Introduction

We live in an interesting age. Over the past thirty years, a concept called the "internet" has revolutionized how we work, play, shop, date, and stay in touch. Smartphones now put the world at our fingertips, and smart homes enable us to turn out the lights from a thousand miles away. Thanks to the internet, we are only one click away from our work, our friends, our shopping, and our information, any time of day and anywhere in the world. Over two decades, the internet has disrupted industry after industry, including: movies, telephones, calculators, watches, shopping, travel, recruiting, taxis, banking, medicine, television, newspapers, magazines, books, and many others.

But all this transformation comes with new challenges, and introduces new risks to our safety and our security. Thanks to the internet, "bad guys" can access hundreds, thousands, or millions of victims with a single click. In 2008 the Conficker worm infected over 10 million computers and placed them under the control of a single set of attackers. The BredoLab botnet gained control of over 30 million computers just a couple of years later. In 2017 the NotPetya attack crippled Maersk shipping by destroying almost all of their 50,000 computers. This one attack disrupted more than 20% of the world's international trade, and cost Maersk more than $250 million in damages. In fact, the NotPetya attack was estimated to have destroyed more than 200,000 computers across more than twenty countries around the world, bringing companies and municipalities to their knees, and disrupting day-to-day life for many individuals.

These incidents have real costs that affect all of us as well as our employers. RiskIQ estimates that global online crime in 2018 cost businesses and individuals more than *$1 million dollars a minute*. Barkly estimated that in 2017, ransomware alone cost over *$5 billion*. Breaches of sensitive personal information abound, with millions of social security numbers, credit card numbers, bank accounts, personal identities, and health care data (that are all supposed to be kept secret) falling into the hands of criminals around the world. According to DarkReading, over 5,000 breaches in 2017 resulted in the compromise of almost *8 billion* information records belonging to regular, innocent people like us. Finally, Statista has reported that between 20% and 50% of all the computers worldwide are infected with some type of malicious software, or *malware*. That is almost a billion computers doing work for the bad guys, every minute of every day.

But there is hope. In this increasingly complex and interconnected digital world, security has become a responsibility not just for business leaders or law enforcement, but for each and every one of us every single day. This book is about how to protect you from the dangers of the internet, while still taking advantage of its benefits, at work, at home, and on travel. This book describes the risks to

DOI 10.1515/9781501506505-207

your digital life, how security experts manage these risks, and how you can contribute to that effort by reducing the risk to yourself, your family, your coworkers, and your friends. So, with all of that said, *Let's get started!*

Your Digital Life

Each of us exists at the center of a "digital life" that includes our home, our work, our relationships, our business, and our friends. This connected ecosystem includes computers, tablets, phones, and numerous other devices that connect us to home and work functions that we enjoy every day (as well as some that we may not enjoy). Most of these devices rely upon the internet to work, so they can communicate with computers, users, and servers hundreds or thousands of miles away. An illustration of this digital ecosystem is shown in Figure I.1.

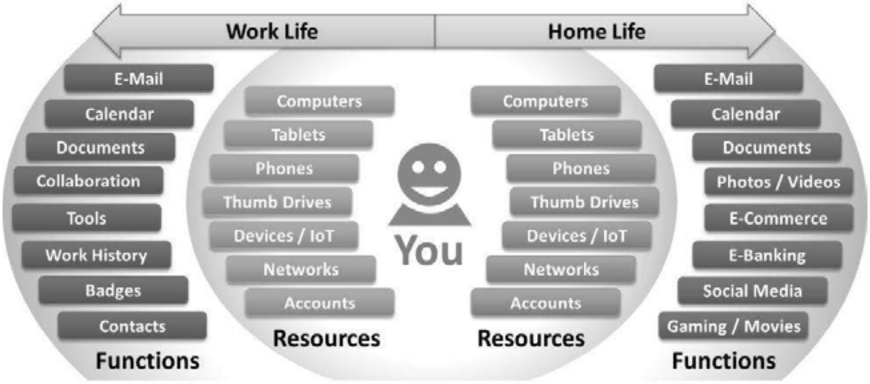

Figure I.1: Your digital life surrounds you with awesome capabilities.

This digital ecosystem includes resources like computers, tablets, phones, devices, networks, and online accounts. We use these resources to access work functions including e-mail, calendar, contacts, collaboration tools, and work documents. We also use these resources to access home functions such as e-mail, personal documents, photos, e-commerce, social media, gaming, movies, and music. Sometimes our devices are dedicated to one function, such as a work computer, but frequently our devices are shared between work and home functions, like when we access our work e-mail from our personal phone or home computer.

For many of the functions that we desire, connectivity to the internet is required. We may get our connectivity to the internet through cellular networks, cable modems, satellite services, public Wi-Fi, or other network connections. To identify ourselves over the internet, we use *digital identities*—most often a username and a password—that identify us to distant computers and prove that we are who we say we are.

Cyber defenses that protect our digital lives must include protections that operate at multiple levels to provide comprehensive protection. These protections must include our devices, our networks, our applications, our online accounts, our online identities, and the online entities we trust with our private and personal information. All of these online resources must be constantly protected from compromise or abuse. Unfortunately, in today's highly interconnected digital lives, a failure of protection in one place may end up having disastrous effects everywhere.

About This Book

This book is about protecting your online digital life at work, at home, and on travel. To achieve such protection, this book provides you with cybersecurity information you should know and can apply in your day-to-day life. This book should help you to answer some of the following cybersecurity questions as you use computers and the internet:

- How do I protect my home or work computer from compromise?
- How do I protect my other home connected devices like phones, tablets, and internet of things (IoT) connected devices?
- How do I protect my online accounts and passwords?
- What is wrong with using kiosk computers, or public Wi-Fi connections?
- What happens when I share information between my work and home computers?
- What rules do I need to follow for my work computer, laptop, or work smartphone?
- What happens when I use my work computer to do personal business?
- Why do I need to worry about online privacy?
- What does my cell phone have to do with my online security?
- What do Google, Facebook, or Amazon really know about me?
- What happens when I use my work computer for personal e-mail, Facebook, or LinkedIn?
- How safe is my credit card when it is in my purse or wallet?
- How safe is my connected home with Alexa, Nest, and Zigbee?
- What happens to cybersecurity when the lights go out?

To help you answer these questions and increase your personal cybersecurity awareness, this book contains guidance on the following cybersecurity topics:

- An understanding of today's cyberthreats and the dangers they pose.
- How to understand cyber risk and use good practices to reduce it.
- Common cybersecurity attacks and how cyberattackers may target you.
- Approaches for protecting yourself at work, at home, and on travel.
- Online security resources that can help you reduce your cyber risk.
- Additional security awareness tips for protecting your digital life.

Who Should Read This Book

This book is intended for a general audience. Everyone should be able to read this book and find useful information about how to protect their online activities at work, at home, and on travel. Readers of this book include the following:

- People who are concerned about security their digital worlds, and the devices and accounts contained within them.
- People who want to understand the cyberthreats targeting them at work, at home, and on travel.
- People who want to understand how their devices, networks, and accounts may be compromised by cyberattackers.
- People who want to learn techniques to secure themselves and reduce their cyber risk.
- Leaders who want to reduce the cyber risk for their teams.

Everyone can use the content in this book to help secure their devices, networks, and accounts at work and at home. By improving their security awareness, people can make it more difficult for cyberattacks against them to succeed.

Contents of This Book

This book is primarily concerned with cybersecurity, while also considering supporting topics that may affect cyber safety. The chapters of the book are meant to be read in sequence, as they build upon one another to help you understand *who*, *what*, *where*, *when*, *why*, and *how* of successful cybersecurity. With that said, you can also flip through this book to specific sections to find useful explanations that may help you reduce your cyber risk.

- Chapters
  - Chapter 1: Security Mindset
  - Chapter 2: Common Cybersecurity Attacks
  - Chapter 3: Protecting Your Computer(s)
  - Chapter 4: Protecting Your Passwords
  - Chapter 5: Protecting Your Home Network
  - Chapter 6: Smartphones and Tablets
  - Chapter 7: Protecting Your Web Browsing
  - Chapter 8: Protecting Your E-Mail and Phone Calls
  - Chapter 9: Protecting Your Identity, Privacy, and Family Online
  - Chapter 10: Protecting Yourself on Travel
  - Chapter 11: When Things Go Wrong
  - Chapter 12: Considering Cybersecurity at Work
  - Chapter 13: Final Thoughts
- Appendices

  The appendices provide greater detail than the chapters and provide additional examples of security concepts described in this book.
  - Appendix A: Common Online Scams
  - Appendix B: The Worst Passwords Ever
  - Appendix C: Online Security Resources
- Glossary

  The Glossary provides an explanation of terms used in this book, *expressed in plain language* for the nontechnical reader.
- Index