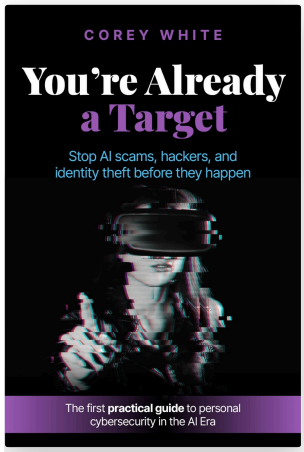


READING GROUP GUIDE

You're Already a Target

Stop AI Scams, Hackers, and Identity Theft Before They Happen

by Corey White

A practical guide to personal cybersecurity for everyone the security industry forgot: parents, adult children of aging parents, and the people who run a business on their own. Thirteen chapters, each built around a real story, each ending with a checklist. Together the checklists close 263 doors that criminals use today.

This guide is for book clubs, library reading groups, church and community circles, and anyone reading the book together. It works for one meeting or two. Most of the questions have no right answer; a few will start an argument, which is the point. And because this is a book about doing, the guide ends with five things your group can do together, so everyone leaves a little harder to fool than when they arrived.

Start here: the beliefs the book takes apart

Every chapter opens with a belief, struck through. Read them aloud. For each one, hands up if you believed it before you read the book. Then ask who still does.

Introduction	~~The system will protect me.~~	Chapter 1	~~There's nothing about me worth stealing.~~
Chapter 2	~~I've been careful, so my data is safe.~~	Chapter 3	~~My wallet is safer than my phone.~~
Chapter 4	~~My bank will make me whole.~~	Chapter 5	~~My password is strong enough.~~
Chapter 6	~~I can spot a scam when I see one.~~	Chapter 7	~~Everything important is on my laptop.~~
Chapter 8	~~The WiFi is fine, it has the hotel's name on it.~~	Chapter 9	~~It's just a photo.~~
Chapter 10	~~Not my kid.~~	Chapter 11	~~My mom would never fall for that.~~
Chapter 12	~~I'm already insured for that.~~	Chapter 13	~~I'm too small to be a target.~~

Discussion questions

★ marks the 12 questions to use if your club has one hour. Meeting one: the Introduction through Chapter 6. Meeting two: Chapters 7 through 13 and the Conclusion. Run the icebreaker at the first meeting and the activities at the second.

Opening INTRODUCTION

1. Corey opens with a rainy October morning in 1994, when a turning station wagon put him on its hood in a crosswalk where he had the right of way. He writes: "I trusted the system to protect me. The system didn't care." Where in your own digital life are you trusting the crosswalk: your bank, your phone company, an app? ★

2. As a child, Corey ran to open the front door for anyone. Today we teach children: "Don't open the door for anybody, even if you might know them, unless they called or texted and said they were coming." We made that shift in the physical world. Why haven't most of us made it online?
3. "Your kindness and trust are being weaponized against you." Which of your good qualities (being helpful, polite, quick to respond, generous) do scammers count on most? Has one ever been used on you, or on someone you love? ★

Part One: The New Reality CHAPTERS 1 AND 2

4. Chapter 1 describes your Evil Digital Twin: a fake you, assembled from breaches, data brokers, LinkedIn, genealogy sites and your own posts. Corey's team catches the fakes of him because they know how he signs off and how he writes. Would the people closest to you spot a fake you? What would give it away? ★
5. The vacation photo that tells a stranger your house is empty for ten days. The back-to-school photo that gives away your child's name, age and school. Did any example in Chapter 1 make you rethink something you have posted? What, if anything, will you change?
6. In Chapter 2, Corey, a cybersecurity expert with excellent credit, is turned down for a large purchase because of a PayPal credit card he never opened. "I had done everything right." How did it feel to read that the expert was hit too? Did it make you feel more exposed, or less alone? ★
7. The book's starting premise is that your personal data is already public, and the only real question is what you do now. Do you accept that? Is it frightening, or strangely freeing?

Part Two: Securing Yourself CHAPTERS 3 TO 9

8. In Chapter 4, a business owner nearly wired $47,000 because of an email thread that matched her own writing style. She was saved only because her bookkeeper happened to call the vendor to check. Who in your life plays that role, the person who picks up the phone to double-check? Do they know it is their job? ★
9. Chapter 4 points out that if you have a business bank account, take payments for your services, or file a Schedule C, the banking system treats you as a business, with different protections. Did that surprise you? How many people in this room have a side business?
10. Chapter 5 opens at the Louvre, where a 2014 security audit recorded the password for its own system as "Louvre." Be honest: what does your password situation look like? What has kept you from a password manager or an authenticator app?
11. In Chapter 6, a new employee buys $500 in gift cards because a text "from the boss" asked him to. "Hackers aren't just exploiting technology, they're exploiting human nature." Think of a time urgency, authority or wanting to help made you act fast. What would have slowed you down? ★
12. "So read this section as if it is about you. It is." The FTC figures in Chapter 6 show people in their twenties lose money to fraud far more often than people in their seventies, while older people lose more each time. Did that change who you picture when you hear the word victim? ★
13. A phone left on the seat of an Uber (Chapter 7). A hotel WiFi network with the hotel's name on it that is not the hotel's (Chapter 8). Which everyday moment from these chapters will you never see the same way again?

14. Chapter 9 begins with a confession: "social media terrifies me," from someone who then decides he has to be on it anyway. Where do you land between being visible and staying private, for yourself and for your children?

Part Three: Shield Your Family, Secure Your Future CHAPTERS 10 TO 13

15. Chapter 10 opens with this: "The people who built social media do not let their own children use it." Parents and grandparents in the room: how did that land? What age, and what rules, feel right in your family? ★
16. Corey calls the adults caught between raising children and caring for aging parents the sandwich generation, and says you are your family's Security Operations Center. Who plays that role in your family today? Did anyone choose it?
17. Chapter 11 tells the story of a 76-year-old man in King County, Washington who lost $800,000 to a sweepstakes call and ended up living in his car. "These aren't stupid people." The chapter argues that education alone fails, and that we have to build a system around our parents instead. Do you agree? ★
18. The book gives a way to raise this with a parent: make it a family issue, share your own near misses, and never open with "What the hell were you thinking?" What would you actually say to your mother or father this week? Try it out loud. ★
19. "No code word, no money. Period." Does your family have a code word? What would make one stick with grandparents, and with teenagers?
20. In Chapter 12, a widow in Lombard, Illinois said she needed to pray about the first request for $20,000. She sent it, and by the end she had sent nearly $1 million, including a home equity loan. Her bank said her answers did not raise concern. Who, if anyone, should have stopped it? What does her story say about loneliness?
21. In Chapter 13, a solopreneur in the middle of a takeover says: "I do not know what is mine." If you run a business, a side hustle or a nonprofit, how much of it depends on one email address and one password? Who else has a key?

Closing CONCLUSION

22. Corey still stops at the curb, looks both ways and waits for a nod from the driver. It takes maybe five extra seconds. "Being right doesn't protect you, but being aware does." What is the five-extra-seconds habit you will take from this book? ★
23. The book counts 263 doors and then says: "Nobody closes all of them. Close yours." Which three will you close before your club meets again? ★

Do it together

Take the score before you meet
Ask everyone to take the free Personal Cyber Score before the meeting. It takes about three minutes. At the meeting, share how many doors you found open, never the details.

Practice the parent conversation
Pair up. One person plays the parent, the other raises the subject the way Chapter 11 suggests: as a family issue, with a story of your own, never as a scolding. Then switch.

Three doors each
Before you leave, each member names three checklist items they will finish before the next meeting. Start the next meeting by asking who closed theirs.

Set a family code word
Each member leaves with a plan to agree on a code word with their family this week, in person, never by text or email. If a call or message claims to be family in trouble, ask for the word. No code word, no money.

Close a door together
Pick one door everyone can close before the evening ends: turning on an authenticator app for email, or checking who can see your photos. Do it at the table and help each other.

The free Personal Cyber Score: cythentic.com/score. The chapter checklists: youarealreadyatarget.com.

Invite Corey to your book club. Corey joins book clubs by Zoom for a 30-minute conversation, free of charge. Email corey@cythentic.com with your club's name, where you meet, how many members you have, and two or three dates and times that work, with your time zone.

A bonus for every reader. Every reader's personal Remi plan is free for life: remi.cythentic.com/book. Get the book: youarealreadyatarget.com/buy. Bookstores and libraries order through Ingram: hardcover ISBN 979-8-9984154-1-8, paperback ISBN 979-8-9984154-0-1.

About the author

Corey White has spent thirty years in cybersecurity. At Cylance he was a founding executive and created ThreatZERO, one of the industry's first outcome-based security services. He then founded Cyvatar, which over seven years protected more than two hundred organizations with zero reported major customer breaches and reached number 605 on the Inc. 5000. He founded, scaled and sold the company. His 2024 talk on AI-based threats was named Talk of the Year at the SANS AI Cybersecurity Summit. He now runs Cythentic, building consumer cybersecurity for individuals, families and solopreneurs, and lives in Southern California.