BART R. MCDONOUGH

CYBER SMART

Five habits to protect your
family, money, and identity
from cyber criminals

WILEY

Cyber Smart

Cyber Smart

Five habits to protect your family, money, and identity from cyber criminals

Bart R. McDonough

WILEY

Cyber Smart: Five habits to protect your family, money, and identity from cyber criminals

Published by
John Wiley & Sons, Inc.
10475 Crosspoint Boulevard
Indianapolis, IN 46256
www.wiley.com

Published simultaneously in Canada

ISBN: 978-1-119-55961-0
ISBN: 978-1-119-55963-4 (ebk)
ISBN: 978-1-119-55964-1 (ebk)

Manufactured in the United States of America

10 9 8 7 6 5 4 3 2 1

Limit of Liability/Disclaimer of Warranty: The publisher and the author make no representations or warranties with respect to the accuracy or completeness of the contents of this work and specifically disclaim all warranties, including without limitation warranties of fitness for a particular purpose. No warranty may be created or extended by sales or promotional materials. The advice and strategies contained herein may not be suitable for every situation. This work is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If professional assistance is required, the services of a competent professional person should be sought. Neither the publisher nor the author shall be liable for damages arising herefrom. The fact that an organization or Web site is referred to in this work as a citation and/or a potential source of further information does not mean that the author or the publisher endorses the information the organization or website may provide or recommendations it may make. Further, readers should be aware that Internet websites listed in this work may have changed or disappeared between when this work was written and when it is read.

For general information on our other products and services please contact our Customer Care Department within the United States at (877) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley publishes in a variety of print and electronic formats and by print-on-demand. Some material included with standard print versions of this book may not be included in e-books or in print-on-demand. If this book refers to media such as a CD or DVD that is not included in the version you purchased, you may download this material at http://booksupport.wiley.com. For more information about Wiley products, visit www.wiley.com.

Library of Congress Control Number: 2018963005

I dedicate this book to my mother, Kaye "Gigi" McDonough. My intelligent, thoughtful, caring, and beautiful mother—your unconditional love and encouragement coupled with your unwavering demand of excellence propelled me forward in my life and career. THANK YOU, Momma!

About the Author

Bart R. McDonough is CEO and founder of Agio, a hybrid managed IT and cybersecurity services provider specializing in the financial services, healthcare, and payments industries. Bart has deep institutional knowledge of the investment world, with more than 20 years of experience working in cybersecurity, business development, and IT management within the hedge fund industry. His core strengths are assessing, defining, advocating, and driving the adoption of risk management strategies, controls, and models, which enable organizations to advance cybersecurity resiliency while successfully complying with evolving regulatory requirements and behavioral transformations.

Harnessing his expertise in alternative investments, Bart and his team of more than 240 employees have developed cybersecurity and managed IT tools tailored to protect financial businesses' most precious assets: money and reputation. Just one example of Agio's industry-changing work included finding and repairing a Bloomberg Professional Services setting that could have compromised more than 300,000 subscribers. As CEO, Bart has grown Agio's roster of clients to exceed 300, spanning hedge funds, private equity firms, asset managers, investment banks, and healthcare providers.

Bart is a board member of several cybersecurity companies. Prior to founding Agio, he worked at SAC Capital Advisors, BlueStone Capital Partners, OptiMark Technologies, Sanford Bernstein, and American Express. Bart attended the University of Oklahoma and received his undergraduate degree from the University of Connecticut. He is married to the two-time Emmy Award–winning television producer Cheryl McDonough, and he has three incredible children: Russell, Ava, and Kya.

Credits

Associate Publisher
Jim Minatel

Project Editor
Gary Schwartz

Production Editor
Barath Kumar Rajasekaran

Copy Editor
Kim Wimpsett

Production Manager
Katie Wisor

Content Enablement and Operations Manager
Pete Gaughan

Marketing Manager
Christie Hilbrich

Business Manager
Amy Knies

Project Coordinator, Cover
Brent Savage

Proofreader
Nancy Bell

Indexer
Johnna VanHoose Dinse

Cover Designer
Marina Mirchevskaya

Cover Image
© blackred/Getty Images-Gold Skeleton Key, © monsitj/Getty Images-Background

Acknowledgments

I'd like to start by thanking the team that helped me get this book published and ultimately distributed: Jim Minatel, Gary Schwartz, and Barath Kumar Rajasekaran at Wiley.

I'd also like to thank the thousands of Agio clients who kept asking me questions at my Cybersecurity Awareness Seminars, which led me to writing this book. I can't wait to share it with all of you.

A huge thank-you to my researcher, Kelly Eley, for all of your valuable time on this project—you were simply a delight to work with, and I can't wait to collaborate with you again. In addition, I'd like to thank Kimberly Peticolas for all of her coaching and advice on getting this idea into a published book.

Next, I have to thank so many of my amazing colleagues at Agio (`https://agio.com/`) for refining so much about what I know about cybersecurity, management, and life. I have to give a big personal shout-out to Ray Hillen for coining the phrase "Brilliance in the Basics." A special thanks to Lori Rabin for her amazing editing capabilities. Others I want to thank personally include Chris Harper, Mark Fitzner, Miten Marvania, Garvin McKee, Kate Wood, Nick Mancini, Jessica Golle, Heather Matthews, Josh Bentley, Greg Blattner, Marina Mirchevskaya, Kaitlin Boydston, Jason Price, Andrew Werking, Eva Lorenz, Laurie Leigh, Emily Ellis, Carrie Bowers, Donato Lalla, Tim Steiner, Steve Foster, Joe McCusker, and the rest of the amazing organization at Agio (`#OneAgio`).

A few clients and colleagues I'd like to thank are David Berger, Danny Moore, Avi Gesser, Barry Ko, Ramin Safai, and especially Chris Corrado.

I have to thank my lawyer and great friend Kevin Malek (well, at least I think we are friends) for all of his assistance in this project and so many others in my life.

I have to thank so many of my "brothers" for all their candid (and, yes, sometimes dumb) questions: Troy Bailey, Neil Berkeley, Travis Warford (no Travis, it's not cheese), Johnny O'Fallon, Brendhan Fritts, Chris Nichols, and Ryan Ball. Troy and Neil, I'd especially like to thank you for yelling at me one night over drinks to just "write the damn book" and giving me the courage to fail.

Everyone who knows me knows Gina Peterson is the engine who keeps me going, and without her, none of the meetings that took place to get this book published would have been possible. A huge thank-you to Gina, and her

husband Nate, for allowing our family to interrupt hers constantly. Andrea Duarte, while joining us late, has been amazing at helping to smooth out our days and lives and giving this book its final polish.

I've been fortunate to have the most loving and caring parents in the world who have always encouraged me to do more and be better and have always supported me along the way. Education, especially the ability to read and write, were always valued in our home. My father has always been such a rock and a great example of hard work. Your work ethic and your devotion to your family continues to inspire me, Poppy! While I didn't appreciate it at the time and it may have led to some tears, I can't thank my wonderful mother enough for never taking the easy way out and letting me turn in terrible writing. Thanks for always pushing back on me (with your red pen!) and making me better, Momma.

Finally, my immediate family. Thank you for supporting me in everything I do. Kya, thank you for always asking the hard, right questions. You always get to the heart of the matter and helped me clarify and simplify my recommendations in the book. Ava, thank you for first calling me "Tech God"—flattery will get you everywhere. Seriously, thank you for allowing me to understand better the teen viewpoint in using the Internet. Russell, you don't know how much your calm demeanor helps me in life. Thank you for insisting on using correct grammar in texts, thank you for putting up with all the test devices I install and use at the house, and thank you for always being so patient and helpful. You are the rock of this family and occasionally are funny too.

Cheryl, my love and my talented superstar, thank you for being patient with me while I took the time to put this book together. Thank you for working tirelessly to keep our lives running while personally working so hard to make the world a better place through your documentaries and not take life too seriously. Thank you for being my best friend—always making me laugh and not to take life too seriously. Finally, thank you for being the audience to all my ridiculous cybersecurity stories; for always perfectly playing the part of the "normal person" (while we know you aren't really normal!), and keeping me in check. And yes, love, you do have to update your computer and phone now.

Contents at a Glance

Contents

Foreword

Statement of Purpose

Cybersecurity is one of the most important, and most disregarded, aspects of our daily responsibilities. Technology has overtaken our lives—the pervasiveness of the Internet has affected how we do almost everything—from communicating to banking. Drawing on his extensive work with hedge funds, private equity firms, celebrities, hospitals, and more, Bart McDonough accurately and thoroughly describes the cybersecurity threat landscape—the who, what, when, where, why, and how—and then helps readers understand how to perform proper "use, care, and feeding" of accounts and devices to avoid exposure in many areas of daily life. Just as people must tend themselves to maintain their health, so too should they practice proper "cyber hygiene" with websites, software, and devices to protect themselves and their families in a world of cyber threats.

As an expert in the cybersecurity field, McDonough has traveled around the world speaking at conferences for the FBI, Goldman Sachs, JP Morgan, Morgan Stanley, Citibank, Credit Suisse, Jefferies, Bank of America, and others, where he addresses crucial cybersecurity recommendations for businesses. However, the most common question he receives from the attendees at these conferences is "How can I protect myself at home, on a personal level, away from the office?" Addressing this very question in this book, McDonough combines his extensive industry knowledge with real-world examples of cyberattacks and how to prevent them as well as how to recover from them.

The idea of identity theft and other forms of cyberattacks can be daunting to the average person in today's society; however, it does not have to be that way. With the proper knowledge, outlined as the five "Brilliance in the Basics" habits in this book, everyone can learn better practices to help prevent bad actors from taking advantage of their money, personal information, and devices. Moreover, the more people who protect themselves, the better off everyone is. While there are several books out there that address the topic of cybersecurity, the majority of these focus on security for businesses and corporations. Few are intended to teach individuals in the general public how properly to protect their money, identities, personal information, devices, networks, and online experiences.

Cyber Smart focuses exclusively on this audience. Written in plain English and using everyday relatable examples, McDonough helps readers easily understand how they can personally update their approaches to Internet and device safety, and he does this through a positive, proactive style. While other comparable titles focus on fear-based conditioning, *Cyber Smart* focuses instead on maintaining the idea that while these technological advances have risks, there is no reason not to take advantage of them as long as you do it with open eyes and an awareness of how to keep your information safe.

Introduction

As technology advances and we adopt new cloud-based services, wearables, fitness trackers, smart home appliances, and cars, we need to balance our rapid consumption of technology with vital knowledge of how safely to use, maintain, and protect these Internet-connected products.

Protecting our identities from the onslaught of endless cyber scams and hackers has become an exhausting effort. It can feel like we need a technical degree to defend ourselves and our families from cybersecurity attacks and ensure we're secure in our day-to-day personal and professional lives. Since we don't hear these cyberattacks knocking at our door or receive real-time evidence of our sensitive information circulating the underbelly of the Web, it's hard to grasp how vulnerable we are at any given moment. In this book you learn how to find your exposed information on the Internet—and discover you've been breached—it can feel like there's nothing you can do to protect your and your family's leaked Social Security numbers, passwords, and more. I am here to tell you there is hope. In this book, you'll learn to practice the essential cybersecurity habits to protect your family from bad actors.

Technology advancement brings opportunities, but it also creates risk, making it necessary to teach ourselves proper "use, care, and feeding" of our devices. If we don't, we risk significant exposure in many areas of our life. Similar to caring for ourselves, we must practice proper "cyber hygiene" with websites, software, and devices.

We know we spend a ton of time online, but we may not realize how our heavy Internet usage can increase our risk of falling victim to cybercriminals. It's as easy as visiting a website with infected ads that harvest our computer's CPU power, so bad actors can "mine" highly profitable Bitcoin cryptocurrency, typing credit card numbers into legitimate-looking, spoofed websites, or accidentally downloading ransomware from a linked "Funny Cat Video" our "friend" sent us. We devote a lot of time and energy to these online interactions. If we neglect the "use, care, and feeding" of technology and our presence in cyberspace, we risk letting bad actors run rampant—infecting and sabotaging our cyber comforts, wiping out years of family photos and personal files to ransomware demands in the thousands of dollars, or repeatedly using and abusing our identity.

If we lived in a "bad" neighborhood with a high level of crime, we would take the necessary precautions to protect ourselves, our family, and our belongings. We are mindful of our surroundings—we lock our doors, install extra locks, don't carry loads of cash on us, and so forth. However, when we are in a good neighborhood with low crime, we tend to be more relaxed around our physical safety precautions.

When it comes to our cyber lives—we all live in a bad neighborhood. And we *all* need to practice essential cyberhygiene precautions, or else we play a risky game of cyber roulette to see how much we *think* we can get away with before the neighborhood bad actors succeed in their cyberattacks against us. Then it's game over—or, at the least, we experience a lot of unnecessary frustration, embarrassment, expense, and cleanup.

This is not said to scare you—it is to help prepare you to have the right mind-set when you are online. My primary goal is to share real stories of people like you—victims of common cyberattacks—and then provide specific recommendations you can use to protect yourself against cyberattacks and scams. The secret to practicing cybersecurity is what I call "Brilliance in the Basics"—five crucial cybersecurity habits that I recommend you perform regularly.

Brilliance in the Basics habits

1. Update Your Devices
2. Enable Two-Factor Authentication
3. Use a Password Manager
4. Install and Update Antivirus
5. Back Up Your Data

Performing these five basic, recurring cyberhygiene principles will work to prevent cyberattacks and serve as a cure for prevalent cybersecurity issues. I will show you how to manage your Internet presence safely, as well as your technology usage, so you can continue to enjoy the pleasures and opportunities that come with the cyberspace you love. You'll discover more about the "Brilliance in the Basics" cyberhygiene habits in Chapter 7.

Debunking Cybersecurity Myths

I will also address and dispel popular cybersecurity myths throughout the book. Recognize any of these?

Hacking Myths

- "Why bother doing anything? If a hacker wants to get me, they will. I mean huge companies and the U.S. government get hacked. I can't do anything to protect myself—it's a lost cause."
- "Bad actors aren't interested in my data. I'm not a celebrity or public figure. I don't have anything of value to them."
- "Websites wouldn't steal my computer's CPU power to 'mine' cryptocurrency, like Bitcoin, just by visiting them."
- "The applications in the Apple App Store or Google Play store are safe. I can't download 'bank account–stealing' malware from a simple crossword puzzle app, can I?"
- "I'm not worried about ransomware. Law enforcement will catch the adversary and get my files back, right?"

File Storage and the Cloud Myths

- "I don't store my information in the cloud because it's not safe."
- "I store my files in the cloud already, using Apple iCloud and Google Drive. They back up my files, right?"
- "I perform backups to an external hard drive that's always plugged into my computer. My files are protected."

Password Management Myths

- "Remembering and keeping up with fancy passwords is too difficult. There's no way I can do it for every site I use."
- "Two-factor authentication takes too long. As long as I have a strong, unique password for each account, I am secure."
- "Cloud-based password managers aren't secure."

Web Browsing Myths

- "Websites with the lock symbol in the URL are safe to use."
- "Public Wi-Fi is secure if it requires a password."

Email Account Myths

- "It's not necessary for me to create a separate email just for banking if I have a strong password for my bank account, even if I use the same password for my email account too."
- "I don't have anything of interest to the adversary in my email account. Good luck reading all my boring emails."
- "Email providers like Google or Yahoo aren't making money from my email conversation with my spouse."

Identity Theft Myths

- "Credit monitoring and fraud alerts will protect me from identity theft. I don't need to activate a security freeze."
- "My child doesn't have a credit history. Their identity won't get stolen, and their credit score won't be damaged."
- "I don't shred sensitive documents when I throw them out. No one would sift through my garbage to steal my identity."
- "I connect with anyone who sends me a friend request on LinkedIn. We're all professionals here, not scammers."
- "I trust my doctor's office with my Social Security number when they request it. They need it for vital reasons, right?"
- "I can't be denied critical medication at a hospital just because someone stole my identity and tampered with my medical files, can I?"
- "I trust retailers and gas stations to protect their card swipe, or dip, machines from skimmers that steal card numbers."

By learning the facts, you can set the record straight and safeguard yourself and your family. Cyber awareness will be like second nature.

In fact, let's dive in and dispel one myth right now.

Myth "Why bother doing anything? If a hacker wants to get me, they will. I mean huge companies and the U.S. government get hacked. I can't do anything to protect myself—it's a lost cause."

Fact You can safeguard yourself from the vast majority of threats. It takes only a few steps, which I list in the ensuing chapters. By learning to protect yourself, you will take a "bite" out of cybercrime. You'll emerge a newfound "Brilliance in the Basics" expert and be ready to share your learned cybersecurity hygiene basics with others.