The Personal Digital Resilience Handbook

An essential guide to safe, secure and robust use of everyday technology

Dr David Wild

The Personal Digital Resilience Handbook:
An essential guide to safe, secure and robust use of everyday technology
mydigitalresilience.com

ISBN: 978-0-578-79692-5

Project Editors:

First Published: November 2020

The information in this book is distributed on an "As Is" basis, without warranty. The author has taken great care in preparation of this book, but assumes no responsibility for errors or omissions. No liability is assumed for incidental or consequential damages in connection with or arising out of the use of the information or programs contained herein.

Rather than use a trademark symbol with every occurrence of a trademarked name, this book uses the names only in an editorial fashion and to the benefit of the trademark owner, with no intention of infringement of the trademark.

Web addresses and menus selections are shown in bold. As shorthand, when describing navigation of menus on a computer to achieve a task, I will separate each part with a ">" symbol (arrow). For example, Apple menu > System Preferences > Users & Groups means to select the Apple menu, then select System Preferences, then select Users & Groups.

Contents

About the Author

David Wild is Professor in the Luddy School of Informatics, Computing and Engineering at Indiana University where he researches and educates in crisis technologies, digital resilience, data science, data privacy, security and ethics, and biomedical data science. He is founder of the *Crisis Technologies Innovation Lab* that is researching and developing new digital technologies for the front line of emergency and disaster response.

Acknowledgements

I am indebted to Eva Galperin for introducing me to the term digital resilience, Michael Bazzell for not only the inspiration of his excellent books on privacy, but also his *This book was self-published* technical guide to self-publishing which provided the framework for publishing this book. I am not sure this book would have happened without that support. Thanks are due also to Sue Wild and Don Gregory for providing feedback on the first drafts of this book, and to my whole family and friends for consistent, loving support.

Introduction

I was first introduced to the term *digital resilience* in a breakfast meeting with Eva Galperin, Director of Cybersecurity at the Electronic Frontier Foundation (EFF). I was struggling to find a term for what I saw as an urgent and growing need for technology to be used in a different kind of way, a way that is more robust and reliable, and with more control over how we use it and what it does. I don't claim to have a monopoly over the use of the term, and others might use it differently, but I define digital resilience as *steps people and communities can take to make their use of digital technologies more robust and less prone to critical failure*. To the extent the term has been used, it has been mostly focused on business processes as an extension of cybersecurity. My interest, and the emphasis of this book, is in *personal* digital resilience, that is how we as individuals, families and communities can use technology in a way which mitigates the vulnerabilities and risks of using technology in the modern world.

Digital technology is incredibly powerful. The Internet has enabled a grand, global experiment in meeting our basic and advanced needs digitally instead of in more traditional corporeal ways. A massive, global infrastructure of compute servers and storage has been constructed by a relatively small number of companies like Google, Amazon and Microsoft, to power this experiment. Others such as Internet Service Providers and cellphone companies create the communications infrastructure to connect these servers to each other and to us. Service companies provide a treasure trove – or maybe a Pandora's Box – of applications layered onto this infrastructure. Food, clothing and lodging can now be purchased using a just-in-time logistics system that is itself dependent on the infrastructure; we get a job through LinkedIn, we Google our medical symptoms, we contact our neighbors on Facebook, and we obtain love and belonging on Tinder or Twitter, where we also gain or lose our self-esteem. The whole system – we might call it the Global Cloud – is now considered essential to our way of life. The Global Cloud has brought many benefits, such as enabling remote work, access to huge amounts of information, and convenient delivery of goods we might not be able to access locally. It has also brought problems, such as excluding those who do not have access to the necessary technologies, almost eliminating privacy, enabling cybercrime and state and corporate surveillance, and enabling monopoly corporations to undercut local businesses.

As I write this, we are in the midst of the global COVID19 pandemic. This has taken us to a level of critical dependency on the Global Cloud that would have seemed extraordinary less than a year ago. For many, it is now the primary source for meeting even basic needs, such as to interact with neighbors and colleagues for work or recreation, to get safety information important to our well-being, and to order goods. Both the benefits and problems of the Global Cloud are now amplified across the world. It is unclear how much this acceleration will persist once the pandemic is over, though it is likely that the Global Cloud will continue to grow unabated.

As well as being powerful, digital technology is also fragile, and this is a big concern given our dependence on it. Most of us are driving at 90mph down the digital freeway in cars that have no seat belts and with rusted axles that could break at any time. Barely a day goes by without a horrendous cyberattack that disables a corporation or a municipality appearing in the news. Until recently this was mainly from distributed denial-of-service (DDOS) attacks which would take a website or server offline for a few hours. Now we see much more devastating ransomware attacks where hackers take over and encrypt entire systems, demanding a ransom to decrypt them. As I write this a news story has just broken about a large national healthcare provider that is completely crippled by a ransomware attack, leaving it unable to run operations at its hospitals. These attacks happen to people like you and me too. Most of us know someone who has experienced a smaller-scale attack, maybe an identity theft or having an online account breached. Even when we are not under direct attack, we are under a kind of indirect attack on our brain. Companies collect huge amounts of data on us from the technology that we use, and they employ it to try to make us more valuable to them by modifying our behavior. This can take the form of selling our data to third parties, or using it to customize the content or advertisements we receive.

It's not just malicious or corporate actors that cause us problems. Technology breaks and fails in all kinds of interesting ways for often the smallest of reasons: a single downed power line brought down the entire North East U.S. power grid in 2003; a botched software update is regularly responsible for entire cloud systems going down. Computer components such as hard drives break often without warning. The impacts of climate change are amplifying our vulnerabilities to infrastructure failure. This year wildfires are ravaging across the western states of the U.S. Adding to the problems, winds are causing the Pacific Gas and Electricity company to impose rolling power blackouts due to the risk of starting new wildfires when power lines come down. Hurricanes and wildfires wipe out the critical infrastructure that the Global Cloud, and thus our lives, depend on. Cell phone towers fail, power and Internet access is lost. If we are lucky, they can be restored quickly. But other scenarios are worse: a cyberattack or solar weather event could disable key parts of the Global Cloud indefinitely; the companies we rely on could simply decide to withdraw services or be pressured to by an authoritarian government, which could also co-opt those services for mass surveillance. We thus have a new kind of vulnerability based on our dependence on the Global Cloud.

This book is a practical and detailed handbook for using digital technology in a way that will make you conscious of and responsive to these risks. By being digitally resilient you will be more safe, secure and private and will have control over your digital life. Chapters 1-4 give practical details about how to secure the important pieces of digital technology in your life like your computer and smartphone. At the end of each chapter is a checklist you can use to measure your progress. It is a check-up for all the digital technology in your life: we'll test the brakes and change the oil in your digital car, and install some seatbelts. Anyone can and should do these steps. Yes, that includes you, Uncle John and Aunt Maude. Kids can do these things too, with a bit of help, and if you are not comfortable doing these steps yourself, a tech-savvy grandchild or friend can likely help you out. Chapter 5 covers advanced digital resilience for those who want to take things further. The information described in this book is primarily for an audience in the United States, but many of the ideas are translatable to other countries.

Throughout the book, I will be anchoring on four basic concepts of digital resiliency. *Reliability and redundancy* is about understanding that any piece of technology will fail, and will sometimes fail spectacularly: as the adage goes, to err is human; to really screw things up requires a computer. Sometimes entire support systems will fail, such as in a power or Internet outage. Digitally resilient people bake this into their use of technology and have strengthened technologies and backup technologies in reserve ready to go. For this, adopt the survivalist's mantra "two is one, one is none": that is, if you have one of something it will break or be lost when you really need it, and then you will be in trouble; if you have two, then when one breaks you still have one. *Security* is about protecting the stuff that is most important to you from attack, from those with malicious intent. *Privacy* is about being able to make informed decisions about what happens with the streams of data that you generate every day, and how to keep information important to us from people you really don't want to have it. *Control* is about being able to make good decisions about who controls the things that are important to you. For example, if you have a stash of dollar bills under your mattress, you have full control of your money, but it may be at risk – from fire or theft. When you open a bank account you cede a lot of control to the bank, relying on them to keep an accurate tally of your balance, and enabling you to access your money through debit cards and ATMs. A bank account is more resilient in terms of security and robustness (in some ways), but less resilient in terms of control.

Digital resilience is not a static thing. The technology changes quickly and the things you need to do to be digitally resilient change too. As a reader of this book, you get access to a website at **https://mydigitalresilience.com** which has links to the resources mentioned in this book and product recommendations. I will keep these links and resources updated as things change including adding new content as needed.

I hope that you will share the information in this book with your family and friends. Why not give a copy as a Christmas or birthday present? You can make big improvements to the digital resilience of yourself and your loved ones. The next few years might well be quite rocky in many ways, from extreme weather events, fallout from the pandemic, political turbulence, cyberattack, and infrastructure failures. By being digitally resilient, you will be prepared and empowered.

Are you ready to be digitally resilient?