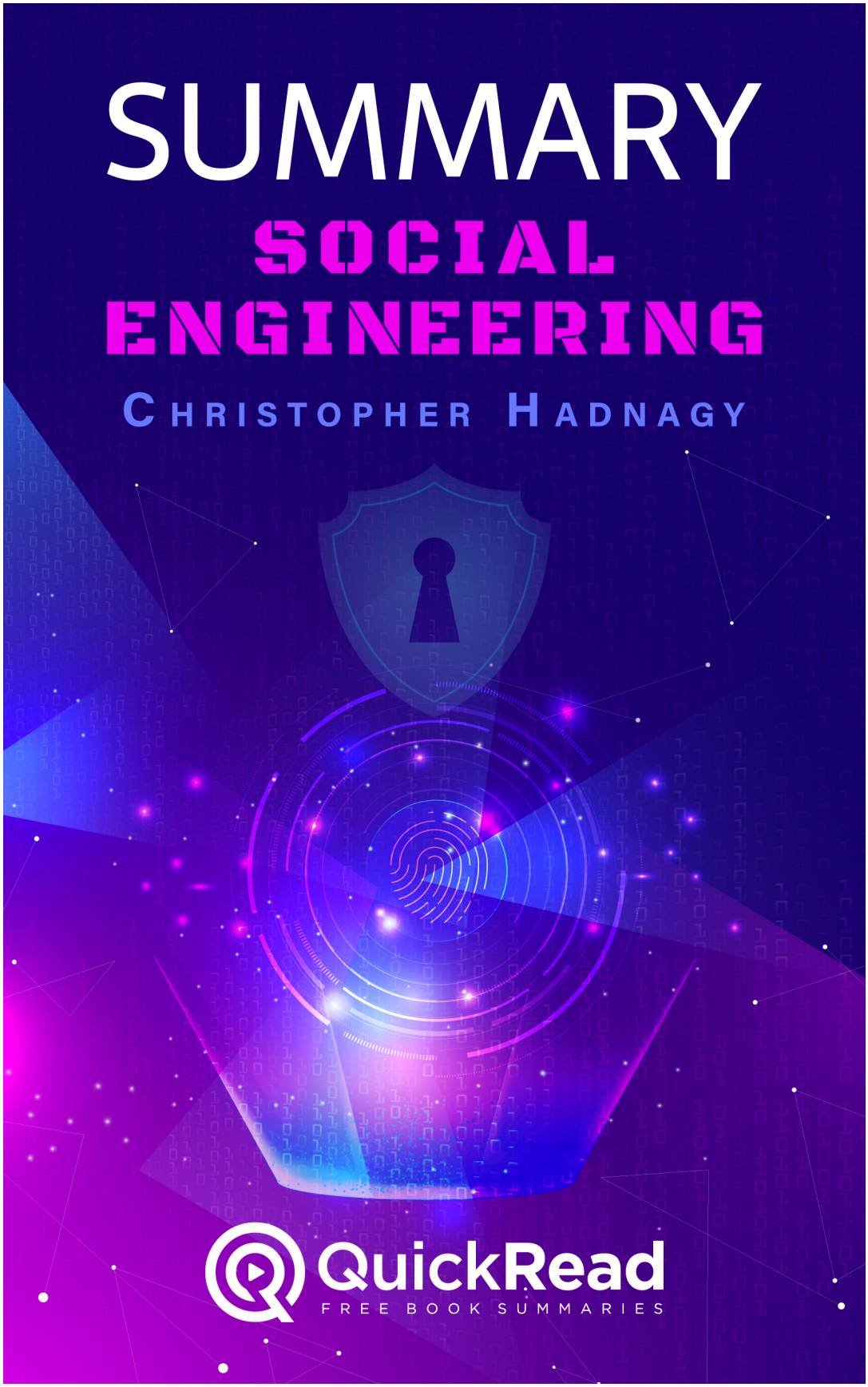
SUMMARY

SOCIAL ENGINEERING

CHRISTOPHER HADNAGY



QuickRead

FREE BOOK SUMMARIES

Summary of “Social Engineering” by Christopher Hadnagy

Written by Lea Schullery

Discover the art of human hacking and how to protect yourself from attacks on your personal information.

Introduction

From a young age, author Christopher Hadnagy has been interested in the art of manipulation. He was always curious about how many times he was able to obtain things or be in situations that would be considered “unreal.” For instance, once in New York City, Hadnagy was able to talk his way into an exclusive party for CEOs at FAO Schwartz by simply asking Linus Torvalds, the creator of the Linux kernel (the operating system for Android and Chrome OS), to autograph his Microsoft toy! Getting what you want isn’t necessarily hard, but it certainly takes strong skills in communication and research. In other words, social engineering is an art that can be mastered by practicing the necessary skills. Through *Social Engineering,* you can get an inside look into the world of social engineering. You’ll learn the skills and tactics these attackers use to gain what they want. By learning the tactics, you can begin to protect yourself, your family, and your company from becoming vulnerable to such malicious attacks.

The Art of Social Engineering

What exactly is social engineering? Well, if you were to look up the term on Wikipedia, you would find “the act of manipulating people into performing actions or divulging confidential information.” In other words, social engineering involves manipulating others to gain access to their private information including bank accounts or even computer system access. However, according to Christopher Hadnagy, social engineering is much deeper than that.

For instance, perhaps you’ve been convinced by a salesperson to buy something that you neither needed nor wanted. Or maybe as a child, you convinced your parents to allow you to do something you probably shouldn’t have. You see, social engineering is used in everyday interactions from teachers convincing their students to complete an assignment to doctors convincing patients to reveal personal information. Therefore, Hadnagy defines social engineering in his own words, he states that “the true definition is the act of manipulating a person to take any action that *may* or *may not* be in the ‘targets’ best interest. This may include obtaining information, gaining access, or getting the target to take a certain action.”

There are many types of social engineers, including hackers, spies, identity thieves, scam artists, disgruntled employees, penetration testers (also known as pentesters), and even salespeople, the government, and doctors and lawyers. These social engineers all use similar tactics to elicit, interview, interrogate and manipulate their “targets” or clients into the direction they want them to take. Nowadays, social engineers employ new tactics and infiltrate their targets by first gaining their trust. For instance, many will take on the role of an IT specialist and convince employees to give them the information they need to infiltrate the system, making stealing information as easy as having a simple conversation.

To show how easy it is for social engineers to acquire information, Hagnady gives the example of the time he saw a placemat at a restaurant that had a

$50 off coupon for a local golf course. To take advantage of the offer, you only had to provide your name, street address, date of birth, and a password for an account that would be set up and sent to your email address. The author only noticed the offer when he witnessed someone writing down his personal information and simply leaving it on the table. People give up sensitive information like this all the time, making it only easier for social engineers to steal it.

The art of social engineering can be used both maliciously and for good. For instance, in 2009 an FBI agent by the name of J. Keith Mularski went undercover to infiltrate the DarkMarket site. DarkMarket was essentially eBay for criminals, it consisted of a group of criminals who traded stolen credit card numbers and identity theft tools. Over the course of three years, Agent Mularski used his social engineering skills to gain the trust of the criminals and even became an administrator of the site. His skills paid off and the sting operation eventually led to 59 arrests and prevented over $70 million in bank fraud.

No matter how social engineering is used, it is a skill that must be mastered to be successful. Similar to cooking, social engineering involves “mixing the right ingredients in the right quantity” so you can have a meal that is full of flavor and excitement. And while you may not cook the meal perfectly the first time, practice will even eventually make perfect. Your recipe begins with your first ingredient: information gathering.

Gathering Information

Before any social engineer goes in for the “attack,” he or she must gather as much information as possible about the target. The more you know, the more likely you’ll be able to influence them to give up the information you need. For example, someone who doesn’t play golf wouldn’t likely respond to the ad offering $50 off a golf game. Once you know more about your target, you can come up with a creative way to manipulate them, and no information is safe.

For instance, Hagnady’s good friend and mentor, Mati Aharoni, who is a professional pentester, was once tasked with gaining access to a company that had an almost nonexistent online footprint. With limited resources, Mati had very few avenues to hack into, which made gaining access to the company prove to be challenging. So he began to scour the internet for any details that could become a potential lead. In one particular search, Mati found a high-ranking company official who used his corporate email on a forum about stamp collecting and expressed interest in stamps from the 1950s.

This seemingly minor piece of information was Mati’s “in.” He quickly registered a URL along the lines of www.stampcollection.com and found pictures of 1950s stamps on Google. He then crafted an email to the company official stating that his grandfather recently passed away and left him with a stamp collection that he would like to sell. He directed the official to the fake website he made which was embedded with a malicious frame and would give control over the target’s computer to Mati. Soon, the target clicked the link and the company’s perimeter was immediately compromised.

As you can see, every minor detail is important and no piece of information is irrelevant. Gathering information can be done in several ways and a good place to start is with the company’s or person’s website. Websites can lead to an understanding of what they do, products and services they provide,

physical locations, job openings, contact numbers, and more. Additionally, finding out the target's personal habits can lead to a chance encounter that can provide even more useful information.

For example, Hadnagy was once able to infiltrate a company by finding out that one of the higher-ups stopped at a local coffee shop at 7:30 a.m. every morning. By creating a "chance" encounter and initiating the man in conversation, Hadnagy was able to, among other things, get a business card and information about the man's upcoming vacation. These small bits of information allowed Hadnagy to gain the trust of the secretary and gain access to the company building where he left USBs filled with malicious software, all he needed was a curious employee to insert the USB into a computer. Sure enough, this method seems to always work and it all started with a simple conversation at a local coffee shop.

Adopting a False Identity or Pretext

Like many FBI agents who go undercover, social engineers must adopt different personas to gain the trust of their target. After you've gathered as much information as you can about your target, it's time to create your pretext. It's important to remember that a quality pretext begins with quality research. For instance, the classic pretext of a tech support guy would fail if the company you tried to infiltrate had their own internal support!

Remember that no information is irrelevant, and something as small as an interest in stamp collection can lead to a pretext involving someone interested in selling stamps. For instance, if the social engineer finds out that every year the CFO donates a bunch of money to a children's cancer research center, then a pretext that involves fundraising for this cause could very likely work. While it may sound heartless to use children's cancer for malicious intent, social engineers will do anything to gain the information they need and will feed on emotions without a second thought.

After the 9/11 attacks, many malicious hackers and social engineers used the losses of these people to raise funds for themselves via websites and emails that targeted people's computers. The same happened after the earthquakes in Chile and Haiti in 2010 in which social engineers developed websites disguised as information on seismic activity or the people who were lost. However, the sites were encoded with malicious codes that hacked people's computers. It's an unfortunate reality that social engineers capitalize on others' misfortune, but it's one of those dark corners of the internet that sadly exists and allows malicious hackers to form successful pretexts.

Another way to create a successful pretext is to involve personal interests and to convince the target that you are credible. If you adopt a pretext that you are interested in, it gives you the ability to portray intelligence as well as confidence. For instance, if you attempt to play the part of a technician

but have never seen a server room or taken apart a computer, then your pretext will be on a quick path to failure. Instead, you could adopt a pretext of a “student” and attempt to gain knowledge through observing! By taking an interest in what your target is interested in, you have a greater chance of a successful pretext.

Lastly, there are many props and tools that can go a long way in convincing a target of the reality of your pretext. For example, magnetic signs for your vehicle, matching uniforms or outfits, and the most important - a business card. Once, Hadnagy was able to get through TSA security at the airport with his lock picks, RFID scanner, and a plethora of hacking gear by simply stating he was a security professional and handing over a business card. After looking at the business card, the TSA agent simply stated, “Oh, excellent. Thanks for the explanation.” and let him go on his way. It was then that Hadnagy recognized the power of a simple business card. Of course, Hadnagy was telling the truth, it wasn’t a pretext, but can you imagine if it was?

The Art of Elicitation

In addition to doing your research to hone your pretext, you should also learn how to have an effective conversation with your target. This is called the *art of elicitation*. Being able to effectively use elicitation means you can fashion questions that draw people out and stimulate them to take the desired path of behavior. This means that an effective social engineer can fashion words and questions in a way that makes the target *want* to answer every request. Elicitation is a tactic used by spies all over the world and is defined by the National Security of the United States government as "the subtle extraction of information during an apparently normal and innocent conversation." So why does it work so well?

- First, most people have the desire to be polite, especially to strangers.
- Professionals want to appear well informed and intelligent.
- If you are praised, you will often talk more and divulge more.
- Most people would not lie for the sake of lying.
- Lastly, most people respond kindly to people who appear concerned about them.

Essentially, human nature is what makes elicitation work so well. For instance, Hadnagy recalls a time in which he was tasked to gather intel on a company and met his target at a local networking event. He approached his target at the bar and opened with "Escaping from the vultures?" His target chuckled and ordered a drink. Hadnagy then introduced himself and pulled out a business card, his target replied by doing the same, stating "I am the CFO for XYZ." Hadnagy then commented on the successful product that the target's company just released, the target then began boasting and telling more about the company.

Soon, the two were conversing over drinks, and Hadnagy discovered some key information that would help him infiltrate the company building. In addition to getting the names of higher-ups and when they would be on

vacation, he also found out the accounting software they used as well as the door locking security. Therefore, Hadnagy was able to plan an onsite visit to repair a “faulty” security box and time clock. By dropping names to the receptionist and giving a reason to be there, he was given access to the building in a matter of seconds without ever being questioned.

Elicitation led Hadnagy to success and didn’t allow the receptionist to ever doubt his pretext. All it takes is a simple, light conversation to get some of the best information out of many people. Of course, you’ll need to learn the art of conversation which can be achieved by understanding these three key steps: Be natural, educate yourself, and don’t be greedy. In other words, have confidence and ensure your stance and posture reflect that confidence. Nonverbal aspects are just as important as the conversation itself. Next, you must have knowledge of what it is you will be talking to your targets about, and never pretend to know more than you do. Lastly, you must be willing to share and give information. No one likes to be bombarded with a bunch of one-sided questions, so keep the conversation moving and offer your own ideas.

In fact, mastering elicitation means learning how to ask the proper amount of questions. Too many questions can shut down the target, whereas too few will make the target feel uncomfortable. Additionally, ask only one question at a time to avoid overflowing the target. Remember, you are merely gathering information to build a profile, to do this you can’t seem too eager or uninterested.

Understanding How Your Target Thinks

What if I told you that one of the most important skills of a social engineer is the ability to *read minds?* You likely wouldn't believe me, reading minds is impossible...or is it? Well, learning how to analyze a person's cues they give in their speech, gestures, eyes, and faces can be just as effective as reading their minds. The first step in becoming a "mind reader" is building a rapport with your target and gaining their trust. So how can you do this?

First, you'll need to understand the *way* people think and in what *modes* they think. While you may be thinking that this sounds like a job for a psychologist, it's actually much easier than it sounds! According to Hadnagy, we mainly refer to three senses in conversation:

- Sight, or a visual thinker
- Hearing, or an auditory thinker
- Feeling, or a kinesthetic thinker

So how can we use these senses to our advantage? If we can learn the mode in which people think, then we can speak in a way that makes the target feel comfortable. People are more likely to feel at ease in their comfort zone and are more willing to divulge information to those they feel comfortable around. So if you find someone who needs to look at you when you talk, you're likely dealing with a visual thinker so you might benefit by asking questions like, "Can you see what I'm saying?" or "How does this look to you?" An auditory thinker remembers the sounds of an event and responds to questions like, "How does this sound?" Lastly, kinesthetic thinkers are concerned with feelings and will feel comfortable with questions like, "How does this feel?" or "How does this grab you?"

Of course, this is not an exact science but can be very useful in gaining the trust of others. A good social engineer doesn't just rely on modes of thinking, but instead, uses it as a tool in their arsenal. Another effective tool that social engineers use is something called *microexpressions*.

Microexpressions are facial expressions that are not easily controllable and occur in reaction to emotions. These expressions are short and involuntary and may seem unimportant to the untrained eye; however, to a social engineer, they can tell a lot about their target.

By using microexpressions, social engineers can learn to manipulate their targets. For instance, one of Hadnagy's colleagues, Tom, noticed how his target would smile every time something positive was said. Therefore, he began clicking his pen so the target would associate positivity with the clicking of a pen. Eventually, Tom clicked the pen when something negative was said which, ironically, made the target smile. Similar to Pavlov's classical conditioning, Tom learned how to manipulate his target and elicit the desired response simply by noticing something as small as a smile.

Microexpressions, similar to modes of thinking, aren't science and social engineers rarely rely on these tools on their own. Instead, these tools are an aid in getting to know the target and make them feel at ease. Don't you feel more comfortable when you think someone understands you?

The Tools of a Social Engineer

In today's world, social engineers are faced with trying to infiltrate more than just the minds of their targets. Sometimes, they must infiltrate buildings by picking locks or infiltrate websites by using passwords. So how do they do this? Well, that's where some tools of the trade come in handy.

Think about your own password strength, do you think your passwords are strong or weak? Recently, Hadnagy was discussing password strength with a friend and revealed how easy it is for social engineers to "guess" people's passwords. He mentioned that many people use the same passwords for every account; suddenly, his friend's face went white as she realized that she does this. He then said that most people use simplistic passwords that combine things like their spouse's name, his or her birthday, or their anniversary date. His friend went an even brighter shade of pale. He continued to say that most of the time, many people choose the simplest "security questions" such as "your (or your mother's) maiden name" which is easy to find out via the Internet or a few fake phone calls.

To prove the weakness of passwords, a hacker known as Tonu copied a social media site using a web address that had recently been dropped. 734,000 people logged into this fake site and Tonu found that 30,000 of these people used their first name as their password. Another 17,601 users used the password "123456." Of course, this happened in 2009 when password strength wasn't a widely known topic. Today, however, social engineers have tools to help them crack passwords when they aren't as simple as a person's first name.

Free software, like Common User Password Profiler, or CUPP can be used to crack just about any password. For instance, when Hadnagy conducts security training exercises, he asks volunteers to type a password they think is secure. Using software like CUPP allows him to crack the password in under two minutes. So how does it work? CUPP takes the target's personal information, including nicknames, birthdays, and spouses' names to create

a file of probable passwords. Typically, it can take just a few days or less to crack weak passwords.

The tools of a social engineer don't always involve a computer, however. They must also be able to penetrate physical security, like a locked room or a locked cabinet. To pick a lock, you only need two items: a pick and a tension wrench. A pick is a long piece of metal that curves at the end, similar to a dentist's tool. They reach inside the lock and move the pins up and down until they are in the correct position. A tension wrench is a small flat metal device that allows you to put pressure on the lock while using the pick.

To pick a lock, first, insert the tension wrench into the keyhole and turn it in the same direction you would turn the key. The skill here is knowing how much tension to add which will take practice. Next, you'll insert the pick and use it to lift the pins one by one until you feel them lock in place. You'll hear a slight click when an upper pin falls into position, and once you get all the pins in position, you'll be free to rotate the lock freely!

Protect Yourself From Social Engineering Attacks

The first step in protecting yourself from attack is learning about the attacks, after all, knowledge is power, right? That doesn't mean you have to become a social engineering expert, instead, looking for the signs that someone is trying to trick you can protect you from future harm. Similar to how you would teach your kids what to do in a dangerous situation, you should do the same when it comes to your online security. Don't simply wait for an attack to happen, arm yourself and teach yourself and others what to look out for.

When it comes to social engineering, any and all information can be useful and valuable to an attacker. Therefore, before giving out information to someone, determine whether the person calling deserves to interact with you. As humans, we feel the need to be helpful, but analyzing the person with whom you are interacting with can save you from becoming a victim. You should look out for many "tricks" by social engineers including those who adopt the pretext of a customer in distress who needs help.

For instance, a social engineer once tested the security of an antivirus company by calling technical support with a "serious problem." The attacker explained that he couldn't get online and he felt it was due to something the antivirus was doing, he wanted the tech support representative to do just one simple thing: browse a website. By driving a victim to a website embedded with malicious code, attackers can gain access to a target's computer and network. In this case, the attacker asked several times if the representative could navigate to the website to check to see if the issue was the antivirus software. The representative declined the attacker's request several times; however, his last-ditch effort included the words, "Please, can you help me out?" This simple plea was all it took for the representative to navigate to the malicious website. Of course, this scenario was just a test but had it been real, the results could have been devastating.

Social engineers will also turn to diversion and charm to gain the trust of their victims. They may ask how the weather is or something relating to work, a product, or anything at all to get as much information as they can. Therefore, it would be useful for companies to do what many of them hate: develop scripts. Okay, not necessarily a script in which an employee must say X if a situation equals A plus B. Instead, developing outlines to help an employee prepare for all kinds of scenarios.

The script can be simple. For instance, say that someone calls and claims to be from the management office and demands compliance of either handing over information or internal data. The employee should first ask for the person's employee ID number and name. Don't answer any questions until you have this information. If the information is provided, ask for the project ID number related to the project he or she is managing that requires this information. By simply asking for these identifying numbers, you can protect yourself from malicious attacks.

Final Summary

As companies become better at protecting their information online, social engineers must hack more than just computers, they must hack the human mind. By understanding how social engineers work, you can better protect yourself from attacks and protect your businesses, your families, your children, your investments, and your life. Hadnagy's mentor, Mati Aharoni, states "the reason the bad guys usually win is because they have the dedication, time, and motivation on their side. Don't let life get in the way of security. Conversely, don't let too much fear of the bad guys keep you from enjoying life." Just as a social engineer hacks the mind of their victim, you can hack the mind of your attacker and arm yourself with the protection and knowledge to prevent such malicious attacks.