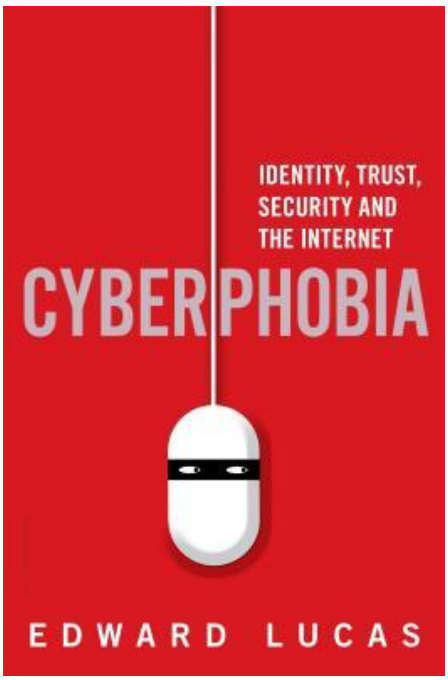

Cyberphobia: Identity, Trust, Security and the Internet

Edward Lucas

Cyberphobia: Identity, Trust, Security and the Internet

Edward Lucas

Cyberphobia: Identity, Trust, Security and the Internet Edward Lucas
Cybercrime is increasingly in the news. 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.

Cyberphobia: Identity, Trust, Security and the Internet Details

Date	:	Published November 17th 2015 by Bloomsbury USA (first published August 27th 2015)
ISBN	:	9781632862259
Author	:	Edward Lucas
Format	:	Hardcover 336 pages
Genre	:	Nonfiction, Science, Technology, Computers, Internet

From Reader Review Cyberphobia: Identity, Trust, Security and the Internet for online ebook

Maryanne Gobble says

I read a lot but this is one of the few books I had to quit because it was repetitive and used too many words to explain simple concepts. It's not the information in the book that is the problem, it's how it was presented. Also, I thought it was poor taste to compare cybercrime against tragedies that involve loss of life - and then act like cybercrime was the biggest tragedy of all.

David Abiani says

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! Well done and well written!

Eric Mesa says

It was concepts I was already aware of but the book put these vulnerabilities into perspective. Great read.

Darren says

After reading this book you could be forgiven for wondering where the off-switch is for your Internet connection; yet it won’t be enough – society is connected and online too deeply. 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. Don’t suffer from cyberphobia.

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.

The type of cybercrime and cyberterror can vary, whilst one person’s credit card number being stolen at a restaurant is individually a bad thing, it is a lot different to a hacker shutting down a car travelling at 100 miles per hour along a motorway or turning off all of an aircraft’s systems at take-off. 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. If it is not criminals and malicious people intending on causing havoc, it can be your country’s enemies; sometimes tomorrow’s enemies are today’s friends and partners…

The author lifts the lid on some of the activities that can plague us today. 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. The then director of America's Central Intelligence Agency was quite forthright with his forecast in 1998, noting that "we are staking our future on a resource that we have not yet learned to protect" – nearly two decades later have we really made great leaps towards this utopian goal?

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. So if a criminal group can figure this out, why can't a team of some of the brightest brains employed by banks and their suppliers do this and react ahead of time?

Some of the attack vectors are simpler and rely on people not knowing better or assuming things. It happened in the author's own family, as he notes: "The easiest way to install malicious programs on other people's computers is to get them to do it themselves. My daughter fell for this on her tenth birthday. I had given her a small £100 ($170) Asus laptop and told her to download Open Office (a free-of-charge program which has most of the functions of the much more expensive Microsoft Office). However, the top entry which came up on Google directed her not to the openoffice.org website, but to another one, where the download came accompanied by some unwelcome search software. This was Mindspark, produced by a legitimate company, but the subject of some controversy because of the way it operates. In my daughter's case it modified her web browser, so that every search produced an avalanche of unwanted information and advertisements. Mindspark's business model is based on funnelling computer users to its customers, and also selling data about browsing habits. There is nothing illegal in that – but it was not something that either my daughter or I had consented to." The consequences, of course, could have been a lot more serious if someone else had a darker intent.

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 9781632862259. YYYYY

Autamme.com

Varun says

A comprehensive and accessible introduction to the fears surrounding cybercrime. An engrossing read that spells out in no unclear terms the danger that the massive blackbox internet has become for the vast majority of its users and how directed influencers, infiltrators, criminals and pranksters are harnessing the vulnerability.

Keith says

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. is not easy. Vital reading for anyone concerned with security and online use.

Joe C. says

This book is an excellent introduction to the world of cyber security for someone unfamiliar with the topic. The author provides enough detail to get the point across without having to lapse into geek-speak.

For me personally, it was a bit more basic than I was wanting, thus my rating. For folks who aren't familiar with the topic and are interested, I'd highly recommend the book.

Vinod Kumar Dasari says

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. "We are staking our future on a resource that we have not yet learned to protect" - George Tenet, Director of CIA in 1998.

How hard to trace Malware codes.. Ex. MS-DOS 4,000 lines., But New Car has 100 million lines of code.

Lightweight Content with Heavy Book... But can get few Good quotes.

Autumn Shuler says

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.

Skip It If
You’re a computer expert who has already created a secure system or wants an explanation more in-depth or technical than something the everyday user would need or understand.

If you'd like to see a slightly more in-depth review, see my blog.

Paul W says

"It’s hard to explain to regular people how much technology barely works, how much the infrastructure of

our lives is held together by the IT equivalent of baling wire. Computers, and computing are broker." Quinn Norton (May 2014)

In this book, Lucas tackles this problem highlighting three big points:

• 'complacent, careless and amateurish behaviour on the internet is as out of place as it is in transport or health. If you do not take elementary precautions … you are a menace not just to yourself, but to others.'

• 'we need to be more cautious about all our behaviour with services that purport to be 'free'.'

• strong digital identities are friends, not foes. You will benefit more from the right to identify yourself to others, than from being anonymous.

Lucas notes that the internet is 'a network which links the most modern, powerful, safe and important computers with the most weakly protected, misused and dangerous ones - was not designed for the reliance we are putting on it.' (p52) 'The internet was designed for resistance to random faults, not to targeted ones. … The same qualities that protect it from random threats make it vulnerable to deliberate attacks.' (p173) 'Because we have increased our dependence on computers and networks faster than we have been able to understand what we are doing, we face a much bigger number of… 'unmitigatable surprises' - events that do damage from which we cannot recover easily, or perhaps at all.' (p27)

Lucas contrasts our attitude to safety in cars, airlines and health with our recklessness when it comes to safety in computer usage noting that 'Though computers are potentially more dangerous, we have not yet learned to handle them as safely as we drive our cars.' While defects in cars result in recalls, there has never been a software recall. While the internet 'is just as vital [as aviation] for modern civilised life. But nothing of the kind exists to keep it safe and reliable. … [It] is much more complicated than aviation, yet it is far more laxly regulated.'

'Manufacturers who discover that their products are dangerous have to make great efforts to let people know.' However 'putting the onus on consumers to deal with manufacturers' mistakes is not the way other industries work.' (p49) 'Software is the only product where customers sign away all their rights to complain, no matter how disastrously it fails…' (p252)

The challenges that these cyber risks present are increasing exponentially. 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 1.9 billion gadgets online in mid-2014; predicted to be 9billion by 2018 - more than computers, smartphones and tablet computers combined. (p164) Lucas cites examples of hacking of thermostats, child monitors, wifi controlled power sockets, hotel rooms routers (one of the most serious security threats) and network-attached storage devices (NAS drives) which combine the serious security threat posed by a router with data.

Security certificates were intended to be part of the solution to the cyber risks the internet presents: 'The entire internet is built on the idea that security certificates are trustworthy.' (p183) However some certificate providers have close ties with their host country's intelligence services. Others have been penetrated by organised crime…' (p182)

As well as shocking the reader out of his or her complacency by clearly explaining the problem, Lucas also talks about solutions.

Lucas notes that it is a 'chance aberration that the internet had grown up with anonymity as the default option. … the anarchic freedoms it has brought have come at a cost - attackers flourish and we pay for it with our safety and freedom.' (p220) 'Our thinking on identity has been muddled. We focus very hard on two rights: to be anonymous and to be private. … We have focused much less on two other rights: to be able to identify yourself, and to know what data others are holding about you.' (p219)

Lucas speculates on whether this means we should change out regulatory approach to the internet and computer security, something that would be an anathema to many: Should an infected computer be reportable - analogous to public health community obligations? (p244) Should there be tougher sanctions for institutional carelessness? (p247) Should companies have reporting obligations for infected computers; or for vulnerable or compromised software or sites?

He cites approvingly, the example set by Estonia, whose citizens enjoy 'secure, convenient digital identity, coupled with a strong privacy protection, and widespread public support.' (p227)

A surprising omission is any commentary by Lucas on the role that social validation of identity might play, through organisations like FaceBook, LinkedIn and LifeTimes, in recreating trust and identity validation.

And, there are some editing errors (eg p 73, p87) - sadly increasingly common in books published today. Notwithstanding this, Lucas's Cyberphobia should be read by everyone.
Perhaps the final word should go to Lucas's sage advice: Humility towards attacks is the first line of defence. Paranoia is the second. (p240)

Timo says

Ajakirja The Economist vanemtoimetaja Edward Lucas on oma raamatus "Küberfoobia" võtnud ette missiooni teadvustada inimesi ohtudest, mis kübermaailmas valitsevad. Kuigi me ei anna endale neist aru, on neid seal väga palju. Küsimus pole vaid mõnes raha saamise eesmärgil saadetud petukirjas. Valesti käitudes võid kaotada kontrolli oma meiliaadressi, oma pangakonto või kogu oma arvutisse talletatud isiklike failide üle, halvemal juhul satud veel väljapressimise ohvriks. Need on täiesti reaalsed ohud, mis meid arvutikasutajatena iga päev varitsevad. Häkkerid ei pea tegelikult sotsiaalmeedia ajastul isegi isikuandmete kättesaamiseks enam pingutama. Neil on ülilihtne koguda informatsiooni avalikult kättesaadavatest allikatest, et panna üles just konkreetsele kasutajale mõeldud küberpüünised.

1998. aastal ütles CIA juht George Tenet, et teeme oma tulevikupanused ressursile, mida me pole veel õppinud kaitsmagi. Ta viitas sellega internetile. See oli aeg kui Facebooki asutaja oli veel 14-aastane ja Google oli alles seatud üles ühte renditud garaaži. Meenutame või 21. oktoobril USAs toimunud üht läbi aegade suurimat küberrünnakut, mis sai teoks aina populaarsemaks muutuva asjade interneti toel. Internet sündis väikese grupi teadlaste omavahelistes laborikatsetustes, mis pidi üle elama tuumarünnaku. Kuid keegi ei arvestanud sellega, kui ohtlikuks võib saada rünnak rösterite ja printerite poolt. Toosama 21. oktoobri küberünnaku ulatus paisus nii kiiresti, et lõi rivist välja terve hulga tuntud veebikeskkondi, mistõttu kasutajad ei saanud enam ligi mitmetele populaarsetele lehekülgedele nagu Twitter, Soundcloud, Airbnb, WhatsApp, Paypal jt.

Mida toob aga selles osas tulevik? Et asjade internet näitab vaid kasvutrendi – 2014. aastal oli online'is 1,9 miljardit vahendit, siis 2018. aastaks on neid seal hinnanguliselt juba 9 miljardit – ei paista siin midagi helget. Võimalused küberkuritegevuseks kahjuks ainult aina kasvavad, sest kõiki neid vahendeid on võimalik häkkida. Nii võib tõeline digitaalne Pearl Harbour olla alles ees, ütleb raamatu autor. "Küberfoobias" näitabki Edward Lucas mitmete näidete varal, et George Tenetil oli tuline õigus: me ei ole senini õppinud end internetis kaitsma.

Erinevalt klassikalisest sõjapidamisreeglitest on kübertandril mäng hoopis teine. Selleks ei ole vaja kallist tehnikat ja hulka inimesi. Rünnaku võib korraldada ka tagasihoidlike eluviisidega inimene, kes ei pruugi silma jäädagi. Rünnaku maksumus tema jaoks võib olla olematu, samas kaitsjale võib see tuua kaasa tohutuid kulusid. Et ründajail suuremaid kulusid pole, siis saavad nad proovida üha uuesti, testida ja muuta oma taktikat, kuni plaan õnnestub. Kaitsjatel aga mänguruumi pole – nemad peavad kaitses olema edukad kogu aeg. Vastasel juhul võivad tagajärjed olla kurvad. Rünnakute all ei ole vaid eraisikud ja nende isikuandmed. Üha suurema surve all on tootjad ja teenusepakkujad, sest tööstusspionaaži eesmärgil vahendeid ei valita.

Edward Lucase raamatu üks põhiküsimusi seisneb selles, et kui me ületame teed, veendume esmalt, et see oleks turvaline, siis miks me arvame, et interetis ei ole tarvis turvalisuse pärast muretseda. Sh ei ole kaugeltki põhjust kogu vastutust viirusetõrje peale jätta. Tänapäeval on ka programme või pahavarasid, mis suudavad petta viirusetõrje edukalt ära. Ülioluline on mõelda sellele, kuidas me internetis ise käitume ja oma turvalisuse tagame ning mõista seda, et meid kasutatakse kogu aeg ära. Seda ka it-teenuse pakkujate poolt.

See raamat näikse olevat küll kirjutatud teemal, mille tegelikest nüanssidest saavad aru vähesed, ometi on Lucas pannud teksti kirja nii hästi, et asja tuuma mõistavad suurepäraselt ka tehnoloogias mitte orienteeruvad inimesed. Kuigi pilt, mille ta maalib, on kahjuks päris ähvardav.

Erika says

EST: Olles väga vähe seda teemat käsitlenud raamatuid lugenud, julgen siiski soovitada. Hea sissejuhatus kübermaailma, mida ilmestavad mitmed näited "päriselust, füüsilisest elust". Lucas küll ütleb mitmes kohas, et võimatu on tuua igapäeva elust näidet, kuid on sellegi poolest keerulised teemad väga mõistetavaks teinud. Eesti e-riik saab ka mitmed setmed kordi pai oma läbimõeldud lahenduse, kasutajasõbralikkuse ja turvalisuse eest.
Küberkäitumine ja interneti elu on valdkond, millest peaksid mõtlema ja rääkima ka tavalised inimesed, mitte vaid sala/vastuluurega seotud kõrged agendid ja valitsuseametnikud. Keskmised harilikud tihti korduva käitumismustriga ja hajutatud tähelepanuga miljonid kasutajad moodustavad selle nii tugeva võrgu, kui on tema nõrgim mutrike. Paroolide regulaarne vahetamine on küll kasulik ent on vähetõhus kübermaailma pahatahtliku tumeda osa eest kaitsma.
Raamat on huvitav, kergesti loetav ja mõtlemapanev.

Russ Mathers says

Very good book. Makes me worry every time my phone or computer acts strangely! Also glad I've got a password encryption app now. Easy read for a non-tech person. Scary how poorly companies protect my information.

Jon Stonecash says

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.

Kathy Cowie says

I am reviewing this book for Global Business and Organizational Excellence, in the January-February issue. It is excellent, but will definitely make you think twice the next time you type a password, or go on the internet, or even turn on your computer!
