their online usage. Of course, even the more experienced of us can get hit; whether by our own laziness, lack of attention or a new, hidden attack vector. We should always be on the alert. Yet the book delivered what it promised and then some. One would rather there was not a need for a book like this, but there is, so there is no use crying about it.

Acting to reduce the threat is the action word of the day. Get to it. Get the book and work on your defensive strategy. Cyberphobia, written by Edward Lucas and published by Bloomsbury. ISBN Feb 28, Jon Stonecash rated it it was ok. This review has been hidden because it contains spoilers. To view it, click here. I confess that I quit reading about half way through. There may be some solid ideas in the second half of the book, but the simplistic and sometimes sensation tone of the first half just put me off. Part of my problem is that I have worked in this field and read fairly deeply in this area. This book was just too oriented to a general reader.

View 1 comment. Sep 20, Dusan Tatransky rated it liked it. This book was easy to diggest, short, comprehensible, with good examples. But in some parts I was confused about the target audience, is the book meant for the laic individuals and small company owners, or is it for somebody interested in geopolitics. Nevertheless, I would highlight 3 strong features of the book: First, the made-up couple Chip and Pin Hakhetts, the author uses to show the cybersecurity needs and dangers in common life, the most readers can easily relate to.

Secondly, I enjoyed t This book was easy to diggest, short, comprehensible, with good examples. Secondly, I enjoyed the part about the Estonian e-governance, it was very interesting, since Mr. Lucas had first-hand insights into the system, being the first honorary digital citizen outside Estonia. And lastly, I find the notes at the end of the book invaluable, if you are as deeply interested and hungry for resources in cybersecurity as I am, you will find many great sources there. Attackers need to be get lucky only once. Defenders need to be lucky all the time Author is correct We are not yet came to Zero Day.

We need to protect ourselves. How hard to trace Malware codes.. MS-DOS 4, lines. Lightweight Content with Heavy Book But can get few Good quotes. Dec 07, Keith rated it liked it Shelves: sci-tech-misc-nonf. Kind of scarey overview of the dangers of the Internet. It was designed to be free and open, not particularly secure. It was based on trust. It has become so essential and huge that defending against cyber attacks, etc.

Vital reading for anyone concerned with security and online use. Jun 30, Jonathan Cantor rated it liked it. The topic is interesting and the book is filled with relevant information. That said the book is structured poorly and jumps from topic to topic haphazardly. But if you need a good overview of cyber security it is a quick and easy read. Jul 25, Paul W rated it really liked it Shelves: technology , cyber-security , internet. Computers, and computing are broker.

If you do not take elementary precautions … you are a menace not just to yourself, but to others. You will benefit more from the right to identify yourself to others, than from being anonymous. But nothing of the kind exists to keep it safe and reliable. George Tenet, Director of the CIA, has said that "We are staking our future on a resource that we have not yet learned to protect". The internet of things is growing rapidly: there were 1. We focus very hard on two rights: to be anonymous and to be private. And, there are some editing errors eg p 73, p87 - sadly increasingly common in books published today.

Paranoia is the second. Jun 27, Florin Pitea rated it really liked it Shelves: until , non-fiction. Interesting and informative. Nov 28, Timo rated it really liked it. Ta viitas sellega internetile. Toosama Mida toob aga selles osas tulevik? Selleks ei ole vaja kallist tehnikat ja hulka inimesi. Seda ka it-teenuse pakkujate poolt. Jan 12, Autumn Shuler rated it really liked it Shelves: non-fiction. TL;DR Review Great for anyone who uses computers read: everyone and needs information on how to protect themselves. Particularly if they aren't techies. Read It If You use any technology and know you could be doing so in a more secure manner. If you'd like to see a slightly more in-depth review, see my blog. Aug 14, David Abiani rated it it was amazing. A comprehensive study in computer and Internet security.

It's not technical but written for non-experts! It uses storytelling to explain what is at stake! It exposes how the free meal of Internet crime concerns us all and how legislation is lacking behind the sophistication of Internet crime. You are sucked in to the stories and are amazed and shocked by the Wild West of cyberspace and what it can do to destroy lives, businesses and national interests!

Cyberphobia: identity, trust, security and the internet

The core thesis here, which has merit, is that nothing else in modern life functions like. Subscription Notification. We have noticed that there is an issue with your subscription billing details. Please update your billing details here. Please update your billing information. The subscription details associated with this account need to be updated. Please update your billing details here to continue enjoying your subscription. Your subscription will end shortly. Please update your billing details here to continue enjoying your access to the most informative and considered journalism in the UK. Stories about weaknesses in cybersecurity like the "Heartbleed" leak, or malicious software on the cash registers at your local Target have become alarmingly common.

Even more alarming is the sheer number of victims associated with these crimes--the identities and personal information of millions is stolen outright as criminals drain bank accounts and max out credit cards. The availability of stolen credit card information is now so common that it can be purchased on the black market for as little as four dollars with potentially thousands at stake for the victims. Possibly even more catastrophic are hackers at a national level that have begun stealing national security, or economic and trade secrets. The world economy and geopolitics hang in the balance.

In Cyberphobia , Edward Lucas unpacks this shadowy, but metastasizing problem confronting our security--both for individuals and nations. The uncomfortable truth is that we do not take cybersecurity seriously enough. Strong regulations on automotive safety or guidelines for the airline industry are commonplace, but when it comes to the internet, it might as well be the Wild West.

Standards of securing our computers and other internet-connected technology are diverse, but just like the rules of the road meant to protect both individual drivers and everyone else driving alongside them, weak cybersecurity on the computers and internet systems near us put everyone at risk. Lucas sounds a compelling and necessary alarm on behalf of cybersecurity and prescribes immediate and bold solutions to this grave threat.

Useful for nonexperts wanting a larger picture of cybersecurity. Another is that, even now, the West doesn't much seem to care that its secrets are being pilfered by a regime that wishes us ill. A remarkably clear, comprehensive and lucid exposition of the growing range of threats that challenge trust in the internet. Lucas s book reminds us of the need for tougher standards--not just for individuals but for the companies that have made the Internet our virtual home. A realistic view of what can and cannot be done on both the individual and at a policy level to protect privacy and deal honestly on the Internet. Even informed readers will benefit from Lucas s synthesis of chilling incidents. Lucas a British journalist who writes for "The Economist" joins others in delivering this warning, but he is more successful than most because he probes the subject without resorting to computer jargon and so conveys the nature of the threat to those who use computers without regard to the fact that they can jeopardize wealth, reputation, and peace of mind.

Cyberphobia: Identity, Trust, Security and the Internet by Edward Lucas

The New Yorker once ran a cartoon of a pair of pooches sitting at a keyboard. He or she sends email, but has never much thought about how it works. Most, probably, will belong to an older demographic. They are vulnerable to scams and viruses, because they click on things they should not, and miss the cues that a younger generation might spot by instinct. The core thesis here, which has merit, is that nothing else in modern life functions like. Subscription Notification. Joseph A. The Finnish-Soviet Winter War — David Murphy. Stalingrad —43 2. Robert Forczyk. Thomas Anderson. Yokosuka D4Y 'Judy' Units. Mark Chambers. The Bronze Lie. Myke Cole. Unfollow Me. Jill Louise Busby. Bill Yenne. The Japanese Home Front — Philip Jowett. British Infantryman vs Mahdist Warrior. Ian Knight. Mark Lardas.

Dien Bien Phu Martin Windrow. Big Guns in the Atlantic. Angus Konstam. German Tanks in Normandy Steven J. Peter E. India, that is Bharat. J Sai Deepak. Indians in London. Arup K. Weapons of the Samurai. Stephen Turnbull. Late Roman Infantryman vs Gothic Warrior. Murray Dahm. Ju 87 Stuka vs Royal Navy Carriers. Robert Forsyth. Warlord Games. Crossing the road, we look both ways. Riding a bicycle at night, we use lights. Driving a car, we wear seatbelts. So why is our attitude towards online security so relaxed? In this lecture journalist, author and LSE alumnus Edward Lucas talks about his new book Cyberphobia: Identity, Trust, Security and the Internet , which reveals the ways in which cyberspace is not the secure or private zone we may hope, how passwords provide no significant obstacle to anyone intent on getting past them, and how anonymity is easily accessible to anyone — malign or benign— willing to take a little time covering their tracks.

The internet was designed by a small group of computer scientists looking for a way to share information quickly. In the last twenty years it has expanded rapidly to become a global information superhighway, available to all comers, but also wide open to those seeking invisibility. This potential for anonymity means neither privacy nor secrecy are really possible for law-abiding corporations or citizens.