*"We all need to protect our digital privacy.
This book provides real-world examples and the guidance
we need to protect ourselves and our loved ones."*

JOHN LEE DUMAS

PRIVACY CRISIS

WORKBOOK

CHRIS PARKER

INTRODUCTION

Privacy isn't just a concern anymore—it's a full-blown crisis. Your data is constantly being tracked, collected, and exploited. But locking down your privacy doesn't mean going off the grid or making your life miserable. You don't have to delete every account, abandon your smartphone, and move to a cabin in the woods.

What do you need? A plan.

That's where this workbook comes in. It is intended to be a companion for readers of Privacy Crisis by Chris Parker. Privacy Crisis is filled with actionable strategies to avoid scams, secure your devices, accounts, and identity, and stop data brokers, hackers, and corporations from exploiting your information.

This workbook is your personal privacy playbook, designed to help you go from "I should really do something about this" to actually securing your digital life.

No fluff, no fearmongering—just practical steps to take back control.

Inside, you'll find exercises to help you spot vulnerabilities, rethink your digital habits, and put real privacy protections in place—without turning your daily routine upside down. Some will take minutes, others a little longer, but each one is designed to move you closer to a safer, more private online presence.

The goal isn't to disappear.
It's to stay visible on your terms.

Let's get started.

—Chris Parker

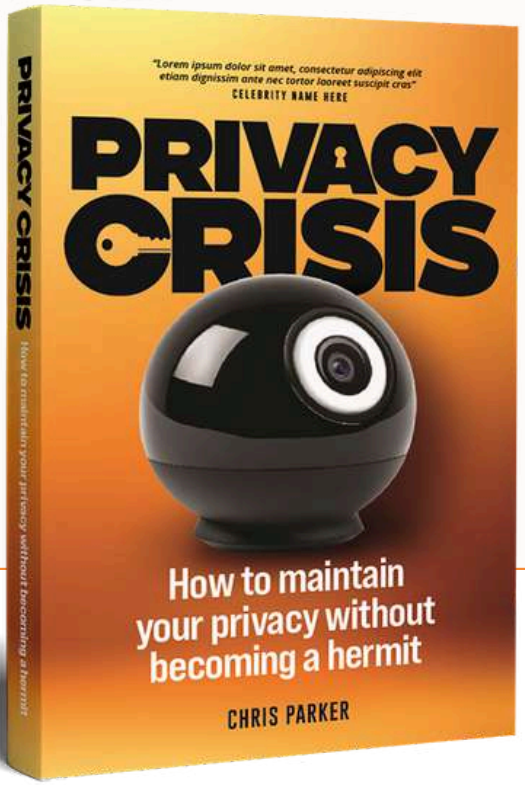
CHAPTER 1

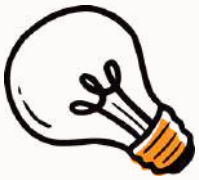
IMMEDIATE ACTIONS TO INCREASE SECURITY

It's time to protect your privacy and increase your security online. Ready to get started?

In this workbook chapter, you will:

- Review key concepts from Ch. 1 of Privacy Crisis
- Identify your own personal motivations for improving your privacy and security
- Consider which action steps may be the most challenging for you
- Complete the 8 essential actions described in Chapter 1





ACTIVITY 1

Let's start with a quick brainstorm.

Take a moment to jot down your thoughts—don't worry, we'll guide you through the details later in the book. For now, just get your ideas down on paper.

Why do you want to improve your privacy and security online?

In Privacy Crisis, we learned that privacy and security are closely related concepts, but there are differences between them.

- Privacy keeps your information hidden.
- Security keeps your information safe.

If you improve one of these areas, the other area benefits, too. Here are some of the reasons why people choose to improve their privacy.

Check off the ones that are important to you.

- [ ] Being at risk of identity theft and fraud
- [ ] Being targeted for Financial theft or scams
- [ ] Being the subject of stalking and harassment
- [ ] Having personal information exposed in data breaches
- [ ] Becoming a target for swatting or doxxing
- [ ] Being manipulated into overspending through targeted advertising
- [ ] Having your behavior and choices influenced by personalized content algorithms
- [ ] Being targeted with disinformation or propaganda based on your data profile
- [ ] Developing addictive behaviors encouraged by engagement algorithms
- [ ] Losing job opportunities due to exposed personal information
- [ ] Having private information used against you in legal situations
- [ ] Being harassed or targeted at work based on leaked data Having medical or health information exposed
- [ ] Having relationships damaged by exposed private details Having your information remain accessible even after you try to delete it
- [ ] Being unable to control how companies buy, sell, and share your data
- [ ] Facing unknown risks as technology and data collection methods advance

Did you find yourself checking most or even all of the boxes? You might have even found yourself checking off items that you didn't even realize were a problem!

ACTIVITY 2

Let's start with a quick brainstorm.

Take a moment to jot down your thoughts—don't worry, we'll guide you through the details later in the book. For now, just get your ideas down on paper.

What changes will be difficult for you to make?

You can do these in whichever order you want! If you want to start with the easiest ones, that's a great plan! If you want to start with

Chapter one asks you to complete several steps you can do *right now* to increase your privacy and security online. Some of these tasks may seem super easy to you, but people often struggle with at least a few. Maybe these tasks feel inconvenient or unnecessary. It could be that you are not sure that you have the technology skills to make each one happen.

Regardless of why some of these might be difficult for you, facts are facts: These are the action steps you can take to be safer *right now.*

RANK THESE 8 ACTIONS IN ORDER OF EASIEST TO MOST CHALLENGING FOR YOU.

- [ ] Completely shut down/power off your smartphone for at least five minutes
- [ ] Lock your mobile phone SIM through your wireless service provider.
- [ ] Encrypt all of your computers and mobile devices.
- [ ] Get a zero-knowledge password manager and migrate all of your account credentials and other secret information to it.
- [ ] Freeze your credit files with Experian, Equifax, and Transunion.
- [ ] Enable one or more methods of strong two-factor authentication for your primary single sign-on account.
- [ ] From now on, distrust by default any request for payment or to change the method of payment, no matter who it seems to be from.
- [ ] Don't unlock or use your phone in a crowded place, and never let anyone borrow it.

ACTIVITY 3

Let's start with a quick brainstorm.

Take a moment to jot down your thoughts—don't worry, we'll guide you through the details later in the book. For now, just get your ideas down on paper.

Accomplish all 8 immediate actions to safeguard your data online

You can do these in whichever order you want! If you want to start with the easiest ones, that's a great plan! If you want to start with the harder ones and reward yourself with easy steps at the end, you can totally do that, too!

However, if you want to be safer online and avoid those pitfalls from Activity #1, it's time to get started on these 8 steps.

Use these checklists to make changes to your privacy habits and security standards.

Power Off Your Smartphone

WHY: Shutting down your smartphone for 5 minutes clears potentially harmful malware from your phone's temporary memory that could be recording your activity.

- [ ] **Save any open work**
- [ ] **Close all apps**
- [ ] **Hold the power button until shutdown options appear**
- [ ] **Select "Power Off" or "Shut Down" (not Restart)**
- [ ] **Wait 5 full minutes**
- [ ] **Power the phone back on**

Lock Your Mobile SIM

WHY: Locking your phone's SIM prevents thieves from transferring your phone number to their device and intercepting your calls, texts, and 2FA codes.

- [ ] **Locate your carrier's website or app**
- [ ] **Log into your account**
- [ ] **Navigate to security settings**
- [ ] **Find SIM card or device security section**
- [ ] **Enable SIM lock/PIN**
- [ ] **Store SIM PIN securely**
- [ ] **Test to see that it works**

Encrypt Your Devices

WHY: Strong encryption makes your data unreadable to thieves—even if they physically steal your device.

If you're not sure where to get started, check out the instructions in Privacy Crisis under the "Encrypt Your Devices" heading.

- [ ] **Check the current encryption status on each device and enable encryption:**
  - [ ] **smartphones**
  - [ ] **tablets**
  - [ ] **laptops**
  - [ ] **desktop computers**
- [ ] **Verify encryption is active**
- [ ] **Create a secure backup of recovery keys (stored in a password manager, locked in a fireproof safe)**

An important reminder: Never store your recovery keys in a digital photo, in the cloud, in an email, in a notetaking app, or in non-encrypted computer files.

Set Up Your Password Manager

WHY: A password manager securely stores all your passwords and sensitive information, making them inaccessible to thieves.

- [ ] **Research recommended password managers, such as Bitwarden, Proton Pass and 1Password**
- [ ] **Choose a zero-knowledge service**
- [ ] **Create master password**
- [ ] **Install desktop application**
- [ ] **Install mobile app**
- [ ] **Enable sync between devices**
- [ ] **Begin importing existing passwords**
- [ ] **Set up emergency access if needed**

Freeze Credit Files

WHY: Freezing your credit prevents criminals from opening new accounts or taking loans in your name.

- [ ] **Visit Experian's website and follow the site's instructions to complete an Experian freeze**
- [ ] **Visit Equifax's website and follow the site's instructions to complete an Equifax freeze**
- [ ] **Visit TransUnion's website and follow the site's instructions to complete a TransUnion freeze**
- [ ] **Save the confirmation details of each freeze**
- [ ] **Take note of the procedures to unlock each credit file later, when you need to**

Enable Strong 2FA

WHY: 2-factor Authentication adds an essential second layer of security, even if someone gets your password.

- [ ] **Identify your main account (Google, Apple, etc.)**
- [ ] **Review available 2FA options**
- [ ] **Choose the strongest available method**
- [ ] **Enable your primary 2FA method**
- [ ] **Set up a backup 2FA method**
- [ ] **Safely save/store backup codes**
- [ ] **Test both 2FA methods**
- [ ] **Document recovery process**

Create Payment Verification Process

WHY: Protects you from scammers trying to steal money through fake payment requests.

- [ ] **List all your legitimate payment methods**
- [ ] **Document normal payment processes**
- [ ] **Create a verification checklist**
- [ ] **Save official contact numbers**

Adjust Your Phone Security Habits

WHY: Good phone security habits prevent unauthorized access to your unlocked device.

- [ ] **Set your auto-lock to shortest practical time**
- [ ] **Use a strong unlock method**
- [ ] **Commit to always being aware of the surroundings**
- [ ] **Keep your screen hidden when possible**
- [ ] **Never leave your phone unattended**
- [ ] **Decline requests to borrow your phone**
- [ ] **Log out of sensitive apps when done**
- [ ] **Conduct regular security audits**