Joseph N. Pelton & Indu B. Singh

DIGITAL
A Cybersecurity Primer
DEFENSE

Springer

Digital Defense

Joseph N. Pelton • Indu B. Singh

Digital Defense

A Cybersecurity Primer

Springer

Copernicus Books is a brand of Springer

Joseph N. Pelton
Executive Board
International Association for the
Advancement of Space Safety
Space and Advanced Communications
Research Institute
Arlington, VA, USA

Indu B. Singh
LATA's Global Institute for Security Training
Los Alamos Technical Associates
McLean, VA, USA

ISBN 978-3-319-19952-8 ISBN 978-3-319-19953-5 (eBook)
DOI 10.1007/978-3-319-19953-5

Library of Congress Control Number: 2015947778

Springer Cham Heidelberg New York Dordrecht London

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Cover image used courtesy of Flickr user Chris Halderman through a Creative Commons license

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media (www.springer.com)

This book is dedicated to the hardworking cyber
security community that seeks to develop antivirus
software, firewalls, and protective systems
to defend against hackers and cybercriminals
that would invade your digital world. We hope
that this book can help to save would-be targets
of cybercriminals and that the advice in this book
will help to stem attacks by those that seek
to use the Internet for ill-gotten gain
and other nefarious purposes.

President Obama's Official Statement of February 13, 2015, on Cybersecurity and its strategic importance to the United States:

America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas.

Statement given on the occasion of the U.S. Cyber Security Summit, February 13, 2015

https://www.whitehouse.gov/…/president-obama-speaks-white-house-summit_on-cyberSecurity.htm

Preface

Cyber-attacks are increasing exponentially in the United States and around the world. Attacks in the United States are now averaging over 550,000 per week, or over 25,000,000 per year. Annual attacks on official U.S. government Internet sites have doubled from 31,000 in 2012 to over 60,000 in 2014. The increase of cyber-attacks is like an epidemic, and the threats to those that are linked to the Net via a desktop computer, a mobile phone, or a wireless local area network (LAN) in an office or router in their homes are of real concern.

In this short book there is straightforward and practical advice about how to defend yourself and your family against these often unprincipled and indeed criminal attacks. If you have an elderly mother or father or grandparent who uses the Internet you might buy this book for them. Or perhaps more likely buy it and go over the most relevant parts with them and arrange with them to purchase at least basic firewall, antivirus, and identity theft protection and set them wise to key Internet scams to look out for.

We hope this book provides lots of useful advice and good counsel. But we believe it can be most useful in helping you to defend your children, your immediate family, and especially elderly family members against the increasingly sneaky trick of cyber criminals. It provides assessments of various cybersecurity offerings and tips on strategies about how to go about obtaining professional assistance from competent computer security firms. The small and usually reasonable annual fees these companies charge can provide you with cyber protection that amounts to far less than the losses you might incur if you do not take these precautions.

Key elements that you will find in this book include:

- A clear and understandable presentation (i.e., no "techno-speak") of the various types of cyber threats that can now come to you via your Internet connections. These include, but are not limited to, viruses that can infect and disable your computer, malware that can allow your computer to send spam (unwanted e-mails out to thousands of others) for many nefarious purposes, and other types of computer trickery you should look out for. These computer tricks by "black hat hackers" (sometimes called "crackers") keep growing. Computer criminal are getting sneakier. Such antics include what are called "phishing" and "pharming." These seemingly legitimate messages are actually from computer criminals and might lead you to give away important passwords that could result in your financial accounts being drained of money, or perhaps worse.

  We also provide advice about coping with "ransomware," data bombs, and Trojans—all of which are dangers to watch out for in today's world. We are moving into a new world sometimes called the "cyber-crime bazaar." These are dark networks where a wide range of cybercriminal activities are conducted. Here you can buy stolen credit card numbers, buy kits to steal information off of wireless instant pay cards, or even find ways to disable alarms and other protective electronic systems. Keyless entry systems are just one of the new frontiers for cyber criminals.
- Practical advice about how to protect yourself and your family from cyber criminals that are variously called "black hat hackers," "crackers," or simply "hackers." We emphasize that you might find this book useful to defend not only yourself but also your spouse, your children, and perhaps most of all elderly parents who are hip enough to go online, write and read e-mail, use a smart phone, and even send out texts and Tweets but may not be the most adept at defending themselves against cyber scammers.

- In today's world, where baby monitors and home security systems can be hacked, smart refrigerators and washing machines can send out spam, and cyber thieves with scanners can roam a neighborhood seeking out unprotected wireless routers so they can hack into bank savings and stock broker accounts, you need to be equipped to know how to protect you and your loved ones against those who would use the Internet and other electronic systems to extort money, empty accounts, capture key credit card or social security information, or steal identities.
- Information about the latest professional services that address cyber-bullying. This abuse of the Internet has become almost an epidemic in the last few years, with dire results such as public humiliation and even teen suicides. There are professional cyber-services one can obtain not only to protect yourself against cybercriminals but also to deal more effectively with cyber-bullying. These services allow those attacked by cyber-bullies to report such attacks and bring those that abuse the Internet to justice.
- An explanation of what is "identity theft" and why this is perhaps one of the worst things that can happen from a cyber-attack. This is because it could not only expose you to substantial financial loss and a very long hassle to correct the problem, but you could end up being charged with crimes that you did not commit because some criminal has assumed your identity.
- There is an up-to-date listing of various computer security services that can offer protective services against cyber criminals. These include providers of such services as "antiviruses," firewalls, password protection, and insurance against identity theft. Although not foolproof these services can go a long way to protect you against cyber-attackers. There is also information on more professional ways to track down those that would seek access to your wireless computer routers and wireless LANs without authorization.
- We provide you a rundown on why you need to be careful when you access the Net via "smartphones" and precautions that you should take when you sign up for automatic online "pay and go" or "tap and go" services such as "Apple Pay," "Blink," American Express "Express," etc.
- There are also some more detailed chapters about vital infrastructure. These chapters discuss other things that some users need to be concerned about. This is because the security of these "hidden digital systems and vital infrastructure" are now key to our daily lives. We depend on digital infrastructure that has widespread impact on lives. Thus we provide up-to-date information for those people who are dependent on satellite services to attain broadband access, GPS navigation, and other space-based services.

There is also a discussion of security issues involving the use of “the Cloud” because the government and more and more companies use the Cloud to store our vital information, process our tax returns, and keep track of our bank accounts.

- Finally we discuss briefly the specialized computer communications networks that control electrical grids, traffic signals, pipelines, water supplies, sewage treatment, and other urban infrastructure. These digital systems are known by the catchy name of “Supervisory Control and Data Acquisition (SCADA)” networks. Many might think that they do not need to know about such things, but it turns out that vital services you depend on from banks, local governments, the federal government, power companies, and more are potentially at risk with this type of cyber hazard. This means that you, too, are at risk. If you find these two chapters on vital infrastructure (i.e., satellites, “the Cloud” and “SCADA systems” in particular) turn out to be more detailed and involved than suit your taste, you can skip over them and proceed to the chapters about the future and the ten essential rules to follow.

Unfortunately there are others out there whose ambitions go beyond stealing money electronically or pulling pranks on people via the Internet. These are techno-terrorists that are seeking ways to use the Internet, information networks, remote and automated control systems, satellite links, or other electronic means to invade key governmental or military data banks. These techno-terrorists are conspiring to launch cyber-attacks against entire communities or even nations. Efforts to stop these sophisticated cyber-attackers, located in countries such as North Korea or within such terrorist organizations as ISIS, will dominate defense efforts more and more in future years.

One of the many problems with cybersecurity is that there are hundreds of terms that computer geeks use in this fairly technical field. To assist you there is a fairly detailed list of terms provided in the glossary to help explain the meaning of acronyms and to explain terms such as “whale phishing” and “near field communications” that are used in the new “tap-and-pay” systems, etc. Our goal, however, has been to use as few of these “techno-speak” terms as possible.

At the end of the book are some appendices that spell out the vital cybersecurity programs that are now being implemented in the United States and aboard for those that would like to know what their governments are doing to protect them against both cyber criminals and, even worse, techno-terrorists that attempt to carry out devastating cyber-attacks.

We have tried to be as comprehensive as possible in addressing the concerns that an individual or small business might have regarding cybersecurity and attacks that cyber-thugs might launch against you or your family. We have tried to explain basic cyber-risks and protective strategies without becoming enmeshed in techno-speak and gobbledgook terms that get in the way of a clear understanding of what the problems and solutions are. We hope you enjoy *Digital Defense*, which is designed to become your basic guide to cybersecurity. This is a book devoted to protecting you, your family, and especially seniors against those that abuse the Internet and digital technology.

Washington, DC, USA
October 2015

Joseph N. Pelton
Indu B. Singh

Acknowledgements

This is to provide acknowledgement for the detailed contributions and corrections of Alexander Pelton, our editor, who substantially helped to perfect this book. We wish to acknowledge the detailed contribution and corrections to the manuscript provided by Alexander Pelton. As our editor he helped to perfect this book. Also we wish to thank Peter Marshall for his review, comments, and suggestions. As always is the case, all errors are the responsibility of the authors.

Contents

1 What Is at Stake? What Should You Do? Why Should You Care? 1

Houston, Texas, and the "Hacked Baby Cam" in the Nursery 1

The Sum of 22,000 lb Transferred from Elderly Mother's Bank Account in London, England 2

Couple Sentenced for False Tax Refund Conspiracy 3

Teens and Cyber Identity Theft 3

Kaitlin Jackson's Campaign Against Cyberbullying Trolls 4

Hacking into Aircraft Communications and IT Wireless Communications Networks 5

Level One Attacks 6

Level Two Attacks 7

Level Three Attacks 7

Level One Threats to Be Taken Seriously 8

- Handle with Care! 8
- CryptoWall 2.0 9
- The Trade in Swipeable Credit Card Information 9
- The Cyber Criminal Bazaar 11
- Cyber Thieves and Medical Records 14
- Nigerian Prince Come-Ons and the Latest in Targeted Online Scams 14
- Protecting Against Personal Cyber Attacks 15
- Phishing and Pharming 15

Level Two Cyber-Attacks 16

- Trojans on the Attack Against Banks 16
- Insurance Collapse Due to Massive Cyber Attacks 17
- The "Internet of Things": A World in Which Cars, Appliances, and Almost Everything Is Connected to the Net 18

Level Three Attacks 19

- GPS Resilience and Vulnerability 19
- Attack on Water and Sewage Systems via SCADA Systems 20
- Transit Systems and Aircraft Safety at Risk 21

A Recap of Why You Should Care 21

References 23

2 **Where to Go for Assistance** **25**
Help Available 25
Electronic Filters That Protect Against Malware Intrusions 27
Recommended Websites 29
Identity Theft Protection 30
Firewalls and Backup Memory 34
Common Features That Personal Firewall Can Offer 35
Limitations of Firewalls 35
Insurance Offerings 37
What to Do 38
And Now How to Protect Your Family Against Cyberbullies, Pornography, Online Hate Messages, and Other Cyber-Related Maladies 39
What to Do About Protecting Your Family's Computers from Cyber Criminals, Stalkers and Bullies 41
What to Do About Pornographic Sites and Sexting 44
Protective Strategies for the Over-50 Crowd 44
Conclusions 46
References 47

3 **Is Anyone Looking Out for You? Your Government? Businesses Where You Trade? Your Neighbor? or Just Yourself?** **49**
Governmental Issues: The "Snowden Factor" 52
Corporate and Industrial Issues 58
Individual Transgressions and Cyber-World Concerns 60
Conclusions 62
References 65

4 **Ten Key Things to Protect** **67**
Introduction 67
The Top Ten Things for You and Your Family to Protect Against and How 68
#1. Protect Stocks, Bonds, and Retirement Accounts 69
#2. Protect Your Bank Account and Credit Card Account Records 71
#3. Protect Your Social Security, Medicare/Medicaid Accounts and Medical Records 72
#4. Protect Desktop Computers, Wi-Fi, and Computer Routing Systems (LANS and WANS) 73
#5. Protect Personal Cell Phones/Smart Phones 74
#6. Upgrade Cyber Security Systems for Vital Infrastructure 75
#7. Protect Big Data and Social Media: And At Least Some of Your Privacy 76
#8. Don't Put All of Your Eggs in One Basket 77
#9. Protect Yourself by Doing Audits 78
#10. Protect Your Personal Things, Your Family, and Your Business Interests, Including Your Last Will and Testament, Plus Donations and Legacy 78
Conclusions 79
References 80

5 **Cybersecurity for Smart Phones, Mobile Apps, and "The Cloud"** **83**
Introduction 83
The Dangers of Wi-Fi Access to the Internet 85
Mobile Applications on Smart Phones 86
Mobile Phone Security and Access 87
Making Your Smart Phone More Secure 88
Cybersecurity and Banking Apps 89
The Cloud 92
Evaluating Personal Cloud Services (Fig. 5.3) 92
Conclusions 100
References 100

6 **Protecting Vital Cyber Infrastructure** **103**
Introduction 103
SCADA Networks in Our Lives that We Never See 105
SCADA Systems Security in a Community 107
Satellite Networks and Cyber Risks 108
Satellites and Cybersecurity 109
Satellite Technology and Systems 110
Application Satellites with Cybersecurity Implications 112
Fixed Satellite Systems and High Throughput Satellites 117
Mobile Satellite Systems 118
Conventional Mobile Satellite Communications 119
Mobile Satellite Systems with ATC Ancillary Terrestrial Component 121
Conclusions 123
References 124

7 **Who Will Control the Future, Black Hat Hackers or the Hacked?** **127**
The Viral Cyber World 127
How Do We Protect Ourselves from Cyber-Attacks Going Forward? 128
Coping with Current and Future Cyber Threats 131
Nearer Term Threats: Computer Fraud, Wi-Fi, Wireless LANs, and the Cloud 132
Wireless Local Area Networks (LANs) and Satellite Networking 133
Security Flaws in The Cloud 134
Best Practices for Companies in the Cloud 134
Cyber Protection of Vital Infrastructure Under U.S. Government and Corporate Management 135
The Smart Grid 138
Vulnerable Apps on Smart Phones and Desktop Computers 138
The Internet of Things 140
Hololens and Cybersecurity 141
Conclusions 142
Post-conclusions: Cyber Opportunities vs. Cyber Threats to Our Lives? 143
References 144

8 Ten Essential Rules for Your Cyber Defense 145
#1. Protect Your Personal Records and Your Passwords 145
#2. Obtain a Secure Place to Store Vital Information 147
#3. Shred All Financial, Medical, and Other Personal Information that You Discard 147
#4. Get AntiVirus Software Protection 148
#5. Prevent Your Identity from Being Stolen 149
#6. Obtain at Least the Basic Personal Firewall Protection 151
#7. Recognize Warning Signs and Respond Quickly to Threats 151
#8. Consider Getting Comprehensive Insurance Against Financial and Cyber-Loss 152
#9. Support the Adoption of Stricter Governmental Legislation and Standards for Cybersecurity 153
#10. Take Common Sense Steps to Guard Against Cyber-Attacks 154
References.. 155

Appendix A Glossary of Definitions and Acronyms 157

Appendix B Current U. S. Priorities on Cybersecurity 175

Appendix C The U.S. Comprehensive National Cybersecurity Initiative (CNCI) 179

Appendix D Cybersecurity Activities and Policies Around the World... 189

About the Authors 201

Index 207

1
What Is at Stake? What Should You Do? Why Should You Care?

If you and your family are accosted by a mugger on the street, then your money or your lives could well be at stake. If you live in Ukraine and Russian-backed invaders take over your town, then your livelihood or your home are likely to be in immediate danger. When a foreign power invades your country, you clearly know that you are most definitely in peril and that you had better fight back to defend your rights and that of your community.

Cyber-crime, however, can be so subtle and hidden, people can ignore the threat until it is too late. Yet today about every 3 s a person is hit by some form of cyber-attack out of the blue. It is estimated that a cyber-attack on the electric grid on which we all depend comes about once a minute. Precautions need to be taken up front to combat cyber-fraud, cyber-attack and most definitely cyber-terrorism. Locking the "cyber-barn door" after a "black hat" hacker has struck is way too late.

And sometimes the threat to you and your family might not be so subtle after all. Here are some frightening case studies in cyber-stalking, cyber-crime, and worse.

Houston, Texas, and the "Hacked Baby Cam" in the Nursery

Dateline January 28, 2015: A nanny named Ashley Standly was looking after 1-year-old Samantha in Houston, Texas, when she had a terrifying moment. It started when she heard a noise near the baby and walked over to investigate. Ashley could not believe her ears. A strange man's voice came

J.N. Pelton, I.B. Singh, *Digital Defense*, DOI 10.1007/978-3-319-19953-5_1

Fig. 1.1 Security cameras that are connected to a home Wi-Fi Internet systems can be hacked

though on the baby's monitor. This particular baby cam had a microphone and a high resolution camera linked to the household's Wi-Fi Internet system. A strange man from nowhere could be heard calling the little girl "cute." The Wi-Fi wireless network had been used by a cyber-lurker to invade the privacy of this Houston household. What had been installed as a safety feature, but without security password protection, had become a portal for a digital voyeur to intrude into the nursery. This feat could unfortunately be achieved via a widely-available smartphone or wireless network app [1] (Fig. 1.1).

The Sum of 22,000 lb Transferred from Elderly Mother's Bank Account in London, England

Dateline February 28, 2015: A 31-year-old Nigerian hacker living in Southsea, England, used special software to access the e-mail account of Ilaria Purini, who lives in London. This is how he learned her passwords and the personal details of her life and her close relationship with her mother, who lives in Italy. In this case it turned out that Ilaria Purini worked for a museum and purchased art for her mother and sent it to her in Italy. Posing as Ilaria Purini in an e-mail the hacker sent instructions to a banker