Chapter 1
What Is Social Engineering?

Social engineering is the manipulation of people and situations to gain access or information that otherwise is not available to you. Social engineering can sometimes be used to bypass physical security—mechanisms in place to prevent access by unauthorized people—but not always.

Organizations pay me to test their security. I use a combination of social engineering and physical attacks to do so. The security I test might be the locks on their doors, the security guards and receptionists, or their computer networks. Most often, it's all of those and much more, as you'll discover as you read about how I break into banks.

In my role as a security professional, I use psychology, body language, charm, flirtation, lock picks, and other tools to break in. Before all that comes a lot of preparation and paperwork.

Social engineering has a long history, albeit usually by another name—*scams*. Before we hear about my adventures, let's look at the first social engineering attack.

The best-known historical piece of social engineering is the Trojan Horse. While almost certainly a myth, it's mentioned in book 2 of the Aeneid, a book of Greek poems, and again in *The Odyssey* by Homer. As I am sure you know, the Greeks pretended to abandon the siege of Troy and left behind a giant wooden horse. The Trojans, thinking it was a gift from the gods, brought it inside their walled city. That night, the Greek warriors hidden inside the horse climbed out, killed the guards, and let the remaining Greek army inside.

I am sure you can see the moral of the story is about trusting what you don't know and letting them past your defenses. Computer viruses are often called *Trojans* because they are disguised as something benign. The myth shows the many things social engineering relies on: deception, a false sense of security, distraction, and making the target feel like they have succeeded—all the while playing into the attacker's hands.

Many years ago, I was asked to provide my security expertise to a prison in England that was prone to riots and escapes. My role was the opposite of most: they wanted me to prevent people from getting out rather than people getting in. While working in and around the prison, I was told the story of an escapee who used a method similar to the Trojan horse.

The prisoner noticed that two of the laundry machines were broken and due to be replaced. They had been disconnected, checked over, and left in a loading area. The day the removal team arrived to pick up the machines, he hid inside one, much as the Greek soldiers hid in the horse. Several miles down the road, he broke out of the machine and out of the lorry and escaped. (He was eventually recaptured.) I wonder if he had ever read *The Odyssey*?

Criminals use social engineering to perform all sorts of attacks, from what we call *phishing* email attacks to get passwords to huge fraud attacks that steal hundreds of millions of pounds.

While many criminals use social engineering to scam people, some people use it daily, sometimes unwittingly. Sales personnel, for example, try to convince you to do something you don't always want to do: spend money. Marketing is all about social engineering: time-pressure sales, discounts, and added values that don't really matter. Supermarkets spend millions on the placement of items in stores to get you to buy things. Why do you think there are sweets near the payment tills? Because you will be standing there in a queue, and your child will beg you to buy the sweets they just have to have. It's an easy sale.

Every day in your office, you make small, political movements, coercing someone to do something for you. I bet you didn't know you were a social engineer! Who doesn't know that smiling or

flattery works to get your way? Consider how many times over the last year you got your way, and think about how you did it.

For my role to be effective, I need to manipulate people into performing actions they would not normally perform. This can be tricky. But my role also includes having skills that attack or bypass physical systems. You can be the best social engineer in the world, but you can't out-smile or flatter a fingerprint reader. A locked door will remain locked unless someone unlocks it, no matter how much you yell at it or ask it nicely to open. This book will show you some techniques and how they have worked for me over the last three decades of my career.

Social engineering is just a fraction of the skills required to do what I do, but it is an essential foundational ability. It will continue to be the number-one attack used by criminals, as it has been for thousands of years. Understanding why it works and how it's used is the only way to recognize how to defend against it and prevent yourself from becoming a victim. As you move through this book, enjoying the anecdotes of my funniest and weirdest moments, try to pick out the "red flags" you could have spotted to prevent each attack. This book is an educational tool as well as an entertaining read; absorb the defense lessons, and honor them by putting them to use in your life.