A MASTER HACKER'S GUIDE

HUMAN HACKING

WIN FRIENDS, INFLUENCE PEOPLE, AND LEAVE THEM BETTER OFF FOR HAVING MET YOU

CHRISTOPHER HADNAGY
WITH SETH SCHULMAN

A MASTER HACKER'S GUIDE

HUMAN HACKING

WIN FRIENDS, INFLUENCE PEOPLE, AND LEAVE THEM BETTER OFF FOR HAVING MET YOU

CHRISTOPHER HADNAGY
WITH SETH SCHULMAN

HUMAN HACKING

WIN FRIENDS, INFLUENCE PEOPLE, AND LEAVE THEM BETTER OFF FOR HAVING MET YOU

CHRISTOPHER HADNAGY

WITH SETH SCHULMAN

HARPER
BUSINESS

An Imprint of HarperCollins*Publishers*

Ebook Instructions

In this ebook edition, please use your device's note-taking function to record your thoughts wherever you see the bracketed instructions [Your Notes]. Use your device's highlighting function to record your response whenever you are asked to checkmark, circle, underline, or otherwise indicate your answer(s).

Dedication

To Areesa, the love of my life. You are my best friend and one of the most beautiful humans I have ever met.

To Colin, watching you become the man you are has given me endless hope. I am so proud of you.

To Amaya, there are no words to describe the depth of my love for you. Your beauty and talent astound me.

Contents

Please Read and Sign Before Continuing

The tools contained in this book are uniquely powerful. Every year, criminals around the world use them to manipulate others to do their bidding, stealing trillions of dollars from businesses and individuals, wreaking havoc on the lives of millions, and altering the political destinies of entire nations. In sharing these techniques with you, I trust that you'll use them for the cause of good, not evil. You'll help others, not just yourself, and you'll refrain from behaving in ways that harm others. This is serious business—lives are at stake here! So, before proceeding, please read and sign the following pledge:

I, _____, solemnly swear not to use these skills to manipulate people for selfish, one-sided gain. While I may use these skills to benefit myself, I will ensure that the others with whom I interact benefit as well, and that they don't compromise their own best interests by acceding to my wishes. Further, I promise to respect the privacy of others in using these skills, and I promise to use these skills to enhance my own self-awareness, so that I can become a better partner, family member, friend, colleague, and neighbor. Most of all, I promise to use these skills in ways that ultimately leave people feeling better for having met me. If I fail in this task, as I occasionally might, I promise to learn from the experience and do better next time.

Signed,

_____

(Sign and date here)

Introduction
Your New Super Power

It's one o'clock in the morning, and we're in a rented black Suburban, creeping along off-road through desert scrubland with our lights off. I squint in the moonlight, navigating around boulders, clumps of underbrush, and the occasional small tree. My buddy Ryan's knuckles are white as he grips the passenger seat. Every few minutes, he cranes his neck to make sure nobody is following us. I take deep breaths, trying to stay calm. Neither of us talks, save an occasional "crap" from one of us when we take a hard bounce or narrowly avert a boulder.

Going just a few miles per hour, we make our way toward a group of boxy, nondescript buildings illuminated by powerful floodlights and other scattered industrial lighting. More precisely, we head toward the ten-foot-high security fence topped with razor wire that stands between us and those buildings.

At one point, about five miles into it, I brake hard as a coyote darts in our path. We shouldn't be doing this, I tell myself.

About a quarter mile from the fence, I spot a large and deep gully cutting down into the earth off to my left. "How about there?" I ask.

"Fine," Ryan says.

I maneuver into the gully, trying not to scratch the car on the thick, dry brush that lines either side. I go as far down as I can before parking so that guards or workers walking around this dusty wasteland can't see the car. From here, we'll proceed on foot. "Any company?" I ask, shutting off the engine.

“Don’t think so,” Ryan says.

“Let’s roll.”

We get out and close the doors softly behind us. Rattlesnakes and scorpions abound in this habitat, so we tiptoe around, alert to the slightest movement. We open the back hatch and pull out an aluminum ladder and some lengths of rope. Aside from the ladder, we’re traveling light—you never know if we’ll have to make a run for it. “Okay,” I say, pointing to a section of fence a bit to our left. “Over there, that dark area. Looks like a light is out. It’s our best bet.”

We walk, carrying the ladder between us. It’s eerily quiet, save for a low hum coming from the buildings and the occasional, soft clanging of the ladder. We’re fifty miles from the nearest town, unarmed and uninvited. If anything happens to us, nobody will know. And something might happen. I’ve been arrested and had guns put to my head. And those were easy jobs compared to this one.

I can’t divulge what kind of facility this is, or where in the world it is located. What I can say is that beyond this barbed-wire fence a powerful organization is keeping watch over something immensely valuable. This “something” is so valuable, in fact, that the organization has spent tens of millions of dollars designing this facility and outfitting it to be, as we were told, “absolutely impenetrable,” one of the most secure facilities on the planet. Besides the barbed wire, dozens of highly trained guards armed with automatic weapons patrol the grounds, making rounds throughout the night. Other guards stand watch inside high turret towers. Powerful spotlights illuminate the fence at regular intervals, with hundreds of cameras monitoring movements on the grounds and around the perimeter. An array of other costly and sophisticated equipment that I can’t reveal is also in place, all with one objective: keep people like Ryan and me out.

We know about the security in such detail because we’ve spent weeks preparing for this mission. Working from a remote location, we gathered reams of detailed information via phishing and vishing (phishing phone calls) attacks. In the course of seemingly innocuous conversation, people working behind the razor wire and at other facilities maintained by this organization revealed operational plans, scheduling details, even the names of employees and managers who worked here—enough of them so that we could piece together large portions of the organization’s management hierarchy.

In recent days, we continued to amass information while poking around the facilities in person. We had learned that the organization was building a new facility near this one, and that they were holding a groundbreaking

ceremony this week. Although no information about the new facility's location was available online, that didn't stop us. Noticing that a local journalist had written articles about the construction, we hatched a plan to pose as this journalist and his colleague from the same news site. To learn the location, we had Debra, one of our female colleagues, call the facility's main office posing as an assistant to the journalist. "Hi," she said, in a cheerful tone. "This is Samantha over at WXTT [not the television station's real name]. I'm Pete Robichaud's secretary. He's coming out to cover the ribbon ceremony on Saturday at ten thirty. I just have a couple of follow-up questions."

"Hold on a sec," a man on the other end of the line said, probably checking that Pete (also not his real name) was on the guest list. "Go ahead."

"Okay, so first off, what kind of ID does he need to bring? He'll need a government ID with a photo, right?"

"Yep. Driver's license is fine, as is a passport."

"Great. So, next question, he's planning on bringing his own camera equipment. Is that okay? Anything he shouldn't bring?"

"That's fine," the man said. "We'll search him on the way in, though."

"Absolutely," our colleague said. "So, my last question is . . . I just want to verify. We seem to have lost his invitation, so I want to verify the facility's location and where he needs to go."

"No problem," the man said. He gave us exactly the information we needed.

It was a seemingly trivial conversation, lasting only thirty seconds. The man on the other end of the line probably didn't give it another thought. But there was more to the exchange than meets the eye. Debra only wanted to obtain one piece of information—the address—yet she posed two warm-up questions, eliciting basic information that we knew the man on the other end of the line would have no problem answering. This technique is what people in our line of work call "concession." The warm-up questions served to get the man comfortable *conceding to* the prospect of answering her questions. Once his brain had answered two of them, it would be better primed to answer the third, so long as that last question wasn't so outlandish as to arouse suspicion. Debra even threw out an answer to the first question for him, signaling that she knew what she was doing, had done it before, and everything was legit.

But Debra was deploying other techniques as well. When she posed the third question, she positioned it as simply "verifying" what she already knew. She was setting up the question by evoking its logic, making it seem a perfectly reasonable question to ask. And before that, when she asked if

there was anything her boss shouldn't bring, she was playing dumb, implicitly asking the man on the other end to teach her. This massaged the man's ego, validating his authority and making him more comfortable and willing to talk—a task made easier by the gender difference between them.

Thanks to this conversation and others like it, we had been able to show up at the facility the day before and nearly gain access. Security personnel became suspicious and briefly detained us, but not before we'd learned numerous details about the security provisions, how the guards were trained, what weapons they carried, what kinds of threats they were alert to, what kinds of cameras the facility used, and so on.

Now Ryan and I are trying again to gain access, in a way that admittedly is far more dangerous. In the middle of the night, with two unidentified men dressed head to toe in black sneaking up to the fence, it would be easy for a nervous guard to shoot first and ask questions later. At six feet three, I'm hardly a small target. I try to push these thoughts aside as we make our way toward the fence, but it isn't easy. My mind keeps returning to the phone call I'd made earlier to my wife and kids, telling them that I love them. With every sound, my pulse races and I suck in my breath. We shouldn't be doing this, I tell myself again.

We reach the darkened section of fence and glance around—all clear. I rest the ladder against the chain link, and we use the rope to ease the razor wire down. With him video-recording on his phone, I climb up to breach the fence. I look around to see if we've been spotted, but fortunately, we haven't.

Over the next hour or so, Ryan and I explore the grounds, break into a couple of buildings and large machines, and take photographs and video-record what we see. Not once do the guards approach us. They apparently have no idea of our presence. Still, every second is pure temple-throbbing, adrenaline-coursing torment.

When we feel we have enough documentation, we head back to our truck and call it a night. Over the next few days, we'll use low-tech tools and psychological techniques to compromise this facility again from other entry points. We'll have guards shouting at us and putting guns to our heads, but only after we've spent hours again wandering around buildings and into the facility's most sensitive, highly guarded areas.

"Absolutely impenetrable"? I don't think so.

Who We Are and What We Do

You might think Ryan and I are government spies, high-end criminals, or fearless thrill seekers looking for another million YouTube followers. You'd be wrong. We're not any of those.

We're hackers.

Most people think of hackers as young techno-thugs who pound Mountain Dew and tap at their computers stealing data, crashing websites, or sending spam about Viagra. But there are good hackers, too, top-security professionals that governments and companies hire to *protect* them from the bad guys. And among these good hackers, there are a select few who don't specialize in the technical side of breaking into computers, but rather the messy, human side. This subspecies of hackers bypasses even the tightest security not by writing code to hack machines, but by hacking *humans*. They're con men, essentially, fast talkers who convince unsuspecting people to let them into machines and secured physical locations. The best of these hackers are so good that they not only get what they want, they make it so their targets *feel better for having met them*.

Ryan and I are hackers of humans. And don't worry, we're good guys. Thinking like the bad guys do, we apply advanced psychological principles and techniques to break into servers and physical sites. When we succeed, which is the vast majority of the time, we help our clients understand and fix their weaknesses, so that their customers and society at large are safer. That's what we were doing in the desert that evening—probing the security of this supposedly ultra-secure facility and identifying weaknesses, so that our clients could fix them before the bad guys broke in and wreaked havoc. We make our living getting perfect strangers to say or do pretty much whatever we want.

I've honed my techniques for more than a decade, using them to compromise the world's most secure facilities and computer networks, prompting one journalist covering the security industry to wonder aloud whether I'm "the most dangerous man in America."[1] That I'm not, but we do teach our methods to spies, military personnel, and security professionals around the world so that they can stay one step ahead of the truly dangerous bad guys. In this book, I'll reveal our secrets to you for use at home and at work. You'll learn how to read people effectively from their body language, how to get people instantly on your side by uttering exactly the right words, how to make requests in ways that dramatically increase your chances of a positive response, how to spot and thwart people who are trying to

manipulate you, how to plot out an important conversation from beginning to end to increase your odds of success, and much more. Whether you seek to land a promotion, get people to give you free stuff, get people to tell you what they *really* think, or improve your relationships by learning to communicate better, our methods will be your new secret weapon. As you'll discover, hacking humans can help anyone win friends, influence people, and achieve their goals. It can help *you*.

A New Kind of Hacking

The notion of hacking people instead of computers might sound strange. Who knew it was a "thing"? I didn't back in the day. In 1991, I got kicked out of college after only two months because of a little stunt I pulled. Actually, it wasn't so little—I messed around with the primitive modems we had on campus and wound up shutting down practically the entire phone system for Sarasota, Florida, for a full day.

Afterward, I drifted. I knew I had this strange knack for convincing people to give me stuff I shouldn't have, so I used it to land jobs that interested me. About a year after dropping out, I was working a job delivering papers when I walked into the office of a twenty-five-unit apartment complex and began chatting with the owner. I had never met this guy before, but in just a few minutes, I got him to tell me his deepest, darkest secrets. It turned out he had some personal issues he needed to resolve out of state. Two hours later, I had a well-paying job—with no relevant experience—as vice landlord renting out apartments and managing the complex. I was just seventeen years old.

I stayed for a while, leaving when I became bored. I got it into my head that it would be cool to be a chef, so I walked into a very fancy restaurant and, with zero kitchen experience, asked for a job. Two hours later, incredibly, I had one.

I got bored of that, too, so I talked my way into yet another job with no experience. Then another. And another. By the time I was in my late twenties, I was working as an international business negotiator for a company that, of all things, made stainless steel industrial products. I was traveling the world wheeling and dealing and making great money. But by that time, I had also talked this woman I loved into marrying me and having kids. Wishing to spend more time at home, I decided to leave and find something else to do.

It occurred to me, given my experience getting kicked out of college, that I might be good at hacking into computers. I went online and found a course offered by a security company on how to do it. I took the course and was the first person in the company's history to break into one of its most hardened servers. The owner offered me a job on the spot helping them to physically break into computer networks using technical methods.

There was one problem: despite having taken the course, I wasn't all that great at the technical methods. What I had going for me was my street smarts and skills as a fast talker. It turned out that this was all I needed. For the next few years, I helped out the team in unexpected ways. My colleagues would be messing around with computer code, trying to find software or hardware vulnerabilities they could exploit to break into a system. They'd go at it for thirty hours, forty, fifty. Eventually, I'd pipe in: "How about I just call this guy and ask for his password?"

They'd shrug and say, "Well, you can try."

In ten minutes, we were in the system.

This scenario played out again and again. Sometimes I'd call people to extract information, other times I'd use phishing emails or just waltz into a facility with no fear and convince people to give me access to their servers. I wasn't using any preexisting methods, just my intuitive people skills and street smarts. But it worked, so much so that I suggested to my boss that we create a course on these methods. To my surprise, he told me to go ahead and make one up. "No way," I said. "I have no clue how to write a course. I never even finished college."

"It's easy," he said. "Just find every book you can that might have relevant psychological theory or research and think about what you're doing every day on the job. Write all of this down and organize it into a simple framework that you can teach to people."

His advice made sense, so I accepted the challenge. In 2009, after almost a year of studying and thinking, I had my framework written. I posted it online, and then largely forgot about it. A few months later, a publishing house cold-called me and said they'd seen my framework. They wondered if I would like to write a technical book for people in the security business. I turned them down at first, telling them I was just a greasy little hacker, and nobody was going to read anything I wrote. I told my boss about the offer, thinking he'd find it as funny as I did. He almost jumped out of his seat. "Are you crazy? Call them back and write the book!"

Again, I took his advice, and *Social Engineering: The Art of Human Hacking* came out in 2010. It was the first "how-to" book on hacking humans and has sold more than 100,000 copies, which is crazy for a nerdy

technical book. In framing what I did as "social engineering," I appropriated a term first coined in the late nineteenth century and popularized during the 1990s and 2000s by the prominent hacker Kevin Mitnick. As I explained to readers, social engineering was "the act of manipulating a person to take an action that *may or may not* be in the 'target's' best interest."[2] I have since altered his definition, distinguishing between influencing people to behave or think as you wish and manipulation, which is the darker art of forcing or coercing them to do so. Given the ethical constraints in which good hackers operate (discussed in a moment), the vast majority of what social engineers like me do is influencing people. We sneakily get them to divulge sensitive information, and we refrain in almost all situations from coercing them.

Cross paths with us, either in person, on the phone, or online, and you'll think you had a delightful if perhaps trivial encounter with another human being. In some small way, you'll feel better off for having met us. But because we framed the conversation in exactly the right way, using specific words and paying close attention to your reactions, you'll almost certainly have also given us a password, a Social Security number, or some other piece of information we needed. The truth is, a well-trained social engineer doesn't need to use manipulation. Influence techniques are powerful enough.

You know that nice old lady who called you yesterday soliciting a charitable donation, and who chatted you up for a few minutes? Or that friendly UPS guy who in the course of asking for directions remarked on your company hat, cracked a joke, and queried you quite innocently about your work? I don't mean to scare you, but she might not have been nice, and he might not have been innocent. These strangers might have been malicious hackers, trying to squeeze you for information. They almost certainly weren't —let's not get carried away—but they could have been. Millions of people get hacked by criminals using influence techniques masquerading as an innocent conversation. The victims don't know they've been had until one day they discover that someone has taken out a small business loan in their name or locked down their computer and demanded a ransom.

Social Engineering laid out the basic principles and techniques for hacking humans, so that security professionals could use them to thwart attacks and keep us safe. In retrospect, I'm not proud of this book—it's pretty weak. But it did help put social engineering on the map. And for me personally, *Social Engineering* was a turning point. Excited about the reception it received in the security world, I started a company that evaluates companies for weaknesses by performing "penetration tests" such as the one depicted earlier, and that trains security professionals in how to hack humans effectively.

In the ten years that we've been in business, my firm has used the principles of social engineering to send 14 million phishing emails and more than 45,000 voice-phishing phone calls. We've broken into hundreds of servers, and physically compromised dozens of the world's most tightly guarded corporate and government facilities, including banks, corporate headquarters, manufacturing facilities, warehouses, and defense installations. If we'd been real thieves, we'd have obtained highly sensitive state secrets, stolen untold billions, and wreaked havoc on millions of lives by stealing people's identities and leaking their most sensitive information. We've been so successful that the FBI has recently invited me to train new agents in their Behavioral Analysis Unit. I've also partnered with law enforcement and used human hacking techniques to catch pedophiles online through a nonprofit I created, the Innocent Lives Foundation.

My team and I think of hacking humans as a super power, a psychological martial art, that we can use to get people we meet to do almost anything we want, and feel better about themselves—and us—in the process. In some ways we're tricking people, but more fundamentally we're wielding finely honed empathy and social savvy to our advantage. Applying insights from psychology, we cue in closely to how people are thinking and feeling, and use that information to nudge them so that they *want* to comply with our requests. Used correctly, social engineering enables others to feel happier, calmer, stronger, and just *better* about themselves by helping us out. They get this small, emotional "gift" from us, and they naturally return the favor, giving us what we want. All in the course of a few minutes of pleasant conversation.

Hacking Humans in Everyday Life

Imagine that you could harness these skills in your personal and professional life. You can. Not long ago, my wife, daughter, and I were in London's Heathrow Airport waiting for our plane. I was dragging around a cart piled high with our luggage, and as I approached the check-in counter, the cart hit a bump and some of the luggage fell off. Mindful that a major highway in London was named the M5, I made a joke: "Oh, a big American accident on the M5." The lady behind the counter laughed, so I said to myself, "Okay, great. At least she's in a good mood."

My wife chatted with this woman for a few minutes. "Before we check in," my wife said, "can I just tell you, your makeup is so immaculate, it matches